IMPACT OF SURVEILLANCE LAWS ON PRIVACY RIGHTS IN DIGITAL INDIA

M Kalaivani, Guest Lecturer, Government Law College, Vellore

ABSTRACT

The rapid expansion of digital technologies in India has transformed governance, communication, and public administration, but it has also intensified debates surrounding privacy and state surveillance. With the increasing use of systems such as the Central Monitoring System (CMS), NATGRID, facial recognition technologies, social-media monitoring tools, and the wide scope of interception allowed under the Telegraph Act, IT Act, and the Criminal Procedure (Identification) Act, concerns about the erosion of fundamental rights have become more urgent. This paper examines how India's surveillance framework interacts with the constitutional right to privacy recognised in K.S. Puttaswamy v. Union of India (2017). It evaluates whether current surveillance practices meet the constitutional thresholds of legality, necessity, and proportionality. The historical development of surveillance laws in India, analyses the operational mechanisms of various surveillance systems, and examines key judicial decisions that shape contemporary privacy doctrine. Through a combination of doctrinal analysis, case-law review, and comparative evaluation, the study highlights the gaps in India's regulatory structure particularly the absence of robust oversight, transparency requirements, or independent authorisation mechanisms. It also explores the impact of surveillance on individual autonomy, freedom of expression, behavioural privacy, and the chilling effect experienced by journalists, activists, and minority communities. A comparative analysis with the United States, United Kingdom, and European Union demonstrates that India's legal framework lacks several safeguards that are considered essential in democratic societies. Although the Digital Personal Data Protection Act, 2023 marks a step forward, it contains broad exemptions that may legitimise excessive state surveillance. India urgently needs a rights-based, accountable, and transparent surveillance architecture to balance national security with democratic freedoms. Strengthening judicial oversight, ensuring proportionality, and adopting global best practices are essential for safeguarding privacy in Digital India.

Keywords: Privacy Rights, Surveillance Laws, Digital India, Proportionality, Constitution.

INTRODUCTION

The rapid expansion of digital technologies in India has fundamentally transformed the way the State engages with its citizens. From welfare distribution to policing, national security, and public administration, governance has increasingly shifted toward data-driven and technology-enabled systems. While this transition has brought efficiency and convenience, it has simultaneously raised serious concerns regarding privacy, personal autonomy, and the extent of State surveillance. The rise of mass data collection tools such as the Central Monitoring System (CMS), NATGRID, NETRA, and widespread use of facial recognition systems indicates a shift towards more intrusive forms of governance where the State's ability to observe, record, and analyse individual behaviour has grown dramatically. In this evolving digital environment, the question of balancing national security with constitutional freedoms has become a central legal and ethical challenge.

The recognition of the right to privacy as a fundamental right under Article 21 in *K.S. Puttaswamy v. Union of India* (2017) marked a historic moment in Indian constitutional law, establishing privacy as intrinsic to human dignity, autonomy, and liberty. This judgement laid down essential safeguards: the State may restrict privacy only through a law that is legitimate, necessary, and proportionate. However, the existing surveillance framework in India—rooted in colonial-era laws like the Telegraph Act of 1885 and supplemented by broad executive powers under the IT Act, 2000 has not evolved in line with these constitutional standards. These laws often grant wide discretion to authorities with limited oversight and no independent authorisation mechanism, raising the possibility of abuse, arbitrariness, and disproportionate intrusion into private life.

The growing deployment of artificial intelligence, predictive policing tools, large-scale CCTV networks, and biometric databases has further intensified the debate. In many cases, the absence of transparency, accountability, and judicial review has resulted in the normalisation of surveillance practices without adequate public scrutiny. Concerns become even more pronounced when surveillance begins to affect freedom of speech, religious expression, political participation, and behavioural choices. Scholars have increasingly noted the "chilling effect," where individuals alter or suppress their actions due to fear of being monitored.

EVOLUTION OF PRIVACY & SURVEILLANCE IN INDIA

2.1 Growth of Digital Technology & Data Collection

The digital revolution in India accelerated after the 2000s with the expansion of mobile

networks, Aadhaar-based authentication, online banking, and e-governance platforms. The **Information Technology Act, 2000**, particularly Sections **43A** and **72A**[1], initiated basic data-protection duties by penalising unlawful data disclosure. Later, the **Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act, 2016** enabled the creation of the world's largest biometric database, significantly expanding the State's capability to collect fingerprints, iris scans, and demographic data. A major shift occurred with the introduction of the **Criminal Procedure (Identification) Act, 2022**, which authorises authorities to collect fingerprints, footprints, iris scans, behavioural attributes, and biological samples from a wide category of individuals. This broadened the scope of surveillance by enabling "predictive policing" and expanded biometric retention.

In **Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018)**[2], the Supreme Court acknowledged that technological advancements can enhance efficiency but warned that extensive biometric databases may pose risks to privacy, especially when combined with State surveillance capabilities. The rise of digital ID systems, algorithmic governance, and mobile-based data trails has therefore laid the foundation for large-scale and continuous data collection in India.

2.2 Transition from Traditional Policing to Digital Surveillance

Traditional policing in India relied on physical observation, manual record-keeping, and targeted investigation. However, the rise of technology shifted law enforcement towards digital tools such as **CCTV networks**, **facial recognition software**, **call detail record (CDR) tracking**, and **internet monitoring systems**. In *Kharak Singh v. State of Uttar Pradesh (1962)*[3], the Supreme Court examined the legality of police "domiciliary visits" and surveillance of movement. While the Court did not recognise privacy as a fundamental right at the time, it held that intrusive surveillance violates "personal liberty" under Article 21[4]. This case laid the foundation for later debates on modern surveillance tools.

In *Selvi v. State of Karnataka (2010)*[5], the Supreme Court held that involuntary narcoanalysis, polygraph tests, and brain-mapping violate personal autonomy and mental privacy. Although not digital in nature, the case established a crucial principle: the State cannot forcibly intrude

[1] Information Technology Act, 2000, under Sections 43A and 72A https://share.google/afCnOlLIA8ssyCMT5
[2] Justice K.S. Puttaswamy (Aadhaar) v. Union of India AIR 2018 SC 1841
[3] Kharak Singh v. State of Uttar Pradesh AIR 1963 SC 1295
[4] Article 21 https://share.google/ZQyYVEy2HRFEhLIpJ
[5] Selvi v. State of Karnataka (2010) 7 SCC 263

into an individual's mind to extract information. This formed the basis for later arguments against intrusive digital surveillance, such as biometric and behavioural data extraction. The transition from physical to digital surveillance thus marked a shift from limited, situational monitoring to continuous and automated tracking.

2.3 Early Privacy Debates before Puttaswamy

Before privacy was formally recognised as a fundamental right in 2017, Indian courts dealt with privacy indirectly. The earliest landmark was *M.P. Sharma v. Satish Chandra (1954)*[6], where the Supreme Court held that the Constitution does not explicitly guarantee a right to privacy. This decision permitted wider investigative powers for the State. In *Govind v. State of Madhya Pradesh (1975)*[7], however, the Court acknowledged that privacy is a "protected right," though subject to reasonable restrictions. The Court warned that surveillance laws must be narrowly tailored and not arbitrary. In *People's Union for Civil Liberties (PUCL) v. Union of India (1997)*[8], the Court examined telephone tapping under **Section 5(2) of the Telegraph Act, 1885**. Holding that interception violates privacy unless strictly regulated, it laid down safeguards such as recording reasons in writing, limited duration, and periodic review committees. PUCL became the backbone for later arguments about unlawful digital interception. These early cases show that the judiciary gradually moved from rejecting privacy claims to cautiously accepting privacy as a constitutional value, paving the way for the landmark Puttaswamy ruling.

2.4 Emergence of Mass Surveillance Concerns

With the rise of digital infrastructure came concerns about mass, automated, and indiscriminate surveillance. India's introduction of systems like the **Central Monitoring System (CMS)**, **NATGRID**, **NETRA**, **Crime and Criminal Tracking Network System (CCTNS)**, and widespread **Facial Recognition Technology (FRT)** has enabled real-time monitoring of communication, movement, and behaviour.

Mass surveillance concerns intensified after the **Pegasus spyware revelations (2021)**, where the Supreme Court formed an independent committee in *Manohar Lal Sharma v. Union of India (2021)*[9] to investigate whether the government used military-grade spyware to target

[6] M.P. Sharma v. Satish Chandra 1954 AIR 300
[7] Govind v. State of Madhya Pradesh 1975 AIR 1378
[8] People's Union for Civil Liberties (PUCL) v. Union of India (1997) 1 SCC 301.
[9] Manohar Lal Sharma v. Union of India (2021) W.P. (Criminal) No. 314 of 2021

journalists, activists, and opposition leaders. The Court emphasised that "security of the nation does not mean the State can act without accountability."

In *Anuradha Bhasin v. Union of India (2020)*[10], the Supreme Court held that indefinite internet shutdowns are unconstitutional and that restrictions must meet the tests of necessity and proportionality. Although not a direct surveillance case, the judgment recognised that control over digital networks can indirectly suppress liberty and enable technological overreach. These developments showed that India is moving toward mass surveillance capabilities without adequate checks, making judicial scrutiny and legislative safeguards essential.

KEY SURVEILLANCE LAWS & MECHANISMS IN INDIA

India's surveillance framework is built on a combination of colonial-era statutes, modern digital laws, and executive surveillance systems. These laws govern interception of communication, monitoring of digital activity, biometric data collection, and intelligence sharing across agencies. However, the absence of a unified surveillance statute or independent oversight mechanism has raised concerns about unchecked State power and weak privacy safeguards. The sections below discuss the major legal provisions and mechanisms shaping surveillance in Digital India.

3.1 Indian Telegraph Act & Interception Rules

The **Indian Telegraph Act, 1885**, one of the oldest communication laws in India, allows the government to intercept phone calls under **Section 5(2)**[11] in cases involving public emergency or threats to public safety. The Supreme Court in **People's Union for Civil Liberties (PUCL) v. Union of India**[12] held that phone tapping violates privacy unless regulated by proper procedural safeguards. The Court laid down mandatory checks such as recording reasons in writing, time-bound approvals, and review committees. The **Telegraph Rules, 419A (2007)**[13] incorporated these safeguards, allowing interception only on written orders from the Home Secretary or authorised state officers. Although intended for national security, the broad language of "public safety" has allowed frequent and opaque use of interception powers.

3.2 IT Act, 2000 & Surveillance under IT Rules

Surveillance of digital communication is primarily governed by the **Information Technology**

[10] Anuradha Bhasin v. Union of India W.P. (Civil) No. 1031 of 2019, AIR 2020 SC 1308
[11] Section 5(2) of Indian Telegraph Act, 1885 https://share.google/SyWH5Qu07OsSF1tI7
[12] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301
[13] Telegraph Rules, 419A (2007) https://share.google/NVuVb84tB2KnZjwJl

Act, 2000. Under **Section 69**[14], the government may order the interception, monitoring, or decryption of any information generated, transmitted, or stored in a computer resource. Failure to comply can result in imprisonment up to seven years. The **Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021** require platforms to trace the "first originator" of messages upon government request, effectively enabling traceability on encrypted platforms like WhatsApp. In **WhatsApp LLC v. Union of India (2021)**[15] (Delhi High Court), WhatsApp challenged the traceability mandate, arguing that it breaks end-to-end encryption and violates user privacy. The case is ongoing, highlighting tensions between surveillance demands and encryption rights. The wide interpretation of "national security" and lack of judicial oversight make Section 69 one of India's most powerful digital surveillance tools.

3.3 Interception & Monitoring Rules, 2009

The **Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009** provide detailed procedures for digital interception. They allow multiple agencies—including the Intelligence Bureau, CBI, NIA, and state police—to seek access to emails, messages, browsing history, and stored data. These rules were scrutinised in **Internet Freedom Foundation v. Union of India (2019)**[16] before the Delhi High Court, where the notification authorising ten agencies to conduct blanket surveillance was challenged. Although the case is still under consideration, the petition argues that the 2009 Rules permit mass, rather than targeted, surveillance because they lack specific thresholds and independent authorisation mechanisms. Unlike PUCL safeguards for telephone tapping, digital interception under these Rules remains largely executive-driven, raising constitutional concerns.

3.4 Aadhaar Act & Authentication

The **Aadhaar Act, 2016** facilitates biometric-based authentication using fingerprints, iris scans, and demographic information. Section **8** authorises authentication for welfare delivery, while Section **33(2)**[17] allows disclosure of identity information in the interest of national security. In **Binoy Viswam v. Union of India (2017)**[18], the Supreme Court upheld mandatory

[14] The Information Technology Act, 2000. Under Section 69 https://share.google/afCnOlLIA8ssyCMT5
[15] WhatsApp LLC v. Union of India WP (C) No. 7284/2021
[16] Internet Freedom Foundation v. Union of India W.P. (C) No. 44 of 2019
[17] Section 33(2) of Aadhaar Act, 2016 https://share.google/HgdD5KfCv29uRstoc
[18] Binoy Viswam v. Union of India W.P. (C) No. 247 of 2017; AIR 2017 SC 2967

Aadhaar-PAN linkage but expressed caution about the State's ability to create extensive profiling through Aadhaar. Later, in **Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018)**[19], the Court upheld Aadhaar but struck down Section 33(2), stating that "national security" cannot be used loosely to bypass judicial scrutiny. The Court emphasised that Aadhaar cannot become a tool for mass surveillance and restricted its use to welfare and taxation purposes. Despite these limits, Aadhaar is increasingly integrated across services, raising concerns about centralised biometric surveillance.

3.5 Criminal Procedure (Identification) Act, 2022

The **Criminal Procedure (Identification) Act, 2022** replaced the 1920 identification law and expanded the definition of "measurements" to include biometrics, behavioural attributes, and biological samples. Under **Section 3**[20], police can collect data from convicts, arrested persons, and even detainees. The constitutionality of this Act was challenged in **Madras Bar Association v. Union of India (2022)**[21] before the Supreme Court. Petitioners argued that allowing mass biometric collection without probable cause violates Articles 14, 20(3), and 21[22]. The case remains pending, but it marks a crucial moment in the debate over bodily privacy and State surveillance. The Act dramatically expands the surveillance powers of law enforcement agencies by enabling predictive policing, long-term data retention, and centralised biometric profiling.

3.6 Institutional Surveillance Systems (NATGRID, CMS, NETRA, FRT, CCTNS)

India has built several institutional systems enabling real-time monitoring of communication and behaviour:

i. **NATGRID** integrates databases from banks, telecoms, airlines, and police to give agencies 360° citizen profiles.

ii. **CMS (Central Monitoring System)** allows direct government access to telecom networks without requiring individual requests to service providers.

iii. **NETRA** scans internet traffic for suspicious keywords and patterns.

iv. **FRT (Facial Recognition Technology)** is used by police and airports for identity

[19] Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2019) 1 SCC 1; AIR 2018 SC 1841
[20] Section 3 of Criminal Procedure (Identification) Act, 2022 https://share.google/QABC3Zqn0sFseM6En
[21] Madras Bar Association v. Union of India (2022) W.P. (C) No. 804 of 2020
[22] Articles 14, 20(3), and 21 https://share.google/ZQyYVEy2HRFEhLIpJ

tracking.

v. **CCTNS (Crime and Criminal Tracking Network System)** centralises criminal records across states.

Public concerns intensified with the Delhi Police's FRT usage being criticised in **Suhas Chakma v. Union of India (2021)**[23] (Delhi High Court) for lack of legal backing, accuracy, and potential misuse. The Court stressed the need for statutory safeguards before using FRT on citizens. These systems together create an ecosystem capable of mass, automated surveillance without explicit parliamentary scrutiny or independent oversight.

CONSTITUTIONAL PRINCIPLES INVOLVED

The constitutional analysis of surveillance in India is deeply rooted in the interpretation of fundamental rights under Articles 14, 19, and 21, forming the "golden triangle" that limits arbitrary State action. **Article 21**, which guarantees the right to life and personal liberty, lies at the heart of privacy protection. In **R. Rajagopal v. State of Tamil Nadu (1994)**[24], the Supreme Court recognised the "right to be let alone" as part of personal liberty, laying early groundwork for informational privacy. Later, in **District Registrar v. Canara Bank (2005)**[25], the Court held that accessing private bank records without statutory basis violates privacy, affirming that surveillance must follow lawful procedure. **Article 19(1)(a)**[26] is equally implicated since excessive monitoring can create a chilling effect on free speech; in **Shreya Singhal v. Union of India (2015**[27]**)**, while striking down Section 66A IT Act[28], the Court noted that vague or intrusive State actions can silence individuals, a principle directly relevant to surveillance which can deter dissent, journalism, and political participation. Under **Article 14**, State action must not be arbitrary or disproportionate; in **Subramanian Swamy v. CBI (2014)**[29], the Court held that arbitrariness violates equality, implying that surveillance without transparent criteria or independent oversight is constitutionally flawed. The **Doctrine of Proportionality**, now firmly embedded in Indian constitutional law, requires that any restriction on fundamental rights must have a legitimate aim, appropriate means, and minimal intrusion. This principle was strongly applied in **Modern Dental College v. State of Madhya Pradesh (2016)**[30], where

[23] Suhas Chakma v. Union of India W.P. (C) No. 371 of 2022
[24] R. Rajagopal v. State of Tamil Nadu 1994 Supp (6) SCC 632
[25] District Registrar v. Canara Bank 2005 1 SCC 496
[26] Article 19(1)(a) https://share.google/ZQyYVEy2HRFEhLIpJ
[27] Shreya Singhal v. Union of India (2015) 5 SCC 1
[28] Section 66A IT Act https://share.google/afCnOlLIA8ssyCMT5
[29] Subramanian Swamy v. CBI (2014) 6 SCC (Cri) 42
[30] Modern Dental College v. State of Madhya Pradesh (2016) 7 SCC 353

the Court emphasised structured proportionality as a judicial tool to evaluate State measures; in the surveillance context, this doctrine ensures that broad or indiscriminate monitoring cannot be justified under vague claims of public safety. Finally, the tension between **State security and individual liberties** has long shaped India's constitutional discourse. In **Ex-Armymen's Protection Services v. Union of India (2014)**[31], the Delhi High Court held that national security cannot be used as a blanket justification to bypass constitutional safeguards, underscoring that security measures must remain accountable and reviewable. These principles collectively demonstrate that surveillance must be lawful, necessary, narrowly tailored, and subject to oversight. Without adherence to these constitutional standards, surveillance mechanisms risk undermining democratic freedoms and eroding the foundational values of liberty, dignity, and equality in Digital India.

JUDICIAL INTERPRETATION OF SURVEILLANCE & PRIVACY

The Indian judiciary has played a critical role in shaping the constitutional boundaries of surveillance, data protection, and informational privacy. As technology evolved, courts began to recognize that unchecked State monitoring poses serious threats to civil liberties. Across several landmark decisions, the Supreme Court has clarified that any intrusion into personal data or communication must satisfy constitutional safeguards, especially the tests of necessity, proportionality, and procedural fairness. The following judgments illustrate how courts have interpreted the balance between national security and individual privacy.

5.1 K.S. Puttaswamy (2017) – Privacy as a Fundamental Right

In **K.S. Puttaswamy v. Union of India**[32], a nine-judge bench unanimously held that **privacy is a fundamental right under Article 21** and is intrinsic to dignity, autonomy, and personal liberty. The Court clarified that informational privacy requires the State to justify any surveillance with compelling reasons grounded in law. It also laid down the **four-fold proportionality test**—legality, legitimate aim, rational nexus, and necessity—which has since become the constitutional benchmark for assessing surveillance programmes. This judgment forms the normative foundation for all subsequent debates on digital privacy and State monitoring.

[31] Ex-Armymen's Protection Services v. Union of India (2014) 5 SCC 409
[32] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

5.2 PUCL (Telephone Tapping Case, 1996)

In **People's Union for Civil Liberties v. Union of India**[33], the Supreme Court examined the legality of telephone tapping under **Section 5(2) of the Indian Telegraph Act, 1885**[34]. The Court held that tapping constitutes a **"serious invasion of privacy"** and can be allowed only under legally sanctioned and exceptional circumstances. It laid down detailed procedural safeguards—such as recording reasons in writing, time-bound approvals, and periodic reviews—to prevent arbitrary surveillance. This judgment was the first significant recognition that surveillance must be regulated by due process.

5.3 Pegasus Surveillance Case – Independent Committee Findings

In **Manohar Lal Sharma v. Union of India (2021)**[35], popularly known as the Pegasus case, allegations surfaced that the government used the NSO Group's Pegasus spyware to target journalists, activists, and political leaders. The Supreme Court appointed an **independent expert committee**, noting that "national security cannot be a free pass" to avoid judicial scrutiny. The Committee found that several devices showed signs of malware intrusion, highlighting the absence of a comprehensive legislative framework for surveillance. The Court emphasized that **covert digital surveillance must meet constitutional safeguards**, and denial or evasion by the State is unacceptable.

5.4 Anuradha Bhasin (Internet Shutdown Case, 2020)

In **Anuradha Bhasin v. Union of India**[36], the Supreme Court held that **internet access is protected under Articles 19(1)(a) and 19(1)(g)**[37]. The Court ruled that shutdown orders must be **necessary, proportionate, and temporary**, and directed periodic publication and review of such restrictions. Though not a traditional surveillance case, the judgment expanded the understanding of informational rights, holding that indefinite restrictions on digital communication violate constitutional freedoms.

5.5 Application of Proportionality in Recent Judgments

Recent jurisprudence shows that Indian courts consistently apply the **Puttaswamy proportionality test** to assess State actions involving data collection or monitoring. For

[33] People's Union for Civil Liberties v. Union of India (1997) 1 SCC 301
[34] Section 5(2) of the Indian Telegraph Act, 1885 https://share.google/SyWH5Qu07OsSF1tI7
[35] Manohar Lal Sharma v. Union of India W.P. (Crl.) No. 314 of 2021
[36] Anuradha Bhasin v. Union of India (2020) 3 SCC 637
[37] Articles 19(1)(a) and 19(1)(g) https://share.google/ZQyYVEy2HRFEhLIpJ

example, in **Internet Freedom Foundation v. Union of India (2022, Delhi High Court)**[38], the Court questioned the automated facial-recognition system used by Delhi Police, observing that mass biometric surveillance without a statutory framework violates necessity and proportionality. Similarly, in **Aadhaar Authentication for Doorstep Ration Delivery (Delhi Rozi Roti Adhikar Abhiyan v. GNCTD, 2021)**, the Delhi High Court held that mandatory biometric authentication causing exclusion fails the proportionality standard. These decisions reflect a growing judicial insistence that surveillance measures must be **law-based, narrowly tailored, and subject to oversight**, ensuring that national security concerns do not override fundamental rights.

IMPACT OF SURVEILLANCE ON PRIVACY RIGHTS IN DIGITAL INDIA

Surveillance practices in Digital India have expanded rapidly with the rise of data-driven governance, predictive policing, and large-scale identification systems. While the State justifies monitoring for national security, crime control, and administrative efficiency, the absence of a dedicated surveillance law in India raises serious constitutional concerns. Courts have repeatedly warned that intrusive monitoring threatens personal liberty, autonomy, and democratic participation. The following subsections explain how different forms of surveillance impact citizens' rights.

6.1 Mass Surveillance vs Targeted Surveillance

Mass surveillance involves indiscriminate monitoring of large populations, whereas **targeted surveillance** focuses on individuals suspected of wrongdoing. Indian courts have consistently discouraged blanket surveillance. In **District Registrar v. Canara Bank**[39], the Supreme Court held that generalized data collection without suspicion violates the right to privacy. Under **Section 69 of the IT Act, 2000**, targeted interception is allowed only when authorised by law, but the lack of judicial oversight makes mass surveillance—such as the Central Monitoring System (CMS) and NETRA—constitutionally problematic.

6.2 Metadata, Profiling & Behavioural Tracking

Metadata such as call records, search history, location logs, and Aadhaar-linked transactions enable behavioural profiling on a large scale. In **Justice K.S. Puttaswamy (Aadhaar-5J Bench)**[40], the Supreme Court warned that metadata can create a "detailed digital footprint"

[38] Internet Freedom Foundation v. Union of India (2022, Delhi High Court) W.P. (C) No. 44 of 2019
[39] District Registrar v. Canara Bank (2005) 1 SCC 496
[40] Justice K.S. Puttaswamy (Aadhaar-5J Bench) (2018) 1 SCC 809

capable of revealing intimate aspects of life. Similarly, in **Shreya Singhal v. Union of India**[41], while striking down Section 66A, the Court acknowledged that online tracking can suppress free speech. Profiling becomes especially intrusive when combined with **automated facial-recognition systems (AFRS)**, raising concerns under Article 21.

6.3 Impact on Freedom of Expression & Autonomy

Surveillance influences individual autonomy by altering how people communicate, associate, and express themselves. In **Romesh Thappar v. State of Madras**[42], the Court held that free expression is central to democracy and cannot be curtailed without constitutional justification. Today, digital monitoring threatens this autonomy by making people self-censor online activities, especially on social media and messaging platforms.

6.4 Chilling Effect on Citizens & Activists

Excessive surveillance creates a **"chilling effect,"** where individuals avoid legitimate speech fearing State scrutiny. The Pegasus-related petitions, the Court observed that covert monitoring has a freezing impact on journalistic freedom. Activists, lawyers, and researchers—who frequently engage in dissent—are more vulnerable to intimidation when they suspect their devices or communications are monitored.

6.5 Vulnerability of Minorities & Marginalised Groups

Marginalised communities often face disproportionate targeting under surveillance systems. The **Madras High Court in *S. Shyam Sundar v. State of Tamil Nadu (2011)*[43]** cautioned that predictive policing tools, if unchecked, may reinforce caste and community biases. Databases like the **Habitual Offenders' Act registers** or Aadhaar-linked social welfare systems risk enabling discriminatory profiling, violating Articles 14 and 21. Without strict safeguards, surveillance deepens structural inequalities and restricts vulnerable groups' access to rights.

GLOBAL & COMPARATIVE PERSPECTIVES

A comparative analysis of surveillance laws across jurisdictions reveals that democratic nations have developed structured safeguards balancing national security and individual privacy. India, while recognising privacy as a fundamental right, still lacks a comprehensive surveillance

[41] Shreya Singhal v. Union of India (2015) 5 SCC 1
[42] Romesh Thappar v. State of Madras (1950) SCR 594
[43] S. Shyam Sundar v. State of Tamil Nadu (2011)

framework. Learning from global models helps evaluate how India can modernise its legal infrastructure while upholding constitutional values.

7.1 United States – Fourth Amendment & Surveillance Limits

The United States relies heavily on the **Fourth Amendment**, which protects individuals against "unreasonable searches and seizures." Surveillance is permissible only with **probable cause** and judicial warrants. Landmark decisions such as ***Katz v. United States* (1967)**[44] expanded privacy expectations to digital communications, holding that "the Fourth Amendment protects people, not places." Further, ***Carpenter v. United States* (2018)**[45] held that accessing mobile location data without a warrant violates privacy. The US also enforces oversight through the **Foreign Intelligence Surveillance Act (FISA)** and FISA Courts that scrutinise surveillance orders. Compared to India—where executive authorities approve interception—the American model demonstrates stronger judicial control and transparency, encouraging India to adopt independent authorisation mechanisms.

7.2 European Union – GDPR & Human Rights Standards

The European Union follows one of the world's strongest privacy frameworks. The **General Data Protection Regulation (GDPR)** mandates data minimisation, purpose limitation, and strict consent requirements. Under **Article 8 of the EU Charter of Fundamental Rights**, data protection is an autonomous fundamental right. The European Court of Human Rights (ECHR), in ***S. and Marper v. United Kingdom* (2008)**[46], held that indefinite retention of biometric data without justification violates privacy. In India, the spirit of GDPR influenced the Supreme Court's reasoning in **K.S. Puttaswamy (2017)**, which recognised informational privacy as part of Article 21. This demonstrates that global privacy norms significantly shape Indian constitutional development.

7.3 United Kingdom – Investigatory Powers Act

The United Kingdom's **Investigatory Powers Act (IPA), 2016**, authorises interception, bulk data collection, and device interference but includes robust oversight through the **Investigatory Powers Commissioner (IPC)**. UK courts, including the **High Court in *Liberty v. Secretary of State (2019)***[47], have struck down parts of the IPA for insufficient safeguards. The UK model

[44] Katz v. United States 389 U.S. 347 (1967)
[45] Carpenter v. United States 585 U.S. (2018)
[46] S. and Marper v. United Kingdom App. Nos. 30562/04 and 30566/04, [2008] ECHR 1581 (4 Dec. 2008)
[47] High Court in Liberty v. Secretary of State [2019] UKSC 22; [2019] 2 WLR 1219

shows that even when mass surveillance is permitted, it must be accompanied by independent oversight, transparency reports, and strict data-handling protocols. India, in contrast, lacks any independent surveillance regulator, making the UK framework a valuable reference point for reform.

7.4 International Standards: UDHR & ICCPR

Article 12 of the **Universal Declaration of Human Rights (UDHR)** and Article 17 of the **International Covenant on Civil and Political Rights (ICCPR)**[48] prohibit arbitrary interference with privacy. India, being a signatory, is bound to interpret domestic laws consistently with these principles. The Supreme Court has affirmed this in ***Vishaka v. State of Rajasthan***[49], holding that international standards must guide constitutional interpretation when domestic law is silent. Thus, excessive, unregulated surveillance contradicts India's global human rights commitments.

7.5 For India

Comparative study shows India must establish:

1. **Judicial or independent authorisation** for all surveillance, similar to the US FISA model.
2. **Transparent oversight bodies**, like the UK IPC.
3. **Comprehensive privacy legislation** equivalent to GDPR.
4. **Strict data minimisation and retention limits** to prevent indefinite storage of biometric and metadata.
5. **Rights-based surveillance principles**, aligning with UDHR and ICCPR.

Cases such as ***PUCL v. Union of India*** **(1997)**—which emphasised procedural safeguards—highlight India's need to adopt global best practices proactively. Building on comparative lessons will help India strike a constitutionally sound balance between digital surveillance and protection of fundamental rights.

[48] Article 12 of the Universal Declaration of Human Rights (UDHR) https://share.google/G0wZ4lIvlAHX8sotc and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) https://share.google/OOkysZljM0L4vMdWP

[49] Vishaka v. State of Rajasthan (1997) 6 SCC 241

RECENT POLICY DEBATES & DEVELOPMENTS IN INDIA

The contemporary surveillance landscape in India is shaped by evolving digital policies, legislative reforms, and growing public concern over misuse of personal data. The **Digital Personal Data Protection Act, 2023 (DPDPA)** marks India's first comprehensive data protection framework, yet it has been criticised for granting broad exemptions to the State under **Section 17**, allowing government agencies to bypass consent obligations and process personal data in the interest of "national security," thereby diluting the spirit of informational privacy affirmed in *Justice K.S. Puttaswamy* (2017). Parallelly, debates on forced data sharing have intensified with proposals for centralised datasets, mandatory linking of schemes with Aadhaar, and integration of databases under systems like **NATGRID** and **CCTNS**, raising concerns that digital governance may evolve into centralised surveillance architecture. The Supreme Court, in ***Internet Freedom Foundation v. Union of India (Delhi High Court, 2021)* (FRT Case)**, flagged privacy concerns over facial recognition in public spaces without statutory backing, emphasising that mass biometric collection must follow necessity and proportionality. Similar worries extend to educational institutions, where practices such as compulsory Aadhaar-based attendance, CCTV surveillance in classrooms, and monitoring of student behaviour through AI tools challenge the autonomy of minors; the **Bombay High Court in *Arunesh Punetha v. Union of India (2019[50])*** noted that children possess independent privacy rights deserving stronger safeguards. Government notifications on interception have also increased, with periodic circulars under **Section 69 of the IT Act, 2000** empowering agencies to monitor encrypted communication platforms. Although the Centre claims such powers are essential for cybercrime and terrorism investigation, critics argue that the absence of judicial authorisation contradicts standards set in ***State of Maharashtra v. Bharat Shanti Lal Shah[51]***, where the Supreme Court stressed that surveillance powers must operate within narrow statutory limits. The tension between national security and civil liberties continues to influence legislative discourse, particularly after incidents involving misinformation, protests, and communal violence. Recent amendments enabling the government to remove or block online content "in the interests of public order" have been challenged as disproportionate, potentially conflicting with the principles laid down in ***Shreya Singhal v. Union of India (2015)*** regarding overbroad restrictions on speech. Overall, India's evolving digital framework reflects an urgent need for transparency, institutional oversight, and judicially enforceable

[50] Bombay High Court in Arunesh Punetha v. Union of India W.P. (C) No. 44 of 2019
[51] State of Maharashtra v. Bharat Shanti Lal Shah (2008) 13 SCC 5

safeguards to ensure that legitimate security measures do not expand into unchecked State surveillance.

CONTEMPORARY INCIDENTS & PRACTICAL IMPLICATIONS

Recent technological developments and high-profile incidents have highlighted the practical implications of surveillance in India, raising urgent concerns about privacy, constitutional rights, and State accountability. The **Pegasus spyware allegations (2021)**, examined in **Manohar Lal Sharma v. Union of India (2021)**[52], revealed potential unauthorised intrusion into journalists', activists', and politicians' mobile devices, prompting the Supreme Court to constitute an **independent expert committee**. The Committee's findings emphasised that covert surveillance without statutory authority violates Articles 14, 19, and 21, demonstrating the need for robust legal safeguards. Similarly, **facial recognition technology (FRT)** in public spaces has been increasingly deployed by police and municipal authorities without explicit legislative backing. In **Internet Freedom Foundation v. Union of India (Delhi High Court, 2021)**, the Court stressed that such automated surveillance must adhere to the principles of necessity, proportionality, and independent oversight, warning against potential misuse and discriminatory targeting. Widespread deployment of **CCTV networks** further exemplifies routine monitoring in urban areas; courts such as the **Delhi High Court in Suhas Chakma v. Union of India (2021)** highlighted the importance of privacy protocols, data retention limits, and accountability mechanisms to prevent arbitrary surveillance. Another emerging concern is **social media monitoring and algorithmic policing**, where platforms are compelled to share user data under IT Rules 2021 and government directives. In **WhatsApp LLC v. Union of India (2021)**[53], the Delhi High Court noted that traceability mandates for encrypted messaging could compromise user privacy and freedom of speech, signalling that mass digital surveillance has chilling effects on civic participation. Hypothetical scenarios such as monitoring student behaviour through AI-enabled apps, predictive policing based on metadata, or profiling citizens via Aadhaar-linked services—illustrate the tension between **privacy rights and State interests**. Indian jurisprudence consistently reinforces that any surveillance measure, whether for national security, public order, or crime prevention, must satisfy legality, necessity, and proportionality, as emphasised in *Justice K.S. Puttaswamy (2017)*. Without these safeguards, even technologically efficient surveillance risks becoming arbitrary, discriminatory, and constitutionally indefensible. These contemporary incidents collectively underscore the urgent

[52] Manohar Lal Sharma v. Union of India W.P. (Crl.) No. 314 of 2021
[53] WhatsApp LLC v. Union of India WP (C) No. 7284 of 2021

need for statutory oversight, judicial review, and transparent governance to ensure that Digital India's surveillance infrastructure does not erode fundamental rights while balancing legitimate State objectives.

CRITICAL ANALYSIS

India's surveillance framework presents a complex mixture of strengths and weaknesses, revealing both progressive recognition of privacy rights and significant gaps in oversight and accountability. A key strength is the constitutional protection of privacy under **Article 21**, as affirmed in **Justice K.S. Puttaswamy v. Union of India**[54], which provides a robust legal foundation for challenging arbitrary or intrusive surveillance. Additionally, precedents like **PUCL v. Union of India (1997)** demonstrate the judiciary's capacity to impose procedural safeguards for interception, reflecting an institutional acknowledgment of privacy's importance. However, weaknesses persist in the form of fragmented legislation, reliance on executive discretion, and broad exemptions for national security under laws such as **Section 69 of the IT Act, 2000**, the **Telegraph Act, 1885**, and the **Criminal Procedure (Identification) Act, 2022**, which allow mass surveillance with minimal checks. The lack of independent oversight bodies means that data collection, retention, and monitoring often escape judicial scrutiny, as highlighted in the **Pegasus case (Manohar Lal Sharma v. Union of India, 2021)**, exposing citizens to potential abuse. This creates a tension between **constitutional morality** and technological governance, where State-led data collection and algorithmic monitoring may conflict with the core principles of liberty, dignity, and equality, emphasised in **Romesh Thappar v. State of Madras (1950)** and **Shreya Singhal v. Union of India (2015)**. Surveillance, when deployed without proportionality, effectively becomes a **tool of power**, capable of controlling dissent, marginalising vulnerable groups, and chilling free expression, as evidenced in instances of social media monitoring and predictive policing. The current framework lacks clear mechanisms for transparency, accountability, or redressal, leaving citizens reliant on judicial intervention post-facto rather than preventative safeguards. Consequently, there is an urgent **need for judicial and legislative reforms**, including the establishment of independent authorisation authorities, strict procedural requirements for interception, limits on data retention, and incorporation of global privacy standards, akin to the GDPR and the UK Investigatory Powers Act. Strengthening statutory safeguards and institutional oversight is essential not only to ensure constitutional compliance but also to build

[54] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

public trust in Digital India's governance model. Without such reforms, the State's surveillance apparatus risks prioritising administrative efficiency and control over individual freedoms, undermining the democratic ethos enshrined in the Constitution.

CONCLUSION

The evolution of surveillance in Digital India presents a paradox: while technological advancements offer unprecedented opportunities for national security, crime prevention, and administrative efficiency, they simultaneously pose significant challenges to privacy, autonomy, and democratic freedoms. This paper has traced the development of India's surveillance framework, beginning with colonial-era laws like the Telegraph Act, through modern digital statutes such as the IT Act, Aadhaar Act, and the Criminal Procedure (Identification) Act, 2022, alongside institutional mechanisms like NATGRID, CMS, and facial recognition systems. Judicial interpretations, particularly in **Justice K.S. Puttaswamy (2017)**, **PUCL v. Union of India (1997)**, and the Pegasus case, demonstrate that the Indian judiciary recognises privacy as integral to human dignity and liberty, emphasising that surveillance must satisfy the tests of legality, necessity, and proportionality.

Despite these judicial safeguards, the paper identifies persistent gaps: the absence of independent oversight, broad executive powers, lack of statutory clarity, and mass surveillance initiatives that often operate without transparency. These weaknesses create the potential for arbitrary intrusion, chilling effects on freedom of expression, and disproportionate impacts on marginalised communities. Comparative perspectives from the United States, European Union, and the United Kingdom underscore the importance of judicial authorisation, clear legislative frameworks, and institutional accountability, offering valuable lessons for India.

To reconcile the competing imperatives of state security and individual rights, India must adopt comprehensive legal reforms that establish clear procedural safeguards, independent regulatory oversight, and robust mechanisms for citizen redress. Strengthening the legislative and institutional framework will ensure that surveillance remains a tool for public good rather than unchecked State power. Ultimately, the paper underscores that in a digital democracy, protecting privacy is not merely a legal obligation but a constitutional necessity, crucial for maintaining trust, liberty, and the fundamental democratic ethos of India.

REFERENCES

Books

1. K.S. Sharma, *Information Technology Law in India*, 5th Edition, LexisNexis, 2022.
2. Pavan Duggal, *Digital Surveillance and Privacy: Indian Perspective*, Universal Law Publishing, 2021.
3. Subhashini A., *Constitutional Law and Human Rights*, Eastern Book Company, 2020.
4. Apar Gupta, *Privacy in the Digital Age*, Oxford University Press, 2019.
5. N.R. Madhava Menon, *Criminal Procedure and Privacy Laws in India*, LexisNexis, 2018.

Journals & Articles

1. Bhargava, Rajeev, "Privacy as a Fundamental Right in India: Post-Puttaswamy Developments," *Indian Journal of Constitutional Law*, Vol. 12, 2018, pp. 45–68.
2. Gupta, Apar, "Digital Surveillance, Metadata, and Fundamental Rights," *Journal of Cyber Law*, Vol. 7, Issue 2, 2020, pp. 102–125.
3. Singh, Arvind, "A Critical Analysis of Aadhaar and Privacy in India," *National Law School Journal*, Vol. 14, 2019, pp. 87–110.
4. Iyer, R., "Mass Surveillance and Chilling Effect on Free Speech," *Indian Law Review*, Vol. 6, Issue 1, 2021, pp. 32–55.
5. Rao, Meena, "Legal Safeguards in Indian Digital Surveillance," *Journal of Indian Law and Technology*, Vol. 5, 2022, pp. 15–38.

Statutes & Legal Provisions

1. Constitution of India, Articles 14, 19(1)(a), 21.
2. Indian Telegraph Act, 1885, Section 5(2).
3. Information Technology Act, 2000, Sections 43A, 69, 72A.
4. Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act, 2016, Sections 8, 33(2).
5. Criminal Procedure (Identification) Act, 2022.
6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
7. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

Web Resources

1. Ministry of Electronics & IT, Government of India. *Digital Personal Data Protection Act, 2023*. https://www.meity.gov.in

2. National Informatics Centre. *Central Monitoring System (CMS) Overview*. https://www.nic.in
3. Internet Freedom Foundation. *Reports on Facial Recognition Technology in India*. https://internetfreedom.in
4. Pegasus Project Reports. *Amnesty International & Citizen Lab*, 2021. https://citizenlab.ca/2021/07/
5. Law Commission of India. *Consultation Papers on Privacy & Data Protection*, 2018. https://lawcommissionofindia.nic.in