

## CHAPTER 8

# Digital Surveillance and Predictive Policing: A Rights-Based Analysis in India

Kumari Sudha and Gurminder Kaur

in *Law in Transition: Rights, Sovereignty and Regulation in a Changing World*, edited by Siddharth Saxena and Bhagyashree Agarwal (VidhiAagaz 2026), pp. 85–96

DOI <https://doi.org/10.63108/VAB.LIT.1.8>

---



## CITATIONS

BLUEBOOK (21ST ED.)

Kumari Sudha & Gurminder Kaur, *Digital Surveillance and Predictive Policing: A Rights-Based Analysis in India*, in *LAW IN TRANSITION: RIGHTS, SOVEREIGNTY AND REGULATION IN A CHANGING WORLD* 85 (Siddharth Saxena & Bhagyashree Agarwal eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Kumari Sudha and Gurminder Kaur, ‘Digital Surveillance and Predictive Policing: A Rights-Based Analysis in India’ in Siddharth Saxena and Bhagyashree Agarwal (eds), *Law in Transition: Rights, Sovereignty and Regulation in a Changing World* (VidhiAagaz 2026) 85.

CHICAGO (17TH ED.)

Sudha, Kumari, and Gurminder Kaur. “Digital Surveillance and Predictive Policing: A Rights-Based Analysis in India.” In *Law in Transition: Rights, Sovereignty and Regulation in a Changing World*, edited by Siddharth Saxena and Bhagyashree Agarwal, 85–96. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LIT.1.8>.

APA (7TH ED.)

Sudha, K., & Kaur, G. (2026). Digital surveillance and predictive policing: A rights-based analysis in India. In S. Saxena & B. Agarwal (Eds.), *Law in transition: Rights, sovereignty and regulation in a changing world* (pp. 85–96). VidhiAagaz. <https://doi.org/10.63108/VAB.LIT.1.8>

---

## SOURCE

<https://doi.org/10.63108/VAB.LIT.1.8>

## LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

## CHAPTER 8

# Digital Surveillance and Predictive Policing: A Rights-Based Analysis in India

KUMARI SUDHA\* AND DR. GURMINDER KAUR\*\*

---

*Artificial Intelligence is the advent of the new tech; it's a development in technology which uses algorithms to analyse the data fed to its system in milliseconds. The term predictive policing is not a new concept for law enforcement departments, since many decades the criminal records were used by the police personnel to predict hotspots of crime commission, policing. But, now after the birth of this technology, this method has now transformed into a new name, i.e. AI enabled predictive policing. Now, these tools are helping the law enforcement departments analyse a large number of datasets or criminal records to predict crime. But, in a country like India, which is still developing and is also experimenting with such technologies in such sensitive areas like law enforcement, proper implementation of such technologies becomes a must. Indian policing continues to operate under the colonial-era Police Act, 1861, supported by the Bharatiya Nagarik Suraksha Sanhita (BNSS) and other laws. With growing technological innovations, police agencies increasingly seek AI tools to anticipate, prevent, and analyse crime for improved public safety.*

*The paper explores and examines how such tools that are being used by predictive policing can lead to reinforcement of societal biasness and targeting of marginalised communities which can also lead to reinforcing of historical biasness, ultimately leading to violation of rights guaranteed under the Constitution of India, as such tools have their own drawbacks and can lead to several human rights issues if used unregulated. Through different tables, data and flowcharts this study explains how AI driven tools work in the different countries and how it can be shaped to be used efficiently in the Indian democracy which would also protect the basic rights of the citizens along with technological advancement.*

**Keywords:** Artificial Intelligence, Predictive Policing, AI-surveillance, Civil Liberties, Ethical Policing

## 1 INTRODUCTION

Advent of Artificial Intelligence has defined the world a new era where things could be simpler and quicker. Several sectors like health, education, business, legal etc are adopting the use of Artificial Intelligence. With its positive aspect of analysing a vast amount of data

---

\* Research Scholar at Pondicherry University, Puducherry, India.

\*\* Assistant Professor at School of Law, Pondicherry University, Puducherry, India.

in seconds and giving conclusions based on its data fed and algorithmic analysis, AI has proved itself the need of today's time.

Predictive policing basically means “to anticipate the crimes before occurring”. It mainly predicts “who is to commit crime? and where the crime would be committed?” Police departments use AI tools to predict the crime beforehand and act before happening. And in India, several states like Delhi, Telangana, Uttar Pradesh and Punjab are experimenting with such technologies in law enforcement. Such tools learn their patterns and give social scoring to individuals in society based on their past records and day to day behaviours, regarding how likely they are to commit crime, which signals police departments to keep an eye, and 24\*7 CCTV surveillance systems are also being analysed by police systems for the same.

This research explores and examines how such tools that are being used by predictive policing can lead to reinforcement of societal biasness, societal injustice and targeting of marginalised communities by reinforcing of historical biasness which could lead to violation of fundamental rights guaranteed under the Constitution of India like right to privacy, right to freedom, right to form associations, right of equality, right to fair trial etc. It's high time to discuss the effects of such unregulated AI tools in areas like law enforcement which deals with people every day, and its decision can affect any individual or a society, based on algorithmic decision made by AI tools.

## 1.1 Literature Review

AI Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them

by Catarina Fontes<sup>1</sup>, in the article the author had examined the use of real-time face recognition technology in public settings to discuss the introduction of AI-powered surveillance systems and employ contact tracking applications designed for managing public health in contemporary society. Law enforcement may require population surveillance, but AI-enabled surveillance technologies have the potential to undermine social norms and established order. This does not imply that populations will not be willing to accept the trade-offs or that benefits will not outweigh potential threats; rather, it means that public authorities will have to exercise ever greater responsibility to control their own power as well as the power claimed by tech companies to provide the means for gathering and managing personal data created by daily activities.

---

<sup>1</sup> Catarina Fontes et al., *AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them*, 71 TECH. SOC'Y 102137 (2022).

*Predictive Policing explained by Tim Lau.* In his article he establishes<sup>2</sup> that though predictive policing is very useful and is also giving some positive results in prediction of crimes and places beforehand, but the local communities and the individuals who are being affected by it do not support this technology to predict crimes. It also establishes that these artificial intelligences are being fed on the historical data which is also raising the concern of biasness and which is resulting in unauthorised search and seizure of individuals who are being predicted by these techs and lacking human judgement.

*Legal and human rights issues of AI: Gaps, challenges and vulnerabilities by Rowena Rodrigues, the literature critically argues<sup>3</sup>* about the AI-driven predictive policing and how it poses serious threats to fundamental human rights, mainly the rights to privacy and personal freedom. The study also focuses on the point that predictive systems rely on ongoing data collection, surveillance technologies, and behavioural monitoring, which significantly extends state surveillance into people's private lives. It also discusses the "Black Box" concern with such tools.

*Algorithmic fairness in predictive policing by Ahmed S. Almasoud<sup>4</sup>,* this article analyses the concerns of using AI-enabled predictive policing and answers how these systems are trained on pre-existing datasets as well as learn from pattern analysis and states how such tools can affect or can intrude upon the rights and freedoms of the individuals. These systems limit personal freedom by predicting criminal risk through pre-emptive policing, increased scrutiny, and heightened police presence in targeted communities. In this article it has been argued that data-driven anticipatory governance via the surveillance can weaken consent, and can also risk reduction of freedom of movement, expression, and autonomy, which are fundamental rights in democratic societies.

## 1.2 Research Problem

The development of AI deployment in various sectors of the society has raised various concerns and challenges to regulate such tools in the most ethical and legal manner. Use of such technology in sensitive areas of society makes it important to be regulated within the constitutional framework of India to safeguard the citizens. These technologies operate within legal frameworks that were not designed to regulate algorithmic surveillance or data-driven decision-making, creating uncertainty about their constitutional legitimacy. This study addresses the problem of how predictive policing can be assessed and governed within

---

<sup>2</sup> Tim Lau, *Predictive Policing Explained*, BRENNAN CTR. FOR JUST. (Apr. 1, 2020), <https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained>.

<sup>3</sup> Rowena Rodrigues, *Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities*, 4 J. RESPONSIBLE TECH. 100005 (2020).

<sup>4</sup> Ahmed S. Almasoud & Jamiu Adekunle Idowu, *Algorithmic Fairness in Predictive Policing*, 5 AI & ETHICS 2323 (2025).

existing Indian legal structures without undermining fundamental rights of the minority groups.

### **1.3 Research Objectives**

1. To examine the existing legal and constitutional framework for regulation of AI enabled predictive policing.
2. To analyse the impact of predictive policing on fundamental rights, particularly privacy, personal liberty, and freedom.
3. To critically assess the risks of bias, discrimination, and arbitrariness in algorithmic policing practices.
4. To propose a rights-based regulatory framework for the ethical and constitutional use of predictive policing in India.

### **1.4 Research Questions**

1. What is the current legal and institutional framework to deal with predictive policing in India?
2. How do the predictive policing tools affect the fundamental rights like privacy, freedom and personal liberty guaranteed by the constitution of India?
3. Do AI enabled predictive policing tools lead to bias, discrimination, or arbitrary state action in law enforcement?
4. What legal safeguards and institutional mechanisms are important to ensure that predictive policing operates within constitutional and human rights limits in India?

### **1.5 Methodology**

This research work is based on the doctrinal method. It analyses the primary sources such as legislations – the Constitution of India, the Police Act of 1861, Bharatiya Nagarik Suraksha Sanhita of 2023 – as well as the important relevant judgements on privacy, liberty, and equality. The secondary sources, including scholarly articles, reports, national and international journals and the comparative legal materials, were examined to contextualise AI-driven predictive policing.

## **2 PREDICTIVE POLICING: MEANING AND CONCEPT**

### **2.1 Meaning**

In simple and literal sense “predictive” means “to anticipate” the future based on certain pre-existing data and the term “policing” means “the steps taken by the police to prevent

crime and maintain law and order”. So, the concept of predictive policing has not been formed after the birth of AI, but it pre-existed in the system before even the Artificial Intelligence existed in the tech world. Police used their crime records based on crime history, experience with their human judgement to predict crimes back then, but after the advent of Artificial Intelligence, the prediction and managing as well as analysing these digital data became simplified and has become easier to predict crimes in today’s era.<sup>5</sup>

As in this tech era, the crime records and police records have to the maximum extent been digitalised, and this digital data is being fed to Artificial Intelligence to predict the commission of crimes, which earlier was done by the human judgement. So, from the eyes of today’s advanced system of AI and large database in the policing department we can redefine the term predictive policing as, the forward-looking use of data analysis driven by algorithms to identify trends and correlations within large datasets, on the basis of which assessments of risk are generated for specific individuals or geographic areas and then translated into focused preventive interventions.

## 2.2 Concept and How It Works

Predictive policing uses advanced AI systems to anticipate the future crime hotspots and criminals. The following figure elaborates the different areas where such tools are aimed at while predicting the crimes. The different modes have been laid down:



FIGURE 1. *Modes of AI in predictive policing*

<sup>5</sup> Craig D. Uchida, *Predictive Policing*, in *ENCYCLOPEDIA OF CRIMINOLOGY AND CRIMINAL JUSTICE* 3871 (2014).

### 2.3 How Predictive Policing Works

Below steps have been framed in chart format to understand the way AI tools function in prediction of crimes for the policing.

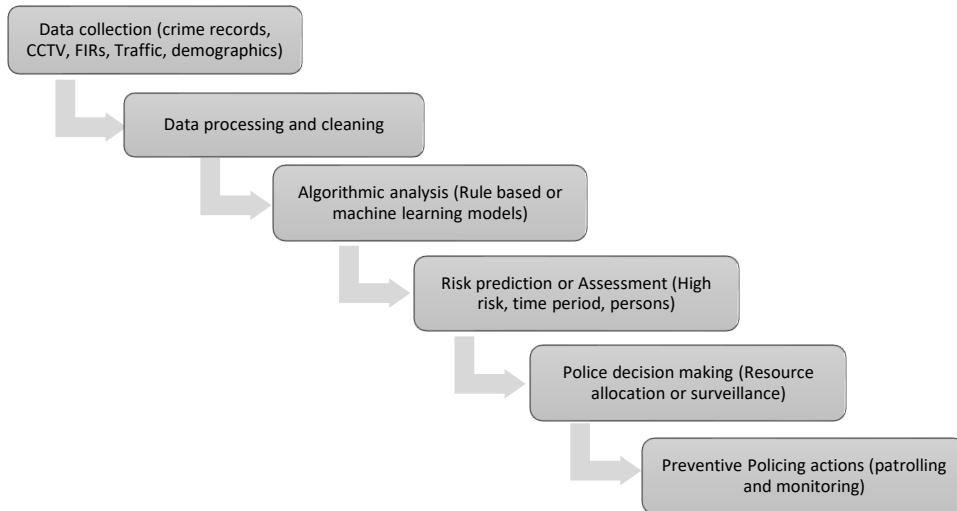


FIGURE 2. *Steps of predictive policing*

### 3 DIGITAL SURVEILLANCE: LAW ENFORCEMENT

With the growth and development of technology and computers, things have started to take a shift that is from pen paper to records in computer. For example, now digital repositories are being stored rather than the large sets piled up case files in court. Evidence recording at crime scene by the police is also being recorded via mobile phones to keep in digital form. Likewise, this shift has escalated after the advent of the artificial intelligence. Now, things are not just kept as record using the systems, but the data kept as digital repositories are now being analysed using AI tools to gain some sort of connection or link, depending on the purpose of the use.

The term digital surveillance refers to monitoring, collecting data and analysing those data via use of any digital device by the government or its representing bodies. In this 21<sup>st</sup> century, it's a way to put an eye on the citizens at public or some private areas too. As far as AI is concerned, its adoption and use have significantly increased in a few years via several areas of the society. And in addition, AI has also helped to provide analytical services. For example, anticipation of crime hotspots via CCTV surveillance. A recent study done by the ESI Thought Lab sponsored by various IT companies, done in 167 cities of the world, found that use of AI can contribute to crime reduction by 30-40%. The study however also

highlights that the cities' law enforcement have started the maximum use of tools like real time crime mapping, CCTV cameras and smart cameras for crowd management etc, for this the personal data of individuals like facial structure, biometric info are being used to about 84%, likewise 55% cities are using the data from body cameras or the in-car cameras, 46% from drones and aerial surveillance and the safety apps trackers are being used for the predictive policing purposes.<sup>6</sup> Via this data it can be concluded that the digital surveillance has spiked the rates of being followed and being mapped by the eyes of the government, and this without the proper law and proper implication can lead to several ethical concerns as well as it also threatens the basic fundamental right of the citizens as stated by the Supreme Court in the famous Justice *K.S. Puttaswamy (Retd.) v. Union of India* judgement, *that the right to privacy is a fundamental right*<sup>7</sup> and it should not be violated by the state at any cost.

#### 4 LEGAL AND INSTITUTIONAL FRAMEWORK OF PREDICTIVE POLICING IN INDIA

In India, predictive policing has started to spread its webs across various states. States like Telangana, Delhi, Tamil Nadu, Uttar Pradesh, Maharashtra have started using AI tools in their policing systems for various purposes and bodies like the Indian Space Research Organization (ISRO) have created the Crime Mapping, Analytics and Predictive System (CMAPS) for the Delhi Police, being one of the most prominent applications regarding predictive policing<sup>8</sup>. CMAPS uses Geographic Information Systems (GIS) and crime data to identify high-incidence areas, support preventive patrols, and deploy resources strategically. Similarly, the Telangana Police have implemented drones, Integrated Command Control Centres, and AI-powered facial recognition systems for surveillance-based policing, especially in Hyderabad.

For example, during the 2020 Delhi riots, Delhi Police used facial recognition software to detain individuals which raised concerns about its validity and the possibility of unjust profiling. Such systems do not have a 100% accuracy rate, which can result in illegal arrest. In this case the digital surveillance affected the fundamental rights of the individual who was anticipated as criminal via the cameras analysis and police prediction.

---

<sup>6</sup> ESI THOUGHTLAB, SMART CITY SOLUTIONS FOR A RISKIER WORLD (2021), <https://thoughtlabgroup.com/wp-content/uploads/2021/03/Smart-City-Solutions-eBook-.pdf>.

<sup>7</sup> (2017) 10 SCC 1.

<sup>8</sup> Vidushi Marda & Shivangi Narayan, *Data in New Delhi's Predictive Policing System*, in PROCEEDINGS OF THE 2020 CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 317 (2020).

#### 4.1 Constitutional Foundation

The Constitution of India gives power to the law enforcement under article 22, exception regarding the preventive detention, but the Supreme Court establishes that such power should not be arbitrary and must be in accordance with the law. Moreover, articles 14, 19 and 21, backed up with the Justice K.S. Puttaswamy (Retd.) v. Union of India judgement, protect citizens from such power<sup>9</sup>.

#### 4.2 Police and Surveillance Laws

Indian policing remains governed by the *Police Act, 1861*, a colonial statute that vests wide and indeterminate powers in the police without incorporating standards of rights protection or accountability, which raises concerns in the use of data being stored by the digital methods as per such outdated law.

Whereas the Information Technology Act, 2000, gives power to the state to intercept, monitor (section 69), block websites (section 69A) and control digital communications under the name of sovereignty, security, and public order. Likewise the Indian Telegraph Act, 1885 allows phone tapping (section 5(2)).

#### 4.3 Criminal Procedural Laws

*Bharatiya Nagarik Suraksha Sanhita, 2023* further provides statutory authority for surveillance, monitoring, and preventive action based on suspicion or apprehended harm. Predictive policing is operationalised through these provisions by substituting human assessment with algorithmic risk profiling. However, the statutory scheme lacks legal standards for data use, transparency, proportionality, or procedural safeguards to test algorithmic outputs. Judgements like *A.K. Roy v. Union of India* (1982) and *State of West Bengal v. Anwar Ali Sarkar* (1952) emphasised the regulation of arbitrary power of the police.

#### 4.4 Data Protection Laws

The newly enacted law, i.e. the Digital Personal Data Protection Act, 2023, protects the personal data of the citizens, but such data can be used by the government in the name of security and public order, which substantially weakens the privacy protection in practice. These carve-outs allow extensive data collection and processing for predictive policing<sup>10</sup> with limited transparency or consent, while core principles like purpose limitation and data minimisation remain weakly enforceable against law enforcement. At the same time, India's

---

<sup>9</sup> (2017) 10 SCC 1.

<sup>10</sup> Matthias Leese, *Staying in Control of Technology: Predictive Policing, Democracy, and Digital Sovereignty*, 31 DEMOCRATIZATION 322 (2024).

surveillance laws, designed for conventional interception methods, fail to regulate algorithmic and large-scale data analysis enabled by predictive policing.

5 IMPACT OF PREDICTIVE POLICING ON FUNDAMENTAL RIGHTS

In the landmark judgement of Justice K.S. Puttaswamy (Retd.) v. Union of India, wherein the Supreme Court unequivocally recognized the right to privacy as an intrinsic facet of the right to life and personal liberty under Article 21, it was keenly observed by Justice D.Y. Chandrachud, that privacy protects the sanctity of personal intimacies, family life, marriage, procreation, domicile, and sexual orientation. So, the unregulated deployment of tools in predictive policing technologies could raise profound constitutional concerns like rights to equality (Articles 14–15), due process (Article 21), and privacy. Moreover, tools trained on biased and incomplete data could lead to more issues for vulnerable groups of the society. Following are points dealt in detail how AI enabled predictive policing impacts the constitutional fundamental freedoms of citizens.<sup>11</sup>

5.1 Judicial Responses and Constitutional Standards

There are various cases which lay down the foundation tone for non-infringement of fundamental rights of the individuals by the honourable Supreme Court of India. Below is laid a table which classifies under five heads describing the rights affected, the impact, related case laws with judgements and lastly their relevance to how the predictive policing is impacting on the fundamental rights protected by the supreme law of India.<sup>12</sup>

TABLE 1. Predictive Policing and Indian Constitution

| Articles under Indian Constitution | Impact by predictive policing              | Case laws                                              | Judgment held                                                           | Relevance                                                               |
|------------------------------------|--------------------------------------------|--------------------------------------------------------|-------------------------------------------------------------------------|-------------------------------------------------------------------------|
| ARTICLE 14                         | Arbitrariness, Biasness and Discrimination | <i>State of West Bengal v. Anwar Ali Sarkar (1952)</i> | Arbitrariness of state action is unethical, legal safeguards are a must | No legal safeguards, lack of laws to regulate predictive police actions |
|                                    |                                            | <i>E.P. Royyappa v. State of Tamil Nadu (1974)</i>     | Arbitrariness is antithesis to equality                                 | AI trained on biased data, inherently arbitrary                         |

<sup>11</sup> Kelly Blount, *Using Artificial Intelligence to Prevent Crime: Implications for Due Process and Criminal Justice*, 39 AI SOC'Y 359 (2024).

<sup>12</sup> Manoj Meena & Aishvarya Joshi, *AI Policing in Criminal Justice: Methods & Concerns in Crime Detection and Prevention in India 2* (2023).

| Articles under Indian Constitution | Impact by predictive policing                            | Case laws                                   | Judgment held                                                                      | Relevance                                                         |
|------------------------------------|----------------------------------------------------------|---------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| ARTICLE 19                         | Right to freedom of Movement, Expression and Association | <i>Kharak Singh v. State of U.P. (1963)</i> | Continuous surveillance impairs personal freedom and movement                      | Continuous surveillance, monitoring free movement                 |
|                                    |                                                          | <i>Anuradha Bhasin v. UOI (2020)</i>        | Restrictions on fundamental freedoms must be necessary, proportionate and reasoned | Preventive and anticipatory policing lacks proportionality        |
| ARTICLE 21                         | Right to Privacy & Personal Liberty                      | <i>AK Roy v. UOI (1982)</i>                 | Preventive powers affecting personal liberty require strict procedural safeguards. | Lack of laws to regulate preventive action of predictive policing |
|                                    |                                                          | <i>KS Puttaswamy v. UOI (2017)</i>          | Laid test of legality, rationality and proportionality                             | Mass data and behavioural prediction fail proportionality test    |

## 6 BALANCING PUBLIC SAFETY AND CONSTITUTIONAL FREEDOMS

### 6.1 Ethical Challenges and Democratic Accountability

As far as ethics in AI is concerned, it's one of its biggest challenges. AI systems work on a concept known as "Black Box", which lacks transparency in its analysis, meaning AI fails to explain how and why it predicted or analyse its conclusion, like prediction of individual as prospective criminal. This drawback of AI systems poses a serious threat when we talk of implementing such technologies in a democratic country like India. Moreover, the lack of proper legal provisions also evolves the challenge of accountability, that if an AI system makes any mistake in recognising or predicting any individual as criminal, then who will be liable for its mistake. This can lead to rise in illegal detentions, unlawful surveillance etc. So, to deal with such issues, it's very important to keep check and balance of technologies with the legal system, so that the proper party responsible could be held liable and accountable as well as to analyse the most important question why such person has been flagged or why not? This could maintain the balance with public safety along with the technological development. Therefore, it is important to critically examine the implications of AI use in policing and development of robust frameworks that prioritise ethical considerations.

## 7 POLICY, LEGAL SUGGESTIONS AND WAY FORWARD

Technology and new systems are inevitable; it's part of growth and development of human nature. So, adoption and use of such tech become part of the process. But, to deal with such tech without hampering the life of people, and without affecting the community, in a way that tech is controlling the behaviours of human, sounds threatening and where it needs an eye on. India lacks proper governance, legal provisions or rules to deal with such technologies when they make any mistake. AI systems work on codes, they analyse and conclude what is fed to them via the codes, so they lack accountability, but if it analyses wrong who should be held liable. Along with this issue several ethical concerns are lined up which needs proper lawful governance, to save the fundamental rights of the citizens. This can pose a big threat on vulnerable communities like women, children, poor people, transgenders etc.

### 7.1 Policy Recommendations for Urban Policing Systems

AI enabled predictive policing in India is growing rapidly, and artificial intelligence is still in its infancy, which means in the long run or coming future, AI will be more advanced and developed. So, with its growth and application in sectors like law enforcement which directly deals with public and individuals and are bound by law to protect their rights, it becomes a must to work under the purview of legal safeguards, for which following recommendations are given to be included for making laws or acts or reforms in AI acts of India or amending present acts in this regard:

1. Inclusion of public in policy development
2. Rights-centric laws should be enabled
3. Comprehensive laws on AI for law enforcement
4. Independent regulating bodies
5. Statutory authorisation and defined scope
6. Non-discrimination and bias mitigation
7. Institutional preparedness and ethical training
8. Continuous evaluation and temporal limits

## 8 CONCLUSION

In India various artificial intelligence tools are being used by various states for the various purposes. India is accepting the transformation from documentation age to digital age, but the development of AI tools and technology not backed up by law raises serious ethical concerns which could lead to violation of the fundamental rights guaranteed to the citizens.

This paper addressed that the growth of artificial intelligence is inevitable, as well as the development and deployment of technologies as such, especially in sensitive domains like law enforcement, which directly deal with the citizens' rights and freedoms be completely prevented. However, in a democratic country like India digital surveillance must come with accountability and transparency and imposing liability in instances of misuse or adverse consequences. This paper clearly analyses via various important judgements and legal regulations and establishes an interrelationship between artificial intelligence and the fundamental rights, implying the potential infringement upon the rights guaranteed under the constitution and moreover the lack of laws to deal with such consequences. It raises several constitutional concerns like arbitrariness, chilling effect on the freedom and privacy etc. Therefore, the need of clear, specific and robust safeguards is the need of the hour now, which must be technology specific and answers the concerns of ethics, transparency and accountability. Therefore, this paper contributes with policy legal suggestions to deal with this concern in coming future by laying down the roadmap and policy recommendations like inclusion of public, enabling a rights-based legal framework, appointing independent multidisciplinary bodies etc, to deal with the concerns and challenges that such system comes with.

However, this paper also identifies a significant gap between the data currently stored in digital repositories and the way such data is used by institutional bodies to train artificial intelligence systems, particularly concerning its relevance to individuals and its future use. Moreover, the issue of the right to be forgotten becomes especially significant in this context, as the continued use of digitally stored data for training AI systems risks preserving an individual's identity indefinitely on digital platforms.

\* \* \*