

STATE SURVEILLANCE IN INDIA AFTER PUTTASWAMY: EVALUATING LEGALITY, PROPORTIONALITY, AND JUDICIAL OVERSIGHT

¹Akanksha Tripathi, ²Dharm Kumar Shivani, ³Bhawna

¹Student, ²Student, ³Student

¹Law,

¹Guru Gobind Singh Indraprastha University, New Delhi, India

ABSTRACT

The recognition of privacy as a fundamental right in *Justice KS Puttaswamy (Retd) v Union of India* transformed The Constitutional analysis of state surveillance in India. The judgment requires privacy restrictive state action to be authorized by law, directed towards a legitimate objective, necessary in the circumstances and proportionate, while remaining subject to procedural safeguards. This article examines whether India's surveillance framework satisfies those requirements. It analyses communications interception, the Central Monitoring System, NETRA, Aadhar and biometric identification, facial recognition and predictive policing technologies, DNA databases, spyware, and public health applications. It also evaluates The Indian Telegraph Act 1885, The Information technology Act 2000, The Information Technology Rules 2021, the Digital Personal Data Protection Act 2023, the Telecommunications Act 2023 and The Criminal Procedure (Identification) Act 2022. The central argument is that India's surveillance architecture remains fragmented and predominantly executive controlled. The existence of statutory powers does not, by itself, establish constitutional validity; the quality of the law, the specificity of the purpose, the necessity of the measure, independent review, notice and remedy remain decisive. The article recommends a comprehensive surveillance statute, prior judicial authorisation for minimisation standard, and an exclusionary remedy for evidence obtained through unconstitutional surveillance.

INDEX TERMS

State Surveillance, Privacy, Puttaswamy, Proportionality, Article14, Article19, Article21, Oversight, Interception, Artificial Intelligence, Aadhaar, Digital Personal Data Protection Act 2023.

1. INTRODUCTION

The digitalisation of surveillance has changed both how large and how it works. Earlier surveillance usually meant a telephone tap, a physical look or a specific search. Modern systems can mix telephone data, identity details, location trails, biometric marks, facial pictures and computer guesses. The Constitutional question is now more than whether a single conversation was tapped. It also asks whether the state can build and analyse data systems that keep people always known and sorted.

The main constitutional basis for looking at these practices comes from the Supreme Court's case *Justice KS Puttaswamy (Retd) v Union of India* known as 'Puttaswamy'. In that case nine judges said that privacy is a right, that The Constitution protects because it comes from promises of dignity, freedom and liberty in Part III. The Court said that privacy is not a common law interest or a small personal choice. It put control over the information; the right to decide for oneself, bodily safety and protection of space inside The Constitution.

After Puttaswamy the issue is not that there are no rules, but that those rules are not applied evenly in how India works. The system is spread over the Telegraph Act, The Information Technology Act rules made by delegation, executive orders, sector laws, identity systems and new data governance laws. Arun calls this communications surveillance system that is a 'mosaic of dovetailing laws. The split makes it hard to find out which body allows a type of watch, which body checks it how long data can stay and what help people can get after a mistake.

The paper looks at that system with four questions. First, does the action have a legal base? Second, does it aim at a public goal? Third, is it balanced instead of just convenient? Fourth, are there safeguards before during and after surveillance? The paper says the biggest problem is the question. When the executive checks and keeps things secret, the body that authorises surveillance can stay too close to the body that uses it. This is hard to match with responsibility especially when surveillance touches political speech, news work, legal help, group activities or minority groups.

2. LITERATURE REVIEW

S. No	Authors	Year	Purpose/Aim	Methodology/Research Method	Major Findings	Policy Implications
1	P. Joshi and Y. Wamankar	2025	To analyse algorithmic policing in cybercrime investigations	Doctrinal and constitutional legal analysis of algorithmic policing practices, judicial standards and	Algorithmic policing can improve investigation efficiency but may create risks of arbitrariness, bias,	Police use of automated tools should require transparency, human oversight, non-

			through Articles 14, 19 and 21 of the Indian Constitution.	fundamental-rights principles.	opacity and violation of due process unless constrained by constitutional safeguards.	discrimination safeguards, auditability and proportionate legal authorisation.
2	A. Verma, B. Mittal and A. Bala	2025	To examine legal challenges to privacy arising from artificial intelligence-enabled surveillance.	Doctrinal and analytical review of AI surveillance technologies, Indian privacy jurisprudence and data-protection law.	AI surveillance intensifies privacy risks through large-scale collection, profiling and automated decision-making; existing legal safeguards may be inadequate for emerging technologies.	India needs technology-specific safeguards, purpose limitation, data minimisation, impact assessments, accountability mechanisms and independent oversight for AI surveillance.
3	R. Matthan	2020	To assess the privacy implications of data technologies during the COVID-19 pandemic.	Conceptual and legal analysis of pandemic data technologies, privacy principles and public-health data governance.	Data technologies can support epidemic response, but their privacy impact depends on purpose limitation, data minimisation, consent, transparency and safeguards against function creep.	Pandemic data systems should be temporary, transparent, minimally intrusive, securely governed and subject to sunset clauses and independent review.
4	M. A. Dar and S. A. Wani	2022	To study personal-data protection and privacy concerns arising from COVID-19 responses in India.	Doctrinal analysis of COVID-19 data practices, Indian constitutional privacy law and data-protection frameworks.	COVID-19 measures expanded state access to personal data, exposing gaps in India's data-protection framework and creating risks of excessive surveillance and weak accountability.	A robust data-protection law is needed with clear limits on state access, independent oversight, transparency, security obligations and remedies for data misuse.
5	A. Dhindsa and S. Kaushik	2020	To evaluate whether Aarogya Setu complies with constitutional privacy requirements.	Constitutional and legal analysis of the Aarogya Setu application, its data practices and the Puttaswamy proportionality test.	The app raised concerns regarding voluntariness, consent, data collection, storage, purpose limitation, transparency and the absence of a comprehensive data-protection law.	Government health applications should be voluntary, transparent, privacy-preserving, data-minimised, independently audited and supported by clear legal safeguards.
6	N. Saroj	2026	To examine judicial interpretations of privacy in Indian criminal investigations and trial procedures.	Doctrinal analysis of judicial decisions on privacy, criminal investigation and trial procedure.	Indian courts recognise privacy as a constitutional right, but its protection in criminal proceedings must be balanced against investigative needs, public interest and fair-trial requirements.	Criminal-justice rules should define clear limits on searches, surveillance, evidence collection and disclosure, while preserving due process and judicial oversight.
7	R. Chandran	2024	To assess whether collection of DNA and creation of DNA databases in India violate genetic privacy under a proportionality analysis.	Doctrinal and proportionality-based legal analysis of DNA collection, database creation and constitutional privacy standards.	DNA databases can serve legitimate investigative aims, but broad collection and retention may disproportionately infringe genetic privacy without adequate safeguards.	DNA legislation should adopt narrow purposes, informed consent where appropriate, strict retention limits, security controls, independent oversight and remedies for misuse.

8	V. Bhandari and K. Lahiri	2020	To explore the future of privacy and criminal investigation in India after Puttaswamy.	Doctrinal and forward-looking constitutional analysis of surveillance powers, criminal procedure and privacy jurisprudence.	Puttaswamy provides a constitutional basis to challenge intrusive investigative technologies, but Indian law still lacks detailed procedural and technological safeguards.	India should modernise surveillance and criminal-procedure law through statutory authorisation, judicial oversight, transparency, data-retention limits and effective remedies.
9	G. Bhatia	2015	To provide a constitutional biography of state surveillance and the right to privacy in India.	Historical-doctrinal analysis of constitutional text, case law and state surveillance practices.	Indian privacy jurisprudence developed unevenly, with limited early protection against surveillance; constitutional interpretation has gradually strengthened privacy protections.	Surveillance powers require clearer constitutional and statutory limits, judicial safeguards, proportionality analysis and stronger privacy protections.
10	A. Dixit	2026	To critically evaluate privacy and state power under India's Digital Personal Data Protection Act, 2023.	Doctrinal and critical legal evaluation of the DPDP Act, its exemptions and implications for state data processing.	The DPDP Act advances a rights-based framework but grants the state broad exemptions that may weaken privacy protection and accountability.	The Act should be implemented with narrow interpretation of state exemptions, strong oversight, transparency, grievance redressal and safeguards against excessive government access.
11	S. Rohit	2025	To critically appraise whether the Digital Personal Data Protection Act, 2023 protects privacy or expands state control.	Doctrinal and critical legal analysis of the DPDP Act's provisions, exemptions and enforcement structure.	The Act introduces important data-protection duties, but its broad government exemptions, limited independence and weak remedies may privilege state interests over individual privacy.	Policy reform should reduce broad exemptions, strengthen the Data Protection Board's independence, improve transparency and provide stronger remedies for violations.
12	G. Nojeim, N. Maheshwari and E. Miglani	2020	To examine the role of encryption in protecting privacy, free expression, security and economic growth in India.	Policy-oriented legal and technical analysis of encryption, government access demands and digital-rights implications.	Encryption is essential for online privacy, expression, cybersecurity and digital commerce; weakening it through mandated access would create security and rights risks.	India should avoid encryption-weakening mandates and instead adopt policies that preserve strong encryption while addressing lawful-access needs through targeted, rights-respecting processes.
13	Sahil and S. Jeet	2025	To analyse predictive policing and AI surveillance in India under the DPDP Act, 2023.	Doctrinal legal analysis of predictive policing, AI surveillance, privacy rights and the DPDP Act.	Predictive policing and AI surveillance can reinforce bias and disproportionate monitoring unless governed by data-protection principles, transparency and human oversight.	AI-based policing should require lawful basis, purpose limitation, bias audits, explainability, human review, data minimisation and independent oversight.
14	P. Agrawal, A. Singh, M. Raghavan, S. Sharma	2020	To propose an operational architecture for embedding privacy by design	Technical architecture design and conceptual framework analysis for privacy-preserving public-service systems.	Privacy-by-design can be operationalised through data minimisation, purpose binding, access controls, consent	Public digital services should adopt privacy-by-design architectures, privacy impact assessments, secure defaults,

and S. Banerjee	in public-service applications.	management, auditability and secure data lifecycle management.	limited data retention and transparent user controls.
-----------------	---------------------------------	--	---

3. RESEARCH GAP

Existing research gives a lot of analysis on privacy, Aadhaar, interception, data protection and artificial intelligence. The main gap is that these topics are not combined into one analysis of post Puttaswamy surveillance. Tech specific studies may ignore the foundation of the system while legal studies may ignore algorithmic bias, retention or evidence use. This article fills that gap by applying legality legitimate aim, necessity, proportionality and procedural safeguards to surveillance technologies and legal rules.

4. RESEARCH QUESTIONS

4.1 OBJECTIVES

- 1.To assess whether Indian surveillance powers after Puttaswamy are legal and proportional.
- 2.To study how interception, biometric identification, AI, recognition, DNA databases and spyware impact Articles 14, 19 and 21
- 3.To determine whether current review mechanisms offer effective oversight.
- 4.To spot reforms that can balance security and law enforcement needs with privacy, equality, expression and due process.

4.2 RESEARCH QUESTIONS

1. Does Indians current surveillance design meet the demands of legality, legitimate aim, necessity and proportionality?
2. Do the Digital Personal Data Protection Act 2023 and Telecommunications Act 2023 sufficiently limit state access, to data and communication?
3. What institutional safeguards are needed to stop convenience from replacing constitutional accountability?
4. How does mass and algorithmic influence free expression, association, equality and criminal procedure?

5. HYPOTHESIS

Indias surveillance framework is still largely controlled by executives and split up legally. Even though Puttaswamy sets a constitutional standard India lacks regular court approval, independent technical checks, clear rules about how long data is kept and strong ways to challenge problems. This makes India risk's that surveillance will not meet the needs of necessity, proportionality or procedural fairness.

6. RESEARCH LIMITATIONS

This study looks closely at Supreme Court rulings, laws, delegated rules and public documents. It also uses the 14 papers, working papers, and online sources that were provided. These sources help find expert ideas, tech risks and policy suggestions; main legal documents are used to argue about The Constitutional laws and court decisions.

The study is limited because many interception orders, intelligence work, technical details and how data is kept are secret. Public information can show that certain powers or technologies exist. It may not reveal how much they are used. The article does not say how many interceptions happen or how classified systems work when no clear public evidence exists.

7. CONSTITUTIONAL FRAMEWORK ARTICLES 14 19 AND 21

7.1 ARTICLE 21: THE INFORMATIONAL PRIVACY

Article 21 protects life and personal freedom except when a law says. After Puttaswamy, Article 21 also protects privacy. The court said privacy covers safety, personal choice, space privacy and data privacy. India must prove India has powered a legit purpose under The Constitution and safety measures against random or heavy intrusion.

Informational privacy matters a lot because data can show more than the fact collected. A location record can show where a person goes for religion, medical care, politics or personal ties. A biometric or genetic ID can stay forever which may affect relatives or future guesses. Chandrans look at DNA databases shows why genetic data needs a careful balance of checks.

7.2 ARTICLE 19: THE CHILLING EFFECT

Surveillance can affect Article 19 even if no case is filed. People who think their messages, searches, moves or groups are watched may stop speaking or joining activities. Thus, privacy of messages ties to the right to speak join groups and press. This links as a problem of balancing India's power with expression. Nojeim and friends also explain why encryption helps free expression and safety of just hiding illegal acts.

So, the legal review should look at expected effects. A system can be illegal not because the system makes wrong decisions, for one person but also because the system's size, secrecy or lack of clarity stops people from using their Constitutional Rights.

7.3 ARTICLE 14: ALGORITHMIC EQUALITY

Article 14 stops action by the state and requires that everyone is equal before the law. AI based monitoring can cause problems under Article 14 in many ways; choosing the data to train the AI creating risk categories how accurate the recognition is, how police use the information and if people cannot challenge the automated decisions. Joshi and Wamankar's study on policing shows how equality, due process and crime investigation interact. The use of technology does not make a government decision neutral. If a system incorrectly identifies or watches communities more; the law must look at both the data and the decision to use the system.

8. LEGALITY AND PROPORTIONALITY ANALYSIS

The law structure is best seen as a four part check.

8.1 LEGALITY

The action must be allowed by law. Legality needs a rule that is easy to find clear enough and limits what the government can do. A broad law might exist on paper, still cause legal problems if it does not say when and why and how long, who makes the decision, how long to keep the data and what can be done if something goes wrong. The current system uses laws instead of one full law. Aruns idea of a "mosaic of overlapping laws" is useful because it shows how different laws together have an effect. Bhandari and Lahiri also say that looking at one power is not enough to understand how crime is investigated and monitoring work.

8.2 LEGITIMATE AIM

National security, stopping and looking into crime, public order and keeping public health safe can be valid goals. When security is used to support monitoring surveillance, privacy and security shows the conflict. A valid goal does not mean the way it used is okay. The government must link the monitoring to the goal and explain why less intrusive ways would not work.

8.3. RATIONAL CONNECTION

The government must show a logical link between the information gathered and the goal. Collecting much information is worse than getting specific information based on individual reasons. Keeping data also needs a check: data collected for one reason should not stay forever for a different reason. Keeping data and police access is important for this.

8.4 PROPORTIONALITY AND SAFEGUARDS

Proportionality means a balance between the benefit to the public and the harm to rights. The check should look at how sensitive the data is, how many people are affected the chance of mistakes, how long the monitoring lasts, if there are less intrusive options the effect on speaking and equality and how good the control is. Procedural protections are not a small step. In PUCCL v Union of India the Supreme Court said these steps are important for the part of phone tapping. The Puttaswamy plan makes it clear that protections should be there during and after the monitoring. These should include approval, written reasons, time limits, less data, safe storage, deletion, checking notice when possible and a real way to fix problems.

9. STATUTORY AND REGULATORY FRAMEWORK

9.1 TELEGRAPH ACT AND TELEPHONE INTERCEPTION

Section 5(2) of the Indian Telegraph Act 1885, allows tapping in emergencies or safety situations and when certain conditions are met. The power must be read with the laws from PUCCL and with the rules from the Indian Telegraph Rules 1951 including Rule 419A. The main question is not if a document is called an interception order but if the decision meets the conditions has good reasons and is checked independently.

9.2 INFORMATION TECHNOLOGY ACT 2000 AND THE 2009 RULES

Section 69 of the Information Technology Act 2000 deals with tapping, monitoring or decoding information through a computer following the laws and steps. Section 69B deals with looking at traffic data or information for security. The information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 give a step-by-step plan. These rules do not mean there is no need for checks, legality is only the first part of the check.

9.3 INFORMATION TECHNOLOGY RULES 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 affect what intermediaries must do how to track people and what the government can ask. Their legal effects include privacy, anonymity, encryption and free speech. Nojeim, Maheshwari and Miglanis analysis of encryption is very important because things that weaken messages might affect regular people, reporters, lawyers and people who share secrets not just those who are suspected of crimes.

9.4 DIGITAL PERSONAL DATA PROTECTION ACT 2023

The Digital Personal Data Protection Act 2023 creates a way to handle digital data but it also has exceptions and powers for the government that need careful legal checks. Section 17 gives some exceptions in situations while section 36 allows the government to ask for information from the Data Protection Board or people who handle data in certain cases. These parts should not be seen as an exception from all privacy rules. Their use must still follow The Constitution, the laws' purpose and court checks. Some people think the law is mainly about protection while others think the exceptions might let the government have power. Dixit, Rohit and the analysis titled 'The Digital Shield or The Surveillance Sword?' all talk about this conflict. The right legal question is whether the exceptions are clearly needed and have checks not whether the law is called data protection.

9.5 TELECOMMUNICATIONS ACT 2023

The Telecommunications Act 2023, changes the rules for telecom. The powers to tap, stop and control networks must be seen with Articles 14, 19 and 21 and with the need for fairness. The Act should not be seen as replacing the ideas from Puttaswamy or the steps from PUCL.

9.6 CRIMINAL PROCEDURE (IDENTIFICATION) ACT 2022

The Criminal Procedure (Identification) Act 2022 allows taking and keeping certain measurements for crime purposes. If the measurements are about biometrics or body parts the legality of taking them must be different from the fairness of keeping, using and deleting them. The issues with DNA that Chandran points out show why biological data can't just be looked at by the time it is taken.

10. TECHNOLOGY SPECIFIC ANALYSIS

10.1 COMMUNICATIONS INTERCEPTION, CMS AND NETRA

The way interception and monitoring systems work leads to two questions: The first is about law and process, The second is about how the system works; can agencies get the data directly how requests are tracked, how selectors are approved, how long the data is. If an independent group can check the system. The research on Indias communication surveillance system shows that several laws and steps are involved, not one clear legal way. It is better to say that CMS and NETRA have been talked about in public and academic writing as tools that raise legal questions. Public information cannot prove that every technical description is true. The legal check should look at the powers used, the data affected and the real protections that are there.

10.2 AADHAAR AND BIOMETRICS

Aadhaar shows the connection between identity getting services and the risk of being watched. Henne looks at Aadhaar as a tool for managing government while Satpathy warns about the dangers of having one place for identity. The Supreme Court's decision on Aadhaar said part of the system is okay but also set some limits but it also started more discussion about how data is stored, how it is used and the connection between identity and getting services. The main idea is that biometric checks should only be for a purpose and have protections against not being included, using data in new ways not allowed checks and serious problems. A biometric ID cannot be treated like information just because it is used for a public service.

10.3 FACIAL RECOGNITION AND PREDICTIVE POLICING

Facial recognition can make public places always watched. Policing systems may also decide who to watch, stop or check before there is normal proof. Verma, Mittal and Bala, Sahil and Jeet and Joshi and Wamankar all say there are problems with how these systems work, being unfair using automated checks and not being fair. A law system should need a purpose check that the system is right checks by independent, people checking for unfairness, a person looking at decisions explaining bad decisions limits on using the data again and a way to fix mistakes. If the system only gives a chance of something happening that chance cannot be seen as proof of a crime.

10.4 DNA DATABASES AND GENETIC PRIVACY

Getting DNA creates a privacy problem because genetic data can show family links and things about a person beyond what is needed for an investigation. Chandrans fairness check supports separating the parts of taking a sample keeping a record searching a database sharing information and using it later. Each part should have its law and rules for keeping it. The government should say when a record must be deleted, who can look at it if checking family links is allowed, how to fix mistakes and what group checks the database. Without these the legal way of taking the data might not answer the fairness question.

10.5 SPYWARE AND PEGASUS

Commercial spyware shows how much watching is happening because it can get into messages, files, sensors and data from a person's device. The Supreme Courts talks about claims about Pegasus shows how important it is to check when national security is used. The Court said national security cannot be the answer to every question but the limited public info means the article should not say who is using the spyware or who it is used on unless proved by real evidence. The protections for breaking into a device should have a standard before the need of court approval and being for one person, strict time limits less data collected checks, by experts and a way to fix things if it is done wrong.

10.6 PUBLIC HEALTH.

Aarogya SETU Public health emergencies might allow for short term data processing. These emergencies do not stop the rules of The Constitution from applying. Matthan and Dar and Wani look at the privacy issues caused by data tools while Dhindsa and Kaushik create a constitutional argument against Aarogya Setu. The important protections include a legal reason limiting the purpose making use voluntary or justifying it if it is required keeping data to a minimum keeping it safe deleting it after the emergency is over and telling the public about how the system works and how long it keeps data.

11. JUDICIAL DECISIONS AFTER PUTTASWAMY

The court cases that came after Puttaswamy should be seen as a growing structure and not as one rule that either allows or stops surveillance. Puttaswamy gives the privacy rule and the way to check if something is fair. PUCL gives steps for how to handle telephone interception. The Aadhaar case shows that the court can support an identity system while setting limits. Anuradha Bhasin v Union of India also shows that rules that affect communication and expression must be checked by The Constitution and reviewed carefully.

The Pegasus case is important because it is hard to deal with surveillance claims while keeping national security safe. The court setting up an expert committee showed the need for finding facts through institutions. Secrecy can still stop people from holding the government responsible and stop individuals from getting help. A lasting surveillance system should not rely completely on sudden court committees once problems are known.

12. JUDICIAL AND INSTITUTIONAL OVERSIGHT GAPS

12.1 EXECUTIVE REVIEW

Indias system for intercepting communications has ways for the executive to check. Executive review can make sure something is legal inside. It is not the same as getting a judge to approve before it happens. The Constitutional problem is the way things are set up: the executive can decide what the security goal is, ask for surveillance approve the action and keep the information. These setups need checks from outside and a clear record of why things were done.

12.2. The ABSENCE OF NOTICE

Some secrecy is needed during an investigation. If it goes on forever, it stops people from challenging it. A system that protects rights should give notice later if it does not harm an investigation and only after an independent group gives a good reason to wait. Without notice the person affected may never know that a constitutional problem happened and may not have a way to get help.

12.3 EVIDENCE AND ACCOUNTABILITY

Ramaswamy looks at how AI surveillances used in court and finds a big problem. If evidence that is taken illegally can be used without punishment investigators may not bother to follow privacy rules. Least courts must be able to reject evidence that comes from serious or intentional violations of law and The Constitution. Courts must also be careful and only reject evidence where it would cause an unfair outcome that is not linked to the surveillance mistake.

12.4 PARLIAMENTARY AND TECNICAL OVERSIGHT

A surveillance system needs more than one case review. Parliament must get both public reports that let it see patterns check if laws are followed and look at spending. An independent technical regulator or inspectorate should check logs, selectors, controls on access how data is kept and how it is deleted. Work that studies privacy by design says that these controls should be built into the system from the start of only fixing problems later through lawsuits.

13. FREE EXPRESSION, EQUALITY AND DEMOCRATIC PARTICIPATION

Mass surveillance affects democracy in two ways. Directly it can expose association, journalistic sources, legal communications or dissenting speech. Indirectly, the feeling of being watched can make people stop speaking. The result is an effect that can happen even if the State does not charge the person. Article 14 adds an angle. Surveillance is not felt the same by all groups. Those who already face policing, border checks, welfare checks or political suspicion may be more likely to show up in databases or risk lists. Algorithmic systems can repeat existing unfairness if their training data show unequal enforcement patterns. A proportionality test must look at who feels the burden of surveillance not just how many records are collected.

14. FINDINGS

1. Constitutional standards are used unevenly. Puttaswamy offers a privacy framework, but surveillance powers keep working through broken statutes and procedures.
2. Legality is not enough A statutory power must also meet an aim, necessity, proportionality and procedural fairness.
3. Independent oversight is still missing. Executive review cannot replace judicial permission, outside audit, and solid remedies after surveillance.
4. Retention and secondary use are not well studied. The Constitutional risk often grows after data is collected when it is stored, mixed, shared, or used for a purpose.
5. AI and biometric systems bring equality and due-process risks. Accuracy, bias, explainability, and contestability must be part of review.
6. State exemptions need limits. The DPDP Act 2023 should not give the state blanket immunity for processing; exemptions must have constitutional limits
7. Secrecy weakens remedies. Without delayed notice of independent investigation and real access to a remedy, unconstitutional surveillance can stay practically unchallenged.

15 RECOMMENDATIONS

15.1 ENACT A COMPREHENSIVE SURVEILLANCE STATUTE

India should pass one law that defines interception, device intrusion metadata analysis, biometric identification, facial recognition, predictive policing and data retention. The law should name the authority to give thresholds, set duration, renewal rules, a minimization duty, a deletion rule, audit requirements and a remedy for each kind of surveillance.

15.2 REQUIRE PRIOR JUDICIAL AUTHORISATION FOR INTRUSIVE MEASURES

Interception device compromise, real-time tracking, biometric searching and access to highly sensitive data should normally need a court's permission. Emergency rules must be tight short-lived. You must be checked by a judge quickly.

15.3 ESTABLISH OVERSIGHT

An independent surveillance commissioner or inspectorate should audit authorizations, technical systems, compliance logs, retention and deletion. A special parliamentary committee should get reports, including secret information when needed. Oversight must see the records and systems, not just executive summaries.

15.4 APPLY DATA MINIMISATION AND PURPOSE LIMITATION

Collect only what is needed for a purpose. Keep data for set time and use it for a new purpose only if a separate legal basis exists. DNA profiles, biometric templates, location data, and device extracted material should have safeguards because they are very sensitive and lasting.

15.5 PROTECT ENCRYPTION AND SECURE COMMUNICATIONS

The law must say that encryption protects privacy, speech, journalism, legal confidentiality, and economic security. Any forced access rule must have necessity, court permission and technical checks. Must avoid creating weaknesses for all users.

15.6 REGULATE ALGORITHMIC SURVEILLANCE

I believe before deployment government agencies must carry out checks on accuracy, bias and human-rights impacts. Individuals must have the right to challenge any automated inference. Probabilistic risk scores must not alone justify arrest, search, surveillance or denial of benefit

15.7 PROVIDE. Remedies

I think delayed notification should be the general rule once secrecy is no longer needed. Courts must be able to order deletion to stop use, award compensation and exclude evidence obtained through serious or deliberate violations. Remedies must be practical, not just theoretical.

16. CONCLUSION

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India established an important constitutional limit on state surveillance in India. However, the existence of legal provisions does not automatically make surveillance constitutional. This study finds that fragmented laws, executive controlled review, inadequate transparency, and limited remedies create significant challenges in protecting individual privacy. Emerging technologies, including facial recognition, biometric identification, predictive policing, and spyware, further increase the risks to equality, freedom of expression, and personal liberty. India therefore needs a comprehensive surveillance law supported by prior judicial authorisation, independent oversight, data minimisation, and effective remedies for unlawful surveillance. National security and law enforcement remain legitimate state objectives, but their pursuit must respect constitutional guarantees. Ultimately, surveillance must be governed by legality, necessity, proportionality, and accountability to ensure that technological advancement does not undermine democratic freedoms.

17. REFERENCES

1. P. Joshi and Y. Wamankar, "Algorithmic policing and due process in cybercrime investigations: a constitutional analysis under articles 14, 19 and 21 of the indian constitution," *Ижтимоӣ тадқиқотлар журнали*, Dec. 2025, [doi: 10.29121/shodhsamajik.v2.i2.2025.57](https://doi.org/10.29121/shodhsamajik.v2.i2.2025.57).
2. A. Verma, B. Mittal, and A. Bala, "Privacy vs. Surveillance: Legal Challenges in the Age of Artificial Intelligence," *International Journal For Multidisciplinary Research*, vol. 7, no. 5, Oct. 2025, [doi: 10.36948/ijfmr.2025.v07i05.58572](https://doi.org/10.36948/ijfmr.2025.v07i05.58572).
3. R. Matthan, "The Privacy Implications of Using Data Technologies in a Pandemic.," *Journal of the Indian Institute of Science*, vol. 100, no. 4, pp. 1–11, Nov. 2020, [doi: 10.1007/S41745-020-00198-X](https://doi.org/10.1007/S41745-020-00198-X).
4. M. A. Dar and S. A. Wani, "COVID-19, Personal Data Protection and Privacy in India," *Asian Bioethics Review*, vol. 15, no. 2, pp. 125–140, Oct. 2022, [doi: 10.1007/s41649-022-00227-0](https://doi.org/10.1007/s41649-022-00227-0).
5. A. Dhindsa and S. Kaushik, "The Constitutional Case against Aarogya Setu," *Social Science Research Network*, May 2020.
6. N. Saroj, "Right to privacy versus right to prosecute: Judicial interpretations of privacy in criminal investigations and trial procedures in India", [Online]. Available: <https://www.ingentaconnect.com/contentone/hsp/jdpp/2026/00000009/00000001/art00005>
7. R. Chandran, "Collection of dna and the Creation of dna Databases in India: A Proportionality Analysis on Whether There is a Violation of Genetic Privacy," *Asia Pacific Journal on Human Rights and The Law*, pp. 1–27, Nov. 2024, [doi: 10.1163/15718158-25030001](https://doi.org/10.1163/15718158-25030001).
8. V. Bhandari and K. Lahiri, "The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World," *Social Science Research Network*, Apr. 2020.
9. G. Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography," *Social Science Research Network*, May 2015.

10. A. Dixit, "Data protection in india after the digital personal data protection act, 2023: a critical evaluation of privacy and state power," Jan. 2026, [doi: 10.65393/Ideo6679](https://doi.org/10.65393/Ideo6679).
11. S. Rohit, "Critical Legal Appraisal of the Digital Personal Data Protection Act, 2023: Privacy Protection or State Control," Aug. 2025, [doi: 10.5281/zenodo.16322052](https://doi.org/10.5281/zenodo.16322052).
12. G. Nojeim, N. Maheshwari, and E. Miglani, "Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth," *Indian Journal of Law and Technology*, vol. 17, no. 1, Jan. 2020, [doi: 10.55496/Ipnz6069](https://doi.org/10.55496/Ipnz6069).
13. Sahil and Dr. S. Jeet, "Predictive Policing, AI Surveillance, and Privacy in India: A Legal Analysis under the DPDP Act 2023," Nov. 2025, [doi: 10.5281/zenodo.18221509](https://doi.org/10.5281/zenodo.18221509).
14. P. Agrawal, A. Singh, M. Raghavan, S. Sharma, and S. Banerjee, "An operational architecture for privacy-by-design in public service applications.," *arXiv: Cryptography and Security*, June 2020.

Copyright & License:



© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.