LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 3 | Issue 1

2025

DIGITAL SURVEILLANCE AND INDIAN PRIVACY LAWS

Kamalpreet Kaur[1]

I. ABSTRACT

"*Privacy is not an option, and it should not be the price we accept for just getting on the Internet.*[2]." These words by technology expert Gary Kovacs highlight the growing concerns relating to privacy in this digital age. Privacy is a fundamental human right that allows an individual to live free from unwarranted public attention and interference.

On the other hand, there is 'Digital Surveillance', the process of monitoring, analyzing, and collecting data relating to the virtual activities of individuals like online communications, social media usage, patterns, behaviors, etc. In this digital era, the internet and technology are growing rampantly and have become an important aspect of almost all spheres of life. This technology is also being used for surveillance by government agencies for various purposes like prevention of crime, national security, etc., and even private entities collect individuals' data for running advertisement campaigns, preventing fraud, etc. However, such practices also raise concerns about individuals' privacy as they violate the Right to Privacy, which, although not explicitly mentioned, has been recognized as an integral part of Article 21 of the Indian Constitution.

Now, as the popular saying goes, "Excess of anything is bad." While unchecked surveillance violates privacy rights, absolute privacy can also be misused. Thus, there is a need for a perfect balance between the surveillance and the privacy laws so that the misuse of any of these laws be checked.

This paper examines the relationship between digital surveillance and privacy laws in India, assessing the effectiveness of existing legal provisions and their ability to balance security needs with individual freedoms. It also explores judicial perspectives,

[1] BABA FARID LAW COLLEGE, PUNJAB

[2] SECTION 3: PRIVACY | FOSTERING CIVIC TRUST: A POLICY GUIDE FOR MUNICIPAL LEADERS

policy gaps, and potential reforms inspired by international best practices to strengthen privacy protection in the Indian context.

II. KEYWORDS

Digital Surveillance, Privacy, Article 21, IT Act, personal data, Right to privacy.

III. INTRODUCTION

In this era of digitalization, the role of digital surveillance is significant in e-governance, national security, and crime prevention. Surveillance of individuals is not a new concept as the individuals' activities have been being monitored by government agencies for a long time for security purposes. But with the advancement of technologies, the modes of this surveillance have remarkable evolution, which is a serious threat to individual privacy. Presently, tools such as artificial intelligence, biometric databases, location tracking, and internet monitoring, are being used by the agencies for Digital surveillance which are in major debate with privacy laws and data security.

In India, digital surveillance is regulated by the statutory provisions of the legislation like the Indian Telegraph Act(1885), the Information Technology Act (2000), Bharatiya Nyaya Sanhita (2023), and the Digital Personal Data Protection Act (2023). These laws provide for provisions such as prior approval from the competent authority for call interception, making data fiduciaries responsible. However, these laws lag behind in matching the technology advancements in the cases of misuse of surveillance powers, providing transparency in surveillance scope and the absence of accountability of data collected and permanently stored by government agencies.

The Supreme Court of India in the case of ***Justice K.S.Puttaswamy(Retd) v. Union of India***[3] recognised the Right to Privacy as a fundamental right under Part III of the Constitution of India. The court of that the right to privacy is an intrusive part of Right to Life and Personal Liberty under Article 21. The Supreme Court strongly

[3] Justice K.S.Puttaswamy(Retd) v. Union of India 2019 (1) SCC 1

emphasized stronger legal safeguards against excessive surveillance by recognizing the doctrine of proportionality.

IV. RESEARCH OBJECTIVES

- To extensively examine the legal provisions regarding digital surveillance under various legislations and how these laws interact with the right to privacy.
- To evaluate the implications of the right to privacy as a fundamental right and its conflict with digital surveillance by the agencies of government in the name of national security and crime prevention.
- To conduct a comparative analysis of India's Digital Surveillance and privacy laws, practices, and mechanism, with that of the other countries.

V. RESEARCH QUESTIONS

- What are the legal provisions under various legislations and rules regarding digital surveillance?
- What are the implications of Right to Privacy as a fundamental right and how it interact the surveillance laws?
- What are raising concerns about the misuse of both the privacy and surveillance laws?
- How effective are the existing legal safeguards against the misuse of digital surveillance, and what further reforms are needed to ensure a balanced approach between security and privacy?

VI. RESEARCH HYPOTHESIS

- With the use of advanced technologies for Digital surveillance privacy rights of individuals are being increasingly threatened and violated.
- Digital surveillance is a double-edged sword used by government agencies to address concerns about National security and the prevention of crimes, which on the other side, is an infringement of the right to privacy.
- There is a need for modification and transparency in the surveillance laws and further strengthening the regulatory framework for data protection.

VII. RESEARCH METHODOLOGY

The research methodology used in this paper is qualitative in nature. It explores the interaction between digital surveillance and privacy laws in India. This study begins with a comprehensive literature review, analyzing the existing Statutes, legal documents, legal articles, etc. to form a theoretical base for this paper. The analysis will review the existing legal provisions regarding digital surveillance and privacy laws in India along with their intersection with each other.

The data collection Involves extensive legal research from online legal databases such as SCC Online, Manupatra, and government reports. Additionally, it includes international case studies and legal frameworks from countries like the USA, UK, and EU to provide a comparative perspective.

The Data collection involves legal provisions, case laws, evolving judicial views, and legislative changes throughout time, along with legal research from online databases like SCC Online, Manupatra, etc. Additionally, it includes international case studies and legal frameworks from countries like the USA, UK, and EU to provide a comparative perspective. It also involves the social impact of surveillance and privacy breaches.

VIII. LITERATURE REVIEW

This paper explores the significant provisions of the Constitution of India, Indian Telegraph Act (1885), Information Technology Act (2000), Bhartiya Nyaya Sanhita (2023), and Digital Personal Data Protection Act (2023) with special regard to digital surveillance and right to privacy under Article 21. This paper covers the various systems used for surveillance in India such as NETRA and NATGRID. This paper also analyses the renowned judgments in cases like K.S. Puttaswamy v. Union of India (2017), R. Rajagopal v. State of Tamil Nadu (1994), Manoj Kumar v. State of Delhi (2012), Shreya Singhal v. Union of India (2015), on the concept of privacy and surveillance. Additionally, the global surveillance and privacy laws, such as the Patriot Act of the USA, highlight best practices and potential legal improvements for India.

The literature reviewed in this paper provides for legal provisions, principles, and judicial pronouncements relating to surveillance, especially digital surveillance and its interaction with privacy laws.

IX. EVOLUTION OF SURVEILLANCE LAWS

The concept of surveillance in the name of national security and crime prevention is not new in India. It finds its traces in the Indian legal framework even before the independence. Indian Telegraph Act of 1885 and the Indian Post Office Act of 1898 are the laws that provided for the interception and monitoring of postal and telegraph communications by government agencies. With digitalization, the methods of surveillance also digitalized, and for that Information Technology Act, of 2000 was passed and now the Digital Personal Data Protection Act, of 2023 has also come into the field. These laws provide for Surveillance framework and other related matters to tackle the problems of national security, and public safety. This evolution from time to time is significant to match the new technological advancements and create a balance with privacy laws.

A. Digital Surveillance Mechanisms in India

In India, various mechanisms have been used to track the internet and other activities of the citizens and companies by the government. These mechanisms like NETRA, NATGRID, and CMS are of utmost importance for their crucial role in tackling threats of terrorism, national security, and other major projects of government agencies and crime investigation. These mechanisms are as follows:

- **Centralized Monitoring System (CMS) -** It is the centralized monitoring system set up by the Government of India to automate lawful interception of telecommunications and internet usage. This system enables security agencies to monitor individuals' phone calls, messages, etc. in real time and without any intermediatory intervention.
- **Network Traffic Analysis (NETRA) –** It is a DRDO-developed surveillance software that is being used by IB, R&AW, and other intelligence agencies for real-time interception of messages, tweets, emails, blogs, internet calls with

keywords like 'bomb', 'blast', 'kill', 'terrorist' etc. and the analysis of voice trafficking through software like GOOGLE. It can also monitor the instant message transcripts and even images.[4]

- **National Intelligence Grid (NATGRID) –** It is the integrated intelligence grid that connects the databases of various National security agencies of the Government of India. Through NATGRID these agencies can keep track of activities related to terrorism, finance, telecom, and more.[5]
- **Lawful Interception and Monitoring (LIM) System –** This system is used to access the communication and location data of individuals through telecom operators and internet service providers like Airtel, Reliance Jio, etc. This system is used by intelligence and police agencies to get call records, locations, and other related data for the purpose of national security and crime investigation.
- **Social Media Monitoring Tools-** To track the social media content and misinformation the intelligence agencies and the Ministry of Information and Broadcasting use various Artificial Intelligence (AI) tools to track and bring down the fake or threatening content and analyse trends.
- **Facial Recognition Systems (FRS)-** The National Automated Facial Recognition System (AFRS) is being deployed for security and law enforcement to track individuals in public spaces.
- **Aadhaar-Based Tracking-** Despite denials by the government for Aadhaar being a surveillance tool, it has been criticized many times for the potential risk of mass surveillance as the Aadhaar database which contains details like name, address, biometrics, date of birth, iris scan of the citizens is being linked to multiple services.

[4] 'Government to launch Netra for internet surveillance' The Economic Times (16 December 2013) https://m.economictimes.com/tech/internet/government-to-launch-netra-for-internet-surveillance/articleshow/27438893.cms?utm_source=whatsapp_pwa&utm_medium=social&utm_campaign=socialsharebuttons accessed 15 February 2025.

[5] 'NATGRID will come into operation by 2020 end: MHA in Lok Sabha' ANI News (20 November 2019) https://www.aninews.in/news/national/general-news/natgrid-will-come-into-operation-by-2020-end-mha-in-lok-sabha20191120145106/ accessed 15 February 2025.

- **Drone Surveillance-** Drones are used by Law enforcement agencies for crowd control, protests, and security monitoring. For instance, drones were used in Kumbh Mela and farmer protests, etc.

X. RELEVANT LEGISLATIONS AND REGULATIONS

There are several laws and regulations passed by the parliament relating to digital surveillance and privacy. From the British era to now independent and digital India, changes have been made in the previous laws and new laws are also being introduced to fulfill the needs of the hour and match the spectrum of advanced technologies in the field of security and crime prevention and investigation. These laws and regulations are as follows:

A. Constitution of India,1950[6]

The Indian Constitution does not provide the right to privacy expressly under any of its provisions. Although, the Right to Privacy has been recognized as a fundamental right explicitly under "***Article 21*** *(Right to Life and Personal Liberty)*" through several judicial pronouncements such as ***"Kharak Singh v. State of U.P.", "Govind v. State of M.P.", "R. Rajagopal v. Union of India", "Justice K.S.Puttaswamy(Retd) v. Union of India.*** Thus, **Article 21** provides for the **Right to Privacy** also known as the **right to be forgotten** or the **right to let alone.**

Article 19(1) of the Constitution provides for *freedom of speech and expression* and it protects against the surveillance that can affect the exercise of this right. However, the right to freedom of speech and expression is not an absolute right. It comes with certain **exceptions** provided under **Article 19(2)** like security of State, Sovereignty and integrity of India, and more.

B. The Indian Telegraph Act, 1885[7]

This Act was the foundation of surveillance laws in India during the British period. Section 5 of the Act provides for the interception, detention, and disclosure of any message or class of messages during a public emergency, for public safety, or for

[6] The Constitution of India, 1950, art. 21.
[7] Indian Telegraph Act, 1885.

reasons like sovereignty and integrity of India, security of the state, maintenance of friendly relationship with a foreign state and public order or for prevention of incitement or commission of an offense.[8]

C. Information Technology (IT) Act, 2000[9]

The IT Act, of 2000 (amended in 2008) is India's primary law governing cybersecurity, digital surveillance, and data privacy.

- **Section 69** of this Act provides for the powers of the Central and State Governments to intercept, monitor, or decryption any information, where it is in the interest of the *sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order of prevention of incitement to the commission of any cognizable offense, or for investigation of any offense.*[10]
- **Section 69A** of this Act provides the Central Government with the power to direct any agency of Government or intermediary to block access by the public and if the intermediary fails to comply with this provision he will have to face imprisonment for the term extending to seven years and fine.[11]
- **Section 69B** provides for the power of the Central Government to collect and monitor traffic data or information for the reasons of enhancing cybersecurity, and for identification, analysis, and prevention of intrusion of computer contaminants.[12]
- **Section 80** of the Act provides for the powers of the officers of the Central Government and the State Government to enter any public place, search, and arrest without warrant any person who is reasonably suspected of having committed or likely to commit any offense under this Act.[13]

[8]

[9] Information Technology (IT) Act,2000.
[10] The Information Technology Act 2000, s 69.
[11] The Information Technology Act 2000, s 69A.
[12] The Information Technology Act 2000, s 69B.
[13] The Information Technology Act 2000, s 80.

D. Digital Personal Data Protection (DPDP) Act, 2023[14]

It is the recent enactment of the Parliament of India for the protection of personal data of individuals and making data fiduciaries liable for data breaches. However, there are certain exemptions to the government bodies that can lead to mass surveillance and breach of privacy.

- **Section 4** of the Act provides for the processing of personal data with consent and for lawful purposes only.[15]
- **Section 8** makes it obligatory for the data fiduciary to protect the data, to intimate the data principal in case of breach, and to erase the data unless necessary if the data principal withdraws the consent. However, there are certain expectations for the government and other agencies.[16]
- **Section 13** provides for redressal of grievances.[17]
- **Section 17** of the Act exempts the government and gives it the right to process the personal data of individuals for using it in the interest of State sovereignty and integrity, public order, safety, prevention, and investigation of crime, and also for research and statistical purposes.[18]
- **Section 33[19] and Section 34[20]** The Act provides for heavy penalties (up to 250 crores) upon the data fiduciaries in cases of a data breach, unauthorized access, or failure to protect data.

E. Indian Telegraph (Amendment) Rules, 2007

These rules provided for lawful interception of telephone calls under **Rule 419A** with prior authorization by the Union or the State Home Secretary. It also provided for the validity of interception orders up to 60 days, extendable up to 180 days, and the assessment of the legality of the order by the Review committee.[21]

---

[14] The Digital Personal Data Protection Act 2023, ss 4, 8, 13, 17, 33, 34.
[15] The Digital Personal Data Protection Act 2023, s 4.
[16] The Digital Personal Data Protection Act 2023, s 8.
[17] The Digital Personal Data Protection Act 2023, s 13.
[18] The Digital Personal Data Protection Act 2023, s 17.
[19] The Digital Personal Data Protection Act 2023, s 33.
[20] The Digital Personal Data Protection Act 2023, s 34.
[21] The Indian Telegraph (Amendment) Rules 2007, r 419A.

F. Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009[22]

These rules issued under Section 69 of the IT Act allow the government and its agencies like IB, RAW, ED, NIA, CBI, and state police to intercept, monitor, or decrypt any digital communication with the approval of the competent authority.

G. Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009[23]

These rules were issued under **Section 69B** of the IT Act which allows government agencies to monitor traffic data for cybersecurity and national security reasons with the approval from the Union Secretary. It permits the reading of traffic patterns only and not the message content.

H. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

These Rules issued under **Section 43A** of the IT Act Define "Sensitive Personal Data or Information (SPDI)", including financial, biometric, and medical records. They make it mandatory for companies and intermediaries to adopt reasonable security practices and require explicit user consent for data collection and sharing.

I. Aadhaar (Authentication) Regulations 2016

It provided for biometric authentication and data storage for Aadhaar verification. It also prohibited the unauthorized tracking and profiling of Aadhar users.[24]

[22] The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules 2009.
[23] The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009.
[24] The Aadhaar (Authentication) Regulations 2016.

J. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[25]

These rules impose the requirements for content moderation and data sharing as they require Significant social media intermediaries like What's App, Facebook, and Instagram to enable the traceability of the first originator of the messages, removal of content within 36 hours of the government order, and the appointment of compliance officers in India. It also brought digital news and OTT platforms under government surveillance.

K. CERT-In (Indian Computer Emergency Response Team) Directions, 2022

These Directions were issued under **Section 70B** of the IT Act. They made it compulsory for the VPNs, ISPs, data centers, and cloud services to store user logs for 5 years and the reporting of Cyber security incidents within 6 hours.[26]

L. Draft Digital Personal Data Protection (DPDP) Rules, 2025

In January 2025, they released the draft for DPDP Rules to operationalize the DPDP Act of 2023. These rules provided for faster resolution of complaints and grievances, the appointment of Digital nominees, the right to data erasure, and so on.[27]

XI. DOCTRINE OF PROPORTIONALITY

In the case famous Aadhaar Case[28], the nine-judge bench of the Supreme Court has ruled that the Right to privacy is an intrusive part of Part III of the Indian constitution under Article 21 dealing with the Right to Life and Personal Liberty. The bench strongly emphasized a balance between the surveillance and right to privacy and for that, the SC established the **Principle of Proportionality** in surveillance. This principle says that the surveillance should be done only to the extent to which it is necessary and required and it should not be excessive and beyond a limit.

---

[25] ***Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021***
[26] The CERT-In (Indian Computer Emergency Response Team) Directions 2022.
[27] The Draft Digital Personal Data Protection (DPDP) Rules 2025.
[28] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

XII. DOCTRINE OF DUE PROCESS OF LAW

In the case of **Maneka Gandhi v. Union of India**[29], it was held that the rights under Article 14, Article 19, and Article 21 can be restricted only in accordance with the procedure established by law and that the procedure of law must be fair and reasonable.

Similar to this, the surveillance under different statutes has to be done in accordance with established legal procedures like prior approval of competent authority and reasonable causes mentioned under the statutes.

XIII. LANDMARK JUDGEMENTS

In the case of **Kharak Singh v. The State of U.P. (1962)**[30] The dissenting judges of the Supreme Court were of the opinion that the right to privacy is an essential part of the Right to Personal Liberty under Article 21 and that the surveillance provisions of the U.P. police regulations were unconstitutional. However, the right to privacy was not recognized as a fundamental right in this case.

In **Govind v. State of M.P. (1975)**[31] The Supreme Court held that the Right to Privacy is not expressly given in the Constitution but can be implied under Article 21. Thus, it is not an absolute right and can be restricted if there is a ***compelling State interest*** that is superior to the right to privacy.

In the case of **PUCL v. Union of India (1997)**[32] The Supreme Court held that the Right to Privacy is a fundamental right under Article 21 and it cannot be curtailed without the procedure established by law. Therefore, the court gave detailed guidelines for the fair, just, and reasonable procedure for call interception under section 5 of the Indian Telegraph Act, of 1885.

[29] Maneka Gandhi v Union of India (1978) 1 SCC 248.
[30] Kharak Singh v State of Uttar Pradesh (1962) AIR 1295 (SC).
[31] Govind v State of Madhya Pradesh (1975) 2 SCC 148.
[32] People's Union for Civil Liberties (PUCL) v Union of India (1997) 1 SCC 301.

In **Justice K.S. Puttaswamy v. Union of India (2017)**[33] the Supreme Court reaffirmed the Right to Privacy as a distinct and independent Fundamental right under Article 21. The court also observed that there is a need for a data protection law in India. The court also held that the exception to privacy is the 'compelling State interest' needs strict scrutiny.

In **Pegasus Scandal Case (2021)**[34] The Supreme Court held that the Right to Privacy is a fundamental right Under Article 21 and the government's interference in the name of national security cannot be used as an excuse to invade the judicial review.

XIV. CONCERNS

Surveillance and Privacy laws are at a crossroads in India. On one side, privacy being a fundamental right is very important for citizens to freely express their thoughts and is also a prerequisite for a democracy.

On the other hand, surveillance is also important in tackling the problems of terrorism, national security, crime investigation, and prevention. Thus, there is a need to establish a balance between surveillance and privacy as both of these are double-edged swords. Absolute privacy can put national security at risk and at the time excessive surveillance infringes on the right to privacy and it is also not good for a healthy democracy.

However, the dilemma is that the laws dealing with surveillance are not transparent, leaving a ground for suspicion and risk of misuse. Instances like the Pegasus Scandal and the Aadhaar Data leak are some of the best examples of misuse and risks attached to surveillance leading to severe privacy infringements. Therefore, there is a need for an independent and accountable surveillance body that can work transparently and under judicial oversight.

XV. SUGGESTIONS

- The provisions for requisition of mandatory judicial warrants should be added by amendments in the legislation like the IT Act, 2000, and Telegraph

[33] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[34] Pegasus Scandal Case (2021) WP (C) No 314/2021 (SC).

Act,1885 providing for interception and monitoring of communications. Also, there should be time to time review of the necessity of surveillance.

- The exemptions provided to the Government agencies under Section 17 of the Digital Personal Data Protection Act, 2023 (DPDP Act) increase the risk of mass surveillance, and to tackle that the amendments should be made to require proportionality tests, detailed transparency reports, surveillance requests and justifications for that.
- The right to be notified should be given to the persons being surveilled unless there is a high-security risk.
- Mandatory Data Deletion policies should be adopted with specifying minimum and maximum periods of data retention by private entities as well as government agencies.
- An Independent Oversight body consisting of judges, privacy advocates, technology experts, and national security experts, should established to oversee the surveillance activities, ensure accountability in case of data breaches, and get periodic reports. This body should be given the authority to approve or deny any surveillance requests.
- Proper mechanisms should be set up for AI-based systems like NETRA and NATGRID, to ensure justified and targeted surveillance rather than discriminated one.
- The principles of the European Union's General Data Protection Regulations(GDPR) should be adopted to strengthen consent mechanisms and algorithm transparency in AI-based surveillance.[35]
- Similar to the UK's Investigatory Powers Act, 2016 judicial commissioners for reviewing surveillance warrants should be appointed.[36]

[35] General Data Protection Regulation (EU) 2016/679.
[36] Investigatory Powers Act 2016 (UK).

XVI. CONCLUSION

Digital surveillance is an essential tool of modern governance, intelligence, and security operations. Thus, there is a need to adopt a more structured and transparent legal framework that aligns with global privacy standards. An independent and accountable system is essential to uphold democratic values, surveillance ethics, and individual privacy while addressing security concerns in this era of advanced technologies.

XVII. REFERENCES

A. Books

- M P Jain, Indian Constitutional Law (9th ed, Lexis Nexis 2023).
- Uday S Mehta, The Right to Privacy in India: Concept and Evolution (1st ed, Eastern Book Co 2021).
- Pavan Duggal, Cyber Law: The Indian Perspective (5th ed, Universal Law Publishing 2022).
- Shivani Verma, Criminology, Penology and Victimology (University Book House Pvt. Ltd. 2023).

B. Online Articles / Sources Referred

- 'Government to launch Netra for internet surveillance' The Economic Times (16 December 2013) https://m.economictimes.com/tech/internet/government-to-launch-netra-for-internet surveillance/articleshow/27438893.cms?utm_source=whatsapp_pwa&utm_medium=social&utm_campaign=socialsharebuttons accessed 15 February 2025
- 'NATGRID will come into operation by 2020 end: MHA in Lok Sabha' ANI News (20 November 2019) https://www.aninews.in/news/national/general-news/natgrid-will-come-into-operation-by-2020-end-mha-in-lok-sabha20191120145106/ accessed 15 February 2025.

- 'Mass Surveillance in India' Wikipedia https://en.m.wikipedia.org/wiki/Mass_surveillance_in_India accessed 15 February 2025.
- 'State of Privacy: India' Privacy International (2020) http://privacyinternational.org/state-privacy/1002/state-privacy-india accessed 15 February 2025.
- Government to launch 'Netra' for internet surveillance – The Economic Times – https://m.economictimes.com/tech/internet/government-to-launch-netra-for-internet surveillance/articleshow/27438893.cms?utm_source=whatsapp_pwa&utm_medium=social&utm_campaign=socialsharebuttons
- https://www.aninews.in/news/national/general-news/natgrid-will-come-into-operation-by-2020-end-mha-in-lok-sabha20191120145106/
- https://en.m.wikipedia.org/wiki/Mass_surveillance_in_India
- http://privacyinternational.org/state-privacy/1002/state-privacy-india
- PRIVACY | FOSTERING CIVIC TRUST: A POLICY GUIDE FOR MUNICIPAL LEADERS

C. Cases Referred

- Kharak Singh v State of Uttar Pradesh (1962) AIR 1295 (SC).
- Govind v State of Madhya Pradesh (1975) 2 SCC 148.
- R. Rajagopal v State of Tamil Nadu (1994) 6 SCC 632.
- People's Union for Civil Liberties (PUCL) v Union of India (1997) 1 SCC 301.
- Shreya Singhal v Union of India (2015) 5 SCC 1.
- Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
- Maneka Gandhi v Union of India (1978) 1 SCC 248.
- Pegasus Scandal Case (2021) Writ Petition (Civil) No. 314/2021.

D. Statutes Referred

- The Constitution of India, 1950, art. 21.
- The Indian Telegraph Act 1885, s 5.
- The Information Technology Act 2000, ss 69, 69A, 69B, 80.
- The Digital Personal Data Protection Act 2023, ss 4, 8, 13, 17, 33, 34.
- The Indian Telegraph (Amendment) Rules 2007, r 419A.
- The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules 2009.
- The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009.
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
- The Aadhaar (Authentication) Regulations 2016.
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.
- The CERT-In (Indian Computer Emergency Response Team) Directions 2022.
- The Draft Digital Personal Data Protection (DPDP) Rules 2025.
- General Data Protection Regulation (EU) 2016/679.
- Investigatory Powers Act 2016 (UK).