

State Surveillance and the Right to Privacy in the Digital Age: Finding the Constitutional Balance

Ms. Dharshini Prishtila R¹, Dr. T. Ambika²

¹3rd Year B.A.Llb(H), School Of Law, Sathyabama Institute Of Science And Technology

²Assistant Professor, School Of Law, Sathyabama Institute Of Science And Technology

Abstract

The rapid growth of digital technology has changed the way governments maintain national security, prevent crime, and provide public services. Today, state surveillance includes tools such as CCTV cameras, facial recognition systems, mobile phone tracking, internet monitoring, and the collection of digital data. While these technologies help protect society, they also raise concerns about the privacy and freedom of individuals. This creates an important constitutional question of how to balance the powers of the State with the fundamental rights of citizens. This paper examines the relationship between state surveillance and the right to privacy in the digital age. It aims to analyse the constitutional and legal framework governing surveillance in India, examine the right to privacy under Article 21 of the Constitution, and study whether the existing legal safeguards are sufficient to prevent misuse of surveillance powers. The study follows a doctrinal research methodology based on the analysis of constitutional provisions, statutes, judicial decisions, books, journal articles, and other secondary sources. The study finds that surveillance is necessary for national security, cyber security, and crime prevention, but it should not lead to arbitrary or excessive interference with individual privacy. The recognition of privacy as a fundamental right by the Supreme Court in the landmark Justice K.S. Puttaswamy v. Union of India judgment highlights the need for surveillance measures to be lawful, necessary, proportionate, and accountable. The paper concludes that achieving a constitutional balance requires effective legal safeguards, transparent procedures, independent oversight, and stronger protection of citizens' digital rights. Such a balanced approach can ensure both national security and the preservation of fundamental rights in a democratic society.

Keywords: State Surveillance, Right to Privacy, Digital Surveillance, Article 21, Fundamental Rights, National Security, Constitutional Balance, Digital Rights, Justice K.S. Puttaswamy v. Union of India, Legal Safeguards.

1. Introduction

The rapid development of digital technology has transformed the way government function, maintain public security and prevent crime. With the increasing use of CCTV cameras, facial recognition, mobile phone tracking, internet monitoring and digital data collection, the State has gained greater ability to monitor individuals and activities. These technologies can play an important role in protecting national security, preventing crime and addressing emerging cyber threats. However, the growing use of State

surveillance also raises serious concerns about the privacy, liberty and freedom of individuals. Excessive or unnecessary surveillance may allow the State to access personal information and interfere with the private lives of citizens. This creates an important constitutional question: how can the State protect national security without unnecessarily interfering with individual privacy? This research examines the relationship between State surveillance and the right to privacy in the digital age, with particular focus on India's constitutional and legal framework. It analyses whether existing safeguards are sufficient to prevent arbitrary or excessive surveillance and explores how principles such as legality, necessity, proportionality, transparency and accountability can help achieve a proper balance between national security and individual privacy.

2. Contemporary Context and Research Problem

Example 1 — Jantar Mantar

During recent student protests at Jantar Mantar, Delhi, there were allegations that Delhi Police used facial-recognition technology, AI-enabled surveillance equipment, cameras and mobile surveillance systems to monitor people at the protest. Protesters and digital-rights groups raised concerns that people were being recorded and potentially identified even when they were simply participating in a peaceful protest. The police, however, have said that the facial-recognition technology was used to identify known criminals or people with criminal histories, and the government has argued that photography and videography are part of maintaining law and order. The important point is: the court has not finally declared this surveillance unconstitutional. The controversy itself raises the constitutional question my paper studies.

Example 2 — Pegasus

Pegasus is a powerful spyware program made by the Israeli company NSO Group. It secretly installs on iPhones and Android phones. It lets the user read messages, look at photos, track locations, and turn on the camera or microphone without the owner knowing. In India, allegations arose that Pegasus spyware had been used to target individuals including journalists, activists and others. The matter reached the Supreme Court, which considered the issue of privacy and surveillance. The Court appointed a technical committee to investigate the allegations. The controversy raised a very simple question: If the State suspects one person, can it secretly enter that person's private digital life without adequate legal safeguards?

3. Concept and Evolution of State Surveillance

State surveillance means the monitoring, observation, collection and analysis of information by the government for purposes such as national security, crime prevention and public safety. Earlier, surveillance was mainly done through physical observation, informants and following individuals. With the development of telecommunication, telephone interception became common. The Supreme Court has recognised that telephone tapping can seriously affect an individual's privacy and therefore requires legal safeguards.¹ Later, CCTV cameras and the internet introduced new forms of monitoring. Today, technology has made surveillance more advanced. Governments may use facial recognition, biometric systems, mobile tracking, social media monitoring, Artificial Intelligence and Big Data to collect and analyse large amounts of information. Thus, surveillance has evolved from simple physical monitoring to large-scale digital surveillance. While it can help protect national security and prevent crime,

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

it may also affect an individual's privacy and fundamental rights. Therefore, State surveillance must be used for legitimate purposes with proper legal safeguards and reasonable limits.

4. State Surveillance in the Digital Age: Necessity and Concerns

The increasing use of digital technology has made State surveillance an important tool for maintaining security and protecting public interests. At the same time, the ability to collect and analyse large amounts of personal information has created concerns about the misuse of surveillance powers. Therefore, State surveillance has both legitimate purposes and potential risks, making it necessary to maintain a proper balance between security and individual rights.

4.1 Need for State Surveillance

State surveillance can be necessary for national security by helping authorities identify and respond to threats to the country. It also assists in the prevention and investigation of crime by providing information that may help identify suspects and establish connections between criminal activities. Surveillance can support counter-terrorism efforts by detecting possible threats and preventing attacks. In the digital environment, surveillance also plays a role in cybersecurity, particularly in identifying cyber threats and protecting government and public systems. CCTV and other monitoring systems can contribute to public safety, while digital monitoring may help detect certain forms of fraud and financial crime. Surveillance can also assist in protecting critical infrastructure, such as communication networks, transportation systems and essential public services. During emergencies and disasters, information gathered through digital systems may further assist authorities in managing situations and protecting the public. Therefore, surveillance, when used for a lawful and clearly defined purpose, can serve important public interests.

4.2 Risks Associated with Excessive Surveillance

Although surveillance can be necessary, excessive or uncontrolled monitoring can create serious risks to individual rights. Continuous monitoring may result in an invasion of privacy, particularly when personal information is collected without adequate safeguards.² The knowledge that communications or activities may be monitored can also create a chilling effect on freedom of speech, as individuals may hesitate to express their views freely. unauthorised collection and use of personal data can expose individuals to further risks. Large-scale data collection may also lead to profiling, where information about a person's behaviour, movements or associations is used to make assumptions about them. Mass surveillance can affect large numbers of people even when there is no specific suspicion against them. If surveillance systems are poorly designed or biased, they may also result in discrimination or unfair targeting. When surveillance powers are not properly controlled, there is a risk that they may be used beyond their original purpose or become a means of excessive State control. Therefore, the central issue is not whether the State should have surveillance powers, but how those powers should be exercised within constitutional limits. This leads to the important question at the heart of this research: When does legitimate State surveillance become unconstitutional surveillance? The answer requires an examination of legality, necessity, proportionality, safeguards and accountability in the exercise of State surveillance powers.

5. Right to Privacy as a Fundamental Right in India

The right to privacy in India has developed gradually through the decisions of the Supreme Court. In M.P.

² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India)

Sharma v. Satish Chandra and Kharak Singh v. State of Uttar Pradesh, the Court considered issues related to privacy and State interference. However, privacy was not clearly recognised as a separate fundamental right at that time. The position changed with the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), where the Supreme Court recognised privacy as a fundamental right under the Constitution. The Court explained that privacy is closely connected with life, personal liberty, dignity and individual freedom under Article 21. It also recognised the importance of informational privacy, which is especially relevant today because individuals share large amounts of personal information through digital platforms and services. Privacy has different aspects, including physical privacy, decisional privacy, informational privacy and communication privacy. Physical privacy protects a person's body and personal space, while decisional privacy protects personal choices and autonomy. Informational privacy concerns the collection and use of personal information, and communication privacy protects private communications from unjustified interference. Therefore, the recognition of privacy as a fundamental right places limits on the power of the State and requires proper justification and safeguards whenever surveillance or other State action interferes with an individual's privacy.

6. Constitutional Limits on State Surveillance

The right to privacy is a fundamental right under the Constitution, but it is not an absolute right. In certain circumstances, the State may need to interfere with an individual's privacy for reasons such as national security, prevention of crime and protection of public safety. However, such interference must be within constitutional limits and should not be arbitrary or excessive.

The first requirement is legality, which means that surveillance must be authorised by a valid law and exercised according to the procedure established by law. Secondly, there must be a legitimate State aim, such as protecting national security, preventing serious crimes or responding to genuine threats. Thirdly, surveillance must satisfy the requirement of necessity, meaning that the measure should be genuinely required to achieve the intended purpose. The principle of proportionality requires the State to ensure that the surveillance used is not excessive and that a less intrusive method is considered where it can achieve the same objective. Finally, procedural safeguards are necessary to prevent the misuse of surveillance powers. Proper authorisation, independent review, oversight and accountability can help protect individuals from arbitrary interference. Therefore, State surveillance must be based on law, serve a legitimate purpose, be necessary and proportionate, and operate with adequate safeguards. These constitutional requirements help maintain a balance between the State's responsibility to protect national security and the individual's right to privacy.

7. Legal Framework Governing Surveillance in India

India has several laws that give government authorities powers to intercept communications, monitor digital information and process personal data. At the same time, these laws provide certain conditions and safeguards to prevent misuse. The legal framework has developed from the older Indian Telegraph Act, 1885 to the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the Telecommunications Act, 2023. Examining these laws is important to understand both the surveillance powers given to the State and the protection available to individuals.

7.1 Indian Telegraph Act, 1885

The Indian Telegraph Act, 1885, particularly Section 5(2), provided a legal basis for the interception of communications in situations involving public emergency or public safety and for specified purposes such

as national security and prevention of offences. The provision also requires certain conditions to be followed. However, as the Act was introduced in the pre-digital period, its suitability for modern forms of communication has been questioned.

7.2 Information Technology Act, 2000

The Information Technology Act, 2000 deals more directly with digital surveillance. Section 69 allows authorised government authorities to order the interception, monitoring or decryption of information stored or transmitted through a computer resource for specified purposes. The provision is subject to prescribed procedures and safeguards. However, the wide nature of these powers makes proper oversight important for protecting individual privacy.

7.3 Information Technology Rules

The Information Technology (Procedures and Safeguards for Interception, Monitoring or Decryption of Information) Rules, 2009 provide procedures for exercising powers under Section 69. They regulate matters such as authorisation, review and handling of intercepted information. These procedures are important because surveillance powers should be exercised according to clear safeguards rather than through unrestricted administrative discretion.

7.4 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is important for protecting informational privacy. It regulates the processing of digital personal data and establishes duties relating to the use and protection of such information. However, the law also provides certain exemptions for State functions, including matters connected with security and prevention or investigation of offences. Therefore, an important concern is whether such exemptions provide sufficient protection against unnecessary State access to personal data.

7.5 Telecommunications Act, 2023

The Telecommunications Act, 2023 provides the present legal framework for telecommunications in India. It also permits interception of messages in specified circumstances, subject to prescribed conditions and safeguards. The Act is particularly relevant to modern communication systems and the growing use of digital telecommunications.

7.6 Other Relevant Frameworks

Surveillance is also connected with criminal investigation, cybersecurity measures, digital evidence and data retention practices. These mechanisms can assist authorities in preventing and investigating offences, but they may also increase access to personal information. Therefore, the effectiveness of India's surveillance framework depends not only on the powers given to the State but also on the safeguards controlling their use.

Overall, Indian law provides surveillance powers for legitimate purposes, but the key issue is whether these powers are exercised with legality, necessity, proportionality, transparency and accountability. A strong legal framework must protect national security while also preventing unnecessary or arbitrary interference with individual privacy.

8. Judicial Response to State Surveillance and Privacy

The Indian judiciary has played an important role in developing the law relating to privacy and State surveillance. The judicial approach has gradually moved from a limited understanding of privacy to recognising it as a fundamental constitutional right. In *Kharak Singh v. State of Uttar Pradesh*, the Supreme Court examined police surveillance, including domiciliary visits and night surveillance, and considered

its impact on personal liberty. Although privacy was not expressly recognised as a separate fundamental right at that stage, the case marked an early step towards protecting individuals from intrusive State action. Later, in *People's Union for Civil Liberties v. Union of India* (1997), the Court dealt with telephone tapping and recognised that telephone conversations form part of an individual's private life. It also laid down procedural safeguards to prevent arbitrary interception. In *District Registrar and Collector v. Canara Bank*, the Court recognised the privacy attached to personal and financial information and emphasised the need for proper legal authority before accessing such information. The most significant development came in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where a nine-judge Bench unanimously recognised privacy as a fundamental right and connected it with dignity, autonomy and personal liberty. The Court also recognised informational privacy, which has particular importance in the digital age. Subsequently, in the Aadhaar case (2018), the Supreme Court examined the collection and use of biometric and personal data and applied the principle of proportionality. These decisions demonstrate the gradual development of Indian privacy jurisprudence from physical surveillance and telephone interception to digital and biometric surveillance. They establish that State surveillance must have a legal basis, legitimate purpose, adequate safeguards and proportionality, ensuring that national security and public interest do not become unlimited grounds for interfering with individual privacy.

9. National Security vs. Individual Privacy

National security and individual privacy are both important in a democratic society. The State has a responsibility to protect people from terrorism, organised crime, cybercrime and other threats. Surveillance can help government authorities gather intelligence, identify potential threats, prevent criminal activities and maintain public safety. In the digital age, where many criminal activities take place through online platforms and communication networks, access to certain information may be necessary for effective law enforcement and national security. At the same time, individuals have a right to live with privacy, liberty and dignity. Excessive State surveillance can interfere with personal choices, private communications and the freedom to express opinions. Continuous monitoring may also create fear among individuals and discourage them from freely expressing themselves. The collection and use of personal information without proper safeguards can further result in profiling, misuse of data and arbitrary State action. Therefore, national security cannot be treated as a justification for unlimited surveillance. The real issue is not whether national security or privacy should be given greater importance in every situation. Both interests are necessary for a democratic society. The State must be able to respond to genuine threats, but it must exercise its powers within the limits of the Constitution. Surveillance should therefore have a clear legal basis, serve a genuine purpose and be limited to what is necessary for achieving that purpose. Proper authorisation, independent oversight and effective safeguards are also necessary to prevent misuse. A balanced approach can allow the State to protect national security while respecting the privacy and freedom of individuals. Security should not require the complete loss of privacy, and the protection of privacy should not prevent the State from responding to genuine threats. The challenge is to ensure that surveillance remains lawful, necessary and proportionate. This balance between security and individual rights is essential for maintaining both effective governance and constitutional democracy.

10. Recommendations and Suggestions

Based on the analysis, India needs a stronger framework to balance national security with the fundamental right to privacy. The following measures are recommended:

First, a clear legal framework for State surveillance should be introduced. The law should clearly specify the circumstances, purposes and authorities under which surveillance may be carried out. Surveillance should have a proper legal basis and should not be exercised arbitrarily.

Second, stronger independent and judicial oversight is necessary. An independent authority should monitor the exercise of surveillance powers, while courts should have an active role in reviewing highly intrusive surveillance measures. This would help prevent misuse of power and ensure accountability.

Third, the principles of necessity and proportionality should be strictly followed. Surveillance should be used only when it is necessary for a legitimate purpose and when less intrusive alternatives are not sufficient. The State should also collect only the information that is necessary and should not retain personal data for longer than required. Measures should be targeted towards genuine threats rather than allowing unnecessary mass surveillance.

Fourth, transparency, accountability and effective remedies should be strengthened. Government agencies should follow clear procedures and maintain proper records of surveillance activities. Individuals affected by unlawful surveillance should have accessible legal remedies and appropriate mechanisms for challenging violations of privacy.

Fifth, surveillance laws and technologies should be regularly reviewed. Rapid technological developments require periodic review of existing laws and surveillance practices. The use of Artificial Intelligence, facial recognition and other advanced technologies should be subject to clear rules, human oversight and safeguards against errors, discrimination and misuse. Independent technology audits can also help identify security weaknesses and unnecessary data collection.

Finally, privacy should be incorporated into the design of government surveillance systems. The principle of privacy by design should ensure that privacy protection is considered from the beginning of developing and implementing surveillance technologies. Strong safeguards should also be adopted to protect informational privacy and prevent the unauthorised use or disclosure of personal data.

Overall, State surveillance should not be completely avoided, as it may be necessary for national security and public safety. However, it must operate within legality, necessity, proportionality, transparency and accountability. A rights-based surveillance framework can therefore help India protect both national security and individual privacy.

11. Conclusion

State surveillance is necessary for protecting national security, preventing crime, fighting cyber threats and maintaining public safety. However, unlimited or excessive surveillance can seriously affect the privacy, liberty and dignity of individuals. In India, the recognition of privacy as a fundamental right requires the State to exercise surveillance powers within constitutional limits. Surveillance should therefore have a clear legal basis, a legitimate purpose, necessity and proportionality. Proper oversight, transparency and accountability are also essential to prevent misuse. The aim should not be to choose between security and privacy, but to maintain a reasonable balance between them. A democratic State must protect its citizens from security threats while also protecting their fundamental rights.

REFERENCES

1. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=State+Surveillance+and+the+Right+to+Privacy+in+the+Digital+Age%3A+Finding+the+Constitutional+Balance&btnG=#d=gs_qabs&t=1787067593137&u=%23p%3DOWWxPau7hn8J

2. <https://www.journal-uamd.org/index.php/IJRD/article/view/394>
3. <http://thecrsss.com/index.php/Journal/article/view/942>
4. <https://www.jstor.org/stable/26431267>
5. <https://www.elgaronline.com/abstract/edcoll/9781786436047/9781786436047.00013.xml>