



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Executive Power Without Law: The Constitutional Limits of Police Facial Recognition Deployment in the Absence of Legislation

*Ishika Ishanvi, Nitisha Hansdah**

National Law Institute University, Bhopal – 462044, India

National Law Institute University, Bhopal – 462044, India

ABSTRACT :

Indian police forces are increasingly deploying facial recognition technology at scale, from the National Crime Records Bureau's centralized Automated Facial Recognition System to state and city programs for watchlisting and live monitoring of political assemblies. None of it is authorized by statute. Rather, authorization is found in budgetary allocation, procurement documents, force orders and ministerial statements to Parliament, while the standards that would typically be prescribed by law match thresholds, retention periods, audit requirements and redress for wrongful identification are unilaterally prescribed by the deploying agency and often undisclosed. In this paper I argue that the resulting constitutional defect is not one of insufficient regulation but of absent legal authority. It argues that reading *Ram Jawaya Kapur* with *Kharak Singh* and *Bharat Singh*, Articles 73 and 162 permit the executive to continue the normal business of administration without legislation, but not to initiate a restriction of a constitutionally protected right; that "law" must be enacted or validly delegated. The deployment thus does not pass the *Puttaswamy* test at the threshold of legality, before the question of proportionality arises. Models from the European Union, the United Kingdom and United States offer a glimpse of what a compliant Indian statute should look like.

Keywords: executive power; facial recognition technology; proportionality; right to privacy; surveillance law

Introduction

In July 2026, two surveillance cars were parked outside a monthlong student protest at Jantar Mantar. One watched live CCTV feeds; the other ran protest footage through facial recognition software that compared faces to a police database. In response, the protesters covered their faces. Two constitutional challenges followed within days, one in the Delhi High Court and one under Article 32. The importance of the episode is not the technology, but the instrument behind it. The deployment was neither sanctioned by an Act of Parliament, nor deemed necessary. This paper is about that absence. The argument is that the problem with police facial recognition in India is a problem of legal authority, not a problem of regulatory design, and that the distinction is important because the two require different solutions.

The argument has three movements: The first is a descriptive one. It traces the ascent of facial recognition in Indian policing using exclusively executive tools, and enumerates three use-patterns with varying constitutional significance: post-hoc identification in a specific investigation, screening against a watchlist, and real-time monitoring of assemblies. The second is doctrinal. It poses the question whether the executive power under Articles 73 and 162 carries with it the power to create a restriction on a protected right without the aid of legislation and answers it in the negative. The Court then considers whether the proportionality standard in *Puttaswamy* is met and concludes that the inquiry collapses at the threshold of legality. The third is corrective. It examines the legislative models of the European Union, the United Kingdom and the United States and describes the design features an Indian statute would require.

The objection developed here is intentionally limited. It does not target facial recognition as a technology, but its use for watchlisting and mass surveillance without any law authorizing it.

Facial Recognition deployment by the police

The NCRB invited bids for a National Automated Facial Recognition System (hereinafter, AFRS) in July, 2019 through a request for proposal and government officials claimed that it is only being developed to help the law enforcement agencies to identify criminals, missing children and unidentified bodies in a scientific and speedy manner. The system integrates with existing databases like NAFIS and CCTNS and includes a mobile application for field-level access by investigating officers. The original 2019 tender for the ₹308 crore National Automated Facial Recognition System was revised and reissued in June 2020 and late 2021 to update technical specifications. Each version aimed to build a centralized, searchable database of photographs to help law enforcement by drawing from existing criminal networks. Although the early bidding deadlines were extended over a dozen

times for administrative reasons, the system has since been finalized at the NCRB Data Centre and operationalized nationwide through the Crime and Criminal Tracking Network & Systems.

What is significant for this thesis is not the technology but the instrument. AFRS has never been the subject of primary legislation, a parliamentary debate on a bill, or a statutory rulemaking process. Its authorisation traces instead to (a) budgetary allocation, (b) an executive Request for Proposal issued by a subordinate office of the Ministry of Home Affairs, and (c) ministerial statements to Parliament and implementation approval was confirmed only in writing, by the Union Minister of State for Home Affairs, informing the Rajya Sabha of the decision rather than seeking its sanction. The NCRB's own defence of the system has been procedural rather than legal. It has represented that AFRS "only automates the existing police procedure of comparing suspects' photos with those listed in law enforcement databases" treating facial recognition as a mere efficiency upgrade to pre-existing police power, not as a new exercise of power requiring its own legal basis.

Beneath the national programme sits a denser layer of state and city-specific systems, procured and operated independently by state police forces under their own executive orders, with no coordinating statute. Delhi Police has operated facial recognition capability since at least 2018, originally piloted for locating missing children, and has since expanded its use into general investigation and, controversially, crowd and protest monitoring. Investigative reporting has found that Delhi Police maintains multiple, poorly-documented facial recognition databases, one reportedly containing over 150,000 "history-sheeters," another of suspected terrorists, and a third said to have been built using images collected from protest footage itself. In response to a 2022 RTI application, Delhi Police confirmed that it treats an 80% similarity score as a positive match, a threshold set entirely by internal administrative choice, with no external, legislatively mandated accuracy or error-rate standard against which it can be tested.

This methodology is applied not only in these areas but also in other regions, which have their own artificial intelligence system to monitor CCTV and video surveillance of people in cars. Such measures are presented as part of the regular police and law-and-order activities, which do not require additional legal authorisation.

The clearest illustration of the constitutional stakes comes from events contemporaneous with this thesis. Following the NEET-UG 2026 paper-leak controversy, a 36-day sit-in protest was held at Jantar Mantar in Delhi beginning 20 June 2026. Delhi Police stationed two specialised vehicles at the site, a Mobile Command and Control Vehicle monitoring live CCTV feeds, and a smaller van, "Ikshana", in which officers ran protest footage through AI-assisted facial recognition software that flagged matches against a police database. A senior Delhi Police officer confirmed to the press that the force ran facial recognition on protest footage against its criminal database. Protesters, in response, began masking their faces to avoid identification and inclusion in police records, a visible, real-time chilling effect on the exercise of the Article 19(1)(b) right to peaceful assembly.

The deployment has since been challenged in two separate proceedings: a PIL before the Delhi High Court filed by former JNUSU president Aishe Ghosh, and a subsequent PIL filed before the Supreme Court (hereinafter, SC) under Article 32 by Rajya Sabha MP A.A. Rahim. The SC petition alleges that since the protest began, Delhi Police subjected thousands of protesters, students and journalists to "continuous and pervasive biometric surveillance," and seeks a declaration that the surveillance was unconstitutional along with an order restraining law enforcement from deploying facial recognition at peaceful public assemblies until Parliament enacts a law specifically authorising such practices. The petition also challenges the use of the NCRB's fingerprint-matching application deployed at the same site. This case is doctrinally significant for three reasons: it involves surveillance of core political speech and assembly rather than ordinary crime investigation, it is defended by the police purely by reference to internal database-matching practice rather than any statute, and it is framed by the petitioners in exactly the terms this thesis adopts i.e., as an absence of legislative authorisation, not merely a proportionality defect.

Three analytically distinct use-patterns emerge from this survey, and they carry different constitutional weight:

1. Post-hoc identification in investigation: matching a suspect's photograph or CCTV still against an existing criminal or missing-persons database after an offence has occurred. This is the use case NCRB and state police most often invoke to justify AFRS, and it maps most closely onto pre-existing, lawful police functions, making the "mere automation" defence most plausible here.
2. Watchlist-based identification: continuous or periodic screening of individuals against curated lists, independent of any specific offence under investigation. This shifts FRT from an investigative tool into a predictive/preventive one, with a correspondingly weaker claim to being an extension of ordinary police power.
3. Real-time surveillance of public assemblies: live facial recognition run against crowds at protests, rallies or other exercises of the Article 19(1)(a) and (b) freedoms, as at Jantar Mantar. This burdens rights beyond privacy alone, is deployed pre-emptively rather than in response to any established offence, and its underlying legal authorisation is the thinnest of the three.

Three features recur across every instance surveyed, and are each doctrinally load-bearing. Firstly, authorisation is uniformly executive in character that include procurement documents, force orders and ministerial statements to Parliament, never a statute or statutory rule. Secondly, the operative standards which would ordinarily be fixed by law, such as match thresholds, retention periods, audit mechanisms, redressal for wrongful matches, are instead fixed unilaterally and often undisclosed, as the 80% similarity threshold and opacity around Delhi Police's database composition illustrate. Thirdly, deployment has moved, without any intervening legal change, from narrow investigative use towards preventive watchlisting and real-time surveillance of political assembly, an expansion in kind as well as scale which has occurred entirely through executive discretion.

Doctrine of executive power without law

India's executive takes its authority from either Article 73 (Union) and 162 (States) of the Constitution, both of which specify that the executive power extends to "matters with respect to which the respective Legislature has power to make laws". The doctrinal issue is whether this language gives the executive power to act on any issue over which the legislature has lawmaking power, including the possibility of curtailing fundamental rights, even if the legislature did not actually pass a law on the matter.

In *Rai Sahib Ram Jawaya Kapur v State of Punjab*, a five-judge bench upheld the Punjab government's textbook-nationalisation scheme, conducted entirely through departmental notifications, in the absence of a governing statute. Chief Justice Mukherjea held that the Constitution does not adopt a rigid separation of powers, but only a separation of functions, and that Article 162 clearly indicates that the powers of the State executive are not confined to matters over which legislation has already been passed. This is therefore cited for the narrower and more defensible proposition that executive power may be exercised in a legislative field even absent legislation but not for any broader claim about what that power may be used to do once exercised.

This cannot, however, be read in isolation. Its recognition of executive power in the absence of legislation operates alongside the Court's separate and later insistence that executive action cannot itself supply the legal authority necessary to invade a protected right. The petitioners' textbook business in *Ram Jawaya* was regulated, not seized without compensation, and the Court was careful to note that no fundamental right was thereby infringed in a manner requiring separate statutory sanction. Therefore, this authorises the executive to carry on the ordinary business of governance i.e., administration, policy execution, resource allocation. Whether it also authorises the executive to originate freestanding restrictions on constitutionally protected liberty is a question *Ram Jawaya* does not itself answer and for that, later authority must be read alongside it.

That latter authority is located in *Kharak Singh v State of UP* and *State of Madhya Pradesh v Thakur Bharat Singh*. In *Kharak Singh*, the SC struck down provisions of the U.P. Police Regulations authorising nocturnal domiciliary visits to persons on a police "history-sheet," holding that a person's right to life and liberty under Article 21 may only be restricted by law and not by executive orders such as departmental police regulations. In *Bharat Singh*, the SC held that every act done by the Government or by its officers must, if it is to operate to the prejudice of any person, be supported by legislative authority.

That sentence does not mean that every executive decision with some adverse effect on some person requires its own Act of Parliament as ordinary administrative action routinely affects individuals without triggering such a requirement. Read in its constitutional context, the decision supports a narrower proposition which is that where executive action itself imposes a restriction on a constitutionally protected right, the executive cannot manufacture the legal authority for that restriction through its own administrative instrument. It was in that specific sense i.e., a restriction on the Article 19(1)(d) freedom of movement, that the *Bharat Singh* order failed. The case does not stand for a general rule against unlegislated executive action as such.

Puttaswamy does not disturb this structural point. It displaced *Kharak Singh*'s holding that there is no fundamental right to privacy, but its recognition of privacy as a fundamental right reinforces, rather than replaces, the separate and pre-existing requirement that any invasion of a protected right have a lawful basis.

Read together, they do not sit in tension so much as describe two zones of the same Article 73/162 power i.e., the executive may act on any subject within legislative competence for the ordinary conduct of governance, without waiting for legislation but where that action itself constitutes a restriction on a constitutionally protected right, the executive's own instrument cannot be the source of authority for that restriction. It is argued that the better synthesis is that beyond that point the requisite "law" must take the form of enacted legislation, or valid delegated legislation made under and confined by such legislation, a proposition this chapter defends as the most coherent account of the case law, rather than one any single judgment states in exactly these terms.

The government's most plausible response to this argument is not that FRT escapes rights scrutiny altogether, but that it is merely a faster means of exercising a power police already lawfully hold: officers have always been entitled to identify suspects, compare photographs, and investigate offences, and FRT simply automates that pre-existing function. On this account, no new legal authorisation is needed because no new power is being exercised.

The constitutional analysis cannot stop at that functional equivalence. Manual identification is targeted, effortful, and self-limiting where an officer can compare a suspect's photograph against a limited set of records, at a scale bounded by human time and attention. Automated facial recognition,

particularly the watchlist-based screening and real-time monitoring of assemblies, can continuously scan a crowd, match every face against a watchlist, and generate a persistent, searchable biometric record of everyone who passed through a camera's field of view, suspect or not. That is not the same power exercised faster, it is a materially different capability in scale, persistence, and reach, directed as readily at people under no suspicion as at people under investigation. A power to identify a particular suspect on reasonable grounds does not, without more, contain within it a power to continuously identify an indeterminate crowd.

Where FRT is confined to the first category i.e., post-hoc matching, the functional-equivalence argument has real force, and the constitutional objection correspondingly weakens. It is watchlisting and real-time assembly surveillance that expand the State's capability in kind, not merely in speed, and it is that expansion that falls on the rights-restricting side. The "mere automation" defence NCRB has offered for the programme as a whole elides this distinction, treating the least intrusive use case as representative of a system whose more troubling deployments it does not resemble.

4. Privacy, Surveillance and the Constitutional Floor

This chapter examines the further constitutional requirements applicable where State action of that kind intrudes upon privacy. Following *K.S. Puttaswamy v Union of India* and the proportionality jurisprudence that it produced, the inquiry proceeds through legality, legitimate State aim, proportionality (including necessity and the availability of less restrictive alternatives), and procedural safeguards against arbitrariness. These four elements are not stated identically across every judgment in this line, and this chapter does not treat "procedural safeguards" as a doctrinally settled fourth prong of proportionality itself so much as a requirement the Court has increasingly insisted on alongside proportionality.

Puttaswamy places the legality of any State intrusion upon privacy at the threshold of a restriction upon privacy having a basis in law. When read together with the Court's broader insistence, discussed previously, that restrictions on protected rights be traceable to a source beyond the executive's say-so, this requirement is not met by merely the existence of some internal instrument of a government authority regulating the practice in question.

Measured against this, the instruments looked into previously do not qualify. The distinction worth drawing precisely is between three things that are easy to confuse: a government department's authority to procure technology, its authority to deploy it operationally, and the constitutional authorisation required once deployment restricts a protected right. The NCRB's Request for Proposal establishes only the first of these i.e., it is a procurement document, specifying technical requirements to prospective vendors, and creates no publicly enforceable standard governing when officers may run a search, what constitutes a match, how long data is retained, or who may access it. Delhi Police's internally fixed 80% similarity threshold provides, at most, the second, an operational rule, set and alterable by the same authority that adopted it, without notice, and lacking any legislative benchmark against which its accuracy could be tested. Neither instrument approaches the third, a government agency may well have the power to procure and operate an identification system for ordinary administrative purposes; it does not follow that the same instruments constitutionally authorise deploying that system in a manner that restricts privacy or assembly rights.

It might be objected that the Digital Personal Data Protection Act, 2023 substantive provisions of which are being phased in following the notification of the DPDP Rules in November 2025, now provides the missing statutory layer. It does not, though the reason requires some care: Section 17(1) of the Act, however, exempts processing "necessary for... prevention, detection, investigation or prosecution of any offence" from the Act's core consent and notice obligations under Chapters II and III. This does not actually establish a constitutional vacuum in the sense Chapter 3 describes, as the DPDP Act's exemption means police FRT sits largely outside the Act's substantive data-protection obligations, and can therefore not draw on it for the general statutory safeguards purpose limitation, retention limits, access controls that might otherwise structure such processing. Whether some other statute individually authorises the intrusion is the separate question the previous chapter already answers in the negative; the DPDP exemption cannot itself substitute for that missing authorisation, and was in any case never designed to.

Crime prevention and detection are undoubtedly proper aims for the state; an investigation into both subsequent to their occurrence can hardly be considered otherwise than a legitimate pursuit, and as such falls squarely within the previous conclusion that this category poses little constitutional challenge. The more pertinent questions regarding the use of FRT for watch-listing purposes in the absence of any particularised offence being investigated, and indeed its continual use for the surveillance of a gathering of people at a location such as Jantar Mantar. Preservation of public order is no less a legitimate aim for the state than crime prevention and detection, as discussed. The problem with continual biometric surveillance of all persons present, however, is one of proportionality in regard to the specific safeguards provided for assemblies by virtue of Article 19(1)(b) is difficult to disentangle from the idea of surveillance targeting the very exercise of the rights named in that article, rather than any legitimate concern with threats to public order stemming therefrom. This difficulty is a matter for discussion in regard to whether the means used are proportionate to the ends sought; it does not, however, vitiate the fact that those ends, as stated, are legitimate.

Even if one were to accept a legitimate aim for the use of FRT as at Jantar Mantar, its application would fail the proportionality test, that is, the requirement of a balance between means and ends, because of the lack of procedural safeguards around its use, which renders it overly intrusive on privacy rights. This conclusion follows from the *Anuradha Bhasin* test, which requires that restrictions on Article 19 freedoms be notified, narrowly tailored and periodically reviewed. The absence of procedural safeguards applies with particular force to FRT, as the instruments do not impose any limits on the retention of biometric data, access to it, or auditing of its use, nor do they require a formal ex-post review of the FRT's functioning, specify a publicly accessible standard of accuracy, detail criteria for watchlisting, or mandate police authorisation for use (rather than internal

authorisation within the using agency). It must be stressed that while this is not necessarily a complete answer to the lack of safeguards, precisely because rules made by Parliament or by the executive, so long as they are democratically accountable, can provide the necessary procedural protections because the protections currently in place for police use of FRT in India are insufficient under Anuradha Bhasin. None of the listed instruments provide such procedural oversight.

The use of biometric data adds another layer of concern to this lack of procedural safeguards. Unlike, say, a password, a person's facial characteristics cannot be changed if compromised. This poses a particular problem for FRT's use in India, where retention limits or procedures for auditing are not in place.

None of this is predicated on FRT being intrinsically illegitimate, and none of it is a refutation of the more limited, investigatory use case that is previously identified as the technology's least constitutionally fraught application. The objection to FRT as currently deployed in India for watch-listing and real-time assembly monitoring is narrower and therefore potentially stronger than a general opposition to the technology. It is harder to answer precisely because the objections to FRT's application in these two domains are grounded in the technology's very capacity to serve its ends. Current Indian law contains neither the legitimate authority for such intrusions upon privacy nor the protective frameworks necessary to oversee their use.

5. Separation of Powers and Rule of Law

The foregoing section demonstrated that police facial recognition fails the proportionality test because the legal framework surrounding it lacks the legal authority and procedural safeguards that the Constitution requires. That conclusion raises a more profound question, and a more basic one. If the problem is that there is no law, can the executive solve the problem by issuing its own detailed standard operating procedures, internal guidelines, or departmental policies? The answer to that question will determine whether the problem identified in this paper is administrative in character, and thus capable of remedy through better executive practice, or constitutional, and thus requiring legislative intervention. The argument made here is that it is the latter, for reasons grounded in the design of executive power under the Constitution and in the demands of the rule of law.

The starting block must be the best argument the state can make. In *Ram Jawaya Kapur v. State of Punjab* the Supreme Court held that the executive power of the Union and the States under Articles 73 and 162 is co-extensive with the respective legislative powers and that the executive can therefore act in any field on which the legislature is competent to legislate without waiting for a statute to be enacted. It might be said that the use of facial recognition is well within the normal administrative powers of the police, since public order and police are matters in the State List and criminal procedure a matter of concurrent competence. Thus, the acquisition and use of a new investigative tool is no different in principle from the procurement of vehicles or communications equipment and does not require legislative sanction.

This argument, however, misreads the scope of the proposition in *Ram Jawaya Kapur*. In that case, the Court was careful to limit its holding to executive action that does not infringe on individual rights. Where such rights are implicated, a separate and more rigorous standard is applicable, one the Supreme Court has repeatedly reiterated. In *State of Madhya Pradesh v. Thakur Bharat Singh*, the Court held that the executive cannot, in the absence of legislative authority, take action which deprives a person of his rights and observed that the State is not free to act to the prejudice of the citizen merely because no law forbids it. This principle was applied most lucidly within the framework of police surveillance in *Kharak Singh v. State of Uttar Pradesh*. The domiciliary visits which were questioned in that case were made under the Uttar Pradesh Police Regulations which were framed by the executive and had no statutory foundation. The Court struck down the practice on the ground that the Regulations did not amount to 'law' within the meaning of Article 21 and an intrusion into a person's life and liberty could not be justified by executive instructions alone. The parallel with facial recognition is straightforward and, for the purposes of this paper, decisive. In each case, the police justify surveillance of individuals by reference to internally-generated rules, rather than by reference to the character of law, and the effect is that the intrusion is constitutionally unauthorized no matter how carefully the internal rules are drafted. The same principle has been laid down in *Bijoe Emmanuel v. State of Kerala*, where the Court has observed that departmental circulars cannot be considered as a law which can impose restrictions on the freedom of expression. The requirement is not only that a restriction be reasonable, but that it be imposed by laws.

The point of these authorities is to prevent the easiest response to the shortcomings mentioned in the last section. A police force that responded to criticism by publishing a comprehensive facial recognition policy, including watchlist criteria, retention schedules, and audit requirements, would not thereby make its deployments legal. The document would remain an executive instrument and under *Kharak Singh* and *Bijoe Emmanuel* an executive instrument cannot provide the legal basis Article 21 requires. Thus, the defect is not in the content but in the source.

The comparative experience of the United Kingdom illustrates the same point in a different way. In *Malone v Metropolitan Police Commissioner*, Megarry V-C refused to hold that telephone tapping was unlawful on the basis that the executive could do anything which was not prohibited by law and there was no legal rule prohibiting the interception of communications. That reasoning was rejected when the matter came before the European Court of Human Rights in *Malone v United Kingdom*. The Court found that the interference was not "in accordance with the law", because the domestic arrangements regulating interception were not sufficiently accessible or precise to enable citizens to foresee in which circumstances their communications might be intercepted. The judgment forced Parliament to enact the Interception of Communications Act 1985. The sequence is instructive: the longer-standing the administrative practice, the more it could not replace legislation once the intrusion upon rights was appreciated. The theoretical aspect of this issue was studied by B.V. Harris in his work on the so-called third source of governmental authority asking whether the

executive may act on the basis of its ordinary capacities where neither statute nor prerogative authorizes the action. Harris concludes that if such authority exists at all, it cannot extend to actions which infringe upon individual liberty.

But there is also the separate matter of democratic legitimacy that the separation of powers is meant to protect, apart from the issue of legal authority. In their study of democratic policing, Barry Friedman and Maria Ponomarenko have argued that US police agencies routinely acquire intrusive surveillance technologies through internal policy and procurement decisions, bypassing the legislative deliberation that would accompany any comparable exercise of government power. Their central insight is that the choice to adopt these technologies is not a technical or operational one, but rather a policy choice of considerable public significance. The decision to use facial recognition must involve choices about who can be suspected, how much error is socially acceptable, whether protest sites and places of worship should be off-limits to surveillance, and how long the biometric records of innocent people can be retained. These are contested questions of value on which reasonable citizens disagree, and they are exactly the kind of questions that the Constitution leaves to the legislature and not to administrative agencies. When they are enshrined in tender documents and departmental circulars, the decision is made without public debate, parliamentary scrutiny, or opportunity for the affected to influence the outcome.

This concern is tied to a settled principle of Indian constitutional law. The doctrine of excessive delegation as enunciated in *In re Delhi Laws Act*, lays down that the legislature may delegate the task of working out the details but it must itself decide the essential legislative policy and give guidance for the exercise of the delegated power. The doctrine is a recognition that the legislature, as elected, should be the body to make fundamental policy choices. If that principle limits the legislature's ability to delegate policy questions to the executive even when the legislature has considered the matter and decided to delegate, then the executive is in an even weaker position when it makes such policy choices without any legislative involvement at all. In acute form this situation is illustrated in India where there is no enabling statute, no delegated authority and consequently no legislative guidance of any kind.

The rule of law is an ultimate and separate objection. The internal requirements of legality identified by Lon Fuller include that rules be promulgated, that rules be clear enough to guide action, and that official action correspond to the rules declared. India's use of facial recognition fails to meet any of these standards. The governing instructions are often unpublished; where policies exist, they are usually so worded as to provide no guidance as to when a person may be scanned or placed on a watchlist; and there is no independent means of checking the correspondence between stated policy and actual practice.

The question of the proper judicial response lingers. Indian courts have sometimes filled the legislative gaps directly, as the Supreme Court did in *PUCCL and in Vishaka v. State of Rajasthan*, laying down binding guidelines to be in operation until parliament legislated. Judicially crafted guidelines, once issued, may relieve the pressure on Parliament to legislate, and may entrench a practice whose legitimacy has never been settled democratically. The constitutional objection to police facial recognition is not just that it is insufficiently regulated in its use but that the decision to use it at all has never been taken by the body competent to take it. And a judicial remedy that offers protections without resolving that earlier question treats the symptom, not the disease. The more principled way is for courts to say that deployment without statutory authority is unconstitutional and to leave it to Parliament to decide whether such a power should exist and on what terms. In the next section, we address this question and look at what legislative models are available for consideration.

6. Comparative Legislature Models

As the previous sections have demonstrated, the conclusion is that police facial recognition needs a legislative foundation and the executive cannot provide one on its own. It does not follow that any statute would do. A law that merely confers a general power to use facial recognition without defining the scope of that power or laying down conditions for its use would fail the *Puttaswamy* test as surely as the absence of law today. This is because the requirement of legality requires not just that a power exists but that it is sufficiently precise to restrict its exercise and to enable those affected by it to anticipate its application. So, the objective of this section is to examine the measures of other jurisdictions in their attempts to comply with this standard and to identify from their experience the design features which will need to be incorporated in Indian legislation. The jurisdictions covered can be characterized in three broad categories: those that prohibit the technology; those that permit it subject to prior authorization and defined limits; and those that remain dependent on guidance and administrative policy. India is currently in the third category and the problems faced therein make the case for legislation more urgent.

The most developed example of the authorisation-based model is the European Union. The artificial intelligence Act builds on a presumption of prohibition: the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is prohibited under Article 5(1)(h). The prohibition is then qualified by narrowly defined exceptions, which allow such use only for the targeted search for victims of specified serious crimes, the prevention of a specific and present threat to life or of a terrorist attack, and the localization of persons suspected of offenses listed in the Regulation. The very structure of the provision is significant. The state, not the police, decides the purposes for which the technology may be used, and it does so by making prohibition the norm and permission the exception, with the burden of justification falling on the state each time. Article 5(3) complements this allocation by providing that each deployment is subject to prior authorization by a judicial authority or an independent administrative authority, except in cases of urgency when authorization must be sought without undue delay thereafter. Importantly, Member States cannot rely upon the exceptions at all unless they pass national legislation allowing their use. This requirement is designed to ensure that the decision to adopt the technology is made by an elected legislature rather than inferred from the silence of the law. Nor does the Regulation prohibit retrospective identification, which it sees as less intrusive than the ongoing scanning of the public, but classifies it as high-risk and therefore

subject to additional obligations such as authorization and reporting requirements under Article 26(10). This distinction between live and retrospective use is one that Indian legislation would do well to adopt, as it allows the state to retain a valuable investigative tool while withholding the power of indiscriminate mass surveillance. We should acknowledge that the European framework is not without its critics. In their Joint Opinion 5/2021 the European Data Protection Board and the European Data Protection Supervisor called for a complete prohibition on remote biometric identification in public spaces and commentators have questioned whether the exceptions in Article 5 are drawn sufficiently narrowly to preserve the general rule.

Conversely, the United Kingdom demonstrates the consequences when governments attempt to regulate facial recognition through guidance alone, and its experience is directly relevant to India as the two jurisdictions face structurally similar problems. Since *Bridges*, English policing has continued to rely on common law powers, the Data Protection Act 2018, the Surveillance Camera Code of Practice and the College of Policing's Authorized Professional Practice on live facial recognition. There is no statute which specifically authorizes the technology, or which sets out the conditions under which it may be used. "This arrangement has been considered to be not adequate. An independent legal review of the governance of biometric data, commissioned by the Ada Lovelace Institute in 2022, found that the current patchwork of codes and policies is inadequate and recommended a dedicated statutory framework along with an independent regulator to oversee the use of biometric technologies. The review was undertaken by Matthew Ryder KC. Similar concerns about the lack of a clear legal basis have also been expressed by the House of Lords Justice and Home Affairs Committee. The lesson for India is a cautionary one. The United Kingdom has tried to regulate facial recognition for several years, and with significant institutional effort, through administrative instruments issued by bodies with real expertise. That effort has not produced a framework that courts or reviewers find adequate, suggesting the inadequacy is in the instrument itself, not in the drafting. The Indian arrangements do not even have an equivalent of the surveillance camera code, and cannot be expected to do better.

In the absence of federal legislation, the United States has generated the broadest spectrum of approaches. Its sub-national experiments show the range of options available to a legislature. At one end of the spectrum is outright prohibition. The Stop Secret Surveillance Ordinance, passed by San Francisco in 2019, banned the use of facial recognition by municipal agencies, including the police, and several other cities followed suit. Such prohibitions are based on a judgment that the risks posed by the technology cannot be sufficiently controlled by procedural controls. Washington State's Senate Bill 6280 of 2020 is a good example of a regulatory not prohibitory approach, allowing state and local agencies to use facial recognition but only if a series of statutory requirements are met: an accountability report to be filed and available for public comment prior to deployment; meaningful human review of decisions that have legal or similarly significant effects; independent testing of the system for accuracy and bias; and for ongoing surveillance, a warrant or its equivalent.

Massachusetts took a different tack in its 2020 police reform law, routing most police facial recognition searches through a handful of designated state agencies. The law creates a record of every search based on written requests and separates the requesting officer from the person doing the comparison. Since then, Montana and Maryland have passed laws limiting use to serious crimes or requiring judicial approval. The point of these models is not that any one of them should be adopted wholesale, but that they demonstrate that the regulatory choices involved are severable: authorization, purpose limitation, accuracy testing, human review and institutional separation can each be adopted independently, and a legislature can combine them according to its own assessment of the risks.

These models can be used to identify the features that can be incorporated in the Indian legislation to remedy the deficiencies identified earlier in this paper. The correspondence between those deficiencies and these features is intentional, because the point of legislation is to supply what the proportionality analysis found wanting. First, the statute should distinguish between prospective and retrospective use, prohibiting the former except in narrowly defined circumstances and subjecting the latter to authorization. This would meet the objection based on necessity that indiscriminate scanning is not the least restrictive means available. Secondly, it should specify the purposes for which the technology may be used in relation to defined offenses, so that Parliament can make the decision as to which investigations warrant biometric surveillance rather than individual officers. Thirdly, there should be a provision for prior authorization for each deployment by a judicial officer or an independent authority. This is the external check that the Supreme Court found constitutionally unacceptable in *PUCL* because of its absence. Fourth, it should set the grounds for inclusion in a watchlist, which is precisely the defect that made the framework in *Bridges* not sufficiently foreseeable to meet the requirement of legality. Fifth, it must require independent testing for accuracy and demographic bias prior to deployment, and periodically thereafter, to be able to address the suitability objection reflected in the error rates documented in the NIST evaluations. Sixthly, it should set strict limits on the retention of biometric data relating to persons not matched, with an obligation of prompt deletion. Seventhly, it should require logging and auditing of every search and regular reporting of the number of deployments, matches and errors, so that the practice is open to public and parliamentary scrutiny. Finally, it should provide an effective remedy for misidentified persons, because a right without a means of enforcement offers little protection in practice.

Two qualifications must be made before these recommendations can be put forward with any confidence. The first relates to the limits of legal transplantation. The European framework is within a supranational legal order, backed by data protection authorities in each member state, and its enforcement depends on institutional capacity that is not equally available in India. The American models operate in a federal framework with States having primary responsibility for policing while in India the distribution of legislative competence between the Union and the States over police, public order and criminal procedure raises questions about the appropriate legislative vehicle which would require separate consideration. The second qualification relates to the interface between any facial recognition statute and the Digital Personal Data Protection Act, 2023. As noted above, Section 17 of that Act allows for the exemption of state instrumentalities on grounds that would easily include police surveillance. In the absence of a facial recognition statute that either preempts that exemption or offers equivalent protections directly, the general law may undermine the protections it purports to establish. The comparative material surveyed here, therefore, does not provide a model to be uncritically adopted. Rather, it offers a

demonstration that the constitutional standard identified in this paper can be achieved through legislation, and a suggestion of the elements which such legislation must include.

None of this is predicated on FRT being intrinsically illegitimate, and none of it is a refutation of the more limited, investigatory use case that is previously identified as the technology's least constitutionally fraught application. The objection to FRT as currently deployed in India for watch-listing and real-time assembly monitoring is narrower and therefore potentially stronger than a general opposition to the technology. It is harder to answer precisely because the objections to FRT's application in these two domains are grounded in the technology's very capacity to serve its ends. Current Indian law contains neither the legitimate authority for such intrusions upon privacy nor the protective frameworks necessary to oversee their use.

6. Conclusion

The constitutional problem with police facial recognition in India arises earlier in the analysis than is generally believed. It is tempting to view the problem as one of inadequate safeguards, and to cure it by published thresholds, retention limits and internal audit. That framing is too much of a concession, assuming the power exists and only asking how it should be used. Under *Kharak Singh* and *Bharat Singh*, no executive instrument, no matter how carefully drafted, can provide the authority for a restriction on a protected right. The flaw is in the source, not the content, and for that reason is not one the executive can cure by improving its own practice.

Two things follow. The first is about the role of the judiciary. Guidelines such as those issued in *PUC*L and *Vishaka* would provide safeguards but would not impact the prior question of whether the power should exist at all - a question the Constitution leaves to the legislature. A judicial remedy that regulates an un-authorised practice risks entrenching that practice and relieving parliament of the pressure to decide. Courts would be better served to find that use of a power without statutory authority is unconstitutional, and leave the design of any such power to where it belongs.

The second is about what that design ought to be. No conjecture. The European Union's distinction between live and retrospective use, its requirement of prior independent authorization, the American models of accuracy testing and institutional separation, and the British experience of what guidance alone cannot achieve, all provide a workable set of features. They cannot be transplanted wholesale given the federal division of competence over police and criminal procedure in India and the exemptions available under the Digital Personal Data Protection Act, 2023. But they demonstrate that the constitutional standard can be met. India does not need a model but a legislative decision to take one.

REFERENCES

- Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
- Bakshi, G. K. (2026, July 28). MP moves Supreme Court against police use of facial recognition technology & biometric surveillance at protest sites. LiveLaw. Retrieved from <https://www.livelaw.in/top-stories/mp-moves-supreme-court-against-police-use-of-facial-recognition-technology-biometric-surveillance-at-protest-sites-543187>
- Bijoe Emmanuel v. State of Kerala, (1986) 3 S.C.C. 615 (India).
- Bingham, T. (2010). The rule of law. London, England: Allen Lane.
- Biometric Update. (2020, March). India authorizes roll out of automated biometric facial recognition in police investigations. Retrieved from <https://www.biometricupdate.com/202003/india-authorizes-roll-out-of-automated-biometric-facial-recognition-in-police-investigations>
- Brut India. (2026, July). Why is Delhi Police using AI surveillance at the Jantar Mantar protest? Retrieved from <https://www.brut.media/in/articles/why-is-delhi-police-using-ai-surveillance-at-the-jantar-mantar-protest>
- Chandra, A. (2020). Proportionality in India: A bridge to nowhere? University of Oxford Human Rights Hub Journal, 3(2), 55–86.
- College of Policing. (2022). Live facial recognition: Authorised professional practice. Ryton-on-Dunsmore, England: Author.
- Criminal Procedure (Identification) Act, No. 11 of 2022, India Code (2022).
- Data Protection Act 2018, c. 12 (U.K.).
- Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
- Digital Personal Data Protection Rules, 2025, Gazette of India, pt. II sec. 3(i) (Nov. 13, 2025) (India).
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, 2016 O.J. (L 119) 89.
- District Registrar & Collector, Hyderabad v. Canara Bank, (2005) 1 S.C.C. 496 (India).
- European Data Protection Board & European Data Protection Supervisor. (2021). Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence. Brussels, Belgium: Authors.
- Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. New York, NY: New York University Press.
- Friedman, B., & Ponomarenko, M. (2015). Democratic policing. New York University Law Review, 90(6), 1827–1907.
- Fuller, L. L. (1969). The morality of law (Rev. ed.). New Haven, CT: Yale University Press.
- Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. Colchester, England: Human Rights Centre, University of Essex.
- Glukhin v. Russia, App. No. 11519/20 (Eur. Ct. H.R. July 4, 2023).
- Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT) Part 3: Demographic effects (NISTIR 8280). Gaithersburg, MD: National Institute of Standards and Technology.
- Harris, B. V. (1992). The "third source" of authority for government action. Law Quarterly Review, 108, 626–651.
- Harris, B. V. (2007). The "third source" of authority for government action revisited. Law Quarterly Review, 123, 225–250.

- The Hindu. (2020, March 4). Facial recognition system will not violate privacy. Retrieved from <https://www.thehindu.com/news/national/facial-recognition-system-will-not-violate-privacy/article61591011.ece>
- Home Office. (2021). Surveillance camera code of practice. London, England: Author.
- House of Lords Justice and Home Affairs Committee. (2022). Technology rules? The advent of new technologies in the justice system (HL Paper 180). London, England: House of Lords.
- In re Delhi Laws Act, 1912, A.I.R. 1951 S.C. 332 (India).
- India Const. arts. 19, 21, 73, 162, sch. VII.
- Indian Telegraph Act, No. 13 of 1885, India Code (1885).
- Interception of Communications Act 1985, c. 56 (U.K.).
- Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
- Justice K. S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 S.C.C. 1 (India).
- Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295 (India).
- Malone v. Metropolitan Police Commissioner, [1979] Ch. 344 (Eng.).
- Malone v. United Kingdom, (1984) 7 E.H.R.R. 14 (Eur. Ct. H.R.).
- Maneka Gandhi v. Union of India, A.I.R. 1978 S.C. 597 (India).
- Mass. Gen. Laws ch. 6, § 220 (2020).
- Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 S.C.C. 353 (India).
- National Crime Records Bureau. (2019). Request for proposal to procure National Automated Facial Recognition System (NAFRS). New Delhi, India: Ministry of Home Affairs.
- Outlook India. (2026, July 24). CJP protest under AI watch: Delhi Police's facial recognition vans spark privacy concerns. Retrieved from <https://www.outlookindia.com/national/cjp-protest-under-ai-watch-delhi-polices-facial-recognition-vans-spark-privacy-concerns>
- People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).
- R (Bridges) v. Chief Constable of South Wales Police, [2020] EWCA (Civ) 1058 (Eng.).
- Rai Sahib Ram Jawaya Kapur v. State of Punjab, A.I.R. 1955 S.C. 549 (India).
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689).
- Right to Information Act, No. 22 of 2005, India Code (2005).
- Ryder, M. (2022). The Ryder Review: Independent legal review of the governance of biometric data in England and Wales. London, England: Ada Lovelace Institute.
- S. & Marper v. United Kingdom, (2009) 48 E.H.R.R. 50 (Eur. Ct. H.R.).
- S.B. 397, 68th Leg., Reg. Sess. (Mont. 2023) (codified at Mont. Code Ann. §§ 44-15-101 to -110).
- S.B. 6280, 66th Leg., Reg. Sess. (Wash. 2020) (codified at Wash. Rev. Code ch. 43.386).
- State of Madhya Pradesh v. Thakur Bharat Singh, A.I.R. 1967 S.C. 1170 (India).
- Stop Secret Surveillance Ordinance, S.F., Cal., Ordinance No. 103-19 (2019).
- Vishaka v. State of Rajasthan, (1997) 6 S.C.C. 241 (India).