WILL THE DIGITAL GAZE SET PRIVACY ABLAZE? A POST PUTTASWAMY ANALYSIS OF THE NATIONAL AUTOMATED FACIAL RECOGNITION SYSTEM (NAFRS) IN LIGHT OF ARTICLE 21

Dhriti Mahajan (LL.M.), University School of Law and Legal Studies, Guru Gobind Singh Indraprastha University

ABSTRACT

The paper critically examines India's National Automated Facial Recognition System (NAFRS) as a constitutional, ethical, and legal dilemma within the post-Puttaswamy privacy framework. It analyzes how the government's move toward biometric surveillance challenges Article 21's guarantees of dignity and autonomy by operating without explicit legislative sanction, judicial oversight, or procedural safeguards. Through doctrinal and comparative analysis, the study evaluates NAFRS against the threefold test of legality, necessity, and proportionality, revealing its failure to meet constitutional standards. Drawing parallels with the EU's GDPR, the UK's Surveillance Camera Code, the US's judicial safeguards, and China's authoritarian model, the paper underscores India's institutional gaps and the risk of mass surveillance becoming normalized. It argues that unchecked technological governance undermines democratic citizenship and informational self-determination. Finally, it proposes a rights-based biometric governance framework emphasizing judicial authorization, independent oversight, privacy-by-design, and legislative accountability. The study concludes that protecting the "right to be left alone" is central to maintaining constitutional morality and preventing India from drifting toward a surveillance state.

Keywords: Facial Recognition Technology; Right to Privacy; Constitutional Morality; Surveillance State; Puttaswamy Judgment; Article 21; Digital Governance; Data Protection; Proportionality Test; NAFRS.

1. Introduction: The Rise of the Digital Gaze

The twenty-first century has witnessed an unprecedented fusion of technology and governance, where surveillance has quietly evolved from a tool of protection to an instrument of power. India's proposed National Automated Facial Recognition System (NAFRS) stands at the heart of this transformation—an ambitious state initiative that seeks to automate identification, monitoring, and profiling through biometric data. Marketed as a leap toward efficient policing and national security, NAFRS simultaneously unveils the unsettling face of algorithmic oversight, where every movement can be tracked and every expression recorded. In a democracy founded on liberty and dignity, such systems demand more than administrative justification—they demand constitutional scrutiny.

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) redefined the contours of personal freedom under Article 21. It established that any state intrusion into privacy must satisfy the tests of legality, necessity, and proportionality. Yet, the emergence of large-scale biometric surveillance tests the resilience of that very framework. Can a state that surveils its citizens also claim to protect their liberty?

This paper explores that dilemma. It investigates whether the digital gaze embodied by NAFRS aligns with India's constitutional morality or risks igniting the very privacy it vows to safeguard—raising a fundamental question about the future of rights in a datafied democracy.

2. The Constitutional Landscape of Privacy in India

The history of the development of privacy as a constitutional right in India is one of progressive but fundamental changes in judicial interpretation, in which the traditional, even procedural, interpretation of the meaning of personal liberty has been changed to a rights-based, substantive interpretation of human dignity. The initial constitutional law of the fifties and sixies did not consider privacy as a right of enforceable nature. In M.P. Sharma v Satish Chandra, the Supreme Court, though it supported the search and seizure authority under the Code of Criminal Procedure, stated that there was no Right to Privacy outlined in the Indian Constitution similar to that under the Fourth Amendment of the American Constitution.[1] And equally in Kharak Singh v State of Uttar Pradesh, the majority dismissed an attack on police surveillance justifying it by the fact that

[1] *M.P. Sharma v Satish Chandra* AIR 1954 SC 300.

privacy was not itself a right guaranteed by the constitution.[2] Nevertheless, the first grain of privacy awareness began with Justice Subba Rao dissent in Kharak Singh when he stated that the right to be left alone is implicit in the clause of personal liberty in Article 21.[3] Though not the majority at the time with his reasoning, he provided the intellectual basis on the future acknowledgement of the right to privacy as a fundamental right.

Factors such as the redefinition of Article 21 in the following decades were decisive in spreading out the concept of liberty. Since Maneka Gandhi v Union of India the Court has stated that the process that takes away an individual their lives and liberties must be just, fair and reasonable [4] to permit Article 21 to embody the new dimensions of individual liberty and dignity. The Court later identified the different aspects of privacy e.g. right against telephone tapping,[5] privacy of medical records[6], and autonomy of reproductive choices[7] even prior to the identification of the right to privacy as a distinct right. All these piecemeal judicial appreciations led to the historic ruling of nine-judges bench Justice K.S. Puttaswamy (Retd.) v Union of India, where the right to privacy was declared as the fundamental right inherent in life and liberty provided in Article 21.[8]

The Supreme Court had given a territorial definition of privacy in Puttaswamy which was beyond spatial or physical limits and included decisions and control over information as well as bodily integrity. The decision placed privacy in a bigger constitutional context of the dignity, liberty and autonomy and saw it as necessary towards achievement of the full potential of the individual. The plurality opinion by Justice Chandrachud stressed that privacy is not just a right in the common law but in the constitution, which was granted by the very fabric of the Constitution itself. It was also determined in the judgment that privacy is relational because it not only safeguards individuals against interference by the state but also against privacy-invading data practices by the individual actors, thus extending the right into the online space.

Among the greatest contributions that Puttaswamy verdict has made is the enumeration of the threefold test of legality, necessity, and proportionality, to which any action of the state that violates

[2] *Kharak Singh v State of Uttar Pradesh* AIR 1963 SC 1295
[3] ibid (Subba Rao J, dissenting).
[4] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
[5] *People's Union for Civil Liberties (PUCL) v Union of India* (1997) 1 SCC 301.
[6] *Mr. X v Hospital Z* (1998) 8 SCC 296.
[7] *Suchita Srivastava v Chandigarh Administration* (2009) 9 SCC 1.
[8] ibid [298] (Chandrachud J).

privacy must pass. The legality test calls on such limitation of privacy having got a legal foundation that is clearly stated in law, necessity that limits action should have some objective of a worthy state purpose and proportionality that the mode taken is minimal and also proportional to the intended goal. This test is to confirm the fact that privacy is not an absolute right but rather a qualified right that can be restricted provided that these restrictions can stand constitutional test. The Court confirmed the applicability of the doctrine to the cyber space in more recent cases such as Anuradha Bhasin v Union of India where they once more stated that the test should be used to evaluate the legality of state imposed internet blockages.

The Puttaswamy framework presents some important questions in the area of technological surveillance on the legitimacy and extent of the state in amassing and processing personal data. Facial recognition, biometric identification, and predictive policing are some technologies that increase the ability of the state to surveil and classify citizens like it has never done before. But in case of systems such as the National Automated Facial Recognition System (NAFRS) the enabling statute is missing which flouts the legality test, the second prong is the second prong the empirical evidence to demonstrate the necessity of the current system is lacking, and the final prong is directly at odds of the proportionality prong where mass surveillance is possible without consent. The dependence of the Indian state on the executive notifications and tender documents instead of legislations in parliament does not therefore substance the constitutional expectation within the Puttaswamy constructs.

In Indian privacy jurisprudence that has emerged since Puttaswamy, there is a resonance of the notion of informational self-determination that was initially coined by the German Federal Constitutional Court in the Census Act Case (1983) in India : It acknowledges the freedom of a person with regard to his or her personal information on how this information is gathered, stored, handled, and distributed. The concurrence by Justice Kaul directly associated privacy with the control of personal information, emphasizing that monitoring data might lead to profiling and discrimination of any kind and thus offering people the power of making wise decisions with the digital ecosystem.

Consent, being a derivative of informational autonomy, becomes the ethical point of the pitch of data governance. Nevertheless, the concept of meaningful consent is made an illusion in the setting of mass surveillance, such as NAFRS. People in whose face information is photographed in the

open areas do not agree or even know what happens to the data and are being denied the right of fairness and responsibility that is an essential part of morality by the constitution and the international data protection codes. In addition, the lack of a well-protected data protection law (although it was assured on numerous occasions since the Justice B.N. Srikrishna Committee Report (2018)) also increases the susceptibility of citizens to uncontrolled data processing.

The Indian constitutional debate on privacy privacy therefore represents a fine balance that interests the goals of state security and the value of a personal freedom. Alcoholiquity to the normative centrality of privacy that Puttaswamy confirmed is the definition of democratic polity, its application in an algorithmic governance era is full of uncertainty. The lack of law and institutional protection against the excessive power of technological advancement threatens the creation of an all-seeing informational condensation of the state. When India is on the verge of implementing systems, such as NAFRS, the difficult thing is not necessarily technology design but maintaining the constitutional guarantee of dignity and liberty in the era of data.

3. Anatomy of the NAFRS: Architecture, Objectives, and Concerns

National Automated Facial Recognition System (NAFRS) is one of the most ambitious surveillance systems taken by the Indian government. Being an outgrowth of the National Crime Records Bureau (NCRB), an organization under the Ministry of Home Affairs (MHA), the project aims at establishing a centralized digitalized infrastructure, which will help track, verify and identify, people using their facial biometric data within the country. The tender document published by the NCRB in 2019 states that the idea is to create a single facial recognition database accessible to both central and state law enforcement agencies.[9] The envisioned system aims at improving the processes of criminal identification by incorporating the current data of the Crime and Criminal Tracking Network and Systems (CCTNS), Interoperable Criminal Justice System (ICJS), passport databases, and state police repositories. Basically, NAFRS would operate as a universal, interoperable, network through linking various biometric and demographic repositories in India and forming a massive digital surveillance grid.

[9] National Crime Records Bureau, *Request for Proposal for National Automated Facial Recognition System* (Ministry of Home Affairs 2019).

Technically, NAFRS works through using algorithms that chart facial characteristics, i.e. distance between the eye, jawline shape, skin texture etc. and create a distinctive facial template or biometric signature.[10] This specific type of templates are then stored in a central database that is maintained by the NCRB and that they may match in real time with images taken out of CCTV feeds, photographs, or any other input of digital information. The software of the system is based on Artificial Intelligence (AI) and Machine Learning (ML) to carry out the so-called 1:N matching, where a single photo of a captured face is compared to millions of stored templates of faces to obtain possible matches.[11] The system is also designed to facilitate the "1:1" authentication where one can verify the identity of an individual against a personality which is known by the system which can be used in such places as airport's security management or operation of public transportation.

The NAFRS design therefore imagines three major parts that include a data ingestion component to gather images of different sources, a processing component that is driven by AI-based analytics to match and predict faces, and a user interface component that is accessed by authorized individuals in the law enforcement departments. This system would allow the other agencies, including state police departments, to harmful visual data in real time and analyze it simultaneously in various agencies that are central to the intelligence field.[12] Although NCRB is the overall coordinator, the actual action falls on state peace organizations, forensic laboratories, and Ministry of Home Analytics data departments. The project consequently aims at converting the disjointed databases of crimes to an integrated database that will offer speed, efficiency as well as accuracy in criminal investigations in India.

The official justification by the government in the development of the NAFRS has the detection of crimes, national security, and identification of missing persons as its main objectives. Under NCRB, it is indicated that facial recognition technology (FRT) will help facilitate quick identification amongst criminals, suspects and victims in disparate databases across jurisdictions.[13]

---

[10] ibid 3.
[11] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017) 112.
[12] Clare Garvie, Alvaro Bedoya and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Georgetown Law Center on Privacy and Technology 2016) 10
[13] Ministry of Home Affairs, 'Crime and Criminal Tracking Network and Systems (CCTNS): Overview' (Government of India 2023) https://www.mha.gov.in accessed 4 November 2025.

It will also be estimated to help in tracking of repeat offenders, identification of unidentified bodies or cases and confirmation of people in case of a large crowd. The reason why the government feels that traditional investigative tools are not sufficient to address the modern day demands of policing is that the country has a population of well over 1.4 billion people. NAFRS, consequently, is introduced as an indicator of predictive and preventive policing, which can be enhanced with human intelligence through algorithm accuracy and solutions.[14] In addition, the proponents of the system argue that it would enhance the efficiency of the Indian Administration, lower the effect of human error and reinforce the counterterrorism architecture of India by assisting in faster identification of high-risk persons.[15]

This has not been without opposition as civil liberties groups, digital rights advocates and even constitutional scholars have been against NAFRS due to these perceived advantages. The first issue which should be highlighted is the fact that such an intrusive system on surveillance is not supported by statute or even parliamentary approval. Contrary to the Aadhaar system, which is based on the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 giving it legitimacy, NAFRS is just an executive decision-making enterprise with no legislative framework delineating its scope, protection, or systems of accountability.[16] Such a violation of the law goes against the requirement of legality of the proportionality test which is established in Justice K.S. Puttaswamy (Retd) v Union of India whereby the Court pointed out that any form of invasion of privacy should have a basis enshrined in law.[17]

Moreover, NAFRS threatens the risks of mass surveillance- the blind gathering and analysis of personal information of massive numbers without the definite suspicions and authorization. The system can undercut Article 19(1)(d) and 19(1) (c) of the Constitution (guaranteeing freedom of movement and association) due to its ability to provide real-time watch on people in areas with bad reception. The prospective occurrence of the so-called function creep, i.e. the gradual increase of possible uses of surveillance beyond their purpose—is especially worrisome. This has been demonstrated in other jurisdictions where systems implemented to carry out narrow law

[14] NCRB (n 1) 5.
[15] ibid 7.
[16] Press Information Bureau, 'Union Home Minister Reviews NAFRS Progress' (MHA 2022) https://pib.gov.in accessed 4 November 2025
[17] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, s 4.

enforcement roles have been modified to serve in political surveillance, quelling demonstrations, or profiling of disadvantaged groups of people, among others.

The other significant issue is the correctness and the biasness of facial recognition algorithms. Research in this field has shown across the world that such technologies tend to be biased in relation to their racial, gender, and age based since training data is not representative and algorithms are limited in certain ways. As an example, dark skin color and women faces are more prone to false positives and misidentification and subsequent wrongful arrest. Such prejudice is especially harmful in the Indian socio-cultural environment, where caste, religion, and geographical differences have already affected the practices of law enforcement. Such a biased design coupled with the lack of control mechanisms can lead to the strengthening of systematic discrimination rather than equality and non-arbitrariness that are embedded in Article 14 and 15 of the Constitution.

Prior to the members nation adoption of NAFRS, some states in India experimented with FRT locally, which provided an insight into the possible outcomes of the large scale adoption. In the example of the Delhi Police, face recognition systems started to be used by the police in 2018 to identify those attending the public events and demonstrations. In 2019, on anti-CAA protests, more than 1,100 children had been identified by the system, prompting criticism of its abuse around consent and usage.[18] Facial recognition by the Telangana Police was implemented in Integrated People Information Hub (IPIH) that combined a CCTV footage and a citizen database to be used in predictive policing .[19] Civil society institutions have also sounded the alarm due to the lack of court checks and balances and the application of FRT to profile the vulnerable groups, such as minorities and protesters.

Equally, Hyderabad Safe City Project is one of the biggest urban surveillance projects in India, which uses thousands of interlinked cameras with face recognition technology. Despite the state government asserting that the system helps in the prevention of crimes, independent hoardings and RTI reactionary assertions have demonstrated that the system operation guidelines, data storage

[18] Internet Freedom Foundation, 'Delhi Police's Use of Facial Recognition Technology: Project Panoptic' (2020) https://internetfreedom.in accessed 4 November 2025.
[19] Internet Freedom Foundation, 'Surveillance State of Telangana' (2021) https://internetfreedom.in accessed 4 November 2025.

policies, and error correction systems are still veiled.[20] All these case studies show that when there is no transparency in accountability and independent verification, then facial recognition applications always become an instrument of total control, instead of a sharp implementer of the law.

Implementation of NAFRS therefore creates structural concerns on the connection between technology, power, and constitutionalism. There is a perspective that the efficiency and security have been highlighted in the story about technological advances by the government, whereas there is a need to guarantee transparency, legality, and proportionality in the practices of state surveillance, which is a constitutional requirement. In the absence of legal protections or comprehensive audits, as well as efficient remedies to grievances, NAFRS will be prone to normalize the habit of state surveillance at all times, the very notion of which is contrary to the democratic ideal of individual autonomy and dignity. The state must be a watchdog on the qui vive: as the Supreme Court has warned in Puttaswamy, it must make sure that the pursuit of safety does not put out the fire of liberty.[21]

4. Post-Puttaswamy Scrutiny: Testing NAFRS on Constitutional Grounds

The constitutional validity of the National Automated Facial Recognition System (NAFRS) can never be put to test, except within the monastic laid in Justice K.S. Puttaswamy (Retd.) v Union of India (2017) in the case, where the right to privacy was held inherent to Article 21 of the Constitution. Based on the decision, any state action violating privacy had to meet the three prongs of the three-fold test of legality, necessity, and proportionality.[22] Using this test on NAFRS would allow gaining a better insight into the fact that the system is working within the legal framework of constitutional abilities or it is the burdening of executive powers on an individual to a point where their constitutional and democratic freedoms will be infringed upon.

The first branch of the Puttaswamy test that is legality, they must have lawful support of their invasion of privacy and cannot just be based on the discretion of the executive. In NAFRS, there is no law in Parliament permitting or controlling the constitution of the Board. The system began with a Request for Proposal (RFP) published by the National Crime Records Bureau (NCRB) in

[20] The News Minute, 'Inside Hyderabad's Safe City Project: Surveillance or Safety?' (10 March 2022) https://www.thenewsminute.com accessed 4 November 2025.
[21] *Justice K.S. Puttaswamy (Retd.) v Union of India* (n 10) [180] (Chandrachud J).
[22] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1 [325].

2019, an administrative not a legislative provision.[23] In contrast, unlike the Aadhaar project, later provided with statutory support by the Aadhaar Act 2016, NAFRS is an executive scheme that lacks any parliamentary discussion or procedure governing policy. This lack of legal military protection makes the project constitutionally weak.

This was clearly stipulated in Puttaswamy where the Supreme Court stated that legality is all about the presence of law not its alignment with the constitutional provisions.[24] Any violation of privacy not anchored on legislative basis is an unreasonable exercise of state power, which is a breach of Article 14 requirement of non-arbitrariness. Equally, in the case of District Registrar and Collector v Canara Bank, the Court ruled that any invasion of private must be provided by a procedure happened by law. NAFRS has no such procedure since it performs its operations through executive instructions without any legislative regulation.

Moreover, a publicly accessible structure that defines the time of retention, the purpose restriction, or the procedures of an immense data warehouse that NAFRS wants to establish is missing. The fact that thisopacity violates the principle of legality is not only offensive to the principle of procedural fairness implicit in the Article 21. The recently taken Digital Personal Data Protection Act 2023 is silent in regards to law enforcement surveillance, therefore, not close this legislative gap. Without a data protection authority, the auditing, investigative, or sanctioning of abuse powers is justified, NAFRS will be a runaway growth of state power.

Necessity is the second arm of the test of proportionality that hypothesizes that any surveillance of privacy action should be intended to fulfill a valid state objective and it must be reasonable to accomplish the objective of the action.[25] The reasons why NAFRS has been defended by the state include: national security, efficacy in law enforcement and one more is crime prevention. Although the following goals are valid, the main question- why are those justification to undertake blanket biometric surveillance of millions of citizens?

In Anuradha Bhasin v Union of India, it was restated by the Supreme Court that the necessity must also mean that the state must show that its actions are necessary and that no alternative action that

[23] National Crime Records Bureau, *Request for Proposal for National Automated Facial Recognition System* (Ministry of Home Affairs 2019).
[24] *Justice K.S. Puttaswamy (Retd.) v Union of India* (n 1) [317].
[25] *Justice K.S. Puttaswamy (Retd.) v Union of India* (n 1) [328].

does not involve such encroachment can serve the same end. On the lower echelon of NAFRS, there are already well-known less invasive forms to monitor criminal events, i.e. traditional CCTV, vehicle surveillance or case specific databases, which are available in the Indian policing system already. CCTNS and other data-driven networks and systems such as Crime and criminal tracking Network and Systems (CCTNS) offers a lot of investigatory potential without the need to constantly process facial data of general population.[26]

Additionally, no empirical data can be created to prove that facial recognition contributes to some measurable decrease in crime rates. As the international studies indicate, the predictive performance of FRT is poor and has high likelihood of large error margins, especially when it is used in an open setting such as in a rally or market of people. The fact that there is no established need makes the premise of the state in taking such an extensive surveillance model hollow. Even the preservation as a means of crime prevention of biometric information, as seen by European Court of human Rights in S and Marper v United Kingdom, must be strictly necessary in a democratic society. By this criterion, NAFRS falls short of the necessity standard since the purpose of the system goals could be accomplished by means of less intrusive means of privacy invasion.

The third criterion is proportionality which is the balance between the degree of the infringement of rights with the value of the goal that is being sought. The Court in Puttaswamy also made it clear that a measure should not be restricted to proportionality so that the means utilized should be minimally restrictive and that the outcome of the benefits to individual rights exceed the resultant limitations imposed on the right to Puttaswamy rights. [27]

The intrusion in the case of NAFRS is so great against its possible benefits. The system also allows simultaneous monitoring of people in both public and private areas and connecting databases, and therefore, making the potential absence of anonymity in daily life impossible. This control of space is what turns the form of the mass media into that of the panopticon and produces a chilling effect on speech, demonstration, and association guaranteed in Article 19. This is only exacerbated by the fact that marginalized groups have been disproportionately affected and are more commonly subjects of over-policing as well as unrepresented in the design of the algorithms which

[26] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637 [68].
[27] Ministry of Home Affairs, 'Crime and Criminal Tracking Network and Systems (CCTNS): Overview' (Government of India 2023) https://www.mha.gov.in accessed 4 November 2025.

exacerbates the constitutional harm, making them even more vulnerable in the implementation of AI sponsorships.

The practice of the Supreme Court in Modern Dental College and Research Centre v State of Madhya Pradesh is an informative analysis parallel since the Supreme Court reiterated the idea that proportionality involves the minimally restrictive means in order to accomplish a legitimate goal This principle can be used to understand that the lack of discrimination in the arbitrary gathering of biometric data at NAFRS is not acceptable in the event that discriminative, warrant-authorized systems could deliver the same outcomes at a much higher level of respect to the liberty of individuals.

In addition, the concept of proportionality is not only of balance but it also involves procedural safeguards. In the case of Internet Freedom Foundation v State of Tamil Nadu, the Madras High court mandated the state government to draft regulations governing installation of CCTV cameras, but to add this, it was mentioned that surveillance efforts carried out by the state should be matched by control, responsiveness and admirable use policies. This is more applicable to facial recognition which is much more invasive compared to the usual video surveillance. This lack of judicial approval, external auditing and grievance remedy makes NAFRS disproportionately unconstitutional.

Along with the technical checks of proportionality, the legitimacy of NAFRS also needs to be checked based on the constitutional morality where the state has the responsibility of enforcing the values of liberty, equality, and dignity even in the exercise of power.[28] Constitutional morality is an checkpoint on majoritarian impulses and executive arbitrariness and serves the purpose envisioned by Dr. B.R. Ambedkar. When surveillance mechanisms such as NAFRS are in place without checks, it will violate these values by making citizens used to being perceived as constant objects of suspicion.

Exceptional due process, then, should be the foundation of balancing between technological proficiency and constitutional morality. One of the mechanisms that would suit such technologies to democratic accountability may be judicial oversight, data minimization, transparency audit, and time-bound data retention. Aadhaar was sustained by the Supreme Court of Puttaswamy (Aadhaar-

[28] *Justice K.S. Puttaswamy (Aadhaar-5J)* v Union of India (2019) 1 SCC 1 [447].

5J) on condition that it required important procedural restrictions and restrictions in the purpose of Aadhaar. Any biometric surveillance project should undergo the same method in order to discourage abuse and ensure that privacy jurisprudence is adhered to.

The debate over the NAFRS cannot be reduced to state surveillance only; it also needs to consider the emergence of the surveillance capitalism, a concept developed by Shoshana Zuboff in an attempt to mark the commodification of personal data as predictive and commercially valuable items. The potential of data leakage between the state agencies and the contracting firms is actual in India since the country is witnessing the development of its digital infrastructure through the application of public-private partnerships. The RFP document of the NCRB itself allows third party vendors to design and maintain fundamental parts of the system, which generates commercial uses of sensitive biometric data opportunities.[29]

This crossroad between surveillance on the part of the government and corporate data analytics blurs the boundary between social protection and commercial monitoring. It also poses the risk of establishing a network of surveillance where individual information turns to be a commodity and the identity of the individual is compromised. Sagolnikov To put data before data is, as Justice Kaul warned in Puttaswamy, one of the core aspects of personal autonomy, and the undermining of it can lead to the citizen becoming nothing more than a data point.

To sum up, NAFRS does not comply with the constitutional standard under the Puttaswamy proportionality model in all three aspects, namely, legality, necessity, and proportionality. The lack of legislative framework, the presence of alternative types which prove to be less severe, and the disproportionality of its influence on the essential freedoms all make it incompatible with Article 21. Australian culture The ABS NAFRS is prone to institutionalizing a mass surveillance culture which is undermining the constitutional promise of liberty, dignity and autonomy unless there is legislative certainty, procedural protection, and independent control.

5. Comparative and International Perspectives

To interpret the constitutional and ethical consequences of the National Automated Facial Recognition System (NAFRS) in India, it is necessary to place it in the overall context of the discourse on surveillance and privacy in the world. In different jurisdiction, states have struggled

[29] NCRB (n 2) 7.

to balance national security and law enforcement goals with the right to civil liberties and data privacy. The cases of European Union, United Kingdom, United States and China give useful comparative inferences on the models of regulation that may apply to the issue of facial recognition technology (FRT). Such comparison structures can elucidate the merits and flaws of different legal systems to provide insights, which India can use to avoid making mistakes on its privacy post Puttaswamy journey.

Building a rights-focused and highly developed data protection framework throughout the world, European Union (EU) continues to have General Data Protection Regulation (GDPR), which became effective in 2018[30]Article 9(1).of GDPR categorically identifies biometric data that are applied to detect and identify individuals as a special category of data that are entitled to greater protection. Such data may not be processed unless required on grounds of particular exceptions-explicit consent, essential public interest or other significant grounds of security before substantiated with solid legal protection.

The main principle that guides the EU model is based on Article 8 of the Charter of Fundamental rights of the European Union; which states that the processing of data have to be necessary, proportionate and limited to the reason that the data is being collected. The national and regional DPAs implement these standards by conducting auditing, imposing fines and impact evaluation on the public. An example is that in France, Commission Nationale de l'Informatique et des Libertés (CNIL) and in the Netherlands, the Autoriteit Persoonsgegevens have prohibited or limited facial recognition use in public view because of issues over a nation-wide scale surveillance. In 2021, the CNIL found the use of FRT in high schools unlawful because it infringed the principle of proportionality and consenting principle. Equally, the European Parliament has proposed the prohibition of real-time facial recognition in the street places citing how it is incompatible with the basic rights to privacy and data protection.

The EU strategy is so described through privacy-by-design, openness, and outside control. Any comparable system, throughout Europe, would have to be accompanied by rigorous data protection impact assessments (DPIAs), express mandates in legislation, and constant oversight by an

[30] European Parliament and Council, *General Data Protection Regulation* (EU) 2016/679

independent authority. This is in contrast to India where the biometric surveillance has no control and has no institutional checks.

Facial recognition technology is regulated in the United Kingdom by the Surveillance Camera Code of Practice (2013), which is published in accordance with the Protection of Freedoms Act 2012. The Code requires that the surveillance systems should be used based on legality, necessity and proportionality that resonates with Article 8 of European Convention of Human Rights (ECHR), right to the respect of the privacy and family life.

The Information Commissioner Office (ICO), the data regulator of the United Kingdom of America, has highlighted the importance of human control and publicity in FRT application. In Bridges v Chief Constable of South Wales Police, the court of appeal decided that the police application of live facial recognition infringed upon Data Protection Act 2018 and Article 8 of the ECHR because it did not establish sufficient safeguards and did not formulate adequate equality impact assessments in the case.[31] The Court did not find any valid justification to implement facial recognition systems that cannot be supported with specific legal frameworks, effect analyses, and non-discriminatory protections despite the legitimacy of law enforcement purposes.

Additionally, the Biometric and Surveillance Camera Commissioner of the UK checks the adherence to compliance, and it is important to ensure that the FRT implementations do not violate the part of human rights and do not erode the development of democratic accountability. Such a hierarchical surveillance system reflects a strong recognition of the fact that technological effectiveness does not have the ability to override essential freedoms, and that is no less applicable to India, whose surveillance supervision systems are still lacking.

Conversely, the United States adheres to the sector-based and decentralized regulatory approach to privacy. The Fourth Amendment to the Constitution has been construed to protect against excessive government surveillance in the form of constitutional protection against unreasonable searches and seizures. In carpenter v United States, the U.S. Supreme Court was of the view that warrantless acquisition of digital data, including cell-site location information, breaches the reasonable expectations of privacy, indicating that the use of technologically enhanced surveillance required judicial approval.

[31] San Francisco Administrative Code, Surveillance Technology Ordinance 2019, s 19B.

Since there is no federal law on privacy, local bans or moratoriums on the use of facial recognition by police officers have been instituted by different municipalities. In 2019, San Francisco became the first city to ban government facial recognition, as facial recognition has been said to be misidentified and racially discriminated against against Black people and immigrants. Other cities like Boston, Portland and Seattle have since followed suit by imposing similar bans.[32] These actions indicate the increasing discontent in people with algorithmic regulation and discrimination supported by surveillance. To restrict the use of FRT on the federal level, legislative initiatives include the Facial Recognition and Biometric Technology Moratorium Act (2021) to suspend the use of FRT by the government before adequate safeguards and accuracy metrics are developed.[33]

The case of America shown that even without the elaborate federal law, judicial control and local self-regulation can serve as effective checks. India, however, has centralized the control of surveillance technology without any decentralized accountability, which poses a great threat of abuse.

On the other extreme higher up the hierarchy is China, where facial recognition is a fundamental blocking element of the Social Credit System and social fabric of public security. FRT is also used by the Chinese government to monitor urban areas (real-time), border controls, smart city projects as well as developing one of the largest surveillance nets in the world.[34] The Golden Shield Project and the Sharp Eyes Initiative combine surveillance cameras with national identification databases, allowing predictive policing and rating the behaviour and compliance of citizens.[35]

Even though China has come up with Personal Information Protection Law (PIPL) in 2021, which is loosely based on the GDPR, its effects are subordinated to the state interests. The legislation also allows the processing of personal data on grounds of national security and public order, which is essentially justification of state surveillance[36]. The surveillance regime in China, in contrast with the European and British, is the one that runs on the authoritarian political system that puts state

[32] Electronic Frontier Foundation, 'Bans on Government Use of Face Recognition Technology' (2022) https://www.eff.org accessed 4 November 2025.
[33] Facial Recognition and Biometric Technology Moratorium Act 2021 (US Congress Bill S.2052).
[34] Samantha Hoffman, 'Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion' (Australian Strategic Policy Institute 2019).
[35] Maya Wang, 'China's Algorithms of Repression' (Human Rights Watch 2019).
[36] Personal Information Protection Law 2021 (China), art 13.

interests on the first plan rather than the right of the individual. The outcome is a society in which there is all-pervasive technological surveillance that instills conformity and suppresses dissent.

Democracies such as India are getting a warning of this model. Although both countries focus on digital modernization, the constitutional framework of India, in all the guise of the rule of law and rights, requires more restraint. Such a re-creation of Chinese surveillance architecture (but without constitutional protections) would undermine those very concepts of liberty and dignity that Puttaswamy was attempting to strengthen.

The comparative analysis points out a number of important lessons to be learnt by India. First, there must be legislative transparency. All financial jurisdictions that have developed FRT deployment codified their legal foundation, whether under the GDPR, the Protection of Freedoms Act in the U.K., or through local ordinances in the U.S. India should do the same with purpose-specific Surveillance Regulation Act that defines the use areas of the technology at hand, the duration of data retention, the prohibition of misuse, and the consequences of its misuse.

Second, they would require independent oversight institutions, such as those of the EU (Data Protection Authorities) or the UK (Surveillance Commissioner) to keep it in permanent check. As it stands, the young Data Protection Board in India does not have the selection or enforcement capability to oversee law enforcement entities.

Third, it must be mandatory to mandate privacy-by-design. This includes designing and operating systems, like NAFRS, with privacy controls, such as anonymization, encryption, and reducing the amount of data stored, in place and operation.[37] Fourth, it requires transparency and accountability with the help of disclosed information, assessments of impacts, and authorized surveillance of law in the real-time in order to have the constitutional legitimacy.

Last but not least, India needs to adopt the normative nature of constitutional morality, which means that the technological governance should as well be aimed towards serving the individual and not the state. The relative examples of Europe, the UK, and U.S. all confirm that only when based on legal, ethical, and institutional regulation, are surveillance technologies compatible with democracy. In the absence of these, a slip towards unregulated surveillance state can be seen in

[37] European Data Protection Board, 'Guidelines on Data Protection by Design and by Default' (2020) https://edpb.europa.eu accessed 4 November 2025.

India but this will coincide with the invasion of authoritarian leanings of the Chinese system as opposed to human rights-defending democracies that it is attempting to imitate.

6. Conclusion and Policy Recommendations

The review of the National Automated Facial Recognition System (NAFRS) in the prism of post-Puttaswamy Indian notion of the constitutional framework displays profound and unresolved contradictions between the demands of the state security and the sacredness of personal privacy. Though no one can refute the interest of the state to ensure there is the upholding of public order, thwarting of crime, and upgrading of security, they should work within the parameters of constitutional morality and legality. The Puttaswamy case solidly defined privacy as part and parcel of Article 21 and the same was compared to human dignity, autonomy, and liberty. It is on this jurisprudential ground that NAFRS was designed, formulated, and implemented without any statutory authority, an external control mechanism, or procedural protection, thus constitutionally unsustainable.

The architecture of the project is a transition between targeted investigation and mass surveillance and diminishes the distinction between citizens and suspects. Through its capacity to identify and track individuals in a distributed manner in the public, NAFRS risks to turn the very concept of democratic citizenship into the state of constant presence. It is this round-the-clock surveillance, which is not accompanied by a court directive or legislative restriction, that runs counter to the idea of proportionality expressed in Puttaswamy and reproduced in Anuradha Bhasin v Union of India. The proportionality doctrine implies that infringement of privacy should be substantiated by the existence of a legitimate goal, which is to be achieved in the least restrictive way, and which the weight of the right violated. NAFRS, on the contrary, is not characterized by any evident need and by such relative protection. Its acting on the principle of an administrative proposal, but not parliamentary law, is another thing that worsens the violating the requirement of legality, in case of the Article 21.

On the more philosophical level, NAFRS serves as a symbol of the increased tension between the authority of the state and individual freedom in an algorithmic area of the new era. Technology is political in its use though it is neutral in nature. It tends to recreate discrimination, marginalization, and domination when implemented as a part of non-transparent bureaucracy. When surveillance becomes random and constant, the state does not hold any ground since the citizens give away part

of their privacy in order to obtain communal security. This lack of meaningful consent, transparency, or accountability basically undermines the very principle that is called informational self-determination, which is known in both Puttaswamy and international privacy law. Any democratic state, which has its citizens living under the constant technological surveillance without the safety of the law or the control of a court, cannot refer to its legitimacy.

Policy Recommendations

India should implement a rights-oriented system of biometric data management to bring the surveillance habits to the standards of the constitutional provisions and democratic principles. The policy recommendations that can be made include the following:

1. Enactment of a Comprehensive Biometric Surveillance Law

The most important is the need to have a specific legislative framework to control facial recognition and other biometric surveillance systems. In such a law, data collection, reasons, limits of such data collection should be clearly understood; they should state in which cases it is to be retained and how it is to be deleted; a mechanism should be in place to hold the abusers accountable. This law should also include some specific rights to persons such as the right to notice, to access, to correction and deletion of personal information. It ought to be based on the international standards such as the EU GDPR and the UK Protection of Freedoms Act with the principles of lawfulness, necessity, proportionality, and data minimization embedded in the law. Notably, any implementation of the surveillance mechanisms must be preceded by parliament authorization, so that it will be democratically accepted.

2. Installation of Judicial Checking Control over Usage of Data.

Considering the invasive aspect of FRT, it is necessary that it should be supervised by the judiciary. Any police unit interested in implementing NAFRS or any such software is supposed to be authorized by a specific court of law, just like the existing model statistics of interception in the Telegraph Act. The process mandates that the requests of the surveillance proposed by the courts meet the proportionality and necessity requirements as established in Puttaswamy. Moreover, the ex post review mechanism must be institutionalized, which serves to have courts audit the surveillance decisions and remedies in case of an abusive data or misidentification. Courts will

provide the check on arbitrariness of the executive and reinstate the separation of powers that is inherent in constitutional government.

3. Independent Data Protection Authority and has power to be enforced.

Development of an autonomous and strengthened Data Protection Authority (DPA) is essential towards long-term supervision. Despite the creation of the Digital Personal Data Protection Act 2023, forming a Data Protection Board, it does not have sufficient autonomy and penalties, which is why it cannot oppose strong state agencies. The redesigned DPA must be empowered to inspect the government departments, give binding instructions, conduct penalties and enforce the privacy requirements. It should also have the ability to stop or suspend projects such as the NAFRS in case they are found to be contravening the principles contained in the constitution or in the statutes. Its main characteristics should be independence, sufficient funding and accountability of the parliament.

4. Compulsory Privacy Impact Assessment (PIAs) prior to Deployment.

In the implementation of any surveillance technology, the concerned agency must take a Privacy Impact Assessment (PIA) to determine the risks to the individual rights and freedoms of democracy. The PIA would consist of the detailed analysis of the purpose of the technology, its necessity, data flow, storage time, and measures against the possible infractions. It also has to be based on a public consultation and has to undergo an independent examination by an expert. It is a required practice under the GDPR, as well as in various other regions around Europe, and it is done to make sure that issues of privacy are not taken up as a reactive measure. Privacy-by-design should also be institutionalized in NAFRS through inclusion of PIAs during its design stage so that the efficiency of the technology does not supersede the constitutional rights.

5. Transparency of the people and Periodic Audits by other parties.

Democratic accountability is based on transparency. Any use of FRT should be accompanied by its public reporting on the purpose of its operation, the geographical location, the time frame in which it stores data and how the information is controlled. This should be periodically subject to independent audit (preferably by statutory auditors or civil society organizations) which evaluate

compliance, misuse and effectiveness. This means that the outcome of the audit must be published to instill confidence and facilitate sound intellectual civic engagement in the discussions of surveillance and privacy.

The dilemma between State Security and Privacy of the Person.

To align the two demands of confidence and freedom, it is important to go beyond the binary concept of security and liberty that one has to be sacrificed to facilitate the other. National security is not created by the act of widespread surveillance but rather by the faith that citizens have in the governments. Unaccountable surveillance has no relation to safety but fear. The Puttaswamy Court identified privacy as vital in the right to be left alone that consequently supports the human dignity and innovations. Any abuse of this right undermines the democratic process by freezing the expression of dissent, throttling of free speech, and self-censorship.

Here the concept of constitutional morality as expressed by Dr. B.R. Ambedkar comes into play. It stipulates that every state action, particularly those where intrusive technologies are used, should not be predone on the letter, but rather the spirit, of the Constitution. Under this principle, India should make sure that its models on digital governance do not override the core principles of liberty, equality, and fraternity. It should be applied as a tool of empowerment and justice and not a tool of suspicion and control with technological tools such as NAFRS.

Summary Conclusion: The Protection of the Right to be Left alone.

Samuel Warren and Louis Brandeis described privacy in 1890 as the right to be left alone and this term rings very strongly in the era of algorithmic governance. With India going into an age of artificial intelligence, big data, predictive analytics, the constitutional promise of individual autonomy is challenged as it perhaps never has been. The threat is not only of surveillance but of normalization of surveillance: when citizens start to see being observed around as the cost of convenience or security.

Protecting the right to be left alone in the twenty-first century requires the moral re-tuning of governance. Privacy as the design of freedom must be enshrined in laws, institutions, and even citizens. The NAFRS discussion is hence not purely on technology, but on the future of democracy

as well. Pre India has two straightforward options: either to be a surveillance state where the priority is control over liberty, or the country to carry on with the constitutional dream, and that is of a republic in which dignity, autonomy and liberty co-exist with technological advancement. To guarantee the latter, long-term monitoring, legislative prudence, and a continued following of the spirit of Puttaswamy, that the state exists to serve the individual, rather than to observe them, will be necessary.