INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 11 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 11 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-11-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

MASS SURVEILLANCE IN INDIA: DEATH OF THE RIGHT TO PRIVACY

AUTHOR – AAYUSH & HARSHWARDHAN YADAV

STUDENTS AT NATIONAL LAW INSTITUTE UNIVERSITY, BHOPAL

BEST CITATION – AAYUSH & HARSHWARDHAN YADAV, MASS SURVEILLANCE IN INDIA: DEATH OF THE RIGHT TO PRIVACY, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 5 (11) OF 2025, PG. 773-782, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

The recognition of the right to privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) marked a constitutional milestone, embedding privacy within the ambit of Article 21. Yet, India's growing surveillance infrastructure comprising programmes like the Central Monitoring System (CMS), NETRA, and NATGRID poses grave challenges to this right by enabling bulk interception of communications with limited transparency or oversight. The Digital Personal Data Protection Act, 2023 (DPDPA), heralded as India's first comprehensive data protection framework, introduces principles of consent, purpose limitation, and fiduciary duties. However, its sweeping exemptions for the State risk legitimising mass surveillance rather than restraining it. This paper critically examines the constitutional trajectory of privacy rights, the statutory framework enabling surveillance, and the implications of the DPDPA. It argues that the Act, by consolidating executive discretion and bypassing proportionality safeguards laid down in Puttaswamy, erodes the balance between security and liberty. The chilling impact on free expression, association, and dissent underscores the democratic costs of unchecked monitoring. The study concludes by proposing reforms including independent oversight, judicial authorisation, and robust accountability mechanisms to ensure that surveillance in India aligns with principles of legality, necessity, and proportionality, consistent with international human rights standards.

Keywords: Mass surveillance; privacy; Digital Personal Data Protection Act 2023; constitutional law; Puttaswamy judgment; national security; proportionality; data protection; India; fundamental rights.

1. INTRODUCTION

In an era where every click, call, and keystroke leaves a trace, the line between security and surveillance has grown perilously thin. India today stands at a critical juncture in this debate. With over 800 million internet users and one of the world's largest biometric databases through Aadhaar,[1225] the State has unprecedented access to personal data. This is further augmented by a growing surveillance ecosystem powered by advanced technologies such as artificial intelligence, automated facial recognition, and social media analytics.[1226] India today finds itself at the centre of this paradox, armed with one of the world's most ambitious digital surveillance infrastructures, yet struggling to safeguard the constitutional promise of privacy.

Flagship programmes like the Central Monitoring System (CMS), which enables direct interception of telephone and internet communications, the National Intelligence Grid (NATGRID), and NETRA form the backbone of India's digital

[1225] R Aksietha, 'Surveillance in India and Its Privacy Challenges in the Digital Age: A Legal and Constitutional Analysis' (2025) 10(3) IJRTI 651, 652.

[1226] Rau's IAS, 'Surveillance in India' (Compass Current Affairs, 6 November 2023) <https://compass.rauias.com/current-affairs/surveillance-india/>accessed 28 August 2025.

surveillance infrastructure. These initiatives, combined with episodic revelations such as the Pegasus spyware scandal and recent reports of "state-sponsored" hacking alerts sent to opposition leaders and journalists,[1227] paint a picture of an expanding surveillance state where citizens' everyday activities are susceptible to continuous monitoring. While officially justified on grounds of counter-terrorism, cyber-security, and public order, such tools increasingly operate in a legal and institutional vacuum, raising serious concerns about transparency, accountability, and the erosion of democratic freedoms.[1228]

The constitutional right to privacy, recognised in *Justice K S Puttaswamy v Union of India*,[1229] was meant to act as a bulwark against such encroachments. Yet, despite the Supreme Court's insistence on the principles of legality, necessity, and proportionality, India's surveillance architecture continues to function under outdated laws such as the Indian Telegraph Act 1885 and the section 69, Information Technology Act 2000.[1230] More recently, the Digital Personal Data Protection Act 2023 (DPDPA) has emerged as a cornerstone of India's data protection framework. But its sweeping exemptions for the State, particularly in the name of "national security" and "public order," risk legitimising bulk surveillance rather than restraining it.[1231]

This paper interrogates whether mass surveillance in India represents not the protection of democracy, but it's quiet corrosion. It argues that unchecked surveillance not only chills free expression and political dissent, but also undermines the very foundation of constitutional liberty. By analysing India's evolving privacy jurisprudence, the laws that enable surveillance, the impact of the DPDPA, and global best practices, this study seeks to answer a pressing question: is the right to privacy in India slowly being sacrificed at the altar of national security?

2. Mass Surveillance Vs Targeted Surveillance

Before delving into the nuances of mass surveillance and its implications for the right to privacy in India, it is essential to first distinguish it from targeted surveillance, as this distinction underpins much of the ongoing legal and ethical debate. Understanding what constitutes mass surveillance and how it fundamentally differs from the focused, individualized approach of targeted surveillance provides the necessary foundation to critically assess the scale and scope of state intrusion into citizens' private lives.

Surveillance may be understood as the systematic observation or monitoring of individuals, groups, or communications for the purpose of gathering information. It operates along two primary models: **targeted surveillance** and **mass surveillance**.

Targeted surveillance refers to the monitoring of specific individuals, organisations, or groups based on reasonable suspicion, intelligence inputs, or judicially sanctioned warrants. It is usually justified on grounds of necessity, as it is limited in scope and aimed at persons reasonably believed to be engaged in unlawful or threatening activity. For example, a police authority may intercept the calls of a suspected

[1227] Pameela George, 'India's Surveillance Landscape after the DPDPA' (IAPP, 6 February 2025) <https://iapp.org/news/a/india-s-surveillance-landscape-after-the-dpdpa> accessed 28 August 2025.
[1228] Chinmayi Arun, 'Thin Safeguards and Mass Surveillance in India' (2014) 26 NLSIR 105, 106–107.
[1229] *Justice K S Puttaswamy v Union of India* (2017) 10 SCC 1.
[1230] Information Technology Act 2000, s 69.
[1231] Pameela George, 'India's Surveillance Landscape after the DPDPA' (IAPP, 6 February 2025) <https://iapp.org/news/a/india-s-surveillance-landscape-after-the-dpdpa> accessed 28 August 2025.

terrorist under a defined statutory authorisation.

By contrast, mass surveillance involves the indiscriminate collection and analysis of communications or personal data from entire populations, regardless of whether individuals are under suspicion. Programmes such as India's Central Monitoring System (CMS), which enables direct interception of all phone and internet communications, or NETRA, which scans bulk internet traffic for "flagged" keywords, exemplify this model. Here, monitoring is not limited to identified suspects but extends to everyone, collapsing the distinction between the innocent and the guilty.

3. Mass Surveillance Is Uniquely Rights-Invasive

Mass surveillance is uniquely invasive when compared to targeted surveillance for three interrelated reasons:

The Expansive Scale of Monitoring: the scale of mass surveillance transforms breach of privacy from an exception into a rule. By placing millions of citizens under continuous watch, it infringe the constitutional presumption of innocence This have a widespread chilling impact on the rights to dissent, association, and expression.

The Opacity of Mass Surveillance: opacity is a characteristic of widespread monitoring. Hardly are people informed that their data has been intercepted, and there is no impartial way to confirm whether the monitoring is required or lawful. An atmosphere of secrecy with little accountability is fostered by the executive branch's consolidation of power without judicial or parliamentary oversight.

Repurposing and Function Creep in Data Use: widespread surveillance makes it possible to repurpose data. Information gathered for one goal (like counterterrorism) can be retained, processed, and utilised forever for unrelated purposes like economic exploitation, political monitoring, or profiling. This runs the risk of "function creep," in which data loses its original purpose and turns into a social control mechanism instead of a valid security measure.

Unlike targeted surveillance, which is narrow, time-bound, and easier to subject to judicial review, mass surveillance establishes an architecture of permanent suspicion, altering the citizen-State relationship in ways incompatible with constitutional democracy.

4. Evolution of the Right to Privacy in India

At the time of drafting of the Indian constitution, there were limited examples of codification of the right to privacy. Common law for instance did not have a clearly articulated privacy doctrine.[1232] At the time, one of the strongest articulations of the right to privacy was found in the European Convention on Human Rights, which was not yet in operation. Nonetheless, the United States of America employed an eclectic array of laws to safeguard privacy in various situations, and the ideas from these laws nearly found their way into the Indian Constitution as an amendment modelled after the US Fourth Amendment.

When creating the Fundamental Rights, the Constituent Assembly did not give the right to privacy the consideration it deserved. This may have resulted from the relative paucity of information available at the time regarding the right to privacy. The house came extremely close to passing an amendment that

[1232] A.G. Noorani, Right to Privacy, 40(9) ECONOMIC AND POLITICAL WEEKLY 802 (26-2-2005).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

would have added a prohibition on unreasonable searches, but ultimately decided against it. As a result, the Supreme Court was first reluctant to include this right in the Constitution. Nevertheless, the right to privacy was subsequently incorporated into the list of fundamental rights by the Supreme Court of India, which has been defining its parameters via the various judgements involving this right.

M.P. Sharma v Satish Chandra[1233] marked the starting point of the jurisprudential journey. In that case the Court refused to read an American-style Fourth Amendment protection into the Indian Constitution and upheld state power of search and seizure, taking the view that the Constitution's framers had not chosen to make such a right explicit. The decision left open the possibility that privacy might be protected in other ways, but it did not recognise a freestanding constitutional right to privacy.

The Supreme Court, however, progressively shifted from this stance to acknowledge that the protection of the right to privacy would have a significant impact on other constitutionally granted rights and liberties. Kharak Singh v. State of U.P.[1234]. marked the start of this procedure. Kharak Singh is often called India's first proto-privacy case: the Court confronted intrusive police surveillance practices (night visits, domiciliary checks and shadowing of so-called "history-sheeters") and considered their impact on Articles 19 and 21. [1235]

While the majority declined to declare an explicit fundamental right to privacy, it held that certain intrusions (for example, nocturnal visits to a person's home) violated the core of personal liberty protected by Article 21, The court recognised "the right of the people to be secure in their persons, houses, papers, and effects" and declared that their right against unreasonable searches and seizures was not to be violated[1236]; the judgment thus acknowledged that unauthorised state intrusion into the home is constitutionally suspect. Justice Subba Rao's partly dissenting opinion argued persuasively that privacy is an essential ingredient of personal liberty and articulated what we now call the "chilling effect", the idea that surveillance constrains free movement, association and speech.

Throughout the 1970s the Court continued to refine the doctrine. In R M Malkani v State of Maharashtra (1973)[1237] the Court took a narrower view in the context of telephone tapping and admissibility of recordings: it emphasised targeted interception aimed at the guilty (and upheld certain forms of interception in that context), signalling an early judicial preference for targeted surveillance rather than indiscriminate monitoring.

The right to privacy as defined by the Supreme Court so far, now extends beyond government intrusion into private homes. A doctrinal watershed occurred in Gobind v State of M.P. (1975). [1238]In Gobind the Court more explicitly recognised that the Constitution protects a penumbral right to privacy, a cluster of liberties implicit in Articles 14, 19 and 21[1239] and articulated that intrusions into privacy must withstand a rigorous standard of justification. The Court in Gobind invoked the concept of a compelling state interest and implicitly

[1233] *M.P. Sharma v Satish Chandra,* AIR 1954 SC 300.
[1234] *Kharak Singh v State of U.P.* AIR 1963 SC 1295.
[1235] The Constitution of India, 1950 art 14.
[1236] *Kharak Singh v State of U.P.* AIR 1963 SC 1295.
[1237] *R M Malkani v State of Maharashtra* (1973) 1 SCC 471.
[1238] *Gobind v State of M.P.* (1975) 2 SCC 148.
[1239] The Constitution of India, 1950 arts 14, 19 and 21.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

accepted a form of narrow tailoring i.e. the means used must be suitably limited to the aim.

The protections brought about by People's Union for Civil Liberties (PUCL) v. Union of India are the most particular to communication surveillance. The Indian Supreme Court ruled in this case that ""the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as 'right to privacy'.., telephone conversation is an important facet of a man 's private life"[1240].

The Court held that telephone conversations are an important facet of private life and that interception would violate Articles 19 and 21 unless authorised by procedure established by law and accompanied by adequate safeguards. Because existing statutes were archaic and lacked sufficient procedural checks, the Court laid down detailed interim procedural safeguards for interception, while acknowledging that the ideal remedy was legislative reform providing independent, robust oversight.

The decisive transformation came with the nine-judge Constitution Bench in Justice K S Puttaswamy (Retd) v Union of India (2017).[1241] In Puttaswamy the Supreme Court finally held that the right to privacy is a fundamental right protected under Article 21 and as part of the freedoms guaranteed by Part III. The Court authored a principled test for assessing invasions of privacy: any restriction must satisfy legality, necessity, and proportionality. Puttaswamy thus enshrined the three-part doctrine as the constitutional yardstick for surveillance and data intrusions.

Since Puttaswamy, Indian courts and commentators have used the proportionality framework to critique state surveillance programmes that rely on dated statutes (the Indian Telegraph Act 1885, the Information Technology Act 2000 and its 2009 Rules) or on executive approvals without independent oversight. Scholars highlight that Puttaswamy requires not only statutory backing but also procedural safeguards; independent prior authorisation, narrow tailoring, data.

The court ruled that surveillance techniques must serve an urgent social need in order to satisfy the necessity requirements. This criterion is undermined by broad requirements under CMS and NETRA, which assume a continuous state of emergency.

5. Legal & Constitutional Framework For Mass Surveillance

5.1 Telecommunication Interception: Indian Telegraph Act and Rules

The Indian Telegraph Act 1885 is one of the earliest statutes conferring interception powers on the State. Section 5(2)[1242] of the Act empowers both the Central and State governments, on the occurrence of any "public emergency" or "in the interest of public safety," to order the interception of messages transmitted through telegraph or telecommunication systems, provided that such action is deemed necessary in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of an offence.

The scope of Section 5(2) is extremely wide, and the conditions of "public emergency" and "public safety" remain

[1240] *People's Union for Civil Liberties (PUCL) v Union of India* AIR 1997 SC 568.
[1241] *K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
[1242] Indian Telegraph Act 1885, s 5(2).

undefined, leaving broad discretion to the executive.[1243] The Telegraph Rules, particularly Rule 419A,[1244] inserted in 2007 which seeks to operationalise these powers by laying down procedural requirements. Interception orders must be issued by the Union or State Home Secretary (or in urgent circumstances, by a senior officer, subject to later confirmation), are valid for sixty days (extendable up to 180 days), and must be subject to periodic review by a Review Committee. These safeguards were largely crystallised following the Supreme Court's decision in PUCL v Union of India, which directed that interception powers under the Telegraph Act be regulated by procedural safeguards to prevent arbitrary exercise.

5.2 Information Technology Act 2000 and 2009 Rules

The rise of the internet and digital communications led to the enactment of the Information Technology Act 2000 (IT Act). Section 69 of the Act[1245] authorises the Central and State governments to direct any agency to intercept, monitor, or decrypt information generated, transmitted, received, or stored in any computer resource, if it is considered necessary or expedient in the interests of sovereignty, security, public order, friendly relations with foreign States, or to prevent incitement of offences. The provision is notably broad and permits extensive intrusion into personal data and communications.

To operationalise Section 69, the government notified the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009[1246]. These rules mirror the structure of Rule 419A of the Telegraph Rules: only the Union or State Home Secretary may issue authorisations (except in emergencies), orders are valid for sixty days (extendable up to 180 days), and a Review Committee is tasked with examining their legality and necessity. Rule 20 requires destruction of intercepted material once retention is no longer necessary, but enforcement remains opaque.

The IT Act also introduced Section 69B, empowering the government to authorise monitoring of traffic data for cyber-security purposes, implemented through the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009.[1247] This further expanded the State's ability to track online communications on a broad scale.

Despite these safeguards, commentators have noted that the system remains executive-centric: critics argue that these powers are plagued by lack of transparency and independent oversight. Authorisations and reviews are all internal to the government, with no requirement for prior judicial approval. Orders of interception are confidential, and affected individuals have no notice or remedy unless a breach is discovered. Consequently, India's electronic surveillance regime is frequently criticised as incompatible with the constitutional standards of necessity and proportionality articulated in Puttaswamy.

[1243] Chinmayi Arun, 'Thin Safeguards and Mass Surveillance in India' (2014) 26 NLSIR 105, 110.
[1244] Indian Telegraph Rules 1951, r 419A (as amended in 2007).
[1245] Information Technology Act 2000, s 69.
[1246] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, rr 3–7.
[1247] Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009, r 3.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

5.3 The Digital Personal Data Protection Act, 2023 (DPDPA)

While the Digital Personal Data Protection Act, 2023 (DPDPA) marks India's first comprehensive legislation on data protection, it remains ill-equipped to regulate or restrain mass surveillance by the State. Three key shortcomings illustrate its inadequacy.

Overbroad State Exemptions: Section 17 of the Act[1248] permits processing of personal data without consent for reasons of "*sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order*" and for the prevention or detection of offences. The breadth of these categories enables sweeping surveillance practices without independent authorisation or effective judicial oversight. Unlike the European Union's General Data Protection Regulation (GDPR), which demands necessity and proportionality in national security derogations,[1249] the DPDPA provides no substantive safeguards against misuse.

Absence of Independent Oversight: Although the Act creates a Data Protection Board of India, its remit is limited to matters such as data breaches and fiduciary compliance, not state surveillance practices.[1250] Crucially, the Board lacks structural independence, being subject to appointments and removals by the Central Government.[4] This institutional design raises questions about its ability to impartially scrutinise government surveillance measures, thereby leaving the most significant intrusions on privacy unchecked.

Failure to Incorporate the Puttaswamy Standard: In Justice K. S. Puttaswamy (Retd) v Union of India,[1251] the Supreme Court established proportionality and necessity as constitutional safeguards against privacy infringements. Yet, the DPDPA does not incorporate these standards into its exemption regime. By granting blanket powers to the State without embedding proportionality tests or requiring independent audits, the Act risks legitimising indiscriminate surveillance rather than restricting it.

Weak Accountability Mechanisms: The obligations imposed on data fiduciaries, such as purpose limitation and data security, are largely inapplicable where State exemptions are invoked.[1252] Moreover, the Act imposes no obligation on government agencies to publish transparency reports, submit to parliamentary scrutiny, or undergo independent audits regarding surveillance. This absence of accountability mechanisms leaves affected individuals with no practical avenues of redress.

The DPDPA, far from constraining surveillance, risks entrenching it within a thin layer of legality. By providing statutory cover for extensive exemptions without corresponding checks, it arguably leaves the surveillance ecosystem largely untouched, if not expanded. In this sense, the Act falls short of reconciling the imperatives of security with the constitutional right to privacy, as articulated in Puttaswamy.

6. Rights Impact & Risks of Mass Surveillance

Mass surveillance regimes, by their very design, entail the systematic and often indiscriminate collection of personal data from large populations, frequently without individualised suspicion. Such bulk collection operates in tension with the very core of the right to privacy, as it

[1248] The Digital Personal Data Protection Act 2023, s 17(2).
[1249] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1, art 23.
[1250] The Digital Personal Data Protection Act 2023, s 19.
[1251] Justice K. S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[1252] The Digital Personal Data Protection Act 2023, s 17(4).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 11 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

transforms the presumption of anonymity in everyday life into a presumption of monitoring. The absence of clear targeting criteria means that the ordinary individual is treated as a potential subject of investigation, eroding the boundary between the private and the public sphere. This inversion of constitutional values undermines the autonomy of individuals, who are deprived of meaningful control over the circumstances in which their personal information is captured, stored, and analysed.

The consequences extend beyond privacy into the domain of democratic freedoms. Knowledge or even suspicion of being watched generates a pervasive chilling effect on freedom of speech, expression, and association.[1253] Journalists, academics, and human rights defenders in particular are deterred from engaging in critical inquiry or dissent, fearing reprisal or surveillance of their communications.[1254] Such an environment fosters self-censorship and weakens the press, thereby striking at the foundation of a democratic public sphere. When surveillance systems incorporate biometric identifiers such as facial recognition technology, they not only enable profiling but also risk systemic exclusion such as denial of access to welfare schemes or public spaces for individuals wrongly identified or categorised.

The risks are compounded by the fragility of data security in an ecosystem where vast databases of sensitive personal information are maintained without robust safeguards. Centralised repositories become attractive targets for malicious actors, increasing the likelihood of breaches with irreversible consequences. Moreover, the phenomenon of "function creep"; further jeopardises individual rights.[1255] Data initially collected for national security or law enforcement may be diverted towards commercial use, political surveillance, or other unauthorised ends, all without the knowledge or consent of those affected. The absence of statutory requirements for notice or accessible remedies leaves individuals powerless in the face of such encroachments.

Most concerningly, surveillance does not affect all individuals equally. Marginalised groups, including religious minorities, political dissidents, migrants, and economically disadvantaged communities bear a disproportionate share of the burden.[1256] These groups are often targeted under the guise of maintaining public order or national security, rendering them more vulnerable to profiling, exclusion, and harassment. The discriminatory deployment of surveillance technologies deepens existing social inequalities and corrodes trust in public institutions. The cumulative effect is the creation of a society in which privacy is not a right enjoyed by all, but a privilege available only to those beyond the reach of suspicion.

Mass surveillance therefore poses not merely a technical or administrative challenge, but a profound constitutional dilemma. It threatens to normalise intrusion, silence dissent, weaken accountability, and exacerbate structural injustices. Unless subject to rigorous legal safeguards, independent oversight, and democratic control, the expansion of surveillance powers risks

[1253] UN Human Rights Committee, 'General Comment No 34: Article 19 – Freedoms of opinion and expression' (2011) CCPR/C/GC/34, para 23.
[1254] UN General Assembly, 'The Right to Privacy in the Digital Age' A/RES/73/179 (17 December 2018).
[1255] European Court of Human Rights, Zakharov v Russia (2016) 63 EHRR 17.
[1256] Report of the Special Rapporteur on the Right to Privacy, A/HRC/46/37 (22 January 2021).

displacing the rights-bearing individual at the centre of constitutional governance with a citizenry conditioned to perpetual observation.

7. Cross-Jurisdictional V2X Governance and International Harmonization

India's current legal framework governing surveillance, particularly in light of the Digital Personal Data Protection Act, 2023 (DPDPA), remains insufficient to safeguard the fundamental right to privacy. A multi-pronged reform agenda is necessary to strike a constitutionally valid balance between individual rights and national security.

Much of India's current surveillance regime originates from legal instruments drafted in eras predating sophisticated spyware such as Pegasus.[1257] Existing provisions are therefore incapable of addressing the risks posed by today's surveillance industry. A Select Committee on Surveillance of Parliament could be mandated to:

a. Review comparative global best practices;
b. Require the Government to submit periodic surveillance reports justifying necessity;
c. Recommend suitable legislative frameworks that integrate technological safeguards with constitutional guarantees.

And based on the report of the Committee on Surveillance of Parliament, a dedicated Surveillance Regulation Act should be introduced to replace the outdated patchwork of provisions scattered across the Telegraph Act 1885, the Information Technology Act 2000, and executive orders. Such an Act must include the following among others:

a. To prevent ambiguity, provide precise legal definitions of surveillance and related capabilities.
b. To avoid indiscriminate surveillance, use stringent purpose limitation and a targeting-first strategy.
c. Demand independent prior authorisation for all interception requests, either from the judiciary or quasi-judicial authority or a specially designated Surveillance Commissioner. Urgent-use carve-outs that are specifically tailored must be promptly reviewed ex post facto.
d. Put in place accountability systems, such as an impartial monitoring committee, recurring audits, penalties for misuse, and legally binding remedies for impacted parties.

8. Conclusion

India's journey into the digital era has been marked by the expansion of an extensive surveillance apparatus, one that increasingly blurs the line between legitimate security imperatives and impermissible intrusions upon constitutional freedoms. While the State may invoke concerns of national security, counter-terrorism, and public order to justify the deployment of mass surveillance systems, these justifications cannot eclipse the foundational principles of legality, necessity, and proportionality laid down in Justice K. S. Puttaswamy (Retd) v Union of India[1258]. Security objectives, however pressing, do not authorise suspicionless and indiscriminate collection of personal data from entire populations.

[1257] Saptaparno GhoshPJ George, "Explained | One Year since the Pegasus Spyware Revelations" (The Hindu, July 23, 2022) <https://www.thehindu.com/news/national/a-year-since-pegasus-revelations/article65666799.ece> accessed 28 August 2025.

[1258] *K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

The persistence of colonial-era laws, coupled with the inadequacies of the Digital Personal Data Protection Act, 2023,[1259] has created a regulatory landscape that entrenches executive dominance while offering little in the way of independent oversight or effective remedies. It has been shown that in addition to weakening privacy, the State's extensive exemptions, ambiguous authorisation procedures, and lack of statutory protections also pose a threat to the freedoms of speech, association, and criticism. As a result, there is a structural imbalance that puts surveillance requirements ahead of constitutional guarantees.

Strict protections, including clear legislative definitions, prior independent permission, limited scope customisation, and strong accountability systems, are necessary if India is to balance its democratic ideals with the realities of digital government. A model for this kind of reform is offered by the proposed Surveillance Regulation Act and DPDPA revisions, which include openness, supervision, and rights-protective technology within the law. In the end, the legality of any monitoring system must be based on its commitment to constitutional norms and individual dignity, not on its technological ability to encroach.

A monitoring system that upholds human rights is a democratic need, not an extravagance. Without it, India runs the risk of normalising constant surveillance, stifling criticism, and widening the gap. Legislators, judges, and civil society face a clear challenge: making sure that the promise of privacy is a reality for all citizens and that the architecture of security does not turn into the architecture of control.

[1259] The Digital Personal Data Protection Act 2023.