

International Journal of Arts, Commerce, Science and Technology

Volume 2 Issue 5, May 2026, pp. 1-13

ISSN (Online): 3108-2998

Homepage: <https://ijacst.com/>



Title:	Right to Privacy and Digital Surveillance in India: A Constitutional and Legal Analysis
Author(s):	Tanisha
Affiliation(s):	Research Scholar, Department of Law, Baba Masthnath University, Rohtak, Haryana, India.
DOI:	https://doi.org/10.65919/ijacst.2026.v2i5001
History:	Received: 12 March 2026, Accepted: 14 April 2026, Published: 30 May 2026
Citation:	Tanisha, (2026). Right to Privacy and Digital Surveillance in India: A Constitutional and Legal Analysis. International Journal of Arts, Commerce, Science and Technology, 2(5), 1-13. https://doi.org/10.65919/ijacst.2026.v2i5001
Copyright:	© 2026 The Author(s)
Licensing:	 This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).
Conflict of Interest:	The author(s) declare no conflict of interest.
Funding:	This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.
Corresponding Author:	Tanisha ✉
Published By:	UnivColl Publications

Right to Privacy and Digital Surveillance in India: A Constitutional and Legal Analysis

Tanisha

Research Scholar, Department of Law, Baba Masthnath University, Rohtak, Haryana, India.

Abstract

The rapid growth of digital technologies has significantly expanded the capacity of governments and private entities to collect, monitor, analyse, and retain personal information. This development has intensified concerns regarding the constitutional protection of privacy in India. The present study examines the right to privacy as a fundamental right and evaluates the legal framework governing digital surveillance. It analyses the constitutional principles established in *Justice K. S. Puttaswamy (Retd.) v. Union of India*, with particular emphasis on legality, legitimate purpose, necessity, proportionality, and procedural safeguards. The study further examines relevant provisions of the Information Technology Act, 2000, the Telecommunications Act, 2023, the Digital Personal Data Protection Act, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023. It explores major forms of surveillance, including communication interception, metadata monitoring, location tracking, facial recognition, biometric databases, social-media monitoring, and automated profiling. The analysis identifies several concerns, such as limited independent oversight, lack of transparency, broad governmental exemptions, mass-data collection, weak accountability, technological misuse, and inadequate remedies. The study concludes that surveillance may serve legitimate objectives, including national security and criminal investigation, but must remain constitutionally controlled. A balanced framework requires clear legal authority, limited data collection, secure storage, defined retention periods, independent review, institutional accountability, and effective remedies against unlawful or disproportionate surveillance.

Keywords: Right to Privacy, Digital Surveillance, Constitutional Law, Data Protection, Proportionality, National Security, Informational Privacy

Introduction

Privacy is an essential condition for individual freedom, dignity, autonomy, and personal development. It allows a person to control access to private life, personal communications, bodily information, family matters, movements, beliefs, and personal data. In the digital age, privacy is no longer restricted to protection against physical intrusion into the home or private space. It also includes informational privacy, communication privacy, protection against continuous monitoring, and control over the collection, processing, storage, and disclosure of personal information.

The rapid expansion of smartphones, social-media platforms, digital payments, biometric identification, cloud services, facial-recognition systems, artificial intelligence, and internet-based public services has significantly increased the amount of personal data generated by individuals. Governments and private companies can now collect information relating to location, online searches, financial transactions, communications, personal preferences, social relationships, and behavioural patterns. Although such technologies support governance, security, commercial services, and crime prevention, their uncontrolled use may expose individuals to profiling, discrimination, manipulation, identity theft, and unjustified surveillance.

Digital surveillance generally refers to the observation, collection, monitoring, or analysis of activities and communications through electronic technologies. It may include interception of telephone or internet communication, examination of metadata, location tracking, facial recognition, monitoring of social-media activity, access to electronic devices, and automated behavioural profiling.

Surveillance may be targeted at a particular person based on a lawful investigation, or it may involve broad and systematic collection of information concerning large groups of people. The constitutional difficulty arises when surveillance is conducted without sufficient legal authority, necessity, transparency, accountability, or independent supervision.

The Constitution of India does not expressly use the term "right to privacy." However, in *Justice K. S. Puttaswamy (Retd.) v. Union of India*, a nine-judge Bench of the Supreme Court unanimously recognised privacy as a constitutionally protected fundamental right. The Court connected privacy with life and personal liberty under Article 21 and with the freedoms and guarantees contained in Part III of the Constitution. It recognised that privacy includes bodily integrity, personal choice, informational control, and the protection of human dignity.

The recognition of privacy as a fundamental right does not make it absolute. State interference may be permitted where it has a valid legal basis, pursues a legitimate objective, satisfies the requirements of necessity and proportionality, and is accompanied by adequate procedural safeguards. These requirements are particularly important in surveillance cases because secret monitoring can affect freedom of expression, association, political participation, professional confidentiality, and the relationship between citizens and the State.

India's legal framework governing digital surveillance is spread across several statutes and rules. Section 69 of the Information Technology Act, 2000 authorises specified government agencies, subject to statutory conditions and recorded reasons, to intercept, monitor, or decrypt information transmitted, received, generated, or stored through computer resources. Sections 69A and 69B separately address blocking of online information and monitoring of traffic data for specified purposes. The Telecommunications Act, 2023 and related rules also regulate lawful interception within telecommunication systems.

The Digital Personal Data Protection Act, 2023 adds an important dimension by regulating the processing of digital personal data. It recognises both the individual's interest in protecting personal data and the need to process data for lawful purposes. It provides requirements concerning consent, security safeguards, breach notification, and organisational responsibility. Nevertheless, questions remain regarding government exemptions, independent oversight, transparency, data retention, facial recognition, and effective remedies against unlawful surveillance.

This study therefore examines the constitutional status of privacy, the legal basis of digital surveillance, the powers granted to public authorities, and the safeguards available to individuals. It also evaluates whether the existing framework achieves a fair balance between privacy, national security, public order, technological development, and criminal investigation.

Objectives of the Study

The study seeks to examine the meaning and constitutional development of the right to privacy in India and to analyse its relationship with dignity, liberty, equality, and freedom of expression. It aims to evaluate the nature and different forms of digital surveillance undertaken by government agencies and private entities. The study further examines the Information Technology Act, 2000, the Telecommunications Act, 2023, the Digital Personal Data Protection Act, 2023, and other relevant legal provisions governing interception, monitoring, data processing, and electronic investigation.

Another objective is to analyse the judicial principles established in *Justice K. S. Puttaswamy (Retd.) v. Union of India* and related decisions, particularly the requirements of legality, legitimate purpose, necessity, proportionality, and procedural safeguards. The study also investigates privacy concerns arising from facial recognition, biometric databases, social-media monitoring, artificial intelligence, location tracking, and large-scale collection of personal data. Finally, it seeks to identify

gaps in the existing legal framework and recommend effective oversight, transparency, accountability, data minimisation, limited retention, and accessible remedies for persons affected by unlawful or disproportionate surveillance.

Concept and Meaning of Privacy

Privacy refers to the ability of an individual to maintain a protected sphere of personal life and to exercise reasonable control over access to the body, home, family, communications, choices, movements, and personal information. It enables a person to develop thoughts, relationships, beliefs, and identity without unjustified interference by the State, private organisations, or other individuals. Privacy does not simply mean secrecy. A person may disclose information for a limited purpose without surrendering every right over its subsequent collection, use, storage, or distribution. The concept therefore includes both freedom from unwanted intrusion and the capacity to determine how personal life is presented to others.

Physical privacy protects the individual against unauthorised entry, observation, search, recording, or interference within personal spaces. It includes protection of the home, private surroundings, belongings, and personal activities. Modern technology has expanded the possibilities of physical intrusion. Closed-circuit cameras, drones, location-enabled devices, biometric scanners, and facial-recognition systems can monitor a person even without direct physical contact. Physical privacy therefore concerns not only entry into a private place but also technological observation capable of revealing a person's movements, associations, habits, and daily routine.

Informational privacy relates to the collection, processing, storage, use, and disclosure of personal data. Digital activities generate substantial information about identity, finances, health, education, employment, location, preferences, online searches, and social relationships. When such information is combined and analysed, it can produce a detailed profile of an individual. Informational privacy gives a person a legitimate interest in knowing what data is collected, why it is required, how long it will be retained, with whom it will be shared, and what safeguards will protect it. The Supreme Court in *Justice K. S. Puttaswamy (Retd.) v. Union of India* recognised informational control as an important aspect of privacy and linked privacy with liberty, autonomy, and dignity.

Communication privacy protects the confidentiality of personal exchanges through telephone calls, emails, messaging applications, letters, video conferences, and other communication systems. Meaningful communication often depends on the expectation that conversations will not be secretly intercepted, recorded, or examined without lawful justification. Unregulated access to communications may discourage individuals from expressing opinions, seeking advice, sharing personal concerns, or associating with others. Communication privacy is particularly important for relationships involving professional confidentiality, such as those between lawyers and clients, doctors and patients, or journalists and their sources.

Decisional privacy protects a person's autonomy in making intimate and personal choices concerning family life, relationships, marriage, reproduction, education, belief, and lifestyle. Bodily privacy concerns control over one's physical body, medical information, bodily integrity, and exposure to physical or technological examination. These dimensions demonstrate that privacy is closely connected with personal autonomy. An individual cannot exercise genuine liberty when important personal decisions are continuously controlled, observed, or influenced through fear of surveillance.

Concept and Nature of Digital Surveillance

Digital surveillance refers to the observation, collection, recording, interception, processing, or analysis of information through electronic and networked technologies. It may involve monitoring

communications, accessing devices, tracking location, examining internet activity, collecting biometric information, analysing financial transactions, or using algorithms to identify behavioural patterns. Surveillance may be carried out for criminal investigation, national security, public safety, organisational management, commercial advertising, fraud prevention, or service improvement. Its legality and acceptability depend upon its purpose, scope, necessity, safeguards, and impact on individual rights.

State surveillance is conducted by public authorities for purposes such as investigation of offences, protection of national security, maintenance of public order, and prevention of serious threats. Section 69 of the Information Technology Act, 2000 permits authorised government agencies, subject to specified grounds, written reasons, and procedural safeguards, to intercept, monitor, or decrypt information generated, transmitted, received, or stored through a computer resource. The Telecommunications Act, 2023 and the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 also form part of the legal structure governing lawful interception of telecommunication messages.

Private surveillance is undertaken by employers, technology companies, financial institutions, social-media platforms, advertisers, educational institutions, housing societies, and other non-governmental entities. It may include workplace monitoring, CCTV recording, application permissions, behavioural advertising, device fingerprinting, facial recognition, and analysis of customer transactions. Although private surveillance may serve legitimate purposes, excessive or hidden monitoring can interfere with autonomy, equality, and informational control. The difference between State and private surveillance is becoming less distinct where private companies hold extensive data and provide information or technological assistance to public authorities.

Targeted surveillance is directed at a particular person, account, device, or group on the basis of defined grounds. Where supported by law and reliable information, it may assist the investigation of serious offences while limiting unnecessary collection of unrelated data. Mass surveillance, in contrast, involves the broad collection or examination of information concerning large numbers of persons without prior individual suspicion. It creates greater constitutional concern because innocent individuals may be continuously observed, profiled, or included in databases merely because they use ordinary communication services.

Online tracking records or infers a person's activity across websites, applications, platforms, and devices. Cookies, location services, advertising identifiers, browsing histories, search records, and social-media interactions may be used to construct behavioural profiles. Profiling involves arranging such information into categories relating to interests, habits, financial capacity, political preferences, or perceived risk. These profiles may influence advertising, employment, credit, insurance, policing, or access to services. When automated systems rely on incomplete or biased data, profiling may also produce discrimination or unfair treatment.

Metadata is information about a communication rather than its substantive content. It may reveal who communicated with whom, at what time, from which location, for how long, and through which device or network. Although a single metadata record may appear limited, repeated records can disclose personal relationships, movements, professional contacts, and patterns of behaviour. Communication monitoring may involve metadata alone or extend to the actual content of calls, messages, emails, and stored files. Both forms can significantly affect privacy and require lawful authority, defined purposes, limited retention, secure handling, and meaningful oversight.

Constitutional Basis of the Right to Privacy

The constitutional protection of privacy in India arises from the combined operation of Articles 14, 19, and 21. These provisions protect equality, fundamental freedoms, life, and personal liberty,

and they collectively limit arbitrary interference with individual autonomy. The Constitution is officially published by the Legislative Department of the Ministry of Law and Justice.

Article 14 guarantees equality before the law and equal protection of the laws. In the context of surveillance, it protects individuals against arbitrary, discriminatory, or irrational State action. A surveillance measure that grants uncontrolled discretion, lacks clear standards, or disproportionately targets particular communities may raise concerns under Article 14. Equality also requires that technological systems used by public authorities should not produce unjustified distinctions through biased data or inaccurate automated decisions.

Article 19 protects freedoms including speech, expression, assembly, association, movement, and profession, subject to constitutionally permitted restrictions. Continuous or secret surveillance may create a chilling effect by causing individuals to avoid lawful speech, association, research, protest, or political participation. Journalists may hesitate to communicate with sources, citizens may avoid expressing unpopular views, and organisations may limit legitimate activity because they fear monitoring. Privacy therefore supports the practical exercise of Article 19 freedoms.

Article 21 provides that no person shall be deprived of life or personal liberty except according to procedure established by law. In the 2017 *Puttaswamy* judgment, a nine-judge Bench of the Supreme Court unanimously affirmed that privacy is a constitutionally protected right arising primarily from Article 21 and the freedoms guaranteed by Part III. The Court understood privacy as including bodily integrity, personal autonomy, intimate choices, and control over personal information.

Privacy and human dignity are deeply connected because dignity requires recognition of the individual as an autonomous person rather than merely as an object of governmental or commercial observation. A person who has no meaningful control over the body, choices, communications, or personal information cannot fully exercise liberty or develop an independent identity. The Supreme Court has subsequently reiterated that privacy is essential to liberty and dignity.

The right to privacy is not absolute. Lawful interference may be justified where it is supported by valid law, pursues a legitimate objective, is necessary and proportionate, and contains adequate safeguards against abuse. Digital surveillance must therefore be assessed not only by the importance of its stated purpose but also by whether less intrusive alternatives were available, whether the collection was limited, and whether effective oversight and remedies exist.

Right to Privacy as a Fundamental Right

The right to privacy protects the personal sphere within which an individual develops identity, forms relationships, communicates with others, makes intimate decisions, and exercises control over the body and personal information. Although the Constitution of India does not expressly employ the term "privacy," constitutional interpretation has established it as an essential component of the fundamental rights guaranteed under Part III. Its principal foundation lies in Article 21, which protects life and personal liberty, but privacy is also closely connected with equality under Article 14 and the freedoms guaranteed by Article 19. These constitutional provisions collectively protect individuals against arbitrary interference with their dignity, autonomy, communications, family life, personal choices, and informational interests.

Privacy cannot be understood merely as secrecy or complete isolation from society. Individuals regularly provide personal information to hospitals, banks, employers, government authorities, educational institutions, and digital platforms for specific purposes. Such disclosure does not mean that the information may thereafter be collected, stored, analysed, transferred, or disclosed without restriction. Privacy therefore includes the individual's legitimate interest in controlling the use of personal data and in being protected against unjustified monitoring, profiling, and disclosure. It

extends to the body, home, communications, location, movements, identity, beliefs, relationships, and intimate decisions.

The constitutional position of privacy was decisively clarified in *Justice K. S. Puttaswamy (Retd.) v. Union of India*. The proceedings arose in connection with a challenge to the Aadhaar programme and the collection of biometric and demographic information. Justice K. S. Puttaswamy, a retired judge of the Karnataka High Court, questioned whether such extensive collection and use of personal information could be reconciled with constitutional liberty and privacy. During the proceedings, a conflict became apparent between earlier and later judicial decisions. Earlier judgments, particularly *M. P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh*, had sometimes been interpreted as denying the existence of a general constitutional right to privacy. Later decisions, however, had protected private communications, bodily integrity, family life, medical information, reproductive freedom, and individual autonomy. This inconsistency required an authoritative constitutional determination.

The question was consequently referred to a nine-judge Constitution Bench of the Supreme Court. On 24 August 2017, the Court unanimously held that privacy is a constitutionally protected fundamental right. The judgment clarified that the absence of the word "privacy" from the constitutional text did not prevent its recognition. Fundamental rights were not treated as isolated provisions but as interconnected guarantees intended to protect liberty, equality, dignity, and autonomy. The Court held that privacy primarily arises from Article 21 and is also supported by the other freedoms and protections contained in Part III.

The judgment identified several dimensions of privacy. Bodily privacy protects physical integrity and control over the human body. Decisional privacy safeguards choices concerning marriage, family, reproduction, belief, relationships, and lifestyle. Informational privacy concerns the collection, processing, use, storage, and disclosure of personal information. Spatial privacy protects individuals against unjustified intrusion into private places, while communication privacy protects confidential exchanges from unauthorised interception or monitoring. The Court also recognised that privacy does not disappear merely because a person enters a public space. Modern technology can combine information concerning movement, communication, location, association, and behaviour to create a detailed personal profile. Constitutional protection may therefore remain relevant even when individual actions are partially visible to others.

Privacy was closely connected with human dignity. Dignity requires that a person be treated as an autonomous individual rather than as an object of unrestricted observation or control. A person who believes that every communication, movement, or association is constantly being monitored may alter otherwise lawful behaviour. Such monitoring can influence speech, association, personal relationships, professional activity, and political participation. Privacy therefore supports the meaningful exercise of liberty and other constitutional freedoms.

At the same time, the Supreme Court made it clear that privacy is not an absolute right. The State may adopt lawful measures for national security, public order, prevention and investigation of crime, public health, protection of citizens, and other constitutionally legitimate purposes. However, the mere existence of a public objective does not automatically justify every form of interference. A restriction affecting privacy must satisfy constitutional standards relating to legality, legitimate purpose, necessity, proportionality, and procedural safeguards.

The requirement of legality means that surveillance or data collection must have a clear basis in valid law. Informal directions, administrative convenience, or unrestricted executive discretion cannot ordinarily justify a serious intrusion into privacy. The governing law should identify the nature of the power, the circumstances in which it may be exercised, the competent authority, and the procedure to be followed. The authority must also pursue a legitimate State objective. National security, public safety, investigation of offences, and prevention of serious crime may constitute legitimate purposes,

but the stated objective must have a genuine relationship with the information being collected or the surveillance being conducted.

Necessity requires an examination of whether the interference is reasonably required to achieve the legitimate objective. A measure should not be broader than necessary, particularly where a less intrusive but equally effective alternative is available. Targeted surveillance based on lawful grounds is ordinarily less intrusive than indiscriminate collection affecting large numbers of persons who are not connected with any suspected wrongdoing. Proportionality requires a balance between the importance of the public objective and the degree of interference with individual rights. The sensitivity, duration, volume, purpose, and future use of the information collected must remain proportionate to the objective being pursued.

Procedural safeguards are equally important. Surveillance orders should be issued by competent authorities, reasons should be recorded, access to collected information should be restricted, records should be securely maintained, retention periods should be defined, and unauthorised disclosure should attract legal consequences. Review and oversight mechanisms help ensure that exceptional powers do not become routine instruments of uncontrolled monitoring.

The *Puttaswamy* judgment did not automatically invalidate all existing surveillance laws. Its significance lies in establishing the constitutional standards by which interception, monitoring, profiling, biometric collection, location tracking, and other privacy-restricting measures must be assessed. A statutory power may authorise surveillance, but the existence of such power does not end the constitutional inquiry. The manner in which the power is exercised, the scope of the order, the period of monitoring, the categories of information collected, and compliance with safeguards remain relevant.

The judgment has particular importance for digital surveillance. Modern surveillance may not always involve direct interception of message content. Metadata, location records, financial transactions, facial-recognition databases, communication patterns, and automated behavioural profiles may collectively reveal highly sensitive information. Such practices must be assessed according to their actual impact on privacy rather than merely according to their technical form.

Legal Framework Governing Digital Surveillance in India

The regulation of digital surveillance in India is distributed across constitutional provisions, parliamentary legislation, subordinate rules, and judicial decisions. No single statute governs every form of electronic monitoring. The applicable legal framework depends upon whether the surveillance concerns computer resources, telecommunication messages, cybersecurity, personal-data processing, criminal investigation, blocking of online information, or collection of electronic evidence. These laws must be interpreted together and remain subject to the fundamental rights guaranteed by the Constitution.

The Constitution of India provides the controlling legal framework. Articles 14, 19, and 21 collectively protect individuals against arbitrary and disproportionate surveillance. Article 14 guarantees equality before the law and equal protection of the laws. Its relevance to surveillance extends beyond conventional discrimination. State action must not be irrational, arbitrary, or based upon uncontrolled discretion. A surveillance system that permits selective targeting without objective criteria, produces discriminatory outcomes, or lacks transparent legal standards may raise constitutional concerns under Article 14.

Article 19 protects freedoms including speech and expression, peaceful assembly, association, movement, and profession, subject to constitutionally permissible restrictions. Surveillance can interfere with these freedoms even when no direct prohibition is imposed. Individuals may avoid expressing lawful opinions, communicating with journalists, joining organisations, participating in

public discussions, or associating with others if they reasonably fear continuous monitoring. This chilling effect demonstrates that privacy and freedom of expression are closely related. Article 21 protects life and personal liberty except according to procedure established by law. Judicial interpretation has connected Article 21 with dignity, autonomy, bodily integrity, communication, and informational control. A procedure affecting these interests must therefore be lawful, fair, just, and reasonable. The Constitution does not prohibit measures necessary for national security, public safety, criminal investigation, or protection of citizens. It requires such measures to be legally structured, limited to their legitimate purpose, and accompanied by adequate safeguards.

The Information Technology Act, 2000 is one of the principal statutes governing electronic records, computer resources, cybersecurity, and digital surveillance. Although it was originally enacted to facilitate electronic commerce and recognise electronic records, amendments introduced specialised provisions relating to security, interception, intermediaries, and computer-related offences.

Section 69 authorises the Central Government, State Governments, or specially authorised officers to direct an authorised government agency to intercept, monitor, or decrypt information generated, transmitted, received, or stored through a computer resource. Such power may be exercised for specified purposes, including sovereignty and integrity, defence, security of the State, friendly relations with foreign States, public order, prevention of incitement to certain offences, and investigation of offences. The reasons for exercising the power must be recorded in writing, and the action must comply with the prescribed procedure and safeguards. Section 69A permits the Central Government to direct the blocking of public access to information available through computer resources. This power may be exercised on specified grounds including sovereignty and integrity, defence, security of the State, friendly relations with foreign States, public order, and prevention of incitement to related cognisable offences. Blocking differs from interception because it restricts public access to information rather than secretly collecting private communications. Section 69B authorises the monitoring and collection of traffic data for cybersecurity purposes. Such monitoring may be undertaken to identify, analyse, and prevent intrusion, computer contaminants, or other threats to computer resources. Traffic data may reveal the origin, destination, route, time, duration, size, location, and type of communication service even where the actual content of the communication is not examined. This makes traffic data highly relevant to privacy because repeated records may disclose detailed patterns of behaviour and association.

Other provisions of the Information Technology Act also support confidentiality and lawful handling of information. Sections 72 and 72A address unauthorised disclosure and breach of confidentiality in specified circumstances, while Section 67C requires intermediaries to preserve and retain information in accordance with prescribed requirements. These provisions demonstrate that surveillance powers exist alongside duties concerning confidentiality, preservation, and lawful use.

The Information Technology Rules, 2009 provide the procedural framework for the exercise of powers under Sections 69, 69A, and 69B. The rules relating to interception, monitoring, and decryption prescribe the procedure for issuing and implementing interception directions. They seek to ensure that surveillance is conducted through competent authorities, recorded orders, and authorised agencies rather than informal or undocumented requests. The framework addresses implementation, confidentiality, responsibilities of intermediaries, review, retention, and destruction of records.

The rules governing blocking of online information establish a separate administrative process for examining requests under Section 69A. They require consideration by designated authorities, recording of reasons, and special procedures for urgent situations. The traffic-data monitoring rules regulate the collection of communication-related information for cybersecurity objectives. Together, these rules convert statutory powers into administrative procedures and provide safeguards intended to prevent unrestricted use. Their effectiveness depends upon strict compliance with documentation, purpose limitation, security, periodic review, and accountability. They must also be interpreted in light of the constitutional standards established in *Puttaswamy*. A formally valid surveillance direction

may still raise constitutional concerns if it is excessively broad, unnecessary, disproportionate, or unsupported by meaningful safeguards.

The Telecommunications Act, 2023 modernises and consolidates the law relating to telecommunication services, networks, spectrum, national security, and public safety. It replaced the principal statutory framework previously provided by the Indian Telegraph Act, 1885 and the Indian Wireless Telegraphy Act, 1933, subject to transitional and saving provisions.

Section 20 permits governmental action during a public emergency, including disaster management, or in the interest of public safety. The Central Government, State Governments, or specially authorised officers may temporarily take possession of telecommunication services or networks and may establish priority-routing arrangements for authorised emergency communications. The same provision also permits interception, detention, non-transmission, disclosure in intelligible form, or suspension of specified messages or telecommunication services.

Such measures may be ordered where considered necessary or expedient in the interests of sovereignty and integrity, defence and security of the State, friendly relations with foreign States, public order, or prevention of incitement to an offence. Reasons must be recorded in writing, and the exercise of power is subject to prescribed procedures and safeguards. The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 supplement the Act by regulating the administrative process for interception orders and their implementation.

The Telecommunications Act also contains provisions concerning network security, cybersecurity standards, encryption, national-security measures, and processing of traffic data. These powers assist in protecting communication infrastructure against disruption, hostile activity, intrusion, and misuse. However, interception must remain connected with statutory grounds, competent authorisation, defined duration, recorded reasons, and procedural safeguards. Information collected for one lawful purpose should not be indefinitely retained or used for unrelated objectives.

The Digital Personal Data Protection Act, 2023 regulates the processing of digital personal data. It recognises both the individual's interest in protecting personal information and the need of governments, businesses, and other entities to process data for lawful purposes. The Act applies to personal data collected in digital form and to non-digital data that is subsequently digitised, subject to statutory scope and exemptions.

The individual to whom the personal data relates is described as the Data Principal, while the person or entity determining the purpose and means of processing is known as the Data Fiduciary. The Act establishes a framework involving notice, consent, lawful processing, security safeguards, grievance redressal, breach-related responsibilities, and additional obligations for Significant Data Fiduciaries. It also provides rights relating to access, correction, erasure, grievance redressal, and nomination.

The Act is relevant to digital surveillance because systematic collection, profiling, retention, analysis, and sharing of identifiable information amount to personal-data processing. Digital platforms, financial institutions, communication services, online applications, and data-analysis companies may therefore be required to process information according to legal duties and security standards.

The Act contains exemptions for certain State functions, law-enforcement purposes, legal claims, and other specified circumstances. These exemptions do not remove the constitutional requirement that governmental interference with privacy must be legally authorised, necessary, proportionate, and protected against arbitrariness. The Act's implementation has been phased, and different provisions and rules become operational according to notified schedules. It nevertheless represents a significant

transition from fragmented confidentiality obligations toward a broader framework of digital-data accountability.

The Bharatiya Nagarik Suraksha Sanhita, 2023 governs criminal procedure and provides the legal framework for investigation, inquiry, trial, and other criminal proceedings. It is not a general surveillance statute and does not independently authorise unrestricted monitoring of citizens. Its relevance arises where investigating authorities require electronic communications, digital devices, documents, or other information connected with an alleged offence.

Section 94 empowers a court or police officer to require the production of documents, electronic communications, communication devices, or other material considered necessary or desirable for an investigation, inquiry, trial, or proceeding. Such power may be used to obtain records from individuals, organisations, service providers, or other lawful custodians, subject to the Sanhita and other applicable laws.

The provisions dealing with search warrants, entry, search, seizure, and impounding regulate the manner in which devices and records may be obtained. Section 105 requires the process of search and seizure, including preparation of the list of seized items and signatures of witnesses, to be recorded through audio-video electronic means. This requirement can improve transparency, preserve an objective record of official action, and assist courts in resolving later disputes about the manner in which evidence was collected.

The Sanhita also provides mechanisms for obtaining evidence situated outside India and responding to requests from foreign authorities. These provisions are important because cloud data, platform records, electronic communications, and digital evidence may be stored in foreign jurisdictions. Territorial jurisdiction provisions also recognise offences committed through electronic communications or telecommunications, while procedural provisions permit certain inquiries, trials, and proceedings to be conducted electronically.

Digital devices commonly contain large quantities of personal information unrelated to the alleged offence. Investigative access should therefore remain confined to legitimate purposes. Authorities must preserve forensic integrity, maintain the chain of custody, avoid unnecessary alteration of data, and respect legally privileged or irrelevant information. The Bharatiya Nagarik Suraksha Sanhita must consequently be applied together with the Constitution, the Information Technology Act, the Bharatiya Sakshya Adhiniyam, telecommunications law, and applicable data-protection requirements.

Taken together, these constitutional and statutory provisions form the principal legal framework governing digital surveillance in India. The framework recognises the legitimate need of the State to protect national security, public safety, communication networks, and citizens from serious offences. At the same time, it requires that surveillance remain legally authorised, connected with a legitimate objective, proportionate in scope, limited in duration, securely administered, and subject to procedural safeguards. The central legal challenge is therefore not to eliminate all surveillance but to ensure that necessary surveillance is carried out within constitutional boundaries and with sufficient accountability.

Major Challenges

The regulation of digital surveillance in India faces several constitutional, institutional, and technological challenges. One major concern is the limited presence of independent oversight over surveillance decisions. Interception and monitoring powers are ordinarily authorised and reviewed within the executive structure. Although statutory procedures require competent authorisation, recorded reasons, and compliance with safeguards, the absence of regular judicial or institutionally independent scrutiny may create doubts about whether surveillance remains necessary and

proportionate throughout its duration. Independent supervision could strengthen confidentiality, accountability, and public confidence without obstructing lawful measures adopted for national security or criminal investigation. A related difficulty is the lack of transparency surrounding surveillance practices. Complete disclosure of operational information may endanger investigations or national security, but excessive secrecy prevents meaningful public assessment of how frequently powers are used, what categories of data are collected, and whether misuse has occurred. Carefully designed transparency reports containing aggregated and non-sensitive information could improve accountability without revealing confidential methods or targets.

Broad statutory exemptions also generate concern. The Digital Personal Data Protection Act, 2023 permits exemptions for specified law-enforcement activities and allows the Central Government to exempt notified State instrumentalities on grounds including sovereignty, State security, public order, and prevention of related offences. Such purposes are legitimate, but broadly framed exemptions require clear necessity standards, purpose limitation, secure handling, and effective review to prevent exceptional powers from becoming routine. The increasing collection of large datasets presents another challenge. Location records, facial images, biometric information, financial transactions, internet activity, and communication metadata can collectively reveal detailed patterns of personal behaviour. Mass collection may include information concerning individuals who are not connected with any suspected offence. The risk becomes greater when different databases are combined, retained for long periods, or used for purposes unrelated to the original collection.

Finally, technological development frequently moves faster than legislation. Artificial intelligence, facial recognition, automated profiling, spyware, cloud computing, and advanced data analytics create surveillance capacities that older laws did not specifically anticipate. The constitutional principles recognised in *Puttaswamy* therefore remain essential: interference with privacy must have a lawful basis, pursue a legitimate objective, and satisfy necessity and proportionality. Continuous legislative review, technical expertise, independent supervision, security audits, limited retention, and effective remedies are necessary to ensure that surveillance protects the nation and its citizens without becoming arbitrary or excessive.

Conclusion

The right to privacy has become increasingly significant as digital technologies expand the ability of governments and private organisations to collect, analyse, and retain personal information. The Supreme Court's judgment in *Justice K. S. Puttaswamy (Retd.) v. Union of India* established that privacy is an essential part of constitutional liberty, dignity, and autonomy. At the same time, the judgment recognised that privacy is not absolute and may be lawfully restricted for legitimate purposes such as national security, public order, protection of citizens, and investigation of serious offences. India's surveillance framework is presently distributed across the Constitution, the Information Technology Act, 2000, the Telecommunications Act, 2023, the Digital Personal Data Protection Act, 2023, associated rules, and criminal-procedure legislation. The Information Technology Act permits interception and monitoring through computer resources on specified statutory grounds, while the Telecommunications Act regulates interception and related action during public emergencies or in the interest of public safety. The principal challenge is therefore not whether surveillance should be completely prohibited, but how lawful surveillance can be reconciled with fundamental rights. A balanced framework must ensure clear legal authority, recorded reasons, limited collection, secure storage, defined retention periods, independent review, and remedies against misuse. Government agencies must be able to respond effectively to terrorism, cybercrime, organised crime, and threats to public safety, but such powers should remain confined to genuine necessity. Future reform should promote institutional accountability, responsible technological use, and protection against unauthorised disclosure. A transparent and constitutionally regulated surveillance system can strengthen both national security and public confidence. Privacy and security should not be treated as opposing values; when governed by legality, necessity, proportionality, and effective safeguards, they can operate together within a democratic constitutional order.

References

1. The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India). <https://www.indiacode.nic.in/bitstream/123456789/20099/1/eng.pdf>
2. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India). <https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf>
3. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India). <https://www.indiacode.nic.in/handle/123456789/1999>
4. The Information Technology (Procedure and Safeguards for Interception, Monitoring or Decryption of Information) Rules, 2009, Gazette of India, Extraordinary (2009). <https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=Information+Technology+%28Procedures+and+Safeguards+for+Interception%2C+Monitoring+or+Decryption+of+Information%29+Rules%2C+2009.&searchradio=rules>
5. Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India). https://api.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
6. Legislative Department, Ministry of Law and Justice, Government of India. (2026). The Constitution of India (English version). <https://www.legislative.gov.in/documents/constitution-of-india/constitution-of-india-AjN2EjMtQWa?pageTitle=Constitution-of-India>
7. The Telecommunications Act, 2023, No. 44, Acts of Parliament, 2023 (India). <https://www.indiacode.nic.in/bitstream/123456789/20101/1/A2023-44.pdf>
8. Kaur, K. (2024). Digital surveillance and indian privacy laws. LawFoyer International Journal of Doctrinal Legal Research, 3(1), 61–77. <https://doi.org/10.70183/lijdlr.2024.v03.4>
9. Rai, N. (2020). Right to Privacy and Data Protection in the Digital Age – Preservation, Control and Implementation of Laws in India. Indian Journal of Law and Justice, 11(1), 115–129. <https://ir.nbu.ac.in/handle/123456789/4009>
10. Kumar, A., & Sharma, R. (2026). The right to privacy in the era of mass surveillance in India: A constitutional perspective. ResearchGate Preprint, 1–15. <https://doi.org/10.13140/RG.2.2.39969.34453>
11. Gupta, S. (2026). Constitutional limits on digital surveillance in India: Privacy, power, and the modern state under the DPDP Act. International Journal of Creative Research Thoughts (IJCRT), 14(5), 5005–5018. <https://www.ijcrt.org/papers/IJCRT26A5005.pdf>
12. Singh, P. (2026). The right to privacy in the age of surveillance. Indian Journal of Law and Legal Research, 8(2), 1–18. <https://www.ijllr.com/post/the-right-to-privacy-in-the-age-of-surveillance>

Disclaimer/Publisher's Note: The views, content, and claims expressed in this article are solely the responsibility of the author(s). The publisher and editors accept no legal liability for any errors, copyright infringement, or loss or damage arising from its use.