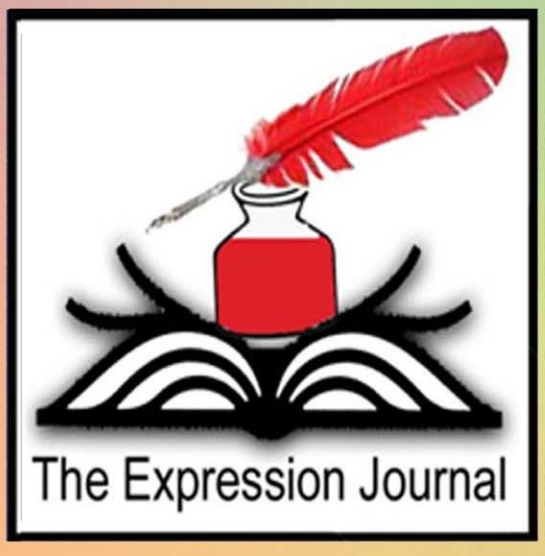
ISSN : 2395-4132

THE EXPRESSION

An International Multidisciplinary e-Journal

Bimonthly Refereed & Indexed Open Access e-Journal



Impact Factor 6.4

Vol. 11 Issue 4 August 2025

Editor-in-Chief : Dr. Bijender Singh

Email : editor@expressionjournal.com

www.expressionjournal.com

The Expression: An International Multidisciplinary e-Journal
(A Peer Reviewed and Indexed Journal with Impact Factor 6.4)
www.expressionjournal.com ISSN: 2395-4132

Facial Recognition and AI Surveillance in Law Enforcement: Privacy Concerns and Regulatory Challenges

Mr. Parag Sharma
Research Scholar
Faculty of Law, Tantia University, Sriganganagar
Dr. Saurabh Garg
Research Supervisor
Faculty of Law, Tantia University, Sriganganagar

Abstract

The fast rate of artificial intelligence development allowed policing firms across the globe to implement the face recognition software and other AI-based monitoring devices to prevent crime and investigate criminal cases, as well as to handle their population and provide them with safety. This converts to the potential costs of such technologies, including the potential of identification of suspects at a much higher rate, but at the same time, concerns of privacy, data protection and the possibility of abuse are also high. Devoid of this strong legal protection the use of AI-facilitated surveillance will cause mass surveillance of people, mis-identification and over- identification of the minorities. This paper explores technological capacity to utilize facial recognition and AI surveillance within the domain of law enforcement, and how it can be used in reference to its ramification of a core right and in a democratic form of governance. It emphasizes the privacy and ethical dangers of such systems, locates the loopholes of the current regulatory frameworks, as well as considers the worldwide methods of regulating AI surveillance. Based on these lessons, this paper provides policy suggestions on achieved by India based on her legal and socio-political experiences, where technology innovativeness and civil liberties protection are to be strike a balance.

Keywords

Facial Recognition, AI Surveillance, Law Enforcement, Privacy Rights, Algorithmic Bias, Regulatory Challenges, Data Protection.

The Expression: An International Multidisciplinary e-Journal
(A Peer Reviewed and Indexed Journal with Impact Factor 6.4)
www.expressionjournal.com ISSN: 2395-4132

Facial Recognition and AI Surveillance in Law Enforcement: Privacy Concerns and Regulatory Challenges

Mr. Parag Sharma
Research Scholar
Faculty of Law, Tantia University, Sriganganagar
Dr. Saurabh Garg
Research Supervisor
Faculty of Law, Tantia University, Sriganganagar

1. Introduction

The past couple of years have seen adoption of artificial intelligence in police work making criminal surveillance, detection and investigations and various police duties to be conducted in new manners. The facial recognition is among the most important of these technologies that may be based on biometric data processing images or video feeds and name the people.[1] Facial recognition, when paired with larger AI-based surveillance infrastructures, including automated number plate recognition, light learning policing analytics, and real-time crowd analytics, will provide any law enforcement agency the ability to track movements and scale behaviour to a degree never seen before.

Such popularity of these tools is not unreasonable: it can be beneficial to expedite the work on suspect identification, simplify the process of searching those individuals who have vanished, and increase the level of security within the hazardous areas. Governments often promote them as multipliers of force which is able to increase the safety of individuals besides reducing the human controlled activities. They are the same traits, which make AI surveillance effective, but controversial at the same time.[2] The capability to monitor the movement of a serial population at the time, capture and cross-match materials, and put them in place without either understanding or approval of the individuals cast somewhat apprehensions on the privacy, proportionality and responsibility elements.

The opponents draw a parallel and warn that AI surveillance will result in a sort of a universal surveillance that annulment of the ideas of democracy without keeping a close eye. Algorithms: It is not just the threat to misidentify a person who has not done

[1] Daniel J. Solove, *Understanding Privacy* 52 (Harvard University Press, Cambridge, 2008)
[2] Mark Andrejevic, 'The Work of Watching One Another: Lateral Surveillance, Risk, and Governance' 2 Surveillance & Society 479 (2005).

an offense, marginalisation, or an attempt to predict individuals, but has been documented being used in various jurisdictions. Through these abuses, there was a need to enact far-reaching and stringent laws that would control the use of biometric information, access, and storage, besides safeguarding their fundamental rights.[3]

There has been an increasingly better growth in the facial recognition program in India, such as the programs that actually identify with law enforcement, stations security in even the crowd management before enacting a law to bind themselves. This creates a gap on governance whereby technology is more sophisticated than what the law governs about and which there comes in a question of unregulated monitoring and violation of the constitutional assurance, especially, that of privacy as famed in Justice K.S. Puttaswamy (Retd.). v. Union of India (2017).[4] To ensure that the innovation is aimed at the benefit of the community (but not the infringement of the civil liberties), one would have to know how this technology functions, the risks it poses and systems which may be used so that to regulate it.

2. Objectives of the Study

This study aims to critically examine the deployment of facial recognition and AI-based surveillance tools by law enforcement agencies, with a focus on their technological, legal, and ethical dimensions. The specific objectives are:

1. To analyse how facial recognition and AI surveillance technology's function and are being applied in law enforcement contexts in India and globally.
2. To identify and evaluate the privacy, ethical, and human rights concerns associated with the use of such technologies.
3. To assess existing regulatory frameworks and explore policy options for creating a balanced legal structure that protects civil liberties while enabling legitimate law enforcement objectives.

3. Facial Recognition and AI Surveillance: Technology and Use in Law Enforcement

One such component of biometric identification technology, the lucidity of which is known as a faceprint, is the facial recognition technology (FRT), which identifies the facial appearance of a person (distinct facial features such as distance between eyes, jawline shape, skin texture) and creates a digital representation of that picture. This face print is then compared with those stored in databases that maybe have mugshot, which can hold ID photos produced by the government or even photos scraped on the internet which is geared towards holding all form of information that can lead to the identification of a person.[5] In combination with artificial intelligence, FRT will be able to process massive amounts of data regardless of time, which significantly expands the sphere and influences the work in the criminal justice system.

The current AI surveillance systems such as that of a spouse are likely to be a mixture of a facial recognition program together with social intelligence to other data collection programs, such as a closed-circuit television (CCTV) system, body-mounted police cameras, automatic number plate recognition (ANPR), and analytics software

[3] Ian Kerr, 'Prediction, Preemption, Presumption: How Big Data Threatens Informational Privacy' 57 Stanford Law Review Online 65 (2014).
[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[5] Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* 14 (Georgetown Law Center on Privacy & Technology, Washington D.C., 2016).

(crowd analytics).[6] The combination of such systems is able to trace people over two or more places, and deconstruct the patterns of movement, and even label suspicious conducts as per the predictive algorithms. The advanced level of such tools enables the law enforcing setups to transcend post event analysis in proactive monitoring and preventive policing.

Table 1: Common AI Surveillance Tools and Their Law Enforcement Applications

Technology / Tool	Primary Function	Law Enforcement Applications	Example Deployments
Facial Recognition (FRT)	Identifies individuals by matching facial features against databases	Locating suspects, missing persons, watchlist screening	NCRB's AFRS in India; UK's live FRT trials
Automatic Number Plate Recognition (ANPR)	Reads and stores vehicle licence plate data	Tracking stolen vehicles, enforcing traffic violations, movement analysis	Delhi Traffic Police ANPR systems; U.S. city-wide ANPR grids
CCTV with AI Video Analytics	Real-time monitoring with motion detection, crowd analysis	Detecting suspicious activity, crowd management, perimeter security	Chinese "Skynet" system; Indian smart city projects
Body-Worn Cameras with AI	Records police interactions with AI-enabled evidence tagging	Accountability, evidence gathering, use-of-force monitoring	U.S. police departments; pilot programs in Indian metros
Predictive Policing Algorithms	Uses data patterns to forecast crime-prone locations	Resource allocation, hotspot policing	PredPol in U.S.; initial trials in UK police forces

Facial recognition in India in India, deployment of facial recognition has grown by a rate in the last 5 years. Other projects such as the Automated Facial Recognition System (AFRS), which was launched by the National Crime Records Bureau (NCRB) in its efforts to streamline the state and national databases in order to help it detect criminals, find missing persons, and strengthen border security. To capture the attention of the citizens of multiple states, AI-based video analytics to control the crowds has been implemented in major events such as political rallies and religious festivals. As an illustration, passengers in airports, metro stations, and other communities have been monitored using facial recognition to identify those on the list of watchlist in real-time.[7]

The AI surveillance by the law enforcement has been even larger in the world sense. In the UK, Metropolitan Police has piloted facial recognition in the street, and China has installed an extensive system of AI-based surveillance auditing the actions of

[6] Anil K. Jain, Arun Ross & Karthik Nandakumar, *Introduction to Biometrics* 44 (Springer, New York, 2011).
[7] National Crime Records Bureau, *Request for Proposal for Selection of System Integrator for Implementation of National Automated Facial Recognition System (AFRS)* (New Delhi, 2019) https://ncrb.gov.in (last visited on 14 September 2025).

millions of its citizens. Its application started as it was widely used by the federal and local governments in the US, but it has faced opposition in the court over privacy and civil rights.[8]

Although new technologies unquestionably increase the ability to investigate, their implementation is not accompanied by the stringent statutory regulation of their application, which involves the risk of authority. The AI surveillance has not been regulated and no guidelines on how and when it should apply compromise the distinctions between law enforcement and mass surveillance. This necessitates looking into the related privacy, ethical, and regulatory issues prior to such systems becoming well embedded within the structure of policing.

4. Privacy, Ethical, and Regulatory Challenges

The introduction of the use of facial recognition and AI surveillance by law enforcement entails with it a number of issues beyond technology itself. These issues access the primary human rights, democratic values, and principles of government. The risks would be more than the desired benefits unless there are explicit laws and protection measures in place.

4.1 Infringement on the Right to Privacy

Facial recognition mechanism works by gathering, procedure and retention of biometric codes or information, which is very personal and non-alterable. Supreme Court, India in India, this case was judged by a Supreme Court Justice K.S. Puttaswamy (Retd.). v. In the case of Union of India (2017),[9] privacy has been reiterated as a fundamental right alongside the state being placed with numerous obligations whereby the infringement must be done in a proportionate and necessary manner. Nevertheless, the fact that FRT based large-scale gathering of biometric data without a specific law on data protection does not imply that resembling a panopticon can be established with no significant checks and balances.

4.2 Risk of Mass Surveillance

All types of AI surveillance can be used together with large, interlinked CCTV systems and central databases and virtually trace individual people around the clock. Although this feature is handy as far as it relates to security in specific events, it may result in lawful surveillance of population groups at any given time. There is a danger that these practices might lead to a free expression and assembly of people because of the fear of being accused of surveillance hence expectancies in fear they reduce freedom of expression, assembly and other democratic activities.[10]

4.3 Algorithmic Bias and Wrongful Identification

Experiments across various jurisdictions have depicted that women, children, and persons with dark skin tones could have greater errors compared to facial recognition algorithms. These prejudices may cause wrong identifications hence letting to undeserved arrests or bullying. Such mistakes are especially harmful in the framework of law enforcement due to causing a loss of trust by the public and placing the agencies in the legal position.[11]

---

[8] Rogier Creemers, *China's Social Credit System and its Implications* (Leiden Asia Centre Report, 2018).
[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[10] David Lyon, *Surveillance after Snowden* 73 (Polity Press, Cambridge, 2015)
[11] Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* 54 (Polity Press, Cambridge, 2019).

4.4 Data Security and Misuse Risks

The success of the use of AI surveillance is predetermined by huge databases with sensitive biometric and individual data. In case such databases are hacked, compromised or misused, the damage is permanent- biometric identifiers have no passwords to switch. Lack of good cybersecurity or insider threats may facilitate unauthorised access to extremely sensitive data.[12]

4.5 Regulatory Gaps and Legal Uncertainty

Although India has sectoral rules and guidelines that address technology use, it does not have an overall legal framework that address the collection as well as the processing within storage and deletion of biometric data that fintech form use in any bid to execute law enforcement duties. The protection of the current laws like the Information Technology Act, 2000, and the rules is limited. There are important questions that this legal gap does not answer: What is the maximum time of data storage? Who has access to it? What is the option of people mistakenly identified?[13]

All these issues cumulatively demonstrate that the safeguarding of the right to facial recognition and AI-driven surveillance lacks effective legal support without the appropriate checks and balances and follows the principles of necessity and proportionality, thus introducing a risk of contravening the democratic values these ideas are supposed to be preserving. These are not the issues dominated by the technical regulation, but the issue of secure technological advancement in accordance with the constitutional right and the rule of law.[14]

5. Global Approaches and Policy Lessons for India

The use of facial recognition and AI surveillance has drawn many worldwide stakeholders and countries have taken different regulatory frameworks. The analysis of these methods would be very useful in formulating a legal system within India.

Table 1: Snapshot of Global Facial Recognition Regulations

Jurisdiction	Notable Facts	Regulatory Emphasis
European Union	Proposed AI Act treats real-time public facial recognition as "high-risk"	Rights-based safeguards and strict authorisation
United States	Over 20 cities have enacted bans or moratoriums	Local governance and community consent
United Kingdom	Landmark *Bridges* case shaped proportionality standards	Judicial oversight and public trials
China	Largest integrated AI surveillance network globally	Security-first approach with minimal privacy focus

5.1 European Union – Strict Data Protection and Proactive Regulation

The European Union (EU) enforces the General Data Protection Regulation (GRD), where the processing of biometric data is defined as a potentially damaging category of the information, except in the strictly defined reasons of general interest. The literature in the proposed AI Act places a higher step forward, and that of real-time

[12] Ministry of Electronics and Information Technology, *Report of the Committee of Experts on Data Protection Framework for India* (New Delhi, 2018).
[13] Information Technology Act, 2000.
[14] Srikrishna Committee Report, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (New Delhi, 2018).

remote biometric identification in the open areas will be considered a high-risk application category, closely authorised and having disclosure standards.[15]
India lesson: Prejudice facial recognition in a rights-based information security policy, need, and proportionality should be confirmed before admitting of enormous implementations.

5.2 United States – Fragmented but Growing Local Restrictions

The U.S has no federal facial recognition law, but many states and cities like San Francisco, Boston or Portland have banned its use in law enforcement. Others such as Washington State have developed oversight requirements such as public reporting and legislative approval of some deployments.[16]
Lesson to India: As much as national laws are necessary, local bodies should have the power to examine and give permissions on surveillance projects: this would increase accountability and make the rules responsive to local circumstances.

5.3 United Kingdom – Judicial Oversight and Public Trials

The Surveillance Camera Code of Practice regulates the activities of using surveillance systems within the UK and all the measures are to be introduced to the human rights laws and the principles of data protection. Face recognition in real time has undergone court and regulator testing, and there is case law - e.g. Bridges v. South Wales Police- defining what's required to be legality, transparency and proportional.[17]
Indian educational point: The court system, along with the pilot projects, can allow experimenting with the accuracy of the technology, its anti-bias, and its adherence to requirements through a controlled environment and test before principles can be applied on enormous scales.

5.4 China – Expansive Deployment with Minimal Privacy Protections

China has one of the greatest AI surveillance networks globally and in policies involving the city management, law enforcement, and even access to services like education, the use of facial recognition is encompassed. There is a tolerance of regulations on technical norms more than on privacy rights and this demonstrates the security-first strategy.[18]
Lesson to India: The Chinese experience illustrates that taking too little rights protection despite its focus on security can too often be risky, and it should recall the need to incorporate civil liberties into the legal system early on.

6. Policy Recommendations for India

- Introduce Comprehensive Biometric Data Protection Legislation - present specific legislation that spells out biometric data, controlling its gathering, keeping, sharing and destruction alongside the clear demonstration of necessity and proportionate requirement.
- Form an Independent Oversight Mechanism - Have an independent regulation institution that has powers to get approval, audit, and investigation of any facial

[15] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679 of the European Parliament and of the Council (Brussels, 2016).
[16] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (Georgetown Law Center on Privacy & Technology, Washington D.C., 2019).
[17] *Bridges v. South Wales Police*, [2020] EWCA Civ 1058.
[18] Samm Sacks, 'China's Emerging Data Privacy System and GDPR' 8 Cybersecurity and Data Privacy Review 67 (2019).

recognition use by the law enforcement and also provide a transparent update on the same to the people at the end of the year.

- Assessing Mandate Accuracy, Bias, and Impact - Demand pre-deployment audits of demographic bias, algorithmic error rates, and impact on the civil liberties in general and publicly publish the results.
- Minimize Scope of Deployment - Limit the extent of application of facial recognition to specific high-risk contexts, like counter-terrorism and finding lost individuals, and do not allow mass surveillance of people in crowd areas.
- Adequately Provide Public Accountability and Remedies - Entitle the citizens to the right to view, rectify, and request the deletion of their biometric information, and a well-developed framework of complaining and restorative actions of wrongful identification or misuse.

7. Conclusion

Surveillance and facial recognition in line with law enforcement has indeed pushed the boundaries of policing as well as provide some capability of identification, tracking and predictive analysis unlike any other time. This paper has shown that, despite the idea that the technologies can enhance security and efficiency in the investigation process, there are severe threats to it regarding personal privacy, civic liberties and stability of the institutes. A mixture of long reports of the biometers, combined with real-time surveillance systems, without there being a restriction of them legislatively, perhaps would generate the type of atmosphere that individuals would be patrolled against to the concern of violation of even the freedoms that the law enforcement is meant to protect. The attempted trend of speedy deployment such systems has been regarded to occur in Indian of a full law on biometric protection and has also sparked fears over how such systems may be abused, the lack of transparency and the event of how such systems utilization can be catastrophically institutionalized.

The global history reveals that the balance between the security commitments and lawful justice of individuals is colossally orchestrated in accordance with robust legal processes, autonomous governance and liable responsibility processes. Rights-based approach has already been demonstrated as one worth pursuing jurisdictions like the European Union have stipulated strict limitations on biometric processing, and placed limitation on each use that should be reasoned. On the other hand, the experience of the lack of or minimal numbers of privacy regulations in specific nations demonstrates the lethality of uncontrollable surveillance, instances of lawful seizure, to the extent of whole-scale profiling of susceptible groupings. The lessons in the case of India will offer the pressing need of adoption of technology in a regulatory ecosystem where there must be justification of a need, proportion and public good. That is not the way to do it will lead to the risk of not only the insult to civil liberties but even the confidence of people- the trusted authority of law enforcing agencies.

In the future, India is a transitional country. The current actions are going to stipulate further destiny of AI surveillance as a highly specialized projectile VIB dedicated to the enhancement of security, or the state suppression apparatus. The policymakers need to take the radical step to present the ambiguation legislations, the independence of the appointed commissioners and verification of accuracy and bias prior to the usability of the commissions. This must incorporate popular knowledge and their consultation with the stakeholders, in which case the regulations would be upheld

by social values as subjective but by the realities of the technology being technologically enacted. With a focus on a form of governance that is rooted in transparency, accountability, and a commitment to the constitutional rights, India can stand the flaws of facial recognition and AI-driven policing and uphold the principle of freedom, privacy, and equality served within the model of a democratic system used in India.