

Digital Privacy and Surveillance in India: Constitutional Challenges to Article 21 in the Modern Era

Jaswinder Kumar

LL.M., Dept. of Law, School of Legal Studies, Central University of Punjab (CUP), Bathinda,
Punjab, India

Dayabir Singh

Ph.D. Scholar, Dept. of Law, School of Legal Studies, Central University of Punjab (CUP), Bathinda,
Punjab, India

Dr. Ravinder Kaur

Assistant Professor, Dept. of Law, School of Legal Studies, Central University of Punjab (CUP),
Bathinda, Punjab, India

Abstract

The growth of technology has brought about a paradigm shift in the dynamics among the individual, the State, and technology companies. With the advent of smartphones, cloud computing, biometrics, artificial intelligence, facial recognition, social media sites, payment systems, and big data analysis, there has been an enormous change in the possibilities for communication, governance, economic growth, and information availability. Simultaneously, the technologies have enabled governments and private companies to gather, process, analyse, store, and distribute personal information more effectively. The constitutional significance of this trend is particularly relevant in India in light of the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The study provides insight into the issues that have emerged regarding digital privacy and surveillance under Article 21 of the Constitution of India. It presents the development of privacy jurisprudence from M.P. Sharma & Kharak Singh through Gobind, Maneka Gandhi, R. Rajagopal & People's Union for Civil Liberties to Puttaswamy. In addition, it discusses current surveillance systems, including interception of communications, biometrics, facial recognition, artificial intelligence, predictive analytics, and corporate data harvesting. The study also evaluates India's legislative regime, including the IT Act, 2000; the Aadhaar scheme; the Telecommunication Act, 2023; the DPDPA, 2023; and the DPDPR, 2025. This is done with the help of an international perspective on human rights standards and foreign legislation. The research is based on the methodology of doctrinal analysis and comparison. It is noticed that privacy protection in the digital age requires a comprehensive rights-based surveillance regime grounded in the principles of legality, necessity, proportionality, independent review, transparency, data minimization, and algorithmic accountability.

Keywords: *Digital Privacy; Article 21; Surveillance; Data Protection; Artificial Intelligence; Constitutional Law; Informational Privacy; Proportionality; India*

Submitted: June 20, 2026

Revised: July 29, 2026

Accepted: August 14, 2026

Published: August 25, 2026

DOI: 10.6084/m9.figshare.33689707



1. Introduction

Modern-day technology has grown into an essential element of social, economic, and governmental activities. Communication, education, medicine, finance, business, transport, entertainment, administration, and politics now rely on digital technologies. Thanks to the development of mobile phones, cloud computing, artificial intelligence, biometric authentication, social networking, digital payments, and big data analysis, the information society has emerged, and large volumes of personal data are continually generated. The digital revolution in India has been especially swift. The implementation of initiatives and systems related to digital governance, biometric identity, digital banking, online public services, and electronic communication has led to greater efficiency and increased service availability. But along with these benefits, digitalization has also turned personal information into an important economic, political, and governmental resource. Modern technology can

provide tools for continuous monitoring, large-scale data collection, biometric identification, facial recognition, metadata analysis, geolocation tracking, and algorithmic profiling. This means that surveillance need not necessarily entail physical invasion and could take place through the acquisition and analysis of seemingly routine information. The importance of privacy in the Indian constitutional framework is closely tied to Article 21. According to Article 21, "no person shall be deprived of his life or personal liberty except according to procedure established by law." The Indian Constitution does not explicitly refer to "the right to privacy". However, the Supreme Court has gradually widened the scope of life and personal liberty. The final stage of this process was reached in Justice K.S. Puttaswamy (Retd.) v. Union of India, where the nine-judge Constitution Bench recognized privacy as a fundamental right.

The rapid development of surveillance technology raises constitutional issues. The State has legitimate aims related to the protection of national security, the prevention of crime, the maintenance of law and order, and efficient governance. In India, significant progress has been made in legislative regulation. The Information Technology Act, 2000, gives important authorities regarding interception and monitoring. The biometric identification system in India, called Aadhaar, is regulated by specific legal provisions. The Telecommunications Act, 2023, regulates lawful interception and the subordinate legal instruments that govern it. The Digital Personal Data Protection Act, 2023, provides the statutory basis for data processing, and the Digital Personal Data Protection Rules, 2025, constitute additional regulations. Data protection and surveillance, however, are different issues. A data protection regime may be limited to regulating the use of personal data, without an all-inclusive approach to intelligence and surveillance. An important aspect of this research paper will therefore be to ensure that the privacy regime in India cannot be measured solely by data protection. Constitutional safeguards on authorizations, necessity, proportionality, oversight, retention, disclosure, accountability, and remedies must independently protect a surveillance regime. The problem statement in this research paper is whether India's Constitution and statutes adequately protect privacy under Article 21 against contemporary digital surveillance methods. It will also determine whether India's framework is well integrated with international standards for privacy protection.

- **Objectives of Study**

- a) To study the history of privacy as a constitutional right in India
- b) To examine the legal frameworks in India governing digital privacy and surveillance
- c) To discuss the constitutional ramifications of contemporary surveillance methods
- d) To assess India against the backdrop of international privacy standards.
- e) To examine the legal and institutional reforms that can address this problem

2. Review Of Literature

There is quite a vast body of literature on privacy and surveillance that spans across many disciplines. Law, politics, sociology, technology, and human rights have all played important roles in the development of the concept of privacy.

2.1 Alan F. Westin: Privacy and Freedom

Alan F. Westin's Privacy and Freedom remain a classic text on privacy in the academic literature. The core of Westin's understanding of privacy consisted of an individual's right to decide the times, manner, and scope of disclosing information about him to others.

The four aspects of privacy proposed by Westin include solitude, intimacy, anonymity, and reserve. These aspects remain relevant in the digital age. For instance, anonymity is endangered in the digital world due to the advent of face recognition technologies, digital identification, and geolocation. This work is particularly relevant in the context of constitutional law, given the nature of privacy. It is more than just a matter of individual preferences, since people need a protected space for self-reflection and communication.

2.2 Daniel J. Solove: Understanding Privacy

The book Understanding Privacy by Daniel Solove rejects the search for one universal definition of privacy. According to Solove, there are many different issues related to privacy, and they need to be defined in the context of harm rather than by a single definition. Solove's taxonomy classifies problems

related to information gathering, processing, distribution, and invasion. This classification can be very helpful in discussing digital surveillance, as modern privacy harms tend to occur not from the disclosure of any particular secret but rather from the processing of information. The Indian case would fit well within Solove's taxonomy, as it concerns how harmless information can become constitutionally significant when aggregated and processed through artificial intelligence and analytics.

2.3 Daniel J. Solove: Nothing to Hide

In *Nothing to Hide*, Solove criticizes the claim that people with nothing to hide and nothing illegal or shameful should be concerned about surveillance. This is because privacy is not just about being secret. It involves the right to privacy, dignity, independence of thought and protection from arbitrary power. The "nothing-to-hide" theory does not consider the aspect of the aggregation of informational harm. People might not complain about having bits and pieces of information collected by themselves. However, the sum of these bits and pieces could yield very detailed information. This information may affect choices and behaviours. *Nothing to Hide* is especially relevant to Article 21 since privacy under the Constitution must not be contingent on what people have to hide.

2.4 David Lyon and the Culture of Surveillance

The works of David Lyon have shown that the practice of surveillance is not limited to policing and intelligence organizations. The practice of surveillance has found its way into the daily practices of payments, shopping, social networking, travel, digital services, and biometric identification. David Lyon's theory of social sorting is particularly important. Surveillance not only involves watching people but also classifying them into different categories. Classification of people might be used to provide differential access to opportunities and resources. Thus, the issue of surveillance goes beyond issues of privacy to include discrimination.

2.5 Shoshana Zuboff and Surveillance Capitalism

In Shoshana Zuboff's book, *The Age of Surveillance Capitalism*, the focus moves beyond government surveillance to corporate power. Zuboff outlines a framework where human experience is transformed into data that can be processed to predict actions and possibly manipulate behaviour. This framework is pertinent to India in that the problem of privacy does not arise solely from the State.

2.6 Neil M. Richards and Intellectual Privacy

Neil Richards's *Intellectual Privacy* is relevant to the relationship between surveillance and freedom of thought. The need for people to have space to read freely, conduct research, develop ideas, and communicate without fear of continuous monitoring is vital. Digital records may indicate reading practices, browsing history, political views, and intellectual activity. As such, continuous monitoring leads to a chilling effect whereby an individual shies away from ideas that may seem unpopular or controversial.

2.7 Indian Constitutional Scholarship

The privacy debate in India's constitutional discourse has examined privacy through the prism of the interplay among dignity, liberty, autonomy, and informational self-determination. In the literature on the *Puttaswamy* case, it has been made clear that privacy cannot be seen as an isolated and limited right. The paper examines the works of M.P. Jain, V.N. Shukla, Julie E. Cohen, Christopher Kuner, and others, as well as international reports and committee materials. The literature highlights that digital privacy is a broad concept that includes informational autonomy, human dignity, democratic participation, and freedom from surveillance. The Justice B.N. Srikrishna Committee Report becomes important because it included principles such as consent, limitation of purpose, limitation of collection, transparency, accountability, and security measures.

The above literature provides a strong theoretical framework for protecting privacy. However, a research gap still exists. Most of the literature discusses data protection or surveillance technologies. Any complete constitutional analysis must examine the relationship among Article 21, surveillance powers, data protection, artificial intelligence, biometric governance, and corporate data extraction.

3. Research Methodology

The research employs doctrinal, analytic, critical and comparative methodologies in legal research. The doctrinal aspect of research is based on the study of primary sources of law, such as the Constitution of India, statutes, secondary law, government papers, and judicial rulings. The focus is made on Article 21 and other relevant constitutional provisions such as Articles 14, 19, 20, 32, and 226. The judicial aspect of research involves the analysis of landmark judgments about privacy and personal freedom such as *M.P. Sharma v. Satish Chandra*, *Kharak Singh v. State of Uttar Pradesh*, *Gobind v. State of Madhya Pradesh*, *Maneka Gandhi v. Union of India*, *R. Rajagopal v. State of Tamil Nadu*, *People's Union for Civil Liberties v. Union of India* and *Justice K.S. Puttaswamy (Retd.) v. Union of India*. The statutory component examines the Information Technology Act, 2000; the Aadhaar Act; the Telecommunications Act, 2023; the Digital Personal Data Protection Act, 2023; and related regulations. Comparative law examines the international human rights documents and other countries' approaches to privacy and data protection, specifically the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the European Union's General Data Protection Regulation. The analytical methodology involves assessing surveillance powers in terms of legality, legitimate aim, necessity, and proportionality. The methodology of critique focuses on weaknesses in the legislative framework, excessive executive powers, and transparency. The research is doctrinal in nature. It assesses the adequacy of the constitutional and legal framework by analysing relevant legal sources and literature.

4. Constitutional Evolution Of The Right To Privacy In India

4.1 The Early Restrictive Approach

Privacy as a constitutional right in India evolved gradually. In *M.P. Sharma v. Satish Chandra*, the Supreme Court took a limited approach to a constitutional right to privacy in the sphere of searches and seizures. This case exemplified the uncertainty about privacy in the Constitution during the early days of the Republic, when the right to privacy was not recognized as a fundamental right. The Supreme Court in *Kharak Singh v. State of Uttar Pradesh* decided on police surveillance and domiciliary visits. While the majority decision did not confer a constitutional right to privacy, it was an important step in personal-liberty jurisprudence.

4.2 Gobind and the Emergence of Constitutional Privacy

In *Gobind v. State of Madhya Pradesh*, the Court held that privacy is a constitutionally protected right but not absolute. This approach was crucial to the development of future surveillance cases. It raised the question of whether state intervention could be justified in certain situations, rather than merely the existence of privacy.

4.3 Maneka Gandhi and the Expansion of Article 21

In *Maneka Gandhi v. Union of India*, there was an important shift in the judicial interpretation of Article 21. The Supreme Court stated that any procedure by which a person is deprived of their liberty must be reasonable, just, and fair. The importance of the *Maneka Gandhi* case in relation to privacy lies in its adoption of a broad interpretation of personal liberty.

4.4 R. Rajagopal and the Right to Be Let Alone

In *R. Rajagopal v. State of Tamil Nadu*, the Supreme Court acknowledged an individual's right to safeguard his privacy from unwarranted publication and disturbance. This case proved the emerging relationship between privacy and dignity.

4.5 PUCL and Communication Privacy

In *People's Union for Civil Liberties v. Union of India*, the issue of telephone interception came before the Supreme Court, and the private nature of telephone communications was upheld.

This principle is important in current times as well. The technological medium of communication may change, but the principle is essentially the same: that state access to private communications requires law and procedures.

4.6 Puttaswamy and Constitutional Recognition

This crucial constitutional development took place through the decision of Justice K.S. Puttaswamy (Retd.) v. Union of India. A Bench comprising nine judges unanimously declared privacy a fundamental right. Privacy was linked with dignity, autonomy and liberty in the judgment. Privacy was

not confined to any particular constitutional article. It was derived mainly from Article 21 along with other rights enshrined under Part III of the Constitution.

The constitutional importance of the decision lies in the enforceability of privacy as a constitutional right against arbitrary State interference.

5. Digital Surveillance And Article 21

5.1 Nature of Digital Surveillance

Digital surveillance differs from conventional surveillance in that it enables the continuous, remote, and massive collection of information. Modern surveillance can include communications interception, location tracking, metadata collection, biometric identification, face recognition, social media monitoring and algorithmic profiling. A piece of information by itself might seem unimportant. However, combining several pieces of information can yield comprehensive insights into an individual's behaviour, relationships, and interests.

5.2 Government Surveillance

There are valid reasons the State should conduct surveillance. National security, counterterrorism, crime prevention, the protection of critical infrastructure, and other important matters may require information. Nevertheless, the presence of reasonable purposes does not mean that there will be no constitutional limits to surveillance activities. Surveillance should be based on law, be reasonable, necessary, and proportionate to the interference with privacy rights. There are valid reasons the State should conduct surveillance. National security, counterterrorism, crime prevention, the protection of critical infrastructure, and other important matters may require information.

5.3 Communications Interception

Interception of communications is undoubtedly one of the best examples of intruding into people's privacy. Personal details can be disclosed through telephone conversations or other kinds of electronic communications, along with related metadata. The laws in India have generally been based on provisions from earlier modes of communication. In light of this, the Telecommunications Act, 2023, and the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 offer a modern-day framework for interception. The 2024 Rules contain procedures for carrying out such interceptions with the help of authorized bodies and competent authorities. However, the presence of such rules is merely an indication that a proper constitutional framework has been established.

5.4 Aadhaar and Biometric Surveillance

There is something unique about the privacy problems associated with biometric information: it is inherently tied to physical identification. Fingerprints, irises, and faces cannot be treated the same way as standard passwords or other replaceable information. In this respect, the controversy surrounding Aadhaar revealed the problem of technological efficiency in relation to privacy. While biometrics may streamline welfare distribution and prevent some types of fraud, centralized information storage and widespread identity linking make any abuses and invasions even more harmful.

5.5 Facial Recognition

There is a particularly high level of concern about facial recognition technology, since it would be possible to identify someone in public without any contact. This technology could be useful for law enforcement, airport security, and crime prevention. Nevertheless, it will become possible to reduce anonymity and constantly track people. Three issues relating to the Constitution may be mentioned. First, facial recognition does not necessarily involve any form of consent. Secondly, there could be biases within algorithms that will target specific people. Thirdly, people will not always know that they are participating in the surveillance database.

Therefore, a rights-based approach should include the following requirements.

5.6 Artificial Intelligence and Predictive Surveillance

Artificial intelligence greatly enhances the scope and pace of surveillance through machine learning algorithms that analyse large datasets and make predictions. The constitutional concern is not just about collecting data; it is about whether there is an automatic mechanism that will use the data collected to make decisions on individuals.

AI systems may perpetuate bias in training data, and their decision-making methods may lack clarity. Lack of clarity makes it hard for individuals to understand what is going on and makes judicial review very hard. Therefore, artificial intelligence-enabled surveillance must involve transparency, explainability, human supervision, and independent auditing.

5.7 Corporate Surveillance

Nowadays, privacy intrusions increasingly come from private parties. Companies gather data via social media sites, search engines, apps, e-commerce websites, digital payment systems, and cloud computing services. Corporate surveillance is economically significant because personal data can be used to build behavioural models, which, in turn, create opportunities for tailored advertising.

The public-private dichotomy complicates the constitutional challenge, since Article 21 applies to State activities, whereas data processing by private parties is subject to data protection statutory regimes.

6. Indian Legal Framework

6.1 Information Technology Act, 2000

The IT Act 2000 continues to be an essential part of India's digital legislation. Clauses about interception, monitoring, and decryption have major privacy ramifications. Section 69 contains provisions regarding interception, monitoring, and decryption of information. These powers may be justified for the public good, but their use under the Constitution should be in accordance with Article 21 and the precedents set by the Supreme Court.

6.2 Telecommunications Act, 2023

The Telecommunication Act, 2023, updates India's telecommunications law and supersedes any previous legislative schemes. The 2024 Rules on lawful interception, formulated under the Telecommunication Act, regulate the interception of messages. The significance of such legislation is that telecommunications technology has advanced far beyond the state it was in when the previous laws regulating interception were developed.

6.3 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, is a significant piece of legislation in India's data protection regime. The objective of the Act is to regulate the processing of digital personal data, taking into account individuals' interests in protecting their personal data, as well as valid grounds for processing it.

6.4 Digital Personal Data Protection Rules, 2025

A significant development following the dissertation is the notification of the Digital Personal Data Protection Rules, 2025, by the Ministry of Electronics and Information Technology on 14 November 2025. The rules operationalize certain crucial components of the DPDP framework and become part of the institutional structure in place to protect personal data in India.

7. International Human Rights Framework

7.1 Universal Declaration of Human Rights

Article 12 of the Universal Declaration of Human Rights protects the individual from arbitrary interference with their privacy, family, home, and correspondence.

The article shows how privacy has traditionally been seen as an important human right. In the current situation, technological monitoring expands the scope of interference beyond anything envisaged at the time of the Declaration.

7.2 International Covenant on Civil and Political Rights

Similarly, Article 17 of the ICCPR protects against arbitrary or unlawful interference with one's privacy, family, home, or correspondence. Arbitrariness is especially important to consider. Although surveillance could be conducted in accordance with domestic law, it would still raise concerns under human rights standards if the law itself or its implementation were disproportionate or unpredictable.

7.3 European Convention on Human Rights

Article 8 of the European Convention guarantees respect for private and family life, home, and correspondence. There have been extensive principles developed in European case law on surveillance, legitimate aims, necessity, and proportionality. It is clear from the European perspective that

importance is attached to independence in supervising State surveillance activities that affect individuals' privacy.

7.4 General Data Protection Regulation

The GDPR is among the most advanced regulatory models for personal data protection. Principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and accountability are some of those included in the GDPR.

7.5 OECD Privacy Principles

The OECD Privacy Guidelines stress collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

These guidelines are beneficial since they shift privacy regulation from consent to organizational accountability.

8. Constitutional Test of Surveillance

The central constitutional question is whether State surveillance satisfies the standards established through privacy jurisprudence.

8.1 Legality: There must be a legal justification for surveillance. Convenience for an executive is no substitute for legality. The law must be clear enough for people to know when surveillance may take place.

8.2 Legitimate State Aim: There must be a legitimate constitutional purpose of surveillance. National security, crime prevention, and public safety are legitimate purposes.

8.3 Necessity: It needs to show that surveillance is indeed required to fulfill a legitimate aim.

If other methods achieve the same aim without being as intrusive, conducting surveillance could pose a challenge.

8.4 Proportionality: Proportionality involves a consideration of the nature of the link between the public goal and the intrusion on privacy. Mass and indiscriminate surveillance is more constitutionally troublesome than targeted surveillance based on particular information.

8.5 Procedural Safeguards: Controls over the issuance, retention period, evaluation, access, and disposal of data should complement monitoring. The lack of independent oversight enhances the likelihood of abuse.

8.6 Effective Remedies: People should have a means to confront any violations of their privacy. A right that cannot be remedied is only a theoretical right. These things are thus crucial elements of privacy protection.

9. Critical Analysis and Research Findings

The research produces several principal findings.

Privacy became part of Article 21 following the Puttaswamy case. This is because privacy became part of the constitutional right to dignity, liberty, and autonomy. The constitutional nature of privacy makes it a firm basis for the analysis of surveillance. Powers of surveillance are scattered across multiple acts, regulations, and administrative processes. These include the Telecommunication Act, the Information Technology Act, the Aadhaar, data protection laws, and several other pieces of legislation that cover different areas of digital information. It is the fragmented nature of the law that creates ambiguity around the procedures and responsibilities. The DPDP Act is an important data protection law, but questions of personal data regulation and State surveillance pose distinct concerns. The need for a constitutional framework for surveillance encompasses interception, intelligence gathering, metadata, algorithmic surveillance, biometrics, and data access.

One of the constitutional issues is how much surveillance can be decided by executive bodies. Independent monitoring plays a significant role, since a decision to conduct surveillance usually involves certain facts unknown to the subject of surveillance. AI-driven surveillance raises concerns about opacity, algorithmic bias, discrimination, and accountability. Legal mechanisms available in ordinary times might not suffice because the individual cannot understand how or why an algorithm has classified or predicted them. Commercial practices related to the harvesting, compilation, and analysis of behavioural data may influence autonomy and democratic engagement. Privacy is not just an issue of personal confidentiality. When individuals feel that their interactions, searches,

connections, and politics are being constantly watched, they will behave differently. A chilling effect may arise in the process, hindering freedom of speech, freedom of association, intellectual growth, and democracy.

10. Recommendations

10.1 Enact a Comprehensive Surveillance Law

India could well do with an exclusive surveillance law that encompasses all aspects of state surveillance, including State interception, metadata collection, digital surveillance, and other innovative methods. This will ensure clarity about surveillance powers and their scope.

10.2 Strengthen Independent Judicial Oversight

Surveillance authorization must, when constitutionally and logistically permissible, include independent judicial or quasi-judicial oversight.

The independent process will minimize the danger of unbridled executive discretion.

10.3 Establish Parliamentary Oversight

With proper security measures in place, parliamentary committees could review the surveillance policy, compile authorization statistics, and assess compliance and legislation.

Oversight should not undermine national security considerations. Instead, it should enhance democracy.

10.4 Introduce Strict Data-Minimization Rules

Only the amount of information that is reasonable for a valid purpose should be collected.

Unrelated information should not be stored indefinitely.

10.5 Establish Clear Retention and Deletion Standards

The surveillance data should be retained only for a limited period for legitimate reasons.

There should be an automated process to delete the data after its validity period has expired.

10.6 Strengthen Algorithmic Accountability

AI systems used for surveillance should be subject to: Documented purpose; Accuracy testing; Bias assessment; Explainability requirements; Human oversight; Independent auditing; and Mechanisms for challenging consequential decisions.

10.7 Regulate Facial Recognition

It should not be used as a general surveillance method without any restrictions. Its deployment needs to be governed by law with respect to its purposes, accuracy, retention, and oversight.

10.8 Strengthen Corporate Accountability

Organizations that process personal data must be forced to have good security, transparency, and accountability measures. High-risk processing needs to undergo a privacy impact assessment and organizational safeguards.

10.9 Improve Transparency

Government departments should disclose aggregate data on surveillance authorizations where such disclosure does not conflict with legitimate security concerns. Transparency facilitates accountability without compromising operational details.

10.10 Protect Whistleblowers and Journalistic Sources

There needs to be increased constitutional protection for private communications between journalists, lawyers, and other professionals.

10.11 Develop Effective Remedies

There should be means through which individuals can contest unlawful surveillance and get an appropriate remedy. These means should not rely solely on the individual's knowledge of secret surveillance techniques.

10.12 Strengthen Privacy by Design

Privacy should be built into digital systems rather than treated as an afterthought once a system has been misused. Data minimization, security, access controls, and privacy impact assessments should be built into government and high-risk digital systems.

10.13 Promote Digital Constitutional Literacy

Individuals need to be educated about their rights concerning personal information, surveillance, and digital services. A legal remedy becomes more effective once people are made aware of their rights.

11. Limitations of Study

The paper is mainly doctrinal, not empirical, research on people's attitudes toward surveillance. It is not an empirical measurement of the number of surveillance warrants issued by governmental authorities or an assessment of the technical accuracy of specific artificial intelligence technologies. This study evaluates constitutional and legal doctrines through legislation, court cases, international standards, publications, and academic literature. Further research can include empirical interviews with lawyers, judges, technology specialists, law enforcement officers, policymakers, and affected parties.

12. Conclusion

The digital revolution has changed the very essence of privacy and its implications in today's world. The digital-age man leaves behind continuous traces of information as he communicates, conducts business, socializes, searches the web, travels with location services enabled, and uses biometric authentication on his device. This results in opportunities for good governance and development on one hand, and unparalleled opportunities for surveillance and profiling on the other. Puttaswamy is significant not only because it declared privacy as a fundamental right. It is more than that as it equates privacy with dignity, autonomy, and liberty. The understanding that privacy is linked to autonomy and dignity in this way provides a normative basis for assessing contemporary surveillance technologies. There have also been legislative developments in India. The Information Technology Act, the Telecommunications Act, the Aadhaar system, and the Digital Personal Data Protection Act are among the legislative provisions in the surveillance regime. The Notification on the Digital Personal Data Protection Rules, 2025, is yet another step toward operationalizing the data protection architecture. However, certain difficulties still exist. Privacy regulation and surveillance regulation are two different things. The Indian surveillance regime is fragmented. Various pieces of legislation deal with the matter. Executive discretion remains a constitutionally delicate issue. The surveillance should function in accordance with legality, legitimacy, necessity, proportionality, transparency, independence and redress. There should be data collection for specific purposes, storage of data for a necessary period, and protection of data from any abuse. The final aim should be to establish a digital constitutional order based on rights, in which technology remains accountable to constitutional principles.

References

Books

- Cohen, Julie E., *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press, 2012.
- Jain, M.P., *Indian Constitutional Law*, LexisNexis.
- Lyon, David, *Surveillance Society: Monitoring Everyday Life*, Open University Press, 2001.
- Lyon, David, *Surveillance Studies: An Overview*, Polity Press, 2007.
- Lyon, David, *The Culture of Surveillance: Watching as a Way of Life*, Polity Press, 2018.
- Richards, Neil M., *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Oxford University Press, 2015.
- Shukla, V.N., *Constitution of India*, Eastern Book Company.
- Solove, Daniel J., *Understanding Privacy*, Harvard University Press, 2008.
- Solove, Daniel J., *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Yale University Press, 2011.
- Westin, Alan F., *Privacy and Freedom*, Atheneum, 1967.
- Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, 2019.

Articles and Scholarly Literature

- Warren, Samuel D. and Louis D. Brandeis, "The Right to Privacy", 4 *Harvard Law Review* 193 (1890).

Richards, Neil M., scholarship concerning intellectual privacy and civil liberties in the digital environment.

- Solove, Daniel J., scholarship concerning privacy taxonomy, surveillance and information-processing harms.
- Lyon, David, scholarship concerning surveillance society, social sorting and surveillance culture.
- Zuboff, Shoshana, scholarship concerning surveillance capitalism and behavioral data extraction.
- Cohen, Julie E., scholarship concerning informational privacy, autonomy and the networked self.

C. Indian Constitutional and Legislative Materials

- Constitution of India, 1950.
- Indian Telegraph Act, 1885.
- Information Technology Act, 2000.
- Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
- Telecommunications Act, 2023.
- Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024.
- Digital Personal Data Protection Act, 2023.
- Digital Personal Data Protection Rules, 2025.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

D. Committee and Institutional Reports

- Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Ministry of Electronics and Information Technology, 2018.
- Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, revised 2013.
- UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021.
- Internet Freedom Foundation, reports and research concerning India's surveillance regime and constitutional safeguards.

E. International Instruments

- Universal Declaration of Human Rights, 1948, Article 12.
- International Covenant on Civil and Political Rights, 1966, Article 17.
- European Convention on Human Rights, 1950, Article 8.
- Regulation (EU) 2016/679, General Data Protection Regulation.

F. Indian Cases

- *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
- *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
- *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
- *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
- *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
- *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2018) 3 SCC 797.
- *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.
- *Shafin Jahan v. Asokan K.M.*, (2018) 16 SCC 368.
- *Common Cause v. Union of India*, (2018) 5 SCC 1.
- *K.S. Puttaswamy v. Union of India* and subsequent Supreme Court jurisprudence concerning informational privacy, dignity and autonomy.