Panjab University Law Magazine (MAGLAW)
ISBN: 2582-3507, Volume IV Issue I, pp 1-16

AI-DRIVEN FACIAL RECOGNITION: HUMAN RIGHTS CONCERNS AND REGULATORY CHALLENGES

Shubham Bhatia*

ABSTRACT

Facial Recognition Technology (FRT), powered by Artificial Intelligence (AI), has become a significant tool in law enforcement, public security, and digital identity verification. While it enhances efficiency and security, its widespread use raises serious concerns regarding privacy, mass surveillance, and algorithmic bias. In India, the absence of a comprehensive legal framework regulating FRT creates challenges in ensuring compliance with constitutional protections, particularly the right to privacy. This study examines the ethical and legal implications of FRT, focusing on issues of consent, data protection, and the risk of discrimination against marginalised communities. It also explores global regulatory approaches, including the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act) in the European Union, which categorise FRT as a high-risk technology requiring strict oversight. The research highlights the urgent need for India to establish a balanced regulatory framework that promotes innovation while safeguarding fundamental rights. Policy recommendations include legislative reforms, independent oversight mechanisms, algorithmic transparency, and ethical AI practices to mitigate risks. As AI-driven surveillance expands, ensuring accountability and fairness in deploying FRT is crucial for protecting democratic freedoms and individual liberties.

Keywords: *Facial Recognition, Artificial Intelligence, Privacy, Human Rights, Regulation*

1. INTRODUCTION

Facial recognition technology (FRT) represents a ground-breaking advancement in artificial intelligence (AI) and biometric systems, enabling the identification and verification of individuals through unique facial features. In India, FRT has gained prominence across sectors such as law enforcement, e-governance, border security, and public safety. However, its adoption has sparked significant debate, particularly concerning its implications for human rights, privacy, and the need for stringent regulatory oversight. The intersection of technological innovation and fundamental rights creates a critical need for legal scrutiny, especially in a country

* LLM, Amity University, Mohali, Punjab

as populous and diverse as India.[1]

India's constitutional and legal framework provides both opportunities and challenges for the adoption of FRT. The landmark judgment of the Supreme Court in ***Justice K.S. Puttaswamy v. Union of India***[2] reaffirmed the right to privacy as a fundamental right under Article 21 of the Constitution. This judgment has since been pivotal in shaping discussions on data protection and surveillance in India. However, the lack of a dedicated legislative framework governing personal data or facial recognition technology highlights a significant regulatory vacuum. The Digital Personal Data Protection Act, 2023 (DPDP Act) seeks to address these gaps by regulating data processing and ensuring accountability, but its limited scope leaves critical areas, such as surveillance and algorithmic accountability, unaddressed.[3]

Globally, facial recognition technology has faced increasing scrutiny, with several countries imposing strict regulatory measures or outright bans. For instance, the European Union's General Data Protection Regulation (GDPR) provides stringent guidelines on data processing, including the use of biometric data, under Article 9. Furthermore, the EU's Artificial Intelligence Act, 2024 categorizes facial recognition as high-risk and imposes specific obligations on its use. The United States has seen city-level bans on facial recognition, such as in San Francisco and Portland, reflecting growing concerns about its potential for misuse. India can learn from these experiences to create a tailored framework that balances innovation with human rights protections.[4]

One of the primary human rights concerns associated with facial recognition technology is its potential to infringe on the right to privacy. Article 21 of the Indian Constitution guarantees the right to life and personal liberty, which, as established in the *Puttaswamy* case, encompasses the right to privacy. However, the use of FRT by law enforcement agencies, such as the National Crime Records Bureau's (NCRB) Crime and Criminal Tracking Network and Systems (CCTNS) and the Delhi Police's Integrated Monitoring System, has raised alarms about

---

1 Amber Sinha, "The Landscape of Facial Recognition Technologies in India" *Tech Policy Press*, March 13 2024 *available at* https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/ (last visited on February 22, 2025).

2 2017 (10) SCC 1.

3 Dr. Pradip Kumar Kashyap, "Digital Personal Data Protection Act, 2023: A New Light into the Data Protection And Privacy Law In India, " 2(1) *ICREP Journal of Interdisciplinary Studies* (2023).

4 Yaser Khalaileh, " Accomodating Artificial intelligence in International Law: An Overview and New Frontier," 19(1) *Journal of Human Security* 22-31 (2023).

surveillance overreach and the absence of safeguards to prevent misuse. [5]

The issue of algorithmic bias is another critical area of concern. Studies from other jurisdictions, such as the United States and the United Kingdom, have shown that facial recognition systems often exhibit biases based on race, gender, and ethnicity, leading to higher error rates for women and individuals with darker skin tones. In India, where socio-economic disparities and diversity in facial features are pronounced, these biases could have severe consequences. For instance, wrongful identification by law enforcement could result in false accusations or arrests, disproportionately affecting marginalized communities. Bharatiya Sakshya Adhiniyam, 2023, and Bharatiya Nagarik Suraksha Sanhita, 2023, provide specific guidelines for evidence and investigation, but their applicability to FRT remains ambiguous. A critical examination of these statutes is essential to ensure that FRT's use in criminal investigations adheres to constitutional principles and procedural fairness.[6]

1.1. OBJECTIVES OF THE STUDY

1. To Analyse the Human Rights Implications of Facial Recognition Technology (FRT).

2. To Assess the Legal and Regulatory Framework Governing FRT in India while comparing it with other countries.

2. RESEARCH METHODOLOGY

The study adopts a doctrinal research methodology, focusing on an in-depth analysis of primary and secondary legal sources. It critically examines constitutional provisions, statutory laws such as the Information Technology Act, 2000, judicial pronouncements, and legislation like the Digital Personal Data Protection Act, 2023 and also national and international precedents. Secondary sources, including academic articles, reports by international organizations, and comparative studies of global regulatory frameworks, are analysed to contextualize the legal and human rights implications of facial recognition technology. By employing this method, the study aims to provide a comprehensive understanding

---

5 Rakshitt C Bajpai, Shivang Yadav "Use of Facial Recognition Technology in India: A Function Creep Breaching Privacy," *OHRH,* January 11, 2021 *available at*: https://ohrh.law.ox.ac.uk/use-of-facial-recognition-technology-in-india-a-function-creep-breaching-privacy/ (last visited February 23, 2025).

6 Gaudys L. Sanclemente, "Digital Tools: Safeguarding National Security, Cybersecurity, and AI Bias" *CEBRI Revista available at*: https://cebri.org/revista/en/artigo/112/digital-tools-safeguarding-national-security-cybersecurity-and-ai-bias (last visited February 23, 2025).

of the regulatory challenges and propose actionable solutions tailored to the Indian context.

3. UNDERSTANDING FACIAL RECOGNITION TECHNOLOGY (FRT)

Facial recognition technology (FRT) has emerged as a transformative tool within the broader domain of artificial intelligence (AI) and biometrics. It enables the identification and verification of individuals by analysing unique facial features, such as the distance between the eyes, the shape of the nose, or the contour of the jawline. [7]

3.1 What is Facial Recognition?

Facial recognition is a biometric technology that uses machine learning algorithms to map, analyse, and compare facial features for identity authentication or recognition. It operates by capturing images or video frames, extracting facial features, and matching them against a pre-existing database. The technology is used for both verification (confirming an individual's identity) and identification (determining an individual's identity from a group).[8]

In India, FRT is increasingly used in public and private sectors, with applications ranging from law enforcement to digital identification systems like Aadhaar. However, the lack of explicit regulations governing the use of biometric data creates a legal vacuum. The *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016* governs biometric authentication in the Aadhaar system but does not specifically address FRT or its potential misuse.[9]

3.2 Evolution and Global Use

Facial recognition technology has evolved significantly since its inception. Early systems relied on 2D images and manual feature extraction, whereas modern

---

7 Sikender Mohsienuddin and Mustafa Sabri, "Facial Recognition Technology," 7(6) *IJIERT Elsevier* 176-181 (2020).

8 "Facial Recognition Technology - Innovatrics - How it Works," *Innovatrics*, 2021 *available at*: https://www.innovatrics.com/facial-recognition-technology/ (last visited February 23, 2025).

9 Sneha Kulkarni, "What is Aadhaar face authentication? These government social protection programs use face authentication," *The Economic Times*, September 2, 2024, *available at*: https://economictimes.indiatimes.com/wealth/save/what-is-aadhaar-face-authentication-these-government-social-protection-programs-use-face-authentication/popularity-of-face-authentication/slideshow/112988712.cms?from=mdr (last visited February 23, 2025).

systems leverage 3D imaging and deep learning to enhance accuracy and adaptability. Globally, FRT is used in diverse applications:

1. **Law Enforcement and Surveillance:** Many countries use FRT for crime prevention and public safety. In India, systems like the Delhi Police's Facial Recognition System (FRS) have been deployed for identifying suspects and locating missing persons. However, these uses often lack statutory oversight, raising concerns under the ***Puttaswamy judgment*** (2017), which emphasized the need for proportionality and safeguards in surveillance.[10]

2. **Border Security and Travel:** FRT is employed for automated immigration checks and airport security. For instance, India's DigiYatra initiative integrates facial recognition to simplify passenger verification. However, its implementation must align with privacy protections under the Aadhaar Act, 2016, particularly with regard to data sharing and consent.[11]

3. **Commercial Applications:** From unlocking smartphones to enabling personalized shopping experiences, FRT is widely used in the private sector. The absence of specific laws governing commercial use in India, apart from the Digital Personal Data Protection Act, 2023, creates significant regulatory ambiguity.[12]

4. HUMAN RIGHTS IMPLICATIONS OF FACIAL RECOGNITION

Facial recognition technology (FRT), while offering significant benefits in areas such as security and identity verification, raises profound human rights concerns. Its ability to collect, process, and analyse biometric data has implications for fundamental rights, including the right to privacy, freedom of expression, and freedom of assembly.

4.1 Right to Privacy and Data Protection

The right to privacy is a cornerstone of individual liberty and autonomy, recognized as a fundamental right under Article 21 of the Indian Constitution. Facial recognition technology poses a direct threat to this right due to its invasive nature, as it involves the collection and processing of sensitive biometric data

---

10 Gyan Prakash Tripathi, "Explained-Delhi Police's use of facial recognition technology" *The Hindu,* August 22, 2022 *available at*: https://www.thehindu.com/sci-tech/technology/explained-delhi-polices-use-of-facial-recognition-technology/article65793897.ece (last visited February 24, 2025).

11 Srushti Kulkarni, "India to implement facial recognition technology for international air travellers" *The New Indian Express*, October 17, 2024.

12 *Ibid.*

without explicit consent. In India, biometric data is primarily governed under the *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016*. However, this legislation is limited to Aadhaar-linked activities and does not extend to other applications of FRT, leaving significant gaps in regulatory oversight.[13]

The *Digital Personal Data Protection Act, 2023*, aims to address these gaps by regulating the processing of personal data, including sensitive biometric information. It emphasizes principles such as lawful processing, purpose limitation, and consent. However, the Act exempts certain government agencies from compliance, particularly for national security and law enforcement purposes, which raises concerns about unchecked surveillance. The lack of transparency and accountability in the deployment of FRT by government entities further undermines privacy protections.[14]

4.2 Freedom of Expression and Assembly

The right to freedom of expression and assembly is guaranteed under Articles 19(1)(a) and 19(1)(b) of the Indian Constitution, respectively. Facial recognition technology, particularly when used for surveillance, has a significant impact on these rights. The deployment of FRT in public spaces, such as protests, public meetings, or places of worship, enables authorities to identify and monitor individuals. This creates a chilling effect, deterring individuals from participating in legitimate expressions of dissent or collective action.[15]

For instance, the use of FRT during protests or rallies raises the risk of targeted harassment or profiling of individuals based on their political beliefs or affiliations. While the Constitution allows reasonable restrictions on fundamental rights under Article 19(2), such restrictions must be narrowly tailored and proportionate to the intended objective. The absence of specific guidelines for deploying FRT creates a risk of arbitrary and disproportionate interference with these rights.

---

13 Sheetal Asrani-Dann, "The Right To Privacy In The Era Of Smart Governance: Concerns Raised By The Introduction Of Biometric-Enabled National Id Cards In India," 47 *Journal of the Indian Law Institute* 53–94 (2005).

14 "The Digital Personal Data Protection Bill, 2023," *PRS Legislative Research available at*: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited February 25, 2025).

15 Soibam Rocky Singh, "Facial recognition technology: law yet to catch up," *The Hindu*, December 31, 2020 *available at:* https://www.thehindu.com/news/cities/Delhi/facial-recognition-technology-law-yet-to-catch-up/article33458380.ece (last visited February 25, 2025).

4.3 Discrimination and Bias Concerns

One of the most pressing human rights challenges of facial recognition technology is its potential for discrimination and bias. Studies from various jurisdictions have shown that FRT algorithms often exhibit higher error rates for certain demographic groups, particularly women, children, and individuals with darker skin tones. These biases arise from unrepresentative training datasets and flawed algorithmic design, resulting in discriminatory outcomes.[16]

In India, where socio-economic and ethnic diversity is vast, such biases can have severe consequences. Marginalized communities are particularly vulnerable, as they are more likely to be misidentified or disproportionately targeted by law enforcement. This exacerbates existing inequalities and undermines the constitutional guarantee of equality before the law under Article 14.[17]

The lack of algorithmic accountability further compounds these issues. Indian law does not currently mandate transparency or fairness audits for FRT systems. While the *Information Technology Act, 2000,* and its rules provide some general safeguards for data processing, they do not specifically address the ethical and technical aspects of AI systems. The *National Strategy for Artificial Intelligence* by NITI Aayog emphasizes the need for responsible AI deployment, but its recommendations remain largely aspirational and lack legislative backing.[18]

5. LEGAL AND REGULATORY LANDSCAPE IN INDIA

Facial recognition technology (FRT) operates at the intersection of technological innovation and fundamental rights, making it imperative to examine the legal and regulatory landscape governing its deployment. In India, the legal framework for FRT remains fragmented, with significant gaps that raise concerns about privacy, accountability, and misuse. This section explores the constitutional provisions, existing data protection laws, and the role of government agencies in regulating FRT.[19]

---

16 Xukang Wang et al., "Beyond surveillance: privacy, ethics, and regulations in face recognition technology," 7 *Frontiers in Big Data* 1337465 (2024).

17 Ram B Bhagat, "State, Enumeration and Marginalised Communities in India," *Economic and Political Weekly*, March 9, 2024 *available at*: https://www.epw.in/journal/2024/10/special-articles/state-enumeration-and-marginalised-communities.html (last visited February 26, 2025).

18 Amlan Mohanty and Shatakratu Sahu, "India's AI Strategy: Balancing Risk and Opportunity," *Carnegie India*, February 22, 2024.

19 *Ibid.*

5.1 Constitutional Framework: Privacy as a Fundamental Right

The Indian Constitution, under Article 21, guarantees the right to life and personal liberty, which has been interpreted to include the right to privacy. This right serves as the cornerstone for regulating FRT, as the technology involves the collection, storage, and analysis of sensitive biometric data. The principle of privacy encompasses not only informational privacy but also bodily and spatial privacy, all of which are directly implicated by the widespread deployment of FRT.[20]

However, the use of FRT in public spaces, such as airports, railway stations, and crowded events, raises questions about the extent to which individuals can expect privacy in such settings. Article 21 mandates that any restriction on privacy must satisfy the principles of legality, necessity, and proportionality. These principles require that the deployment of FRT be backed by a valid legal framework, serve a legitimate purpose, and minimize intrusion into individual privacy.[21]

In addition to privacy, the Constitution protects other fundamental rights affected by FRT, such as equality (Article 14), non-discrimination (Article 15), and freedom of expression and assembly (Article 19). These provisions collectively underscore the need for a regulatory framework that balances technological innovation with the protection of constitutional rights.[22]

5.2 Existing Data Protection Laws and Gaps

India's regulatory framework for data protection is currently governed by the *Information Technology Act, 2000* (IT Act). The IT Act, under Section 43A, mandates reasonable security practices for handling sensitive personal data, including biometric information. However, these provisions are limited in scope and do not specifically address the unique challenges posed by FRT.

The *Digital Personal Data Protection Act, 2023* (DPDP Act) aims to create a more robust framework for personal data protection. It outlines principles such as lawful processing, purpose limitation, and consent-based data collection, which are critical for regulating FRT. For instance, under the DPDP Act, biometric data

---

[20] Subodh Asthana, "Article 21 of the Indian Constitution" *iPleaders*, 2024 *available at*: https://blog.ipleaders.in/article-21/ (last visited February 27, 2025).

[21] Ranjeet, "The Urgent Need for Legislation to Regulate Facial Recognition Technology in India," *available at*: https://www.legalserviceindia.com/legal/article-16792-the-urgent-need-for-legislation-to-regulate-facial-recognition-technology-in-india.html (last visited February 27, 2025).

[22] *Ibid.*

qualifies as sensitive personal data and requires explicit consent for its collection and use. Despite these advancements, significant gaps remain in the existing legal framework. The DPDP Act provides broad exemptions for government agencies, allowing them to bypass consent requirements for purposes such as national security, public order, and law enforcement. This raises concerns about unchecked surveillance and potential misuse of FRT by state authorities. Additionally, the Act does not address algorithmic accountability, data retention policies, or the right to explanation in automated decision-making, all of which are critical for ensuring transparency and fairness in FRT systems.[23]

In India, one of the acts that indirectly deals with the use of FRT for identification is the *Criminal Procedure (Identification) Act, 2022*. The act replaced the older *Identification of Prisoners Act of 1920.* The act deals with matters of collection, preservation and identification of records of prisoners as well as convicts and for identification and investigation in criminal matters. The act while dealing with forensic and biological aspects by allowing technological and scientific techniques for taking physical, biometric and biological samples, fails to take into account the use of modern technologies like FRT and its implications on data protection laws and further rights of prisoners and convicts.[24]

5.3 Role of Government Agencies

Government agencies play a central role in deploying and regulating FRT in India. The National Crime Records Bureau (NCRB) and state-level police departments are among the primary users of FRT for law enforcement purposes. Initiatives such as the Crime and Criminal Tracking Network and Systems (CCTNS) and state-level Integrated Command and Control Centres utilize FRT for crime prevention, suspect identification, and public safety.[25]

While these applications aim to enhance security and efficiency, they often operate without a clear legal mandate or oversight mechanism. For instance, there is no statutory requirement for prior judicial approval, impact assessments, or public consultation before deploying FRT systems. This lack of transparency

---

23 Karthika Rajmohan, "First Read on the Digital Personal Data Protection Rules 2025: Here's what you need to know" *Internet Freedom Foundation*, 9 January 2025.

24 Shaifali Dixit and Chandrika, "PROCEDURE (IDENTIFICATION) ACT, 2022: A Comprehensive Analysis of Constitutional, Criminal, and Forensic Dimensions," 5 *Shimla Law Review* 167 (2022).

25 "Deployment of Facial Recognition Technology for State Surveillance and Monitoring," *Software Freedom Law Center, India,* January 16, 2024 *available at*: https://sflc.in/deployment-of-facial-recognition-technology-for-state-surveillance-and-monitoring/ (last visited February 28, 2025).

undermines accountability and raises concerns about surveillance overreach. In addition to law enforcement, government agencies also use FRT in other sectors, such as aviation and public administration. Initiatives like DigiYatra, which uses FRT for seamless passenger verification at airports, and Smart Cities projects, which integrate FRT for urban surveillance, demonstrate the technology's growing adoption. However, these deployments often lack explicit guidelines on data sharing, retention, and consent, leaving individuals vulnerable to privacy violations.[26]

At the national policy level, NITI Aayog's *National Strategy for Artificial Intelligence* emphasizes the need for responsible AI deployment, including the regulation of biometric technologies like FRT. However, the strategy remains non-binding and lacks the force of law. Similarly, the absence of a dedicated regulatory authority for overseeing FRT systems further exacerbates accountability gaps.

6. JUDICIAL PRONOUNCEMENTS

One of the first judgments that dealt with the right to privacy was ***R. Rajagopal v. State of Tamil Nadu***[27], where the Supreme Court dealt with issues surrounding the right to privacy and state surveillance. The case affirmed the principle that the state must respect individual privacy unless justified by law. This case reinforced the importance of ensuring that any surveillance, including the use of FRT, does not infringe upon the privacy rights of individuals without adequate legal justification and safeguards.

One of the most significant cases on privacy rights issues in India is ***Justice K.S. Puttaswamy (Retd.) v. Union of India***[28], where the Hon'ble Supreme Court recognized the right to privacy as a fundamental right under Article 21 of the Constitution. The judgment emphasized that privacy is integral to the preservation of human dignity and individual autonomy. The case dealt with the constitutionality of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and how it affected the privacy rights of an individual. Although this case did not specifically address FRT, it set a precedent for how biometric data, such as that collected by FRT systems, should be treated under the Indian legal framework. The court's reasoning stressed that any surveillance system, including FRT, must be lawful, necessary, and

---

[26] Dr. A.S. George, Dr. S. Sagayarajan ,*et.al.*, "From Paperwork to Biometrics: Assessing the Digitization of Air Travel in India through Digi Yatra," 1(4) Partners Universal International Innovation Journal 110-124 (2023).

[27] (1994) 6 SCC 632.

[28] (2017) 10 SCC 1.

proportionate to avoid violating the right to privacy. The court showed a major concern about the possible misuse of Automated facial Recognition Software (AFRS) without having a stringent and structured legislative framework in place.

The **Puttaswamy judgment** has led to subsequent discussions about privacy regulations in India, particularly in the context of biometric data. In ***Union of India v. Facebook Inc.***[29], the issue of data protection in the digital realm came into focus, when the Supreme Court examined the sharing of personal data by social media platforms. While not directly related to FRT, this case highlighted the importance of transparency, consent, and accountability in the collection and processing of personal data, principles that are essential for regulating the use of FRT.

While discussing the Indian jurisprudence over FRT, it becomes essential to look at the international level case laws. One of the most landmark cases on the use of Automated Facial Recognition (AFR) is ***R. v. The Chief Constable of South Wales Police***[30], also known as the **Bridges Case**. This was the first case to challenge the use of AFR stating it to be a violation of privacy and data protection laws. The case was filed by Ed Bridges, who challenged the use of AFR and live facial recognition by South Wales Police in public. The Court of Appeals, while overturning the lower court's decision considered the use of this technology to be a breach of privacy rights in the absence of a strong legal framework. The court held that there is a very intricate line between the legitimate and illegitimate use of this technology and that the use of FRT in this case did not comply with Article 8 of the European Convention on Human Rights Convention which provides the right to respect for private and family life.

In ***Glukhin v. Russia***[31], The European Courts of Human Rights expressed strong concerns of use of FRT against protestors and demonstrators in Russia. The court remarked that the use of FRT and AFRS is a growing threat to the fundamental rights of a person in the modern digital age.

7. GLOBAL PERSPECTIVES AND COMPARISONS

As facial recognition technology (FRT) continues to evolve globally, different countries have adopted varied regulatory approaches to address its implications for privacy, data protection, and human rights.

7.1 Regulatory Approaches in the United States

29 (2020) 3 SCC 208.
30 [2020] EWCA Civ 1058.
31 App. No. 11519/20 (ECHRT) (2023).

In the United States, the regulatory landscape for facial recognition technology is fragmented, with a combination of federal, state, and local laws governing its use. There is no comprehensive federal law specifically regulating FRT, which has resulted in a patchwork of legislation at the state and local levels.[32]

At the federal level, agencies such as the Federal Trade Commission (FTC) and the Department of Commerce have issued guidelines on the use of FRT, emphasizing transparency, accountability, and consumer protection. However, these guidelines are not legally binding, and FRT usage by government agencies, particularly in law enforcement, has largely been unregulated. The *Clarifying Lawful Overseas Use of Data (CLOUD) Act* of 2018, which facilitates data access by law enforcement agencies, does not specifically address biometric data or FRT, further underscoring the regulatory gaps.[33]

At the state level, some jurisdictions have enacted more robust regulations. For instance, California's *California Consumer Privacy Act (CCPA)*, effective from 2020, grants consumers the right to opt-out of the sale of their personal data, including biometric information. However, the CCPA does not comprehensively regulate FRT, and its enforcement mechanisms are still evolving. Other states, such as Washington and Oregon, have enacted laws that impose stricter requirements on the use of biometric data by both private companies and government entities.

Several U.S. cities have also taken steps to limit the use of FRT. For example, San Francisco and Boston have passed ordinances banning the use of FRT by city agencies and contractors. These localized bans reflect growing concerns about privacy, racial bias, and surveillance overreach. However, the lack of a cohesive federal framework for regulating FRT means that legal protections remain inconsistent across the country, resulting in uncertainty for businesses and citizens alike.

7.2 European Union: GDPR and AI Act

In contrast to the United States, the European Union (EU) has taken a more comprehensive and proactive approach to regulating facial recognition technology,

---

[32] James Andrew Lewis and William Crumpler, "Facial Recognition Technology: Responsible Use Principles and the Legislative Landscape" *available at*: https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape (last visited March 2, 2025).

[33] "FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies," *Federal Trade Commission*, 2012 *available at*: https://www.ftc.gov/news-events/news/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition-technologies (last visited March 2, 2025).

placing a strong emphasis on data protection, privacy rights, and the responsible use of artificial intelligence (AI). The EU's *General Data Protection Regulation (GDPR)*, which came into effect in 2018, provides a robust legal framework for the processing of personal data, including biometric data used in FRT. The GDPR recognizes biometric data as sensitive personal data and mandates stringent conditions for its processing. According to the regulation, biometric data can only be processed if explicit consent is obtained from the individual, or if processing is necessary for reasons of public interest or legal obligations. Furthermore, the GDPR emphasizes the importance of transparency and accountability, requiring organizations to inform individuals about the purpose and scope of data collection and use.[34]

One of the most significant aspects of the GDPR is the provision of data subject rights, including the right to access, rectify, and erase personal data. This gives individuals greater control over how their biometric data is used and processed. Additionally, the regulation imposes heavy penalties for non-compliance, with fines reaching up to 4% of a company's annual turnover, underscoring the EU's commitment to data protection and privacy rights.[35]

The *Artificial Intelligence Act (AI Act)*, introduced by the EU in 2024, seeks to regulate the use of AI technologies, including facial recognition, based on the level of risk they pose to individuals' rights and freedoms. The Act categorizes AI systems into four risk levels: minimal, limited, high, and unacceptable. FRT systems are likely to fall under the "high-risk" category, subjecting them to stringent requirements such as transparency, accountability, and human oversight.[36]

8. CHALLENGES IN REGULATING FACIAL RECOGNITION IN INDIA

The regulation of facial recognition technology (FRT) in India presents numerous challenges, reflecting the complexities of balancing technological advancement with the protection of fundamental rights. The absence of a clear, comprehensive legal framework to govern FRT has created significant regulatory gaps.

---

[34] "Art. 9 GDPR – Processing of special categories of personal data," General Data Protection Regulation (GDPR), 2016 *available at*: https://gdpr-info.eu/art-9-gdpr/ (last visited March 3, 2025).

[35] Scott Robinson, Rich Castagna and Tréa Lavery, "What is GDPR? Compliance and conditions explained" *TechTarget*, 29 July 2024.

[36] Graham Greenleaf, "EU AI Act: The 2nd most Important Data Privacy Law," *Privacy Laws & Business International Report* 23 (2024).

8.1 Lack of Comprehensive Legislation

India currently lacks a unified and comprehensive law specifically addressing the use of facial recognition technology. While the *Aadhaar Act* regulates biometric data for the purpose of the national identity system, it does not account for the use of FRT by private entities or government agencies in public spaces. The *Digital Personal Data Protection Act, 2023*, aims to address some of these concerns, but it does not provide clear guidelines for the deployment of FRT in public surveillance or law enforcement. The absence of specific legislation to regulate FRT's use across various sectors leaves significant room for abuse and poses a challenge to protecting privacy and civil liberties.[37]

8.2 Enforcement Challenges

Even with existing laws, the enforcement of data protection and privacy regulations remains a challenge in India. *Digital Personal Data Protection Act, 2023*, establishes a Data Protection Authority, but questions remain about its capacity and independence to oversee the widespread use of FRT. Furthermore, local law enforcement agencies may lack the technical expertise and resources to properly implement data protection requirements, leading to inconsistent enforcement of regulations. The absence of stringent penalties for violations further undermines deterrence.[38]

8.3 Technological and Ethical Concerns

FRT systems often suffer from issues of algorithmic bias and lack of transparency. Indian facial recognition systems are frequently criticized for inaccuracies, particularly when identifying individuals from marginalized communities. Without clear ethical standards or oversight for the development and use of these technologies, there is a risk of perpetuating discrimination and violating fundamental rights such as equality before the law.

8.4 Balancing Security and Civil Liberties

India faces the ongoing challenge of balancing national security and public safety with the protection of civil liberties. While FRT has significant potential for crime

---

[37] Pam Dixon, "A Failure to 'Do No Harm' -- India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S," 7 *Health and technology* 539–67 (2017).

[38] "Regulating Facial Recognition Technology in India," *Drishti*, July 3, 2024 *available at*: https://www.drishtiias.com/daily-updates/daily-news-analysis/regulating-facial-recognition-technology-in-india/print_manually (last visited March 4, 2025).

prevention and improving law enforcement, its unchecked use can lead to mass surveillance and erode privacy rights. The lack of clear guidelines on proportionality and the necessity for surveillance further complicates the matter, making it essential for India to find a regulatory balance that ensures both security and individual freedoms.[39]

9. CONCLUSION

Facial recognition technology (FRT) has rapidly emerged as a powerful tool with significant applications in law enforcement, security, and even customer service. However, its deployment raises profound ethical, legal, and human rights concerns, particularly with respect to privacy, data protection, and potential misuse. In India, where constitutional guarantees such as the right to privacy are enshrined in law, the widespread use of FRT challenges the balance between technological advancement and individual freedoms.

The *K.S. Puttaswamy* case, which established privacy as a fundamental right, has underscored the need for stringent safeguards when collecting and processing biometric data, including facial recognition data. The decision calls for any intrusion on privacy to be justified by a legitimate aim, supported by clear laws and a process that meets the standards of necessity, proportionality, and procedural fairness. This makes the legal regulation of FRT in India urgent, especially as the technology is being adopted by both government agencies and private entities without a comprehensive legal framework.

Although the *Digital Personal Data Protection Act, 2023* provides some hope for a robust data protection regime, it still lacks provisions that specifically regulate FRT. Key issues remain around transparency, consent, and data retention, which must be explicitly addressed to avoid the risks of mass surveillance, racial profiling, and discrimination. Furthermore, the absence of specific legislation to govern the use of FRT across different sectors, especially law enforcement, complicates efforts to prevent abuses.

The global landscape offers valuable lessons, particularly from jurisdictions such as the European Union, where the *General Data Protection Regulation (GDPR)* and the *Artificial Intelligence Act* provide a comprehensive framework for regulating biometric data and ensuring algorithmic accountability. However, India's unique socio-political context necessitates a regulatory approach that is attuned to its legal, cultural, and technological realities. A one-size-fits-all model may not be appropriate, but India must certainly take inspiration from international

---

39 *Ibid.*

best practices while ensuring that its regulations safeguard its citizens' rights effectively.

10. SUGGESTIONS

As India continues to grapple with the use of facial recognition technology (FRT), there are several suggestions that should be considered to ensure its responsible and ethical deployment.

1. **Comprehensive Legislation**: A dedicated law specifically addressing the regulation of facial recognition technology is crucial. The *Digital Personal Data Protection Act, 2023*, while a significant step forward, should be amended to include specific provisions that govern the use of FRT. This would ensure that its deployment is consistent with privacy rights and includes clear guidelines on consent, data retention, and accountability.

2. **Independent Oversight and Accountability**: Establishing an independent regulatory body to oversee the use of FRT systems is essential. This body should be empowered to monitor compliance with data protection laws, ensure transparency, and investigate complaints related to misuse. Regular audits and impact assessments should be conducted to evaluate the technology's societal impact and ensure its ethical deployment.

3. **Clear Guidelines on Use in Public Spaces**: There should be clear and transparent guidelines regarding the use of FRT in public spaces, particularly by law enforcement agencies. These guidelines should outline the purposes for which FRT can be used, limit the scope of its application, and provide checks and balances to prevent overreach and abuse.

4. **Bias Mitigation and Algorithmic Transparency**: It is essential to ensure that FRT systems are regularly tested for bias, particularly with regard to race, gender, and socio-economic status. The government and private sector should mandate the publication of algorithms used in FRT to ensure transparency and public trust in the technology.