THE DIGITAL PANOPTICON: FACIAL RECOGNITION, AI-DRIVEN POLICING AND CIVIL LIBERTIES IN INDIA: A CONSTITUTIONAL AND COMPARATIVE STUDY

Maitra Varun Chotia, PhD Research Scholar, Central Sanskrit University, New Delhi

ABSTRACT

Indian law enforcement is increasingly using Facial Recognition Technology (FRT), which is an application of Artificial Intelligence (AI). Supporters claim that it will be effective in the detection of crimes, yet opponents claim that the unrestricted application is dangerous because it is threatening privacy, equality and other rights. This paper is a critical analysis of the legal and constitutional framework in India (Articles 14, 19, 21) in relation to FRT and AI policing. We evaluate the current laws (the IT Act, Aadhaar Act, and the recently introduced Digital Personal Data Protection Act 2023) and observe the gaps in legislation and the process outlined by researchers[1]. Based on historic rulings (e.g. Puttaswamy v. Union of India on privacy and proportionality) and recent petitions (e.g. PUCL v. Telangana [2]We examine how biometric surveillance has been addressed in the decisions of the courts challenging FRT)[3] We place the problems of India in a global perspective, whereby ICCPR Article 17 and UDHR Art. 12 safeguard privacy on a global level, and organizations such as UNESCO and the Council of Europe have encouraged strict restrictions on mass surveillance[4]. A simple comparison of both the US and EU reveals that they are heading in different directions: multiple American cities have already prohibited police FRT, and the GDPR and the suggested AI Act in the EU provide strict regulations on biometric processing[5]. We also discuss how the bias of algorithms can solidify the existing discrimination, benefiting particularly the Muslims, Dalits, and

[1] *Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis* (report), https://3fdef50c-add3-4615-a675-a91741bcb5c0.usrfiles.com/ugd/3fdef5_1761915a67c841edaede945d4180bb32.pdf (last visited Dec. 12, 2025).
[2] A new legislation expands the government's surveillance powers, *The Caravan*, https://caravanmagazine.in/law/criminal-procedure-act (last visited Dec. 12, 2025).
[3] *Telangana HC issues notice in challenge to FRT*, Internet Freedom Foundation, https://internetfreedom.in/telangana-high-court-issues-notice-in-indias-first-legal-challenge-to-the-deployment-of-facial-recognition-technology/ (last visited Dec. 12, 2025).
[4]UNESCO, *UNESCO Adopts First Global Standard on the Ethics of Artificial Intelligence*, https://www.unesco.org/en/articles/unesco-adopts-first-global-standard-ethics-artificial-intelligence (last visited Dec. 12, 2025).
[5] *MAGLaw — Article Download*, Panjab University School of Law (maglaw.puchd.ac.in), https://maglaw.puchd.ac.in/index.php/maglaw/article/download/345/74/1298 (last visited Dec. 12, 2025).

other marginalized people[6] . The paper finds that, in the absence of sound protection (legal requirements, control mechanisms, and the evaluation of algorithmic impact, and transparency), [7]FRT will have a chilling effect on free assembly and expression (Art. 19), undermine the right to equal protection (Art. 14) and infringe personal liberty (Art. 21). We provide specific policy suggestions such as prohibiting face-scanning outright or requiring legal approval and audit by independent organizations to bring the policing inventions in India to the constitutional and human rights pledges of the country.

Keywords: Facial Recognition Technology, AI policing, privacy, discrimination, constitutional rights, India.

Introduction

The AI-based surveillance tools have been adopted by the police forces in India in recent years. Facial Recognition Technology (FRT) - systems that compare live or recorded images of faces to databases - are now commonplace in most states in criminal investigations, in public safety and even in crowd monitoring[8]. An example is that the Delhi Police used FRT in the 2020 anti-CAA protests and in their investigation of the 2020 Northeast Delhi riots[9]. The Police Commissioner of Hyderabad describes Telangana as the most policed location in the globe after installing the control centre in the city[10] with FRT-enabled cameras[11]. The government has put a lot of money in it: according to one report, about 9.6 billion has been spent on FRT development[12].

However, this has led to a fast deployment, which has surpassed the law. No particular Indian statute governs the use of FRT, and its usage is not directly permitted by law. According to one legal commentator, there is a total legislative vacuum in India in relation to biometric surveillance, even though there are partial regulations (the IT Act, the narrow Aadhaar

[6] Jauhar Vipra, *Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies*, JURIST (Feb. 2022), https://www.jurist.org/commentary/2022/02/jauhar-vipra-frt-constitutional-challenges-law-enforcement/ (last visited Dec. 12, 2025).
[7] *Ban the Scan* (Amnesty International campaign page — Hyderabad), https://banthescan.amnesty.org/hyderabad/index.html (last visited Dec. 12, 2025).
[8] *Telangana HC issues notice in challenge to FRT*, supra note 3.
[9] Oxford Human Rights Hub, *AI Surveillance and Privacy in India: Human Rights in the Age of Technology*, https://ohrh.law.ox.ac.uk/ai-surveillance-and-privacy-in-india-human-rights-in-the-age-of-technology/ (last visited Dec. 12, 2025).
[10] *As AI Took Over Policing in Delhi, Who Bore the Brunt?*, Pulitzer Center, https://pulitzercenter.org/stories/ai-took-over-policing-delhi-who-bore-brunt (last visited Dec. 12, 2025).
[11] *Telangana HC issues notice in challenge to FRT*, supra note 3.
[12] *Ban the Scan*, supra note 7.

provisions) and only advisory guidelines. The new Digital Personal Data Protection Act 2023 (DPDP Act) is a step forward of individual rights over personal data, yet researchers warn that it does not pay much attention to the role of government surveillance and algorithms accountability[13]. As a matter of fact, police gather and distribute facial photographs through apps (such as Telangana's "TSCOP" mobile app) that search databases of the National Crime Records Bureau and Aadhaar files without any obvious legal framework or consent[14].

The intrinsic aspect of the facial recognition is that the individual profile is repositioned in a permanent state archive. It enables detection of regular citizens anywhere that the cameras are faced as opposed to individuals on the lists of suspects. The analysts caution that the growth of FRT may lead to a freeze of street protests, free debates and even impromptu celebrations on the streets in case everyone realizes that they are under surveillance[15]. Furthermore, FRT systems are also reported to be technically unreliable, biased, more likely to give false matches to darker-skinned people and women[16], which brings the issue of wrongful arrests. In a single recorded incident, two Muslim men were arrested by the Delhi police on riot charges as a result of FRT "matches" which numerous lawyers have claimed were clearly erroneous, an example of how the algorithmic error can meet the communal bias.

This paper discusses these problems in a legal context. It poses the question: does the constitution and laws of India safeguard (or not) the citizens against the intrusion of AI-driven policing. We are going to examine the pertinent legal provisions (Articles 14, 19, 21 etc.), case law (especially Puttaswamy on privacy), and the recent issues (e.g. the Telangana FRT petition). We also put the situation of India into the international and comparative perspective, which takes into account such norms as ICCPR and UDHR, and regulatory practice in EU and US. The objective is to conduct a rigorous doctrinal and comparative analysis of the constitutional implications of FRT, the implications of the policy on the marginalized communities, and the policy instruments required to protect rights in the AI era.

Hypothesis

The current research is conducted under the premise that unregulated use of facial recognition

[13] *MAGLaw — Article Download*, supra note 5.
[14] *Telangana HC issues notice in challenge to FRT*, supra note 3.
[15] *Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis*, supra note 1.
[16] Jauhar Vipra, *Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies*, supra note 6.

in the Indian policing system is a significant threat to the basic rights. Namely, it theorizes that, in the absence of explicit legal power and regulation, FRT use usurps the right to privacy and personal liberty (Article 21), the right to equality (Article 14) and the right to the freedom of speech and assembly (Article 19). Besides, we suppose that algorithmic bias will aggravate the disadvantages of historically marginalized groups (e.g. religious minorities and lower castes), which erodes the substantive equality. Lastly, the paper presupposes that the international human rights standards require powerful restrictions on surveillance technology. Thus, our implicit assumption is that a sensible legal framework (with potential ban, strict intent restrictions and responsibility controls) is needed in order to curb the demise of constitutional principles in India by FRT.

Research Questions

The analysis is structured around the following key questions:

1. How do Articles 14, 19 and 21 of the Indian Constitution (and related provisions) apply to biometric surveillance by FRT and AI policing? To what extent do these guarantees currently protect individuals from arbitrary face-scanning?

2. What does Indian jurisprudence (for example, *K.S. Puttaswamy v. Union of India* on privacy and proportionality) suggest about the legality of facial recognition? Have courts addressed FRT or related surveillance (e.g. in Aadhaar or electronic evidence cases), and how? Conversely, where do legislative lacunae exist?

3. What guidance does international instruments (UDHR, ICCPR, Human Rights Council) and global best practices (EU GDPR, draft AI Act; U.S. city bans) provide for regulating FRT? What lessons can India draw from other jurisdictions' approaches to biometric policing?

4. How do FRT and AI-driven law enforcement affect vulnerable communities? What evidence is there of biased design or discriminatory outcomes (for instance, false positives disproportionately impacting minorities), and how might this violate equality and dignity?

5. What legal and policy measures can ensure AI policing aligns with human rights? Should some uses be banned outright? How can transparency, accountability and non-

discrimination be built into FRT deployment?

Research Methodology

The study is based on a doctrinal-legal and comparative approach[17]. The methodology is primarily doctrinal legal analysis of primary materials, backed up by secondary scholarly and policy materials. The paper analyses the manner in which these decisions and laws put rights and police powers in perspective to privacy, equality, speech and assembly. Secondary sources are law review articles, peer-reviewed research, think-tank reports (e.g. Internet Freedom Foundation, Amnesty International), and credible news investigations (e.g.). The Wire). Policy analyses and guidelines (e.g. NITI Aayog, UNESCO) are also taken into consideration by us in order to know normative principles.

The international human rights law and foreign legal developments are drawn on through comparative analysis. We analyze the applicable international practices (ICCPR, UDHR, standards of the Council of Europe), and review the best practices in other jurisdictions (e.g. European Union (GDPR, AI Act); certain states/cities in the United States (e.g. Illinois Biometric Privacy Law)). The normative human rights reasoning provides the direction of the inquiry, and evaluates whether FRT practices comply with the principles of legality, necessity, proportionality, transparency and equality[18]. We pay special attention to scholarly and NGO accounts of the social consequences of AI policing (e.g. bias research by Buolamwini and Gebru, the Ban the Scan movement organized by Amnesty). Where possible, reliable data (e.g. arrest statistics, government admissions of FRT use) are being used to base the discussion.

The methodology, therefore, incorporates both the doctrinal legal research and empirical reports and international law so as to bring about a holistic and interdisciplinary analysis .

Literature Review

There is a limited academic literature on AI policing in India. Some of the main themes are privacy, data protection, bias and governance. Generally, Indian researchers focus on the constitutional right to privacy (provided by Puttaswamy 2017) as a protective measure against

[17] *MAGLaw — Article Download*, supra note 5.
[18] *Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis*, supra note 1.

surveillance technologies[19] . According to the analysis conducted by Jauhar and Vipra (2022), dozens of states implement FRT without much transparency, and it leads to the voiciferous arguments on the rights infringements[20]. They emphasize that the very concept of FRT is incompatible with the principle of informational autonomy: people will no longer have the ability to control their biometric information after scanning by state systems. The existed Puttaswamy test (legality, legitimacy, proportionality) is also mentioned by the scholars as the measure to which any FRT deployment should be applied[21] .

Critics such as NGOs abound with the regulatory vacuum in India. In a single IJLLR article, a total absence of legislative protection of data protection is noted, which puts biometric tools mostly unregulated. The petition on internetFreedom.org (*Masood v. Telangana*) makes the same argument: it claims that there is no legislation to authorize the use of FRT in Telangana, and thus the status of existing practices is unconstitutional according to Puttaswamy. According to the research conducted by Vidhi, the absence of a proper limit makes FRT applications violate due process and equality since police discretion is not restricted. The Amnesty report on the Ban the Scan also indicates that the Automated Facial Recognition system in India is intended to create a nationwide database with no privacy guarantees[22].

The literature relies much on international research. According to Buolamwini and Gebru (as cited in Jauhar and Vipra), in their study, FRT algorithms have higher error rates with darker-skinned women. Indian commentators (and Vidhi critics, as well) have stressed that such a move as the implementation of FRT into a pre-existing discriminatory policing context only exacerbates injustice[23]. An example of this would be a Vidhi study that approximated that the implementation of FRT in Delhi would more significantly impact the Muslims, as they are also in comparatively over-policed neighborhoods. Amnesty also observes that FRT has the capability of intensifying discriminatory policing of the Muslims, Dalits, Adivasis and other underprivileged segments.

[19] *MAGLaw — Article Download*, supra note 5.
[20] Jauhar Vipra, *Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies*, supra note 6.
[21] *Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis*, supra note 1.
[22] *Ban the Scan*, supra note 7.
[23] Jauhar Vipra, *Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies*, supra note 6.

Comparative and international literatures are also appealed to. Responses by scholars: the GDPR is particularly strict in its biometric data handling, and the AI act proposed by the EU (classification of FRT as high-risk) is frequently cited as an example of best practice[24]. The U.K. ruling on police use of live FRT (R. v South Wales Police, 2020) that was overturned is also cited in academic commentaries, and several campaigns in civil society that are seeking moratoria. According to international human rights groups (Amnesty, Article 19), mass FRT cannot be rights-compatible at all, and that no number of safeguards will make it completely so[25]. Therefore, although there is an increased awareness of the stakes, without a doubt, the bulk of the literature consists of policy reports and law journal essays; there is limited systematic empirical research on the effects of FRT in India. Our paper is based on these sources to give a systematic legal discourse within the Indian constitutional context.

1. Legal and Constitutional Framework in India

The Constitution of India entrenches equality, liberty and dignity as values in the country. The evaluations of any AI surveillance regime must be against such guarantees as the main Articles 14, 19 and 21.

Article 21 (Life, Liberty and Privacy): In *K.S. Puttaswamy v. Union of India* (2017), the Supreme Court unanimously stated that the right to privacy was a fundamental right as enshrined in Article 21. This encompasses the informational privacy - the right to control personal data. It was also believed by Puttaswamy that any action of the state, which infringes on privacy, should have passed a triple test: the act must have a legal basis, must serve a legitimate state interest, and must be proportionate (least restrictive means) . FRT obviously gathers and processes biometric information on a personal basis. Such collection by Puttaswamy, however, can only be legal in a case where a statute specifically authorizes it and proper precautions are constructed. So far, there is no particular legislation that permits police to conduct blanket FRT surveillance. In this way, any deployment would probably fail the first branch of legality. Furthermore, although advanced on the justification of protecting the society, a court requires that such an end must be minimally invasive - a requirement that is readily broken by mass, indiscriminate scanning[26].

[24] *MAGLaw — Article Download*, supra note 5.
[25] *Ban the Scan*, supra note 7.
[26] *Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis*, supra note 1.

Article 21 also secures dignity and autonomy besides privacy. Biometric surveillance also becomes an issue of dignity[27]: the forced scanning of faces is the one that rearranges the profile of the individual as a piece of public information, which, seemingly, dehumanizes human dignity. Although Article 21 is not a hard rule, exemptions (e.g. due to security) are accompanied by very high procedural safeguards. Puttaswamy reinforced the idea that even in the national security cases the restrictions should be just, fair and reasonable, which are not present in the current use of FRT.

Article 19 (Freedom of Speech and Assembly): Articles 19(1)(a) and (b) provide the freedom of expression and assembly. Such rights can be chilled by surveillance technologies, such as FRT. According to the Oxford Human Rights Hub, it is dangerous to think that because protestors are aware that any gathering is controlled by surveillance, they will be discouraged to protest and reduce dissent. Indian precedent (e.g. *Anuradha Bhasin v. Union of India* [28]on internet shutdowns) believes that any limitation to speech or assembly, should be legally justified and reasonable. The fact that FRT is implemented preemptively (e.g. at rallies) without any discussion or legal regulation is a red flag according to Article 19.

Article 14 (Equality and Non-discrimination): Article 14 guarantees equal protection under the law. This may be unintentionally broken by algorithmic tools, which create disproportional results among different groups. Jauhar and Vipra note that the bias of FRT against dark-skinned people is documented, so Article 14 issues can be involved: in case police are guided by technology that has high errors, some groups of people can be disadvantaged on a whim. The petition by Telangana directly proposes that design flaws and false results of FRT infringe upon equality. Also, when the state applies FRT selectively (e.g. to specific neighbourhoods) this may constitute unconstitutional discrimination. The lack of explicit statutory provisions that help to avoid prejudice in automated policing threatens the fulfilment of the promise of Article 14, which implies equal treatment.

Other Provisions: Article 20(3)- right against self-incrimination - may be involved in case compulsory collection of biometrics is deemed personal evidence. Critics observe that facial images are similar to testimonials that may incriminate an accused. Non-testimonial treatment of identification procedures (such as photographs) has however been mostly applied by Indian courts. However, due to the wide scope of information collection by FRT, new issues of self-

[28] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

incrimination and a fair trial are posed. Article 50(duty to respect rule of law) and Article 51A(d) (obligation to respect human rights) highlight the fact that a state has a role to play in ensuring that rights are upheld implying that the unregulated use of FRT could be against constitutional obligations.

Statutory Law: The current statutes in India provide incomplete solutions to the problem but they also contain some loopholes. Personal data is regulated somewhat by the Information Technology Act 2000 (e.g. section 72A punishes data breaches), but biometric surveillance is not fully covered. The Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act 2016 directly restricts applications of Aadhaar data - in 2018, the Supreme Court prohibited the use of Aadhaar on other purposes other than welfare and taxation[29]. This was however a close call: it was applied to Aadhaar only and not a blanket privacy law. The Digital Personal Data Protection Act, 2023, which gives data rights to everyone, has been noted to be limited in its scope, and fails to explicitly regulate state surveillance. Specifically, DPDP fails to explicitly limit the use of FRT or algorithmic profiling by government agencies, which creates a key blind spot.

In the recent past, Parliament had granted additional powers to police to gather biometric data through the Criminal Procedure (Identification) Act, 2022. This legislation replaces a 1920 statute and permits the gathering of photographs, fingerprints, iris images and even DNA of suspects and convict. The fact that it was passed demonstrates a legislative acknowledgment that contemporary policing is associated with biometric evidence. However, commentators have cautioned that the over-reach of the Act is that it may violate the privacy, equality and self-incrimination rights [30]. Most importantly, the Act does not directly deal with FRT and regulate the way collected images can be utilized to conduct mass surveillance. Therefore, in a way that it legalizes the seizure of an image of a suspect, it does not establish boundaries in the prospective scanning of CCTV images of strangers.

In short, the constitutional rights of equality and liberty in India are broad and Puttaswamy pointed out that informational privacy is implied in Article 21. However, the legal system of biometric data is still inconsistent. According to academic commentators, this vacuum is something that encourages arbitrary surveillance. The current legal system does not specifically

[29] *Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis*, supra note 1.
[30] A new legislation expands the government's surveillance powers, *The Caravan*, supra note 2.

prohibit FRT, but it is not guaranteeing sufficient protection. It therefore seems that much of the present FRT applications do not have the explicit law and procedural protection that is needed in Article 21. This environment preconditions judicial disputes and legislative changes to establish the balance between AI policing and the constitutional rights.

2. Indian Case Laws on Facial Recognition and Surveillance

No Indian court has, as yet, directly determined the use of facial recognition by the police. Nevertheless, a number of landmark rulings present inspirational principles against which FRT should be considered based on basic rights.

The case in point is Justice *K.S. Puttaswamy v. Union of India* (2017). It was against this that the Supreme Court upheld the fact that privacy (bodily and informational privacy) is a right of fundamental entitlement in Article 21. The Court stated the three-part test: any state action that has an impact on privacy has to be (1) legislatively sanctioned, (2) have a legitimate purpose, and (3) be reasonable in relation to that purpose. Practically, any FRT application by police has to meet these requirements. To date, according to the petition of Telangana, FRT is not given any special legislation to operate; its purposes are not always made clear; and random face-scanning can be more than reasonably advantageous. In the case of Puttaswamy, though, FRT practices are probably all three limbs.

The other important case is that of *K.S. Puttaswamy v. Union of India* also known as Aadhaar II,. Although primarily regarding Aadhaar, the ruling stated that biometric data obtained via Aadhaar could not be used to do surveillance. The Court invalidated clauses that permitted the dissemination of Aadhaar data to law enforcement on the ground of the so-called function creep. This indicates that the courts are cautious of the wider policing by centralized biometric identification. It highlights that even the welfare-centered data collection schemes should not be massively identified under any guise without immediate restrictions.

There are other precedents related to privacy. In *Selvi v. State of Karnataka* (2010) banned forced narco-analysis and brain scan by asserting the right of an individual not to self-incrimination and privacy of the body. Analogically, forcing biometric face print of a person (or scanning a video of his/her face) can involve the same personal autonomy issues. Although the decision of *Kharak Singh v. U.P*[31]. (1962) allowed certain degree of police surveillance, it

[31] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).

stated that the right to privacy of the home and individual liberty in the Constitution is sacred. Although the facts vary, these early cases indicate the general dislike of the Court to unchecked surveillance.

The Criminal Procedure Code (as amended by the 2022 Act) now clearly permits police to capture the photograph of a suspect and their fingerprints. Nevertheless, adapting evidence law to new technology is unresolved. The rules applied to videographic evidence and to the electronic records are in Section 65A-B of the Evidence Act, yet they are about conventional digital records, and not algorithmic inferences. Jauhar and Vipra remark that the identifications generated by FRT do not simply belong to the existing evidence regime. We can take an example, the Hyderabad petition mentions that where an officer post a face to a database and picks a match, it is seldom recorded using the formal protection of an identification parade. Two cases of Delhi riots have had courts granting bail where judges noted that no witness supported the FRT "identification" and that the video analysis by an algorithm was not self-evident[32]. Therefore, the output of FRT might require a stronger procedural context to be admissible even in this case.

The Telangana High Court (Hyderabad bench) is the first Indian court to take a petition against FRT. In *SQ Masood v. State of Telangana*[33], the petitioner (filed Jan 2022) challenges the use of FRT as being in violation of Articles 14, 19 and 21.

Related technology has been occasionally touched on by the lower courts. There is no precedential support of FRT bluntly monitoring crowds. The basic rights paradigm of Puttaswamy, Anuradha Bhasin, and equality jurisprudence will be used to conduct the analysis until the ruling of a higher court. In *Navtej Singh Johar v. UOI*, 2018[34]. the Court also broadened Articles 14 and 21 to cover sexual orientation and dignity, That ruling confirms the fact that privacy and equality rights are broad and dynamic. Through analogy, it can be argued that the same should be afforded strong protection to digital identity and location data.

Summing up, FRT has not been dealt with squarely by Indian case law yet, but it offers effective means of analyzing it. Puttaswamy ascertains that no law and protection may be violated to enter the body and data of the citizen. Aadhaar II shows the judicial suspicion that

[32] *As AI Took Over Policing in Delhi, Who Bore the Brunt?*, supra note 10.
[33] S.Q. Masood v. State of Telangana, W.P. No. 25064 of 2020 (Telangana High Ct. filed Jan. 2020).
[34] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1 (India).

biometric databases are being abused in the interest of surveillance. These precedents suggest that no FRT regime can be shoved down the throat without being finely crafted to be constitutional. The application of facial surveillance is constitutionally dangerous until the courts either directly deal with FRT, or Parliament passes special constraints.

3. International Law and Framework of Human Rights

India is a signatory to major international human rights documents, which are used in the domestic law. In the Universal Declaration of Human Rights (UDHR, 1948), Article 12, it is written that no one should be arbitrarily interfered with his privacy, or attacked on his honour and reputation. Similar guarantees are provided in the International Covenant on Civil and Political Rights (ICCPR, 1976) which India acceded to in 1979. The Article 17(1) of ICCPR reads as follows: No person shall be arbitrarily or unlawfully intruded on his privacy, family, home or correspondence[35]. These clauses provide an international standard, that privacy is guaranteed unless any interference is legal, necessary and proportional (against the three-part test of Puttaswamy).

It guarantees the freedom of expression and assembly by the ICCPR: Article 19 on expression and Article 21 on peaceful assembly (no restrictions except stipulated by law on the basis of legitimate purposes). The UN Human Rights Committee (in its General Comments) has pointed to the fact that surveillance technologies may result in a chilling effect on these rights. Therefore, the usage of FRT on demonstrations or on mass events involves implicature of these norms. To illustrate, the UN Special Rapporteur on Freedom of Expression has cautioned against the use of facial recognition of protesters as an anti-dissent mechanism.

Recently, UN entities have published advice regarding AI and human rights. The Recommendation on the Ethics of Artificial Intelligence (2021) provided by the UNESCO requires AI to safeguard fundamental rights, and with transparency and accountability. Its news release indicates that there are serious risks to privacy, dignity and agency, and the risk of mass surveillance brought about by AI. In its text, UNESCO explicitly recommends the prohibition of the so-called invasive applications of AI systems to mass surveillance. Likewise, the UN Guiding Principles on Business and Human Rights and the UN High Commissioner on Human

[35] U.N. Office of the High Commissioner for Human Rights (OHCHR), *International Covenant on Civil and Political Rights*, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (last visited Dec. 12, 2025).

Rights also emphasized that emerging technologies should be utilized in a manner that does not violate human rights such as privacy, equality and non-discrimination.

These standards are supported by regional instruments. The right to the right to private life (Article 8) is guaranteed by the European Convention on Human Rights (ECHR), and the European Court of Human Rights has ruled out indiscriminate retention of biometric data (S. and *Marper v. UK, 2008*[36]) as violating privacy. Although India is not a member of ECHR, such rulings influence the international standards of surveillance and data. It is worth noting that the Indian Supreme Court in Puttaswamy observed international jurisprudence on privacy. The Court cited EU standpoints on data protection and U.S. Article 21 can be interpreted through cases in the fourth amendment.

Other UN tools strengthen the issues of fairness and equality. Article 26 of the ICPR provides equality before the law and the ban of discrimination based on factors such as religion, caste or status (implied in the context of biased policing results). The UN Human Rights Council has issued resolutions to understand and regulate AI, including focusing on transparency and avoiding bias and assessing the impact of AI on human rights. The UN Secretary-General Roadmap on Digital Cooperation, which provides that data-driven surveillance should be lawful and should not violate rights, was also negotiated with the assistance of India itself.

In short, the international obligations of India require that the FRT applications should be thoroughly checked. The universal human rights system demands a prior legal approval and necessity test to any surveillance (reflecting our constitutional legislation). It cautions against discrimination, too: any algorithm that increases racist policing (the phrase used by Amnesty) may infringe on non-discrimination provisions of ICCPR. According to a UN report about AI, such decisions impacting millions of people must be equitable, open and debatable[37]. These international standards will always give us an edge in analyzing Indian law.

4. Comparison: FRT Regulation in the US and the EU

The analysis of other jurisdictions gives an insight into the potential regulatory strategies. The General Data Protection Regulation (GDPR) in the European Union considers biometric data (including faceprints) to be a special category that needs an express consent or a strong

[36] S. and Marper v. United Kingdom, 48 Eur. Ct. H.R. 50 (2008).
[37] *Telangana HC issues notice in challenge to FRT*, supra note 3.

justification. Article 9 of the GDPR in general restricts the processing of such sensitive data to few reasons (e.g. vital interest, employment, or public interest work). More importantly, the proposed Artificial Intelligence Act (AI Act, enacted in 2023 and coming into force in 2024) by the EU considers remote biometric identification by law enforcement to be a high-risk activity. This would place powerful constraints: tight data control, human supervision, and bans on real-time face recognition in the streets except where strictly justified by law as having a strictly limited purpose. The AI Act is representative of a precautionary policy: it is neither more nor less innovative nor more or less protective of rights. Its high-risk designation implies that FRT needs to have certain obligations such as transparency and impact measurements.

In the meantime, there is no national privacy law in the United States, and thus the states and cities have led the way. Interestingly, San Francisco (2019) and Portland, Oregon (2020) prohibited the use of FRT on a municipal level altogether, pointing to the problem of civil liberties. Other bans on police and government use are similar in several other cities (e.g. Boston, Oakland, Somerville). Other states such as Illinois, such as the Illinois Biometric Information Privacy Act (BIPA), have enacted tougher laws on biometric privacy: the Illinois Biometric Information Privacy Act (BIPA) pre-requires companies to obtain informed consent to the collection of biometric identifiers and provides the ability to bring hefty private lawsuits to breaches. Federal legislators have introduced bills like the Algorithmic Accountability Act (2019) to make impact assessments mandatory, none of which have been passed. The U.S. courts have started to listen to Fourth Amendment (unreasonable search) cases against FRT with decisions awaiting. The overall tendency in the U.S. is conservative: in the case of FRT, the supporters demand warrants or case-by-case court decisions.

4.1 International Case Law: *The R. v. South Wales Police* [38](2020) case of the U.K. Court of Appeals prohibited live FRT protesting due to their breach of the data protection legislation and human rights. FRT regulation is also being studied in Australia and Canada. These changes indicate a worldwide confrontation: most democracies are demanding either legal prohibitions or even bans on AI surveillance of the population.

4.2 Lessons for India: India can attract these models. India may also borrow data protection standards (e.g. the need to expressly use biometric processing and supervise it) and think about banning unregulated real-time scanning, adopted by the EU. The concept of a high-risk

[38] R. (Bridges) v. Chief Constable of S. Wales Police, [2020] EWCA Civ 1058 (UK).

category is instructive: it implies admitting that FRT is qualitatively different to lower-risk AI and should be regulated respectively. India, in its turn, may take into account the influence of litigation and civil liberties organizations in reform making in the U.S. As an illustration, privacy experts have proposed judicial control (a warrant is needed to search in FRT). The BIPA of Illinois has already spawned dozens of class-action lawsuits demonstrating that legal responsibility (and fines) can be used to enforce the consent.

Among the major comparative lessons, one should note the value of consent: people in Europe can usually decline consent to be included in the facial databases but in the contemporary situation in India there is no consent requests. Auditability is another possible lesson: the EU proposals suggest open algorithmic audits and transparency. These concepts can be used to make policy in this place.

Put simply, the comparative experience highlights that the democratic societies are struggling with FRT through reinforcing legal guardrails or even halting its implementation. The strategic choice of India can be synthesized with its own background: since India has the tradition of judicial review, and since it is not the worst example within the international human rights obligations, it can be used to address the current regulatory gap.

5. Enforcement and Bias: Effect on Marginalized Community.

The important issue with AI policing is its impact on vulnerable populations. There is a documented accuracy issue in facial recognition algorithms on some demographics. It has been demonstrated by studies by Joy Buolamwini and others (as cited by the commentators in law) that most FRT systems falsely identify darker-skinned women at much higher rates than light-skined men. Minor error rates can have enormous impacts on policing: a false match can result in a false arrest. Furthermore, the errors that are made by an FRT system are not accidental, but in many cases, they are race- or gender-related.

These technical prejudices are overlapped by social realities in India. Religious, caste, tribal minority communities tend to reside in more populated cities that are highly monitored. The researchers at Vidhi discovered that the FRT implementation in Delhi would disproportionately target the Muslims because the Muslim-majority areas were over-policed. Amnesty highlights that FRT may only make the current problem of discriminatory policing more severe: despite the alleged functioning of the algorithm, it can still be used to a greater extent in relation to

Muslims, Dalits, Adivasis or other historically marginalized populations. An example is the cases of riots in Delhi where the reported instances were that of young Muslim men. In another instance, a Muslim undertrial (Ali) spent years in jail after police recognized him through FRT using CCTV video-recordings despite the fact that several lawyers and family members claimed that he was innocent[39] . The investigation by The Wire showed that 750 or more of 758 cases of riots were solved using FRT , which indicates that the application of this technology was almost entirely dependent. The lack of accountability brings up the possibility that bias (intended or not) is constructed into a whole criminal justice process.

Equality issues also arise to gender and disability due to FRT. Most surveillance cameras are usually tall and record standing adults- which is a disadvantage to children, elderly people and people who are not able to stand. The algorithms that are based on the old binary gender markers can misgender transgender people. Although there is not much India-specific data available, previous experience in other countries shows that such harms are probable in this case as well.

It is not only those who are wrongly identified that have an effect on society. The fact that the citizens of a specific community are aware that they are being monitored at all times by a flawed system brings about an atmosphere of fear and stigma. The awareness of the fact that it will be recorded may discourage the common citizens to gather and express themselves freely. According to the article by Oxford HR Hub, extensive FRT surveillance is a threat to street demonstrations, candid discussions, even impromptu street parties. This chilling effect silences marginalized voices in disproportion, as these voices are already wary of going out. Activists and civil society have sounded an alarm that FRT in protest areas (as was the case with anti-CAA protests) can result in selective policing: e.g. a human rights activist was recognized and followed by the police using FRT while protesting .

Prejudice can be reinforced on internal police practices. The private sector research has demonstrated that when a dataset is biased (e.g. more images of a certain community) adding FRT will not remove it, but instead increase it. It is not the first time when police profiling based on religion or caste is alleged in India. The introduction of AI will keep those biases behind the facade of impartiality. As an example, two Muslim men who were caught in the case of riots in Delhi reported that there was no identification parade, the police already knew

[39] *As AI Took Over Policing in Delhi, Who Bore the Brunt?*, supra note 10.

them and only FRT was used to formalize the arrest. These anecdotes are indicative of a dangerous process: human prejudice can set the system, FRT offers a ready-to-wear match, and then the courts can make this part of the evidence.

Also, there are procedural equity issues. Other jurisdictions have demonstrated a lack of rigorous validation on FRT "hits". In the absence of a policy requiring secondary verification (e.g. compulsory identity parades, or forensic examination of non-facial evidence), there is little that marginalized suspects can do. In a case in Delhi, a bail order actually stated that the video evidence relied on FRT results which were not reliably tested. The attorney claimed that the evidence was weak (the suspect was referred to during his arrest as a terrorist, although the police knew who he was in advance). Back in prison, the people recognized by FRT were abused (Muslim prisoners claimed that they were referred to as terrorists and dedicated to menial work). This repressive treatment is an expression of how a stigmatizing label by a broken system can increase discrimination at all levels.

To conclude, AI policing is not an impact-neutral event. It runs the danger of reproducing and exaggerating social prejudices. Article 14 further provides that such disparate impact can also be a breach of equality in the event that it is caused by arbitrary state action. The little information we possess by demonstrating a trend towards bias indicates that marginalized groups are already the initial victims of FRT policing. This disparity has to be dealt with in any policy implementation: treating people the same way in software is not a guarantee of equitable results. This fact is what guides our policies.

6. Implementation and Societal Impact Challenges

In addition to rights and prejudices, real-life issues make FRT implementation difficult. Technical constraints are still a matter of concern. False positives and false negatives of many FRT systems are still non-negligible. According to leaked testing data, one of the Delhi police FRT systems was only accurate 2% of the time (Amnesty reports)[40]. That is, 98 percent of so-called matches may be wrong. Even in ideal conditions, side-profile or low-quality images decrease the accuracy. The Telangana petition observes that police use CCTV shots which in most cases capture side or rear shots, and thus identification becomes very inaccurate[41]. However, in reality, police evidence in courts has occasionally swept these doubts under the

[40] *Ban the Scan*, supra note 7.
[41] *Telangana HC issues notice in challenge to FRT*, supra note 3.

carpet. The pilots exposed by journalists demonstrate how police are putting their trust on the FRT outputs which even common lay observers can find questionable, which poses serious questions of due process. These systems cannot be trusted by the courts as well as by the people without strict standards and independent audit.

There is also the pitfall of operations. The contemporary FRT scanning in India is performed by selecting an item in a list of potential matches created by the algorithm by a human analyst. This step is prone to cognitive bias: an analyst who thinks that a suspect of a particular description might commit a crime may choose a target that is more probable. It lacks transparency: the final decision is not captured and reasoned out and sometimes no alternative hypothesis is tested. There are no policy guidelines as to when to abandon an analysis yielding low-confidence candidates. The IFF reports indicate that police are at their own will to scan who and where, i.e. innocent people can be involved in criminal investigations without any suspicion.

Technology and size: Indian government has developed massive data and camera systems. By 2022, there is more than half a million CCTV cameras installed by police in Telangana alone[42]. The National Crime Records Bureau is building upon its Automated Facial Recognition System to store tens of millions of images[43]. Several years down the line, one can trace the movements of anyone in big cities in real time. This scale implies that errors or misconducts would not touch a few people but millions. Besides, the threats to data security are serious: big biometric databases are the best victims of hacking. The most recent examples (e.g. a police face database breach in Tamil Nadu) indicate that sensitive data can be easily leaked. There are however, no strict legal conditions in India to obtain or to reduce FRT data as in the EU.

Societal and psychological effects: FRT enforcement changes the way citizens relate to the state besides granting them legal rights. The fact that any protester or passerby can be identified and recorded cultivates self-censorship. This compromises the democratic freedom of dissent. Even human rights activists have cautioned that the very existence of facial scanning cameras in rallies will deter attendance. In fact, an activist with Telangana says that police even compelled him to take off his face mask in order to capture a photograph of him - an intimidating act that prompted him to launch the constitutional petition. Societies that were

[42] *Telangana HC issues notice in challenge to FRT*, supra note 3.
[43] A new legislation expands the government's surveillance powers, *The Caravan*, supra note 2.

historically the victims of surveillance (e.g. Muslims in some areas) complain of anxiety and fear. When individuals think that moving in a place under the control of the police might result in unfair arrest by a machine, then they will obviously avoid such places, which will nullify the freedom of movement.

Lastly, there is the issue of institutional opacities. India does not have a public book of FRT projects. The accuracy, retention times, cross-matching procedures or committees overseeing data are predominantly top secret government information. This non-transparency in itself is against the principles of good governance. Civil society reports are based on leaks and RTIs to assemble how these systems operate. With a rights-based approach, this secrecy is not permissible. It displays an avoidance of democratic responsibility: people have no power to agree or disagree to a technology they cannot even confirm.

With these challenges in mind, namely, technical fallibility, human biases, infrastructural risks and social harm, it is clear that FRT should not be uncontrolled. Its enforcement does not only raise legal issues that are isolated, but also a significant challenge to the democracy ethos of India.

7. Policy Recommendations

An effective policy framework is required in order to utilize the benefits of FRT without causing the harms of the latter. Considering the analysis conducted above, we propose the following measures:

- Pass Effective Laws: India must embrace a wide law that governs the applications of facial recognition by the police just like very explicit laws on wiretapping or DNA collection. This law must make it clear that FRT can be used to perform specific functions (e.g. investigating serious crimes) and not to perform other functions (e.g. general surveillance). At least, there should not be deployment without a legislative order. Any such restriction on privacy, or, as FRT term suggests, free assembly, must be justified by law and must be subject to proportionality test, as per the Telangana petition.

- Purpose and Use Limits: The law needs to reduce the scope of FRT. The possible solutions are: prohibiting live facial recognition in public areas (as in

the EU/UK); a court order to any post hoc FRT search of video footage; and no use of FRT data in any other task than the original criminal investigation (to avoid function creep, as Aadhaar II did). It may be permitted on the public-interest basis such as finding missing children, but with severe restrictions. This can be prevented by prohibiting the automated search of general databases of citizens (e.g. all voters or license holders).

- Data Protection and Security: Bio metric data derived through FRT must be regarded as very sensitive. The DPDP Act ought to be revised or added with an explicit government biometric database which ought to have a minimum of one-year retention and high-security storage requirements. The information gathered in a single case must be erased upon the closure of the case. The agencies are required to carry out privacy impact assessment and certification of security protocols. Cases of unlawful access or violations ought to be severely punished.

- Algorithmic Accountability: Insist on FRT algorithm independent auditing both prior to and during application. Any system implemented needs to be demonstrated to achieve a high threshold of accuracy (in terms of low false-positive rates) on the relevant populations. Periodic testing of the systems on varied datasets may be required by the government, and controlled by a neutral body (e.g. a data protection authority or forensic science committee). Audit outcomes are to be made public so as to build trust among the community.

- Human Oversight and Evidence Rules: Assistance, not decisions, need to be automatized. Police must not be left to depend on a computer-generated match as a factor to base arrest and prosecution. The law may dictate that any FRT hit should be confirmed by other evidence (such as witness testifying or physical evidence-related information). Policymakers might avoid cognitive bias by making it mandatory to verify by two officers (one checking matches and the other one checking matches). In the law of evidence, Parliament may revise the Evidence Act, 65A-B, and may establish new provisions which provide the treatment of AI-generated "identifications" and allow defendants the right to check and object to the algorithmic procedure.

- Judicial/Administrative Supervision: Have a system of control. Indicatively, the

use of live FRT might need a warrant or pre-authorization by a magistrate (similar to interception of telecom). Or establish a statutory Surveillance Ombudsman or charge National Data Protection Authority (under DPDP Act) with the responsibility of monitoring FRT in the law enforcement sector. This authority would check complaints, compliance audit, and make binding recommendations on facial surveillance.

- Transparency and Public Reporting: Police departments are to post regular reports on the use of FRT: how many scans and matches and false positives/negatives (as found) and the demographic composition of the scanned population. Openness assists in identifying behavioral tendencies of abuse or discrimination. FRT policies should also be designed by consulting the masses by the government. As part of democratic values, consultations with the civil society in terms of impact and open dialogue should exist.

- Way to Redress Affected Individuals: The victims of wrongful FRT identification need channels to claim redress. As an illustration, the law might permit compensation or expungement of records in the future in case it would be established that an arrest or data recording was unwarranted. Interested guarantees like the right to be forgotten (suggested as part of DPDP) could be used to delete personal pictures on databases.

- Training and Guidelines: The police have to undergo training on the constraints of FRT. Whether cameras and algorithms can be applied should be made clear in official statements (caution is required, e.g. "FRT results are presumptive and need to be supported). It is important to note that the officers must know that the surveillance tools are not a panacea. Mitigation of prejudice in interpretation of results must also be introduced through ethical training (safeguarding minority groups).

- Restricting the role of the Private Sector: Since there are reports of commercial development of infrastructure by private firms (e.g. in the control center of Telangana), the law must restrict commercial access to sensitive biometric databases. The same rules of confidentiality and accountability to the government should be applied to the case of the private vendors who offer FRT

tech to police. Human rights organizations have called on the prohibition of exportation of Indian images to other foreign technology companies; the cross-boundary information exchange should be highly restricted.

These suggestions are based on the best practices. In particular, the Vidhi Centre notes that FRT should be consistent with the Indian own AI policy vision, which proposes responsible and safe AI[44]. Amnesty has a campaign across the globe that demands a moratorium on FRT until the safety measures have been enacted. We believe that total prohibitions (except on the most obtrusive applications) can be excessively severe; instead, we would promote a stringent system of regulations. It is not intended to criminalize useful technologies (e.g. finding lost children with the help of FRT), but rather human rights should be taken into account at each stage. Importantly, any framework has to be innovative and at the same time, follow the promise of the Constitution that the issues of the fundamental rights will be handled through the judicial review, as Puttaswamy does.

8. Conclusion

Artificial intelligence-based surveillance and facial recognition is at the intersection with the constitutional order of India. On the one hand, innovative technologies provide means of improving the safety of people and the investigation of crimes. Conversely, they present massive threats to liberty, equality and dignity. As we have demonstrated, the current legal measures in place in India (Articles 14, 19, 21) have a robust rights-based base, but this is threatened by the dangerous dissonance between theory and practice. Puttaswamy, the Supreme Court demanded "stringent protection" over privacy-invasive technology; nowadays FRT deployments have minimal form.

Left unchecked, FRT surveillance may end up destroying the very democratic values it is supposed to protect. This has been the case in history where the power to police freely has ended up being abused against the vulnerable. The number of documented wrongful arrests made using only a faulty face scan is a wakeup call: in essence, AI is merely a weapon and can reflect on human biases. The judiciary and the legislature of India should take the initiative. In fact, Puttaswamy cautions us that rights are not maintained by neglecting technology but by

[44] Jauhar Vipra, *Addressing Constitutional Challenges in Use of Facial Recognition Technology by Indian Law Enforcement Agencies*, supra note 7.

making reforms of law concerning the same.

So, it can be concluded that we should have a reinvention, rather than a facelift of rules to regulate FRT[45]. The government and the courts should make sure that as they safeguard the citizens, they do not take away the constitutional liberties. India can make AI not an instrument of uncontrolled state power by making transparent laws, obligating AI policing, and instilling accountability into it. This way, the nation would not just be defending its own internal principles, but would also be setting the example of how a pluralistic democracy navigates in the era of biometric surveillance.

[45] *Facial Recognition Technology and the Right to Privacy in India: A Constitutional and Regulatory Analysis*, supra note 1.

Bibliography

1. K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
2. Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1 (India).
3. Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
4. Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295 (India).
5. S.Q. Masood v. State of Telangana, W.P. No. 25064 of 2020 (Telangana H.C. filed 2020) (India).
6. S. and Marper v. United Kingdom, 48 Eur. Ct. H.R. 50 (2008).
7. R. (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA Civ 1058 (Eng.).
8. The Constitution of India.
9. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
10. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).
11. Criminal Procedure (Identification) Act, 2022, No. 11, Acts of Parliament, 2022 (India).
12. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
13. Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India).
14. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
15. Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).
16. Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1.
17. European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.

18. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard Univ. Press 2015).

19. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

20. Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* (7th ed., Wolters Kluwer 2021).

21. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1 (2018).

22. Manpreet Kaur & Munish Sabharwal, *Role of Artificial Intelligence in Crime Prediction and Pattern Analysis Studies Published Over the Last Decade: A Scientometric Analysis*, Artificial Intelligence Review (2024).

23. Fatima Dakalbabb et al., *Artificial Intelligence & Crime Prediction: A Systematic Literature Review*, 4 Soc. Sci. & Humanities Open 1 (2022).

24. Vidhi Centre for Legal Policy, *Facing the Future: Facial Recognition Technology and Law Enforcement in India* (Working Paper, 2021).

25. Vidhi Centre for Legal Policy, *Regulating the Use of Facial Recognition Technology in India* (Policy Report, 2021).

26. Internet Freedom Foundation, *Automated Facial Recognition in India: Issue Brief and Legal Analysis* (2020).

27. Amnesty International, *Ban the Scan: Facial Recognition and Human Rights Violations* (Report, 2021).

28. Centre for Internet & Society (CIS), *Facial Recognition Technology in India: A Primer* (Policy Brief, 2021).

29. NITI Aayog, *Responsible AI for All: Operationalizing Principles for Responsible AI* (Discussion Paper, 2022).

30. UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

31. European Data Protection Board, *Guidelines on Facial Recognition Technology Under GDPR* (2020).

32. South Wales Police, *Data Protection Impact Assessment for AFR Locate* (2019).

33. Pranav Dixit, *Delhi Police's Expanding Facial Recognition System*, BuzzFeed News (2020).

34. Vijaita Singh, *Delhi Police Says Facial Recognition 80% Accurate*, The Hindu (Jan. 2020).

35. "Telangana HC Issues Notice on PIL Against Facial Recognition," Times of India (Jan. 2022).

36. "Hyderabad Police Denies Mass Surveillance Allegations," The News Minute (Feb. 2023).

37. S. Ghosh, *Inside India's National Automated Facial Recognition System Plan*, The Indian Express (2019).

38. "Delhi Police Used FRT in 1100+ Cases, RTI Reveals," The Wire (2021).

39. Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1–14/99 (U.S.).

40. Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology (2016).

41. U.S. Office of Science & Technology Policy (OSTP), *Blueprint for an AI Bill of Rights* (2022).