



**Graphic Era
Hill University**
DEHRADUN CAMPUS

ISSN No: 3049-4311
(ONLINE) _____

GEHU LAW REVIEW

A Journal of Contemporary
Legal Research

Volume & Issue:

Volume [I], Issue [II]

Publication Period:

December 2025

Institutional Affiliation:

School of Law, GEHU
Dehradun, Uttarakhand,
India



LIST OF JOURNAL ARTICLES

1. Digital Surveillance vs Right to Privacy After Puttaswamy: A Constitutional Conflict in Criminal Investigations (Sachin Verma & Prof. (Dr.) Mohd Ahmad)1
2. Sustainable Governance of AI-Enabled Remote Sensing Systems for Environmental Compliance: Need for A Dedicated Legal Framework in India (Dr. Gyanashree Dutta & Dr. Upankar Chutia)23
3. The Normative Foundations of Online Dispute Resolution: A Jurisprudential Analysis (Dr. Sheema S. Dhar).....37
4. Self-Incrimination Vis a Vis Forensic Investigation (Dr. Gurleen Kaur).....62
5. Criminal Law Reforms and Their Impact on the Administration of Justice (Snigdha Sharma & Nikhil Sharma).....72
6. Faculty Contracts and Equality Rights: A Legal Perspective on Academic Hiring Practices (Priyam R Sharma).....91
7. Reimagining Health Governance in the Post-COVID-19 Era: Legal Lessons, Policy Gaps, and Future Directions (Ram Krishna Mani Tripathi).....110
8. Laws in Books versus Laws in Action: Implementation Hurdles in the Enforcement of New Criminal Laws (Rangoli Singh).....130

**DIGITAL SURVEILLANCE VS RIGHT TO PRIVACY AFTER PUTTASWAMY: A
CONSTITUTIONAL CONFLICT IN CRIMINAL INVESTIGATIONS**

Sachin Verma**Research Scholar, Faculty of Law, University Of Lucknow****& Prof. (Dr.) Mohd Ahmad****Professor, Faculty of Law, University of Lucknow**

ABSTRACT

India's rapid growth of digital technology has brought a massive transformation in the way criminals are being investigated. Call detail records, CCTV surveillance, mobile phone forensic, metadata analysis and AI-based systems are now playing a vital role for law enforcement agencies. These technologies facilitate investigation and assist with the solution of contemporary crimes, but are also extremely problematic in terms of privacy and uncontrolled State power. These concerns gained constitutional importance post the Supreme Court's landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) where the Supreme Court stated that the right to privacy is a fundamental right under Article 21, Constitution.

The paper explores the inter-relationship of digital surveillance practices and the constitutional right to privacy in the post-Puttaswamy era. It examines how the jurisprudence relating to privacy in India has changed, and how the State has increasingly become involved in criminal investigations, with new standards of legality, necessity and proportionality that guide State action. The research critically reviews the prevailing statutory provisions like Information Technology Act, Telegraph Act, Bharatiya Nagarik Suraksha Sanhita and the Digital Personal Data Protection Act with a focus on the need for better oversight, accountability and procedural protection. The paper also explores the theoretical and scholarly work focusing on informational privacy, surveillance capitalism, and digital constitutionalism that contributes to the understanding of these tensions.

The paper also considers judicial reaction to surveillance such as cases involving phone tapping, the closing of Internet, digital searches, and use of spyware. It makes a point of the

VOLUME I | ISSUE II | DECEMBER 2025

fact that although courts have enhanced the constitutional protections, legislative changes are insufficient. The study ends with recommendations for enhanced surveillance, legal clarity and independent oversight systems to guarantee that good policing does not lead to the erosion of individual dignity, autocratic power and democratic rights.

Key words: Digital Surveillance, Digital Constitutionalism, Constitution, criminal investigation, facial recognition, etc.

1- INTRODUCTION

Today, the advent of digital technologies has revolutionized the way criminal investigations are conducted in India. In the last ten years, policing has gone from traditional policing to technologically advanced methods that track people in physical and online environments. This increase is partly due to the rise of cybercrime, highly sophisticated national security risks and the growing prevalence of encrypted communication among technologically advanced criminals. Call detail records, internet metadata, CCTV analytics and algorithm-based predictive policing are all part of the digital footprints that have become a vital component of criminal justice processes today. However, these tools will also have a negative impact on the constitutional dimension of unlimited State authority and the loss of individual autonomy.

Significantly, the constitutional provision on privacy has undergone a sea change after the landmark judgment of *K.S. Puttaswamy v. Union of India*, (2017), which led to a unanimous decision of a nine-judge bench that privacy is a fundamental right enshrined in dignity, liberty and autonomy under Article 21. The judgment represented a constitutional paradigm shift as it recognized privacy as a constitutional right that is not only about not being touched, but also is multidimensional with two other dimensions: being informed and being free to decide. Post-*Puttaswamy*, any kind of State surveillance is subject to strict constitutional checks and must have a constitutional basis, a legitimate aim and must pass the necessity and proportionality test.¹ The doctrine change has far reaching consequences for digital policing practices, which traditionally have worked with little transparency and oversight from judges.

¹Shyam Divan & Arghya Sengupta, "Privacy as a Fundamental Right: The Indian Supreme Court's Decision in *Puttaswamy*", 13(2) *Indian Journal of Constitutional Law* 45 (2018).

VOLUME I | ISSUE II | DECEMBER 2025

In today's digital age, the tension between privacy and the powers of the State to investigate has thus emerged as one of the most important constitutional issues. The State can use digital technologies for tracking large populations by collecting metadata, conducting mobile forensics, engaging in AI-based risk assessment, and integrating and/or amalgamating several mega-databases like NATGRID and ICJS. These systems allow for both live monitoring and live behavioural mapping, on scales never seen before. Researchers and scholars studying surveillance capitalism have noted that the systematic extraction of personal data isn't only capturing human actions, but influencing them and altering them as well, producing striking power-imbalanced dynamics between the person and those who are monitoring them. Today, it is no longer possible to argue that surveillance is limited, targeted, and exception-driven, as is traditionally thought.

In this background, the present study attempts to explore the conflicts of the Constitution, doctrinal paradoxes and regulatory lacunae in relation to digital surveillance in India. The aim of this article is to look at the interactions between the basic right to privacy after Puttaswamy and the investigative practices, including the ones covered through the process of digital extraction, metadata mapping and the predictive algorithms.

The objectives of the article are: (i) to track the development of privacy law before and after the Puttaswamy judgment; (ii) to analyse the legal and proportionality framework of existing surveillance systems; (iii) to analyse the appropriateness of existing laws like the IT Act, Telegraph Act, BNSS, and DPDP Act; (iv) to examine new technologies that threaten privacy like facial recognition, AI-based predictive policing, and commercial spyware; (v) and to identify new norms and institutional reforms required to bring the Constitution into line.

The importance of the study is that it helps the debate that is still ongoing with respect to the regulation of State surveillance in democratic societies. With the aim of modernizing the criminal justice system in India with the help of AI-driven solutions, digital forensics and a national integration platform of data and information, the need for a coherent rights based framework is inevitable. The study aims at examining the changing jurisprudence and locating structural deficiencies and to contribute to an accountable, proportional and constitutionally sound surveillance regime.

2- Constitutional Right to Privacy After Puttaswamy

VOLUME I | ISSUE II | DECEMBER 2025

The Supreme Court in the nine-judge bench judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India made privacy a fundamental right in India. The Court did not define privacy as a claim that could be derived from any of the other rights but based it on the dignity, autonomy and personal liberty embedded in the Indian constitutional scheme. As described in the judgment, privacy is not a vague concept but is essential to ensuring significant human freedom. This recognition resolved prior doctrinal confusion, that the framers considered personal freedoms even if they weren't explicitly listed in the text.

The term "privacy" is understood in a multidimensional sense, covering aspects of bodily integrity, decisional autonomy, spatial sanctity and informational control. The protection of the home and private environments has traditionally been regarded as part of spatial privacy, which provides a limitation of intrusions into intimate life.² It is now at the core of the debate on informational privacy because of the growing process of datafication, which entails the capacity to control the collection, storage, processing and disclosure of one's personal data, especially when the State has unparalleled technological capacities. These dimensions illustrate the fact that privacy is not a single concept but a group of interlocking protections which ensure that the person is protected from the power of an oppressor and from the power of anyone who is not regulated.

Scholarly discussions have added much to the knowledge of the practical requirements of informational privacy. In a style that can be described as digital constitutionalism, theorists have expressed the idea that privacy is not just a matter of privacy, but also of the ability to take part in social, political and economic life without being observed constantly. This view of privacy as an empowering and not just a defensive tool is consistent with the Puttaswamy Court's framing of informational self-determination as a constitutionally protected value. Furthermore, surveillance capitalism scholarship has shown that the collection of information on a large scale becomes the commodification of personal behaviour, which allows for the control by the State as well as the manipulation of consumer decisions by the companies.³ But the constitutional dimension to such use is not limited to the moment of intrusion, it is the

²Paul M. Schwartz & Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law", 106 Georgetown Law Journal 115 (2017).

³Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019) 63–67.

VOLUME I | ISSUE II | DECEMBER 2025

structural loss of autonomy itself brought about by the use of these systems in the process of investigation without due care.

David Lyon's work on surveillance studies also offers insights into how surveillance works in the modern world in the form of a “surveillance assemblage,” that is, a network of interrelated data streams gathered from various institutional sources.⁴ This model of integration is quite similar to the integrated architecture of data in India – NATGRID, CCTNS and Central Monitoring System – in which information from banks, telecom, immigration records, courts, etc are enabled to be used in a pool of intelligence.⁵ The implications of such integration on the Constitution are far-reaching: if the purpose is to monitor in a comprehensive way and not to monitor with proportionality in mind, then the requirement to exercise proportionality as contained in the Puttaswamy case becomes very difficult to meet.

The Supreme Court adopted the three-part test of legality, necessity and proportionality to limit the power of the State, which has to be (i) lawful, (ii) necessary for a legitimate aim, and (iii) proportionate to the legitimate aim. The principle of proportionality, which was derived from comparative constitutional law, makes sure that privacy invasions are the least intrusive possible. It also guarantees transparency, accountability and oversight, which have been lacking in Indian surveillance practice in the past.

The decision has implications that immediately come to mind for criminal investigations. Traditional laws allowed investigative agencies a great deal of latitude, none of which was directed by court orders or legislated. Puttaswamy has set strict standards on investigative techniques, including phone tapping, digital forensics, device search, tower dump, and algorithmic surveillance, which must be accompanied by “safeguards” required by the Constitution. Criminal investigation now has to be necessary and non-intrusive procedures. Judicial warrants, selective extraction and strict data-retention limits are now constitutional tools, not practices, to be used.

Lastly, the judgment takes the domestic privacy jurisprudence to be in line with India's international commitments, under treaties like the Universal Declaration of Human Rights and

⁴David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001) 13–15.

⁵Siddharth Narrain, “Mapping Mass Surveillance: A Comparative Study of NATGRID and ICJS”, Alternative Law Forum Working Paper (2019).

VOLUME I | ISSUE II | DECEMBER 2025

the ICCPR which give emphasis to freedom from arbitrary interference and uphold the principle of ensuring that interference is lawful, necessary and proportionate.⁶

3- Expanding State Surveillance in the Digital Era

Digital surveillance in India has expanded rapidly because criminal investigations now depend heavily on technology. Digital tools allow agencies to track behaviour, gather information, and analyse personal data in ways that were not possible a decade ago.⁷ Digital surveillance has therefore become a major part of policing, intelligence work, and preventive security measures.

Digital surveillance begins with large CCTV networks that now operate across major Indian cities. CCTV systems increasingly use facial-recognition software to identify people moving through public spaces.⁸ Digital cameras record movements in real time, and facial-recognition systems compare images with police databases. Digital tools allow investigators to create movement patterns and identify suspects even when no physical witness exists.

Digital investigations also depend on Call Detail Records (CDRs). CDRs allow agencies to track phone numbers, call duration, cell-tower location, and communication patterns.⁹ Digital CDR analysis helps investigators identify networks, associations, and routes taken by individuals. Internet Protocol Detail Records (IPDRs) extend this capacity by tracking online activity, timestamps, and digital connections, adding a second layer of surveillance by linking physical movement with online interactions.

Digital surveillance also includes social-media monitoring. Agencies watch public posts, comments, photographs, and online interactions to understand behaviour patterns or signals of unlawful activity.¹⁰ Metadata collection further strengthens this surveillance. Metadata includes information such as time, location, device identity, and communication routes. Although metadata does not reveal the content of a communication, it exposes habits, networks,

⁶UN Human Rights Committee, General Comment No. 16 on Article 17 ICCPR (Right to Privacy), UN Doc HRI/GEN/1/Rev.9 (Vol. I), 1988.

⁷*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, pp. 180–182.

⁸*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, pp. 180–182.

⁹*Ibid.*

¹⁰*Id.*

VOLUME I | ISSUE II | DECEMBER 2025

and life patterns with considerable precision.¹¹ Digital metadata can therefore be more revealing than the communication itself.

Digital systems also use automated number-plate recognition (ANPR). ANPR cameras scan vehicle plates and link them with transport and crime databases.¹² Mobile forensics extract deleted messages, photographs, locations, contact lists, browser history, and app data. Cloud extraction extends this by allowing access to remote storage, backups, and cross-device data.

¹³ Digital forensics give investigators deep access to a person's private life and relationships.

Digital surveillance has now moved to AI-based predictive policing. Predictive policing uses algorithms and large data sets to "predict" where crime may occur or which individuals might be "high-risk."¹⁴ Legal scholars have warned that predictive policing may create bias, over-policing, and discrimination, particularly against marginalised communities.¹⁵ Digital surveillance using AI therefore raises constitutional concerns about equality, fairness, and transparency.

Digital surveillance also expands through mass-data infrastructures. Systems such as NATGRID, CCTNS, ICJS, CMS, and NETRA link information from multiple agencies.¹⁶ These networks create unified profiles of individuals using information from many different sources, enabling both real-time and retrospective tracking of behaviour at a scale that raises profound constitutional questions.¹⁷

Digital surveillance creates a constitutional challenge because these tools operate with speed, scale, and secrecy. Digital technologies allow the government to gather information about citizens even when individuals do nothing unlawful.¹⁸ Digital systems therefore demand strong

¹¹Rupinder Kaur, "Surveillance and Privacy: A Ramification of Article 21", International Journal of Reviews & Research in Social Sciences, Vol. 6, Issue 3 (2018).

¹²Vrinda Bhandari & Karan Lahiri, "The Surveillance State, Privacy and Criminal Investigation in India", University of Oxford Human Rights Hub Journal, Vol. 3(2) (2020).

¹³Varun Kalra & Ramisha Jain, "An Armistice Between Right to Privacy and Right of Surveillance", Juni Khyat, Vol. 15, Issue 06 (2025).

¹⁴Committee of Experts under Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

¹⁵Daniel J. Solove, "I've Got Nothing to Hide", (2007) 44 San Diego Law Review 745.

¹⁶Internet Freedom Foundation, *Secret Operating Procedure for Digital Snooping Revealed* (Report).

¹⁷NUJS, "Commentary on Surveillance and Proportionality in Criminal Investigation".

¹⁸Varun Kalra & Ramisha Jain, "An Armistice Between Right to Privacy and Right of Surveillance", Juni Khyat, Vol. 15, Issue 06 (2025).

safeguards, clear legal standards, and transparent oversight, especially after *Puttaswamy* affirmed privacy as a fundamental right.

3A- Emerging Technological Threats to Privacy: Facial Recognition, Predictive Policing, and Spyware

In addition to these already existing surveillance technologies, three new technologies are causing disproportionate harm to the right to privacy in India: large-scale facial recognition systems, AI predictive policing platforms and commercial spyware. All of these technologies enable the extension, in some capacity, of the reach of State surveillance, over an area where legal structures are inadequate to respond.

The police in India have been using facial recognition technology (FRT) in various states for crowd management, criminal identification and verification at public gatherings. The police in several Indian states, such as Delhi, Telangana and Tamil Nadu have been using facial recognition technology (FRT), primarily for crowd management, criminal identification and verification at public events. It is based on technology that matches biometric data of those who appear on CCTV cameras with police databases as they happen. The constitutional challenge is instant: With facial recognition, every public place becomes a place where all occupants are constantly and biometrically monitored, even without individual suspicion. The bias of commercial facial recognition algorithm systems has been consistently shown to be more errors for female, darker skin tone, and minority communities—all of which have led to a concern for equality under Article 14.¹⁹ In an environment like India, where social profiling and communal discrimination are known problems, the lack of statutory oversight and independent monitoring of the deployment of FRT poses significant risks to the possibility of targeted wrongful identification.

Predictive policing is a phenomenon spurred by artificial intelligence that arouses some common concerns. Data systems that compile criminal records, socio-economic information, and behavioural data to create risk scores for people or geographic areas reinforce and extend social inequities in automated decision making processes. If the algorithm is derived from historically biased police data that identifies certain neighbourhoods as “high crime zones,” it

¹⁹Joy Buolamwini & Timnit Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification”, *Proceedings of Machine Learning Research*, Vol. 81 (2018) 1–15.

VOLUME I | ISSUE II | DECEMBER 2025

reinforces patterns of over-policing of communities already over-policed.²⁰ These systems are also opaque, and the constitutional issue is that the output of these algorithms can be considered an objective prediction, not a value-laden judgment, so there is no way for the individual to contest the input that has led to their flagging. This is a breach of the principles of reasoned State action and natural justice underlying the Article 21 protection.

The Pegasus spyware discussion took an extra dimension of tech threat to the courts and public eye. The NSO Group's Pegasus is a sophisticated commercial surveillance tool designed to steal messages, emails, photos, access to the device's microphone and camera, along with location data from a target device, without leaving any trace of compromise on the target device.²¹ On the back of investigative reportings pointing towards the Indian journalists, lawyers and political leaders as possible targets, petitions were filed before the Supreme Court of India. The Court established a technical committee to review if the software had been used by the State agencies and, if it had, what legal basis had been used.²² The controversy highlighted a disturbing lack of regulation: today's interception laws in the Telegraph Act and the IT Act consider interception via the service providers, not via the illicit infections of individual devices. Spyware of this type is not part of this system and therefore statutory review committees are not effective and there is no procedural protection for individuals. Executive orders crafted for a different technological age cannot satisfy the constitutional imperative of lawful authority as read strictly in the context of Puttaswamy.

They all have the same constitutional failing: they allow for surveillance that is, intentionally, covert, extensive and unproportional at the time of use. To deal with them, it is necessary not just to make incremental adjustments to the statutory rules, but to establish a dedicated technology-specific impact assessment framework, independent audits, pre-authorisation by judges and enforceable remedies for wrongful surveillance.

4- Digital Surveillance: the Statutory Framework

²⁰Bernard Harcourt, *Against Prediction: Profiling, Policing and Punishing in an Actuarial Age* (University of Chicago Press, 2007) 10–14.

²¹Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (Amnesty International Ltd, 2019) 5–9.

²²Rohan Venkataramakrishnan, “The Pegasus Project: What We Know and What It Means for India”, *The Wire* (19 July 2021).

VOLUME I | ISSUE II | DECEMBER 2025

Digital surveillance in India is implemented via several laws that allow for data capture, monitoring and interception for the purposes of criminal investigations. The development of the statutory framework has been piecemeal and each of the laws gives different powers to State agencies. The lack of such an overall surveillance law has led to ambiguity about what the power of the State is and what individual rights are. The technology, executive decision and fragmented legislation now constitute the mechanism of digital surveillance today.

The main statute dealing with digital interception is the Information Technology Act, 2000. Section 69 gives the Government the power to order the interception/monitoring or decryption of information where it deems it necessary for national security or public order, or to prevent offences. Section 69A allows the blocking of online content, while Section 69B allows for monitoring the flow of information. These allow for very broad powers, but are implemented primarily by executive authorization.²³ The rules in section 69 call for review committees, but they do not specify that they must be supervised by judges. This raises concerns about the lack of transparency and proportionality with regard to digital interception under the IT Act.

The Telegraph Act, 1885 is also a significant surveillance piece of legislation. Interception of telecommunication signals is permitted under section 5(2) for public emergencies or for public safety. Most of the uses of this colonial provision remain in force today for telephone tapping, though the communication technologies which have developed are much more invasive than the framers of the Act had envisioned. While it is accepted by courts that Section 5(2) requires a basis for interception to be recorded in writing, the discretion of the executive is also considerable.²⁴

The Bharatiya Nagarik Suraksha Sanhita 2023 has put in new provisions in respect of search, seizure and processing of electronic evidence. Legislation allows the police to take digital devices and do electronic searches, and to make copies of data, as part of investigations. BNSS also advocates for the video recording of searches, and requires forensic examination in certain serious offences. An electronic search, however, does have the potential to result in over-

²³Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 3.

²⁴Indian Telegraph (Amendment) Rules, 2007, Rule 419A; *see also* People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

VOLUME I | ISSUE II | DECEMBER 2025

collection as electronic devices contain a wealth of personal information that may be unrelated to the offence that is being investigated.

The Bharatiya Sakshya Adhiniyam (BSA) 2023 lays down rules on the admissibility of electronic records. The Act includes a recognition of electronic evidence, including digital documents, metadata, logs, and digital statements. While BSA emphasizes authenticity and integrity, the case for proof remains on the investigators' shoulders. Digital evidence can be easily altered and there is no common forensic standard, which makes it easier to have unreliable material in evidence.

The Digital Personal Data Protection Act (DPDP Act) 2023 offers a model of data protection, however, its attention to State surveillance has significant structural restrictions. The Act lists general exemptions that enable public bodies to use personal information for national security, public order, criminal investigation and law enforcement purposes in a way that doesn't require consent and doesn't limit the purposes of the data use. The data-protection obligations under this Act are subject to wide latitude of discretion of the Union Government, as is evident from Section 17 thereof, which allows the Government to exempt from the Act, any instrumentality of the State by notification.²⁵ This translates to the fact that the State, the biggest threat to citizens' privacy, is the least limited by the law that is supposed to protect personal data. Civil society groups have pointed out that these exemptions echo the structural flaws of previous proposals for data governance, without providing meaningful remedies for the abuse of citizens' data by the State. Another major blow to the protective value of the Act is the lack of an independent data protection authority with appropriate powers to review government surveillance as recommended by Justice Srikrishna Committee.

The special criminal laws also include provisions for increased surveillance. Extended monitoring, interception and collection of data is permitted under the Unlawful Activities (Prevention) Act, Prevention of Money Laundering Act and Narcotic Drugs and Psychotropic Substances Act. These laws grant more leeway to investigators, as they address issues like

²⁵Srikrishna Committee Report, *A Free and Fair Digital Economy* (Ministry of Electronics and IT, 2018) Ch. 9 (recommending an independent Data Protection Authority).

VOLUME I | ISSUE II | DECEMBER 2025

terrorism, organised crime and drug networks. But there's a lack of robust procedural protections, which calls into question its potential misuse.²⁶

India still does not have a specific surveillance regulation law. Each of the laws that confer surveillance powers lacks an overarching framework to authorise, monitor or report on such powers.²⁷ There is a need for a modern surveillance law that sets limits, provides judicial oversight, and makes sure digital policing is not inconsistent with the right to privacy.

5- Judicial Approach to Surveillance and Privacy Before and After Puttaswamy

Judicial understanding of privacy and surveillance in India has been shaped over time, as technology advances and as the courts interpret the constitution. Telephone tapping was first brought before the Courts in the early years in the case of *People's Union for Civil Liberties v Union of India (PUCL)*.²⁸ The Supreme Court acknowledged that interception of communication might be a valid investigative tool but it was an intrusion into personal privacy. The Court reiterated that such action should be in accordance with statutory safeguards provided in the Indian Telegraph Act, 1885, and can only be taken by higher officers in specific situations. Arbitrary or indiscriminate tapping was found unconstitutional and there was to be a review committee for accountability.

PUCL's impact goes beyond the case of telephone tapping. For the first time, the Judgment clarified the constitutional status of the right to privacy in the field of personal communication even if it is not specifically mentioned in the fundamental rights as listed in the Constitution. The Court relied on the words of freedom and human dignity in Article 21 to find that any procedure that allows for interception must be just, fair and reasonable. It also acknowledged that the lack of judicial pre-authorisation was not sufficient to make interceptions unconstitutional provided that the procedural protections and post hoc review were adequate and there was sufficient executive authorisation. Questions remained, though, that would be forced to be revisited by future cases, especially in the digital age, under this pragmatic "safe harbor" for security concerns.

²⁶Unlawful Activities (Prevention) Act, 1967, ss. 43A–43F (powers of search, seizure and interception).

²⁷Usha Ramanathan, "India, the UIDAI and the Question of Surveillance", *Economic and Political Weekly*, Vol. 45(35) (2010) 30–34.

²⁸*People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

VOLUME I | ISSUE II | DECEMBER 2025

Before the recognition of privacy as a fundamental right, the Indian courts had shown inaction in granting constitutional protection to personal communication. The Court, in such cases as that of *Kharak Singh v. State of Uttar Pradesh*²⁹, and *M.P. Sharma v. Satish Chandra*³⁰, dismissed the notion of protection of privacy under the Constitution. PUCL, however, prepared the ground by stating that interference with personal communications must go through a just and reasonable process – laying the groundwork for the constitutional importance of this process.

The nine-judge bench decision in *Justice K.S. Puttaswamy (Retd) vs. Union of India*³¹ marked a paradigm shift in the judiciary. The Court has acknowledged the right to privacy as an integral part of personal liberty in Article 21 of the Constitution and linked it with Article 14 and 19. The judgment importantly established the ‘necessity and proportionality test’ of assessing State action with regard to privacy. It highlighted that any surveillance, interception or data collection procedure must have a legitimate objective, be legally authorized and must be proportionate to the objective sought.

Since the Puttaswamy judgment, Courts have used this test in a range of situations. The Bombay High Court in *Vinit Kumar v. Central Bureau of Investigation*³² declared that the orders for phone interception lacked any tangible threat to public safety, particularly regarding the public's right to privacy. The Court again emphasized that the interception must be necessary and proportionate, which is a commitment that was made in the post-Puttaswamy era. Likewise, the Madras High Court in 2025 set aside an order passed in 2011 for not observing the procedural safeguards, thereby clarifying that it was necessary to abide by the statutory procedures to respect constitutional rights.

With the advent of Internet communication a new set of privacy issues arose. In *Anuradha Bhasin v. Union of India*,³³ the Supreme Court struck down any prolonged internet shutdown in Jammu and Kashmir and ruled that such internet shutdowns must be legally authorised, necessary and proportionate. The judgment was a major expansion of the principles laid out by

²⁹*Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

³⁰*M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

³¹*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

³²*Vinit Kumar v. Central Bureau of Investigation*, 2019 SCC OnLine Bom 1198.

³³*Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

VOLUME I | ISSUE II | DECEMBER 2025

Puttaswamy to the area of communication rights. The Court recognised Article 19(1)(g) to guarantee the freedom to practise a trade or profession online, and Article 19(1)(a) to guarantee freedom of speech and expression, which includes access to the internet as a medium for this freedom. Most importantly, the Court made it clear that internet shutdowns should be published so that the impacted persons can approach competent authorities in challenge. This transparency obligation, as part of the proportionality principle, was a change from the opacity that had been typical of the restrictions on the exercise of executive powers in the area of surveillance and communication.

The relationship between surveillance, speech and democratic participation was also considered in *Anuradha Bhasin*, with doctrinal implications. The Court, as it did in many other decisions, implicitly acknowledged that the right to communicate, access information and to engage in digital public discourse is part of a constitutional liberty, not a side issue. This logic is important for arguments that the ability of AI to surveil and recognize faces, even if it is not formally restricted, should be subject to the same proportionality standard.

The courts have been drawn into this issue of secret digital surveillance in recent years thanks to the Pegasus spyware scandal. Petitions by organisations like Internet Freedom Foundation, had contended that the use of spyware by the State infringes on the fundamental right to privacy and demanded judicial intervention. The Supreme Court's establishment of a technical expert committee to investigate the allegations showed its interest in investigating allegations of State surveillance, even without the Government's cooperation, and highlighted that the constitutional safeguards against surveillance cannot be evaded through the use of the national security blanket.

Courts have also been slow to embrace the search and seizure of digital devices. The judiciary has accepted that mobile phones, laptops and the like may store a lot of personal information and that searches must be carried out with the authority of law and be proportionate and necessary. From such limited privacy rights in pre-Puttaswamy era to a strong constitutional protection in the digital era, Indian jurisprudence has progressed, and so has the Constitution, in order to ensure that personal liberty is a core tenet of constitutional governance.

6- Constitutional Conflict: Surveillance vs. Privacy in Criminal Investigations

VOLUME I | ISSUE II | DECEMBER 2025

In India, the duty to maintain law and order is a responsibility of the State while the right to privacy is an individual right, and this gives rise to conflict in criminal investigations. This conflict comes into sharp focus when law enforcement authorities want to access personal data without a warrant or blanket access, such as call records, metadata, or digital communications. *People's Union for Civil Liberties v. Union of India*³⁴ puts a strong emphasis on the requirement of strict safeguards on telephone tapping even if it is permitted by the statute to prevent arbitrary interference in one's personal communication.

One of the big worries is whether this is mass surveillance or targeted surveillance. Under mass surveillance, information is gathered from groups of people, but not from specific individuals because of their suspicions; under targeted surveillance, it is gathered from individuals who are reasonably suspected of criminal activity. The Court has repeatedly emphasized that indiscriminate collection of metadata/communications is disproportionate intrusion, in violation of Article 21.

This is complicated by the fact that digital devices are now ubiquitous in society as a place to store personal information. Arrests at airports and the subsequent searches of mobile phones and laptops present some significant constitutional questions. In *Puttaswamy vs. Union of India*, the Court acknowledged that possession of the personal devices is an extension of privacy.³⁵ All searches and seizures are subject to the principles of legality, necessity and proportionality. Absence of these safeguards could mean the evidence is arbitrary and unconstitutional.

The problem is compounded by the presence of data on the clouds that crosses borders and can be accessed by investigators without a judicial order. This can lead to disproportionate intrusion (“function creep”) that extends from the initial, specific investigations into monitoring larger populations.³⁶

Unchecked surveillance also impacts on freedom of speech, association and dissent, as people may be discouraged from engaging in lawful protest activity or political behaviors for fear of

³⁴ *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

³⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, pp. 180–182.

³⁶ Philippa Lawson, “Function Creep in State Surveillance and Data Sharing: A Comparative Analysis”, 34(2) Windsor Yearbook of Access to Justice 89 (2017).

VOLUME I | ISSUE II | DECEMBER 2025

what they might be caught doing. The Court drew attention in *Anuradha Bhasin v. Union of India*³⁷ to the fact that the restrictions on internet usage and digital communication have an adverse impact on the freedom guaranteed under Articles 19(1)(a) and 19(1)(c).

The law enforcement industry has said that access to communications and data stored in the cloud is critical to fight financial fraud, organised crime and terrorism. After the Puttaswamy case, courts have held that the powers must meet the requirements of legality, necessity and proportionality, and that the State's action does not trample on the fundamental rights.

Procedural safeguards like independent oversight, clearly defined scope and duration of access, clearly defined data retention limits and judicial authorisation are required for the prevention of abuse. The courts have made it clear that the exercise of investigative powers is not free and unlimited, but must not encroach upon the boundaries of the Constitution so as to infringe upon the rights to a person's liberty and dignity.

Criminal investigations, in turn, highlight the tension between privacy and police needs in investigations. The cross-border retrieval, mass monitoring, function creep, and warrantless access all pose different threats to fundamental rights. Effective policing does not infringe on constitutional freedoms, because of judicial enforcement of necessity, proportionality and prior authorisation.

7- Necessity and Proportionality Tests in Surveillance Jurisprudence

In a criminal investigation, surveillance is sometimes a conflict with the right to privacy. A framework has been developed by courts to make sure that any intrusion is justified. There are three elements that play an important role in the framework, namely: legality, necessity and proportionality. This is used to ensure privacy protection and still allow for lawful surveillance.

For surveillance to be considered legal, there must be a clear and explicit provision in statute. The law has to specify in detail and procedure. Telephone tapping must be conducted in accordance with the statutory provisions and have to be authorized through a competent body,

³⁷ *Anuradha Bhasin v. Union of India*(2020) 3 SCC 637

VOLUME I | ISSUE II | DECEMBER 2025

the Supreme Court ruled in *PUCL v. Union of India*. No arbitrary action should take place without the proper documentation and approval.

There must be a necessity for surveillance to be conducted, meaning that it must be necessary for achieving the investigative goal. Investigators to employ the least intrusive methods. Authorities should take into account other means of communication before intercepting. In *Puttaswamy v. Union of India*, the Court had decided that the intrusion must be essential for a legitimate purpose, and cannot be a routine one.

The balance between intrusion and the seriousness of the investigation is the key to proportionality.³⁸ If surveillance is legal and legitimate it may be invalid if it is more than proportionate to the goal. Proportionality helps to avoid arbitrary or excessive measures which might be counterproductive to civil liberties.

Transparency, accountability and oversight are key parts of the framework. There are mechanisms in place to prevent misuse, including reporting, audit and review. Unlike democratic countries which have their own authorisation bodies which monitor surveillance, there is no independent body in India to monitor it. This lack can create opportunities for unlimited violations of privacy.

Even with the guidance of the judiciary, the surveillance regime in India is still poorly developed. There is limited accountability and transparency with respect to the number and kind of interceptions. Independent review and reporting would be improved to bolster compliance with the necessity and proportionality framework.

8-Challenges, Risks, and Ethical Concerns in Surveillance

➤ Mass Surveillance and Technological Over-Reach

The State has increased its capacity to monitor citizens, thanks to modern surveillance technologies. This is good for criminal investigations – but bad for technological over-reach. Mass surveillance gathers information in a general way; not targeted at certain suspects. This can become a normal practice, and may be detrimental to privacy and democratic values.

³⁸Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press, 2012) 3–5.

VOLUME I | ISSUE II | DECEMBER 2025

➤ Lack of strong legal safeguards and no judicial warrants

One of the important issues in India is the inadequacy of the legal protection of surveillance. There are numerous powers that an individual can use without court permission. For example, as per Telephone Act and IT Act there is no need for independent judicial order for certain interceptions based on Executive order. Lack of adequate monitoring mechanism raises the danger of arbitrary monitoring.

➤ Bias and misuse in the AI-powered systems.

There are extra risks to be considered with AI-powered surveillance systems. Automated tools can process and analyze large amounts of data in a short amount of time, but can also be biased in their prediction or identification. Mistakes in facial identification or predictive policing can result in misidentification and mis-targeting of people or communities. Algorithmic bias can impact vulnerable populations and undermine fairness in the justice system.

➤ The Adverse effect on participation in democracy

Surveillance measures may have a chilling effect on democratic participation.³⁹ Citizens who know they will be constantly monitored may limit their free expression or refrain from exercising their right to free expression. This has a direct bearing on the freedom of speech and the right to freedom of expression as provided in Article 19(1)(a) and 19(1)(c) of the Constitution. Restriction on Internet access, like shutdowns, can be an indirect infringement on freedom of expression and assembly as noted by Courts.

➤ Breach of privacy due to data breaches.

Data breaches and not-secured government databases have potential to compromise personal data collected on the surveillance. Poor data management or weak cyber security can lead to the release of sensitive data. This will not only damage personal privacy, but will have social and economic repercussions for those affected.

➤ Balance between speedy of investigation and due process

³⁹Neil M. Richards, “The Dangers of Surveillance”, 126 Harvard Law Review 1934 (2013).

VOLUME I | ISSUE II | DECEMBER 2025

The speed of an investigation is always in conflict with due process rights for the authorities. The need for rapid access to data could justify an exception to the procedural safeguards, however, if the fundamental rights are affected. In the courts, the principle of legality, necessity and proportionality has been stressed as a measure to safeguard civil liberties in the context of surveillance.

Surveillance in India is fraught with many difficulties and moral dilemmas. Inadequate safeguards, potential for bias in AI systems, chilling of free speech and the risk of data breaches are among the areas where oversight is currently lacking. A balance between the investigative requirements and privacy and the democratic freedoms is critical.

9 – Suggestions

1- Strengthening Legal Safeguards

The first one of the most important measures is to improve legal protection of surveillance. What government can intercept communications is limited, although there are current laws, such as the IT Act, 2000 (Sections 69 and 69A), and the Telegraph Act. A clear statutory obligation for all surveillance measures to be authorised by court will reduce arbitrary intrusion and help to respect constitutional rights to privacy.⁴⁰

2- Create a Dedicated Surveillance Statute

Currently, there is no single legislation in India to regulate digital surveillance. An all-encompassing Surveillance Regulation Act should establish what types of surveillance are allowed, the criteria for authorisation, data retention periods and the extent of the retention, and the remedies to be provided for people affected by illegal surveillance. Such a legislation would make India compliant with those jurisdictions which have specific interception and intelligence oversight laws and would be the only landmark legislation with regards to the legality prong of the post-Puttaswamy proportionality framework. The statute should also cover new technologies like predictive policing and facial recognition with specific provisions, requiring assessments of the technologies before they are deployed.

⁴⁰Prashant Iyengar, “Privacy and the Information Technology Act”, in Rakesh Shukla (ed), *Privacy in the Age of Information* (Human Rights Law Network, 2012) 88–95.

3- Setting up Independent Oversight Mechanisms

India does not have a regulatory institution to keep an eye on surveillance activities. Establishment of a judicial/parliamentary oversight body can improve accountability. A body of this kind could be established to review requests for interceptions, audit records and ensure that the necessity and proportionality principles are adhered to. Oversight would also serve as a protection against misuse of the AI-driven systems and mass surveillance.

4- Amendment to DPDP Act

The DPDP Act, 2023 needs to be meaningfully amended to significantly reduce the broad exemptions of the State from meaningful data protection obligations, currently afforded to government surveillance activities. Specifically, Section 17 needs to be amended to stipulate⁴¹ that any exemption from the provisions of the Act by the government must have legislative necessity and be subject to an independent review. The Act should also allow for the establishment of an independent Data Protection Board with the jurisdiction to examine and punish the misuse of personal data by government agencies. If the DPDP Act is brought into conformity with Puttaswamy constitutional guidelines, namely, legality, necessity and proportionality, then it would become a complete privacy protection Act applicable to the State as well as private bodies.

5- Ensuring transparency and accountability

Actions of transparency are the key to retaining the public's trust. There should be periodic reporting of collated statistics from surveillance activities without identifying individual data. Clear accountability processes should be established for the use of monitoring. The provision of 'publishing guidelines' and 'publishing criteria' for surveillance would also help to keep investigations both legal and within the confines of privacy.

6- Addressing AI Bias and Ethical Concerns

Useful as surveillance tools may be, they can be subject to bias through the use of AI. Algorithm audits and risk evaluations are needed before the use of AI in law enforcement.

⁴¹Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?", Carnegie India Working Paper (2020).

VOLUME I | ISSUE II | DECEMBER 2025

Testing and validation can help to avoid wrongful identification or discrimination, when performed regularly. Ethical guidelines for AI surveillance will also ensure its operations are in line with constitutional principles and human rights commitments.

7- Protecting Data Security

Data breaches and unsecured government databases pose a threat to privacy, which needs to be mitigated. Adopting strict cyber security practices, encryption measures, and conducting periodic audits of government databases can help reduce these risks. Reducing data storage and access to sensitive data only to authorised individual(s) will also add to protections.

8- Promoting Public Awareness

The public should be made aware of their rights in the context of surveillance and protection of data. Educational outreach, readily available information, and legal assistance can help inform people about illegal surveillance and hold perpetrators accountable. Awareness also puts pressure on the public for more good governance and ethical implementation of surveillance laws.

10- CONCLUSION

Digital surveillance and the right to privacy is one of the most important constitutional challenges of today's times. The State's ability to monitor individuals has grown far beyond what previous laws could have envisioned, as investigative agencies have been making use of technologically advanced tools from automated facial recognition and digital forensics to metadata analysis and integrated national database. Such instruments, of course, fortify the battle against cybercrime, terrorism and organised offence, but can also be dangerous in the sense of over-reach, function creep and impact on civil liberties.

In Puttaswamy, the Supreme Court changed the dynamics of the Constitution by asserting the right to privacy as a fundamental right that imposes substantive restrictions on the State's surveillance. Newly, any intrusion must meet the criteria of: legality, legitimacy, necessity and proportionality. But current surveillance laws are also fragmented, outdated and overly biased in favor of executive discretion. Legislation, including the IT Act and the Telegraph Act, are subject to little meaningful scrutiny, and the DPDP Act (with its wide-ranging State exemptions) is insufficient to provide the broad privacy protection needed at the constitutional

VOLUME I | ISSUE II | DECEMBER 2025

level. The rise of facial recognition, AI predictive policing, and spyware threats only further highlight these systemic shortcomings, given how little was written to regulate such advanced and pervasive technologies.

The scholarly discussion of surveillance capitalism and digital constitutionalism offers insights into why it is necessary to go beyond the technical solutions and incremental statutory changes. To ensure privacy safeguards are observed in the architecture of digital life, which is built into infrastructure, embedded within government systems, and delegated to automated algorithms, privacy protection must be structurally embedded in the constitution not just compliantly followed. A rights-based surveillance system needs to be based on the principles of mandatory judicial authorisation, transparency, data retention limits, reform of the DPDP Act, and independent, enforcement-empowered oversight bodies.

Finally, the question is not so much whether technology should be used in criminal investigations as how to make it part of a constitutional system that safeguards dignity and autonomy. The more the privacy protections are strengthened, the more that technology is used to reinforce, and not weaken, democratic values. Therefore the future of surveillance in India should be done in a manner that balances the two fundamental rights of security and fundamental rights.