ALGORITHMIC POLICING AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL BLIND SPOT

Swati Singh[*]

ABSTRACT

The growing reliance on algorithmic and data-driven technologies in law enforcement has significantly transformed contemporary policing practices. In India, predictive policing tools, facial recognition systems, and large-scale digital surveillance mechanisms are increasingly deployed to enhance efficiency and prevent crime. However, this rapid technological expansion has largely occurred in the absence of a comprehensive legal framework regulating surveillance practices, accountability mechanisms, and the protection of individual rights. This article critically examines algorithmic policing in India through the lens of the constitutional right to privacy and procedural due process under Article 21 of the Constitution. Drawing upon the principles articulated in Justice K.S. Puttaswamy v Union of India, the paper argues that existing policing practices frequently fail to satisfy the constitutional requirements of legality, necessity, and proportionality. It further highlights concerns relating to opacity, bias, and the gradual erosion of procedural safeguards. By situating algorithmic policing within Indian constitutional jurisprudence and comparative regulatory approaches, the article advocates for a rights-based legal framework to ensure that technological innovation in policing remains consistent with constitutional values.

Keywords: Algorithmic Policing, Right to Privacy, Due Process, Surveillance, Article 21.

INTRODUCTION

Technological advancement has increasingly reshaped the manner in which states exercise their policing powers. Law enforcement agencies across jurisdictions now rely not only on human judgment and conventional investigative techniques but also on algorithmic systems capable of processing vast datasets and generating predictive insights. These technologies are often

[*] LLB, FIRST YEAR, SYMBIOSIS LAW SCHOOL, PUNE.

promoted as tools that enhance efficiency, accuracy, and proactive crime prevention. Nevertheless, their expanding use raises serious concerns relating to personal liberty, accountability, and constitutional governance.

In India, the adoption of algorithmic policing tools has been rapid and predominantly executive-driven. Predictive crime-mapping software, automated facial recognition systems, and integrated criminal databases have become central to modern policing initiatives. While such measures are frequently justified on grounds of public safety and administrative efficiency, they operate within a legal framework that remains insufficiently developed to address their constitutional implications.

The recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v Union of India* marked a watershed moment in Indian constitutional jurisprudence. Despite this development, the deployment of algorithmic tools in policing continues without a clear statutory framework or consistent judicial oversight. This article argues that such practices constitute a constitutional blind spot, wherein technological governance has advanced faster than legal regulation, necessitating closer constitutional scrutiny.

CONCEPTUALISING ALGORITHMIC POLICING

Algorithmic policing refers to the use of automated systems, artificial intelligence, and data analytics to assist or guide law enforcement decision-making. These systems rely on algorithms trained on historical and real-time data to predict crime patterns, identify potential suspects, and allocate policing resources.

In India, algorithmic policing manifests in multiple forms. Predictive policing software is employed to identify crime-prone areas and individuals deemed “high-risk”. Facial recognition technology is used to identify suspects by matching facial data captured through surveillance cameras with existing databases. Additionally, large-scale surveillance mechanisms enable continuous monitoring of public spaces.

Although these technologies are often portrayed as neutral and objective, algorithms are inherently shaped by the quality of data on which they are trained and the assumptions embedded in their design. Biased or incomplete datasets can reinforce existing social prejudices, leading to discriminatory outcomes. Moreover, the opacity surrounding algorithmic decision-making makes it difficult for affected individuals to understand or challenge adverse state action.

THE RIGHT TO PRIVACY UNDER INDIAN CONSTITUTIONAL LAW

The Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v Union of India* conclusively affirmed privacy as an intrinsic component of the right to life and personal liberty under Article 21 of the Constitution.[1]The Court recognised privacy as encompassing bodily integrity, informational self-determination, and decisional autonomy.

Crucially, the judgment laid down a three-fold test to assess the constitutionality of state action infringing privacy:

i. the existence of a valid law;
ii. the pursuit of a legitimate state aim; and
iii. proportionality between the means employed and the objective sought to be achieved.

Algorithmic policing practices in India frequently struggle to satisfy this constitutional threshold. Most deployments are based on executive decisions or internal police guidelines rather than explicit legislative authorisation, raising serious concerns regarding legality. Furthermore, the necessity and proportionality of large-scale data collection and predictive surveillance remain largely unexamined within Indian constitutional jurisprudence.

PRIVACY IMPLICATIONS OF ALGORITHMIC SURVEILLANCE

One of the most significant concerns associated with algorithmic policing is the erosion of informational privacy. These systems depend on extensive data collection, often conducted without adequate notice, consent, or transparency. The aggregation of personal data, including biometric and behavioural information, enables continuous monitoring that intrudes upon private life.

Facial recognition technology illustrates these concerns in a particularly acute manner. The indiscriminate scanning of individuals in public spaces risks transforming citizens into permanent subjects of surveillance, thereby altering the relationship between the individual and the state. Such practices raise serious constitutional concerns under Article 21.

[1] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.

These issues are further compounded by the opacity of algorithmic systems. When policing decisions are informed by complex algorithms whose functioning remains undisclosed, individuals are deprived of the ability to understand or effectively challenge state action. This lack of transparency undermines the constitutional requirement that state power be exercised in an accountable and reviewable manner.

BIAS, DISCRIMINATION, AND EQUALITY CONCERNS

Algorithmic systems are often perceived as neutral and objective. In practice, however, they frequently reproduce and amplify existing biases present in the data on which they are trained. In societies marked by structural inequalities, policing data often reflects patterns of over-policing and discrimination.

In the Indian context, algorithmic policing tools may disproportionately affect marginalised communities that have historically been subjected to heightened surveillance. Predictive models trained on biased data risk reinforcing stereotypes and perpetuating cycles of criminalisation. Such outcomes raise serious concerns under Article 14 of the Constitution, which guarantees equality before the law and prohibits arbitrary state action.

The absence of robust accountability mechanisms exacerbates these concerns. Without transparency requirements, independent audits, and oversight, algorithmic decision-making remains insulated from meaningful scrutiny, undermining constitutional commitments to fairness and non-arbitrariness.

DUE PROCESS AND PROCEDURAL FAIRNESS

The deployment of algorithmic tools in policing also implicates fundamental principles of due process and procedural fairness. Decisions informed by automated systems can significantly affect individual liberty, including surveillance, arrest, and preventive action. However, Indian criminal procedure law has yet to adequately respond to the challenges posed by algorithmic governance.

The Supreme Court in *Maneka Gandhi v Union of India* held that the "procedure established by law" under Article 21 must be just, fair, and reasonable.[2] Algorithmic opacity undermines

[2] Maneka Gandhi v Union of India (1978) 1 SCC 248.

this principle by depriving individuals of the opportunity to understand the basis of adverse decisions or to challenge them effectively.

Further, in *Anuradha Bhasin v Union of India*, the Court emphasised that restrictions on fundamental rights in the digital sphere must satisfy the test of proportionality and be accompanied by procedural safeguards.[3] This reasoning applies with equal force to algorithmic policing practices, which warrant heightened scrutiny due to their intrusive nature.

COMPARATIVE REGULATORY APPROACHES

Several jurisdictions have begun addressing the constitutional challenges posed by algorithmic decision-making. The European Union's General Data Protection Regulation (GDPR) restricts automated decision-making and grants individuals' rights relating to transparency and explanation.[4] Similarly, courts in the United Kingdom have scrutinised the use of facial recognition technology, emphasising the need for clear legal frameworks and safeguards.[5] These comparative developments demonstrate the importance of embedding algorithmic governance within a rights-based legal framework. India can draw valuable lessons from such approaches while tailoring regulatory solutions to its own constitutional context.

THE NEED FOR A RIGHTS-BASED LEGAL FRAMEWORK

The absence of a comprehensive statutory framework governing algorithmic policing represents a significant constitutional gap. While data protection legislation marks progress toward regulating personal data, it does not adequately address the specific challenges posed by law enforcement surveillance and automated decision-making.

There is an urgent need for legislation that clearly defines the scope, limits, and oversight mechanisms applicable to algorithmic policing. Such a framework should mandate transparency, independent audits, data minimisation, and meaningful human oversight. Judicial review must remain central to ensuring that technological innovation does not erode constitutional guarantees.

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

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).

[5] R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.

CONCLUSION

Algorithmic policing represents a profound shift in the exercise of state power. While technological tools may enhance efficiency and crime prevention, their unchecked use poses serious risks to privacy, equality, and due process. In India, the rapid adoption of algorithmic policing has outpaced the development of legal safeguards, creating a constitutional blind spot. The right to privacy and procedural fairness under Article 21 demand that state surveillance practices be subjected to rigorous constitutional scrutiny. Technological progress cannot justify the dilution of fundamental rights. A constitutional democracy must ensure that algorithmic governance operates within clearly defined legal limits grounded in transparency, accountability, and respect for individual liberty.