



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DOES AI-BASED PREDICTIVE POLICING IN PREVENTIVE DETENTION MEET INDIA'S CONSTITUTIONAL PROPORTIONALITY STANDARD?

Sreenidi R.N

ABSTRACT

Artificial Intelligence tools are increasingly being incorporated into the Indian police forces, from Delhi Police's Crime Mapping, Analytics and Predictive System (CMAPS) to Bengaluru's C4i platform and Akola's Project Trinetra. These algorithms serve the purpose of assigning machine-generated risk scores to repeat offenders, or identify areas of possible crime occurrence, to predict crime before it occurs. As of now these systems are not considered formal triggers for preventive detention. But the path from area-based hotspot mapping, to individual risk assessment or scoring makes that step seem likely. This paper takes up an analysis regarding the prospective proportionality of this method. Would a regime using AI-generated risk scores formally to inform decisions to invoke preventive detention, under statutes such as the National Security Act, 1980, state Public Safety Acts, or Section 151 of the Code of Criminal Procedure, 1973, satisfy the four-fold proportionality standard as conceptualized in Justice K.S. Puttaswamy (Retd.) v. Union of India. It also looks into the requirement for concrete safeguards to exist before such a system could be constitutionally defensible.

INTRODUCTION

Preventive detention holds an unusual place in Indian constitutional law. In most liberal democracies, detention without trial is regarded to be an emergency exception. However, in the Indian Constitution, it is expressly contemplated and regulated through Article 22(3) to (7)¹, thus allowing the state to deprive a person of liberty not for the commission of an offense, but for the apprehension of presumable possibility of the commission of an offense. This power already sits

¹ INDIA CONST. art. 22, cls. 3, 7.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

in contrary to the provision of Article 21, which guarantees personal liberty. Adding an opaque, statistically-driven prediction engine, powered on data which may not be unbiased, on top of that power, raises the stakes considerably.

The idea is not being experimented with abstractly by the Indian Police forces. Operations at scale have already begun using predictive tools: Under the Bengaluru Safe City Project,² the Bengaluru city police have introduced AI-driven 'Preventive' and 'Predictive' Policing, integrating facial recognition, prior existing databases, including traffic and crime data into a central command system that flags individuals as 'suspicious' and dispatches patrols. Akola's Project Trinetra³ uses a Repeat Offender Risk Scoring model to evaluate individuals based on their conviction history and movement patterns, which are used to then assign machine-learning-based probability scores. The CMAPS operation of the Delhi Police⁴, however, remains unaudited due to exemptions under the Right to Information Act.

These tools, however, are not a documented legal trigger as of now for a preventive detention order. However, the shift, from mapping places to scoring individuals, assessing them, is becoming increasingly evident. Legal scholars have already identified the specific mechanism through which this could easily result in unlawful detention: predictive policing increasing the risk of preventive detentions under Section 151 of the CrPC, now Section 170 under the BNSS, by influencing the officer's discretionary decision to act on 'apprehension' of a cognizable offence, which would remain mostly unreviewable. This paper examines the constitutional challenge of whether AI can constitutionally displaced human judgment in preventive detention decisions, and if so, what would the required legal framework have to contain to comply with the set constitutional principles.

² The Hindu Bureau, *How are predictive policing and traffic management tools used on India's roads | Explained*, The Hindu (Feb. 27, 2026)..

³ *Project TRINETRA – Police Department Akola*, SKOCH Exhibition (Feb. 4, 2026).

⁴ Ramachandran Murugesan, *Predictive policing in India: Deterring crime or discriminating minorities?*, (Apr. 16, 2021).



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

PREVENTIVE DETENTION WITHIN THE CONSTITUTIONAL SCHEME

Preventive detention does not have the ordinary protections of arrest, the detainee does not have the right to be produced before a magistrate within 24 hours, or the right for legal representation. Instead, there are separate safeguards provided by the Constitution: grounds of detention must ordinarily be communicated under Article 22(5)⁵, and the detention must be reviewed within a stipulated period by an Advisory Board. In *A.K Roy v. Union of India*⁶, the Supreme Court upheld the constitutionality of the National Security Act⁷, but they still stressed the strict adherence to procedural safeguards as necessary due to the substantive basis for detention. The executive's subjective satisfaction is treated as largely non justiciable.

This aspect of non-justiciability is concerning since Courts have held repeatedly that they will only review whether the satisfaction of the detaining authority was honestly and rationally arrived at, not the sufficiency of the material itself which is presented to said authority. In the case of *Rekha v. State of Tamil Nadu*⁸, the Supreme Court defines preventive detention to be a 'jurisdiction of suspicion', and warned that the utilization of the same must not be a substitute for instances of ordinary criminal law which can be sufficiently addressed through prosecution, and must be confined to narrow limits.

Additionally, the Supreme Court, in the case of *Ameena Begum v State of Telangana* ⁹sets out the discrete tests required to examine the legality of a preventive detention order, and several out of the 10 stipulated prongs are pertinent here: whether the satisfaction is based on materials of rationally evidentiary value; whether it reflects a live and proximate link between past conduct and the need to detain, rather than material that is stale; and whether the grounds are precise and relevant enough to give the detainee a fair opportunity to make a representation. The purpose of

⁵ INDIA CONST. art. 22, cls. 5.

⁶ *A.K. Roy v. Union of India*, (1982) 1 SCC 271.

⁷ The National Security Act, 1980, No. 65, Acts of Parliament, 1980 (India).

⁸ *Rekha v. State of T.N.*, (2011) 4 SCC 260.

⁹ *Ameena Begum v. State of Telangana*, (2023) 9 SCC 587.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

these tests is to ensure that suspicion, left unexamined, does not lead to arbitrariness. It attempts to elaborate on the “jurisdiction of suspicion” an outer limit while still deferring to the subjective judgement of the executive.

The problem is that each of these tests was built around an epistemic object, which is the belief of a human officer composed of discrete, nameable facts-which can be, at least in principle, unpacked, dated, and weighed. An algorithmic risk score is another kind of object entirely, and it eludes these tests not by failing them but by being of the wrong shape for them. Let us take rationally probative value first. The test assumes that the reviewing court, or at least the detaining authority itself, can trace why a particular document proves the inference derived from it-a witness account speaks to a specific act, a previous FIR speaks to a specific pattern. A proprietary risk score provides no such traceable chain of inference; it provides an output. Unless the statute or record requires the output model’s features, weights or basis training to be disclosed, the “probative value” of such material is something the detaining authority accepts in faith from the system, a different epistemic posture than forming one’s own belief from evidence and then being required to explain it.

The live-and-proximate-link test performs even worse. It is tailored to identify only one failure mode: a detaining authority taking into account conduct so old that it can no longer support a real fear of further harm. A risk score complicates this problem: the “conduct” a model draws on is not one individual action on a particular date but an aggregate of various patterns based on a historical dataset-arrests, associations, geography-each individually may be old, sparse, or not particularly relevant to the detenu, but the combination could produce a high score. The live-and-proximate-link analysis presupposes a specific incident against which recency can be tested; an aggregate of individual incidents has no analogous temporal focal point.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

The most straightforward failing, and the most closely related to constitutional concerns as it relates to Article 22(5)'s¹⁰ guarantee to notify a detenu of the grounds for his detention, is the disclosure test. A ground such as “associated with persons of criminal antecedents in the locality, per risk assessment” or simply expressed as a percentile fails to give a detenu anything to dispute in the way Ameena Begum understood it to be, to wit, anything “precise, pertinent, and relevant... as a suitable representation.” The detenu cannot meaningfully challenge a score's calculation unless the basis of its calculation is disclosed, which is almost routinely withheld on the ground of it being proprietary or being of particular relevance to law enforcement agencies.

The issue is not whether the algorithmic risk scores are more accurate than human judgement, but that these tests rely on the assumption that the reasoning for the algorithmic identification can be traced and examined. However, Algorithmic reasons only make it harder to identify these reasons. This allows the record to pass through A. K. Roy's procedural protections and Ameena Begum's ten-factor test without actually being tested by them.

The theory of subjective satisfaction was developed for an era of individual human judgment, albeit a messy one. It was not developed to encompass decisions that are heavily reliant on a statistical model, trained on historical arrest records - which, as researchers of Indian predictive policing highlight, tend to be of low quality and amplify the pre-existing enforcement biases, instead of rectifying them.

¹⁰ INDIA CONST. art. 22, cls. 5.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

THE PROPORTIONALITY STANDARD

This “proportionality doctrine” was introduced to Indian constitutional jurisprudence in the case of *Om Kumar v. Union of India*¹¹, and gained momentum through the *Modern Dental College and Research Centre v. State of Madhya Pradesh*¹². The court stated there would be “a sequential analysis” or four progressive inquiries:

1. “whether the state action is aimed at achieving a legitimate State purpose”;
2. “whether the means used is suitable for the achievement of such a purpose” (that is to say, “whether there is a rational relationship between the measures and the purposes”;
3. “whether there is any less intrusive measure that would achieve the same purpose” (that is to say, whether it was “necessary”); and
4. “whether the impairment of a fundamental right is excessively disproportionate to the purpose achieved” (that is to say, the balancing, or the strict proportionality, analysis).

These four stages were “firmly placed upon the bedrock of our Constitution” by the nine-judge bench in the landmark judgement of *KS Puttaswamy*¹³, which had already unanimously established privacy to be a fundamental right. This was a right that would not survive any state invasion that did not pass the four stages; legitimate aim, rational nexus, necessity and proportionality. Later

¹¹ *Om Kumar v. Union of India*, (2001) 2 SCC 386.

¹² *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353.

¹³ *K.S. Puttaswamy (Aadhar-5J.) v. Union of India*, (2018) 1 SCC 809.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

applications of proportionality indicate how it is not simply reserved for informational-privacy cases. In the case of *Anuradha Bhasin v. Union of India*¹⁴ the court applied it to analyse internet shutdowns, which restricted freedom of expression and movement, and treated it as a general standard for the testing of any state intervention into liberty necessitated by national security – which is a category in which preventive detention falls. Since then, it has made also entered into discussions around the traceability of encrypted communication, the disclosure of information under the Right to Information Act, and even the Aadhaar scheme itself, in which, to their opposite conclusions, the majority of the judges applied all four of the *Modern Dental College* sub-tests. Justice Chandrachud's dissent applied the same four-part test and arrived at the contrary outcome, thus illustrating that whether the test yields a positive or negative outcome will turn heavily on how strictly each stage, particularly necessity and proportionality being balanced is actually interrogated rather than simply addressed. Reviewing under a proportionality framework can either be deferential, rubber-stamping the justification offered by the executive branch of the State, or searching, requiring empirical evidence to support each component. It is already true that the preventive detention regime benefits from extraordinary judicial deference, due to its subjectivity-satisfaction criteria; the addition of an algorithmic layer, unaccompanied by an increased level of rigour in applying the proportionality test, would increase the existing deficit in accountability, rather than reduce it.

¹⁴ *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

IV. RUNNING AI-TRIGGERED PREVENTIVE DETENTION THROUGH THE PROPORTIONALITY TEST

A. Legitimate Aim

Crime prevention and public order are undisputably legitimate state interest aims, and the Puttaswamy court accepted that national security concerns can justify restrictions on privacy.

On this alone, an AI-assisted preventive detention regime would likely pass: preventing a cognizable offence before it occurs is a purpose the Constitution itself sanctions through Article 22(3)¹⁵. The difficulty is not in identifying a legitimate goal; it lies in whether the specific area chosen actually serve that purpose, which is where the remaining points do the real work.

B. Suitability and the issue with the Bias Problem

Suitability asks whether there is a rational connection between the preventive measure and the goal. An AI system can only be a suitable means of preventing crime if its predictions are reasonably reliable. This is where the present gap of a legal framework for algorithmic accountability becomes constitutionally significant, more than a policy gap. Indian predictive-policing academia has already identified that these systems are trained on 'inferior quality datasets'. This refers to historical arrest and FIR records, that themselves reflect decades of discriminatory over-policing of particular localities, castes, religious minorities, and economically marginalised groups. An algorithm trained on such data does not predict crime; and instead, it predicts where police have historically chosen to look, and ensures that they keep looking there. The output only supports historical bias into a facially neutral, technical score, which paradoxically makes it harder

¹⁵ INDIA CONST. art. 22, cls. 3.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

to challenge than an openly discriminatory human decision, because it wears the mask of objectivity.

Bengaluru's own C4i system illustrates the mechanism concretely: it flags a person as suspicious partly because the police database already labels them a 'history sheeter',¹⁶ meaning the algorithm's 'prediction' is substantially a re-presentation of a prior police categorisation, not an independent forecast. Where the underlying categorisation was itself shaped by biased enforcement patterns, the AI layer adds a veneer of technical authority to what remains, at bottom, a self-reinforcing profiling loop. A measure built on such a loop struggles to satisfy suitability in any rigorous sense, because it is not clear the tool measures propensity to offend at all, as opposed to propensity to have already been policed.

C. Necessity

Necessity enquires whether a less restrictive, equally effective alternative exists. This is the requisite that is most directly implicated by the absence of a dedicated legal framework. Two structural facts support this. First, India's Digital Personal Data Protection Act, 2023¹⁷ exempts processing carried out for law-enforcement and public-order purposes from significant portions of the Act's rights framework. The European Union's General Data Protection Regulation¹⁸, on the other hand, grants data subjects a right to explanation and to contest solely automated decisions with legal effect. Second, unlike the EU's approach to high-risk AI systems, the DPDP Act does not establish any regime specific to automated decision-making, profiling, or algorithmic risk-

¹⁶ *CCTVs and safety islands: Bengaluru's 'Safe City' project hits March 2024 target*, (Sept. 22, 2023).

¹⁷ Digital Personal Data Protection Act, 2023, § 17, No. 22 of 2023, India Code (2023).

¹⁸ Regulation 2016/679, 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 and on the Free Movement of Such Data (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1, 46 (EU).



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

scoring by police, and does not offer any statutory route, by which a person can learn that a risk score contributed to their detention, let alone contest its accuracy.¹⁹

This is not a marginal gap; it prevents the necessity inquiry almost entirely. A court cannot evaluate whether a less restrictive alternative was there, or whether the algorithmic input was reliable, if the detainee has no legal mechanism to obtain the algorithmic assessment, the model's basis, or an opportunity to defend themselves against it before the Advisory Board. Compare this to place-based predictive tools, which direct patrol resources without depriving any individual of liberty, it is a plainly less restrictive alternative that achieves comparable deterrence without the same cost of rights. A regime that scores individuals and utilizes that score into a preventive detention decision, without disclosure or chance for questioning, it is difficult to justify it as necessary when a less intrusive, already applicable alternative exists.

D. Balancing:

A Deprivation Compounded by Opacity The final prong weighs the severity of the intrusion of rights against the security benefit it creates. Preventive detention already represents one of the more severe intrusions permitted by the Constitution, which is the deprivation of liberty without trial, without the ordinary protections of Article 22(1)²⁰ and (2)²¹, justified by suspicion rather than proof.

¹⁹ Simarjeet Singh Satia, *Regulating AI-Based Policing in India: Lessons From the EU AI Act for Surveillance, Accountability, and Investigative Practices*, Atlantis Press (2026).

²⁰ INDIA CONST. art. 22, cls. 1.

²¹ INDIA CONST. art. 22, cls. 2.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Where that detention is substantially informed by an unexplainable assessment generated from biased historical data, the equilibrium is further disrupted towards the state. The purpose of security is uncertain, given the suitability concerns above. This is due to the fact that while the liberty cost is compounded: the detainee faces not only the ordinary difficulty of challenging a preventive-detention order, but also the opacity of an algorithmic input that current law does not require anyone to disclose. A fair balance is difficult to strike when the actual reliability of the algorithmic justification cannot be examined at all.

THE REGULATORY VACUUM

Every condition of the proportionality test above connects to a basic premise: India has no specific laws for regulating the use of artificial intelligence in policing. The Information Technology Act, 2000, and rules made under it were not created keeping in mind algorithmic risk-scoring. The DPDP Act's Section 17²² provides an exemption allowing the state to process personal data for law enforcement with "substantially minimal constraint". This has been noted by commentators as empowering "sweeping immunities" without requirement to demonstrate a "narrowly tailored nexus between the activity granted exemption and its justification for the promotion of national security", which defeats the purpose for which necessity and balancing prongs are created to avoid.

There is a lack of any requirement to test the algorithm for bias prior to deployment, no requirement of algorithm audit trails, and no independent oversight body to oversee AI usage by the police. There is also no clear right of a data principal, whose liberty is being impacted, to know that the outcome of their detention was determined by an algorithm.

²² Digital Personal Data Protection Act, 2023, § 17, No. 22 of 2023, India Code (2023).



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

There is a striking asymmetry here, because, on the one hand, the Constitution imposes a high-four-part standard of proportionality in order to curtail rights, but, the rest of the legal framework has no necessary institutional support, in terms of disclosure obligations, audit mechanisms, challenge mechanisms. There is no procedure to enable the enforcement of the standard against an algorithm. The legal standard of already exists, and is fairly developed. The issue is that there is no clear framework that allows Advisory boards, Courts, or even detainees, to use the test to test or examine algorithmic records.

PRIVACY AND SURVEILLANCE: THE STRUCTURAL BACKDROP

AI based risk-scoring doesn't operates depending on the continuous, often non-consensual collection of data, such as CCTV feeds linked to facial recognition, criminal databases, mobility and movement data, and increasingly cross-referenced state databases. The Puttaswamy Judgement understood informational privacy to be intrinsically linked to dignity and autonomy. Thus, the accumulation of individual data points, even if harmless, into a composite profile as in itself a discrete privacy violation, since this aggregation allows for inferences the individual neither consented to, nor can they readily anticipate its outcomes. A risk-score is essentially a composite profile reduced to a single figure to indicate whether an individual should be under surveillance, questioned or ultimately detained.

The surveillance aspect further complicates the detention question as the surveillance precedes it. The individual has already been exposed to the prior data collection, by the time a risk score is generated. They have no real opportunity to protest it under a legal regime which explicitly excludes law enforcement data processing from the DPDP Act's core consent and purpose-limitation safeguards.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

This we have two primary issues, the surveillance and profiling stage, which is ungoverned, and which in turn leads to an ungoverned trigger stage, with no realistic proportionality review.²³

ALGORITHMIC BIAS AS A CONSTITUTIONAL PROBLEM

The bias present in the policing algorithm, may be considered to be an engineering flaw which may be corrected with more robust training data. However, from a constitutional lens, the primary issue is more about due process and equality than a mere technical error. Article 14, for instance, prohibits the state from taking arbitrary action, and had the requirement for the classifications for have a clear rational nexus to the objective the state wishes to achieve.

When the algorithm is trained, the data may have patterns correlating to communities that have historically been over policed, and hence have more reported offences. This does not mean the communities are more likely to commit an offence, but because the policing has targeted that area. This is a classification which will not receive the threshold constitutional scrutiny on the basis of the rational nexus analysis. This will arise even before addressing the issues of privacy or liberty under Article 21.

This kind of algorithmic classification also has the risk of perpetuating profiling on the basis of caste, religion, geographic location. There are no mechanisms in place to assess the data available or prevent any bias. Privacy, surveillance, and bias concerns reinforce each other. The non transparency of algorithms makes it difficult to challenge decisions taken on their basis. It undermines the reliability of the assessments and the continuous collection of data increases the privacy intrusion. This makes it harder to justify the usage of these algorithmic systems. These

²³ Purushraj Patnaik, *Algorithmic Policing in India: The Case for a Governing Framework*, (May 29, 2026).



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

concerns are not theoretical when applied in a context where predictive systems are being used already.

TOWARD A CONSTITUTIONALLY COMPLIANT FRAMEWORK

A regime that hopes to survive proportionality review, should AI risk-scoring formalise into a detention trigger, would need at minimum:

To implement this system formally in the future, there are certain suggestive requirements which should be brought forth, such as:

- A legal framework, or amendment in the DPDP Act. The AI systems whose output can contribute to decision depriving an individual of liberty must fall under certain regulations, not be exempt. And it must be ensured that the collection of data should be limited to genuine necessity only.
- Any AI risk scoring tool must be mandatorily tested, and go through an assessment for an independent audited bias and accuracy. There must also be regular and publicly available audit trails.
- The detainees must be granted the statutory rights to be informed of the algorithmic assessment, an explanation of its basis and the chance to contest it before an advisory board, as it would fall under Article 22(4).
- A heightened necessity threshold for algorithmically-informed detention specifically, given the availability of less restrictive, already-deployed place-based alternatives that achieve similar deterrence without depriving any individual of liberty.
- Require a higher threshold for AI based preventive detention, due to the availability of less restrictive methods.



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

- An independent oversight authority, analogous to a data protection board but with policing-specific expertise, empowered to suspend a tool's use pending review of demonstrated disparate impact.
- The creation of an independent oversight authority, with the required expertise in policing, to be able to suspend the mechanism in cases of unfair or discriminatory outcomes.

These proposals are similar to already present recommendations and also mirror protections available under comparable regimes such as the GDPR's Article 22²⁴. The absence of the same currently makes AI-triggered preventive detention constitutionally precarious.

CONCLUSION

India's proportionality doctrine, has evolved from Om Kumar from landmarks judgements such as the case of Modern Dental College²⁵, to the Puttaswamy judgement, to Anuradha Basin, all theoretically able to test the probability of a future where algorithms that provide assessments of risk scores formally determine whether preventive detention is the appropriate tool. If applied rigorously, the test would be difficult to satisfy, due to the conditions faltering on biased training data, the lack of disclosure, algorithmic opacity, and the exemptions under the DPDP Act. The deeper issue, however, is not necessarily the failure of not being able to meet the proportionality review. It is the lack of a mechanism by which a review could meaningfully occur. Addressing that regulatory vacuum would be a more pressing constitutional task as the policing infrastructure moves to include a predictive approach.

²⁴ Regulation 2016/679, 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 and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1, 46.