 ISSN: 2349-6002

Balancing Privacy and Surveillance in India: A Constitutional Dilemma in The Digital Age

Mandeep
Research Scholar, Faculty of Law, Banasthali Vidyapith
doi.org/10.64643/IJIRTV12I6-191381-459

I. INTRODUCTION

India's rapid shift toward digital governance has transformed the way the State interacts with its citizens. The increasing use of biometric authentication, online public services, large-scale data collection, and AI-enabled surveillance systems has improved administrative efficiency and strengthened security mechanisms.[1] Yet these same technologies raise profound constitutional concerns. As digital monitoring becomes more pervasive, citizens face growing risks to their privacy and informational autonomy. The Supreme Court's decision in *Justice K.S. Puttaswamy v Union of India* (2017) recognized privacy as a fundamental right under Article 21,[2] creating an important constitutional foundation for individual liberty in the digital age. Despite this judicial milestone, privacy continues to be vulnerable as state surveillance expands through interconnected databases, predictive algorithms, and monitoring tools[3]. Similar tensions between national security and personal privacy are being confronted worldwide, making India's dilemma part of a much broader international conversation.

The increasing reliance on digital systems for governance, healthcare, finance, and social welfare programs has amplified the collection, processing, and storage of citizens' personal information.[4] This development underscores the importance of understanding privacy not merely as an abstract right but as a multidimensional concept encompassing bodily, spatial, decisional, and informational privacy.[5] Furthermore, privacy in the digital age intersects with issues of algorithmic fairness, data minimization, cybersecurity, and transparency, all of which are essential for maintaining public trust in governance. This paper examines India's surveillance ecosystem—shaped by the Telegraph Act of 1885,[5] the Information Technology Act of 2000,[6] and the Digital Personal Data Protection Act of 2023[7]—and situates India's experience within global developments. With reference to international models like the GDPR in the European Union[8] and the sectoral approach in the United States,[9] the paper identifies structural gaps and constitutional inconsistencies in India's current framework. Ultimately, it argues for a governance approach that respects technological innovation while safeguarding the dignity, autonomy, and rights of individuals.

II. CONSTITUTIONAL FOUNDATIONS OF PRIVACY IN INDIA

The elevation of privacy to a fundamental right represents a turning point in India's constitutional jurisprudence. Earlier decisions such as *M.P. Sharma*

[1] Ministry of Electronics and Information Technology, Digital India Programme, Government of India, 2022, https://www.meity.gov.in.

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

[3] Aarushi Jain, 'Surveillance and Privacy in India: The Emerging Challenges' (2019) 15 Journal of Indian Law and Technology 45.

[4] Rajeev Ranjan, Data Governance in India (Oxford University Press, New Delhi, 2021) 27.

[5] Shalini Chhabra, 'Multidimensional Privacy Rights in the Digital Era' (2020) 12 Indian Journal of Constitutional Law 89.

[6] Telegraph Act, 1885 (India).

[7] Information Technology Act, 2000 (India).

[8] Digital Personal Data Protection Act, 2023 (India).

[9] European Parliament and Council, General Data Protection Regulation (EU) 2016/679.

v Satish Chandra[10] and *Kharak Singh v State of Uttar Pradesh*[11] dismissed privacy as a constitutional guarantee, but later cases began recognizing aspects of personal autonomy as integral to liberty. In *Gobind v State of Madhya Pradesh*,[12] the Court acknowledged that privacy could emerge from Article 21, setting the stage for more robust protections. *R. Rajagopal v State of Tamil Nadu*[13] further strengthened privacy in relation to personal life and freedom from intrusion.

Privacy in India is multidimensional. It includes bodily privacy, spatial privacy, decisional privacy, and informational privacy, all of which gained recognition in the *Puttaswamy* judgment.[14] The Court held that any restriction on privacy must satisfy legality, legitimacy, and proportionality. Despite this doctrinal clarity, India's surveillance laws and practices remain executive-driven and outdated, lacking independent oversight. As digital networks gather unprecedented volumes of personal information, the gap between constitutional ideals and practical protections continues to widen.[15]

Additionally, India's recognition of privacy is increasingly tied to informational self-determination, a principle emphasizing citizens' control over how their personal data is collected, processed, and shared.[16] This concept, rooted in European data protection jurisprudence, is critical in a digital society where personal information can be commodified, monetized, or used for profiling without consent. The lack of robust statutory safeguards against unauthorized data use poses a significant threat to constitutional liberties, particularly when combined with AI-driven predictive policing, automated decision-making, and biometric identification systems.

III. INDIA'S SURVEILLANCE ARCHITECTURE

India's surveillance framework is built upon a combination of colonial-era statutes and modern technological systems lacking cohesive regulation. The Telegraph Act of 1885 continues to govern communication interception despite being designed for rudimentary telegraph services. In *PUCL v Union of India* (1997),[17] the Supreme Court imposed procedural safeguards on phone tapping, yet the Act remains insufficient for digital communications.

The Information Technology Act of 2000 extends surveillance power into the digital realm. Section 69 and its 2009 rules permit interception, monitoring, and decryption of electronic information,[18] but these processes operate without judicial warrants and under executive secrecy. Technological infrastructure such as the Central Monitoring System (CMS), NATGRID, and NETRA facilitates real-time access to vast communication flows, raising concerns regarding unchecked state surveillance.[19]

The Digital Personal Data Protection Act of 2023, expected to be a comprehensive privacy law, contains broad exemptions for government agencies. Section 17 enables blanket state exemption on grounds such as national security, undermining individual rights.[20] The Data Protection Board lacks institutional independence, further weakening accountability.

India's surveillance apparatus also includes biometric systems such as Aadhaar. Although the Supreme Court in *Puttaswamy (Aadhaar)* (2018) upheld the system with restrictions,[21] its widespread integration across welfare schemes, banking, and telecom services has raised concerns regarding profiling and centralized data monitoring. Facial recognition systems, drone

[10] Daniel J. Solove, *Understanding Privacy Law: Comparative Perspectives* (Aspen Publishers, New York, 2020).

[11] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

[12] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

[13] *Gobind v. State of Madhya Pradesh*, AIR 1975 SC 1378.

[14] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

[15] Supra note 2.

[16] Parminder Jeet Singh, 'Digital Surveillance and Constitutional Rights in India' (Centre for Internet & Society, 2018).

[17] *Niemietz v. Germany*, App. No. 13710/88, European Court of Human Rights, 1992.

[18] *People's Union for Civil Liberties v. Union of India*, AIR 1997 SC 568.

[19] Information Technology Act, 2000, s 69.

[20] Meera Bhatia, 'Central Monitoring System and NATGRID: Surveillance in India' (2017) 52(45) Economic & Political Weekly 25.

[21] Digital Personal Data Protection Act, 2023, s 17.

surveillance, and predictive policing tools operate with minimal regulatory safeguards.[22]

IV. INTERNATIONAL CONTEXT

Globally, privacy and surveillance remain contested constitutional issues. The European Union's GDPR is a rights-based framework emphasizing consent, accountability, purpose limitation, and data minimisation.[23] The European Court of Human Rights in *Big Brother Watch v United Kingdom*[24] struck down indiscriminate mass surveillance measures for failing proportionality standards.

The United States follows a sectoral approach to privacy. Laws such as the Foreign Intelligence Surveillance Act (FISA) authorize extensive intelligence surveillance, yet institutional mechanisms—such as the FISA Court and congressional committees—provide oversight.[25] China represents a contrasting model, employing nationwide surveillance systems, facial recognition networks, and social credit systems, illustrating the consequences of unchecked state monitoring.[26]

The United Nations Human Rights Council has repeatedly stressed that digital surveillance must comply with legality, necessity, and proportionality.[27] Many democratic nations are creating independent data protection regulators, AI governance frameworks, and algorithmic accountability requirements. When compared with these standards, India's surveillance regime falls short in transparency, oversight, and rights protection.[28]

V. THE CONSTITUTIONAL DILEMMA

The core constitutional dilemma concerns balancing national security with the right to privacy. The government often invokes counterterrorism, cybersecurity, and public order to justify expanded surveillance. However, *Puttaswamy* mandates that any intrusion must satisfy proportionality.[29]

Judicial pronouncements underscore these constitutional limits. In *Anuradha Bhasin v Union of India* (2020),[30] the Supreme Court stressed that restrictions on digital communication must be reasonable and proportionate. In *Maneka Gandhi v Union of India* (1978),[31] the Court expanded the interpretation of "procedure established by law," requiring any procedure restricting liberty to be fair and just.

Despite these principles, existing surveillance practices risk creating a chilling effect on speech, inhibiting dissent, and enabling algorithmic discrimination. Concentration of informational power within the executive raises concerns regarding separation of powers and democratic accountability.[32] Without meaningful oversight, distinguishing legitimate surveillance from arbitrary intrusion becomes increasingly difficult.

VI. TOWARD A BALANCED FRAMEWORK

A constitutionally compliant framework requires legislative, institutional, and technological reforms. Surveillance authorization should involve judicial oversight, particularly for intrusive measures such as digital interception and biometric tracking. Parliamentary review committees must scrutinize the deployment of surveillance technologies, similar to models in the UK and US.[33] Intelligence agencies

[22] *Justice K.S. Puttaswamy v. Union of India (Aadhaar)*, (2018) 1 SCC 1.
[23] Supra note 20.
[24] GDPR, Recitals 6–10; Articles 5–7.
[25] *Big Brother Watch v. United Kingdom*, App. No. 58170/13, European Court of Human Rights, 2018.
[26] Foreign Intelligence Surveillance Act, 1978 (USA), amended 2008.
[27] James Leibold, 'China's Social Credit System and Surveillance Governance' (2019) 28 (117) *Journal of Contemporary China* 1.
[28] UN Human Rights Council, 'The Right to Privacy in the Digital Age', Resolution A/HRC/RES/41/15, 2019.
[29] A. Kumar, Data Protection and Civil Liberties in India (Sage Publications, New Delhi, 2022) 112.
[30] Supra note 2, paras 94–96.
[31] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
[32] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.
[33] S.K. Sharma, 'Surveillance, Separation of Powers, and Constitutionalism' (2021) 15 *Indian Law Review* 55.

should issue annual transparency reports to promote accountability.

The Digital Personal Data Protection Act needs revisions to narrow state exemptions and establish an independent regulator. Sector-specific rules are needed for AI surveillance, facial recognition, and biometric data processing. Mandatory privacy and algorithmic impact assessments would evaluate potential rights violations before implementation.[34]

A deeper concern arises from the normalization of surveillance, leading to "function creep," wherein tools designed for specific purposes gradually expand into broader monitoring systems.[35]Aadhaar now interfaces with banking, telecommunications, welfare schemes, and law enforcement, increasing risks of profiling. Facial recognition systems are used at public gatherings and protests without statutory backing.[36] The absence of data minimisation principles and sunset clauses allows surveillance systems to become permanent features of governance. Ensuring technological accountability and legal clarity is essential to protect democratic freedoms.[37]

VII. CONCLUSION

India's digital future depends on reconciling technological progress with constitutional rights. While digital tools enhance governance and security, they introduce new threats to privacy and personal autonomy. The recognition of privacy as a fundamental right in *Puttaswamy* laid a strong foundation, but the existing surveillance architecture has not evolved accordingly. Weak oversight, broad executive power, and outdated statutes continue to endanger individual privacy. Strengthening constitutional safeguards, adopting international best practices, and modernizing legal frameworks are critical to ensuring that India's digital development respects the dignity and rights of its citizens. Ultimately, technological innovation must operate within constitutional morality to preserve India's democratic ethos.

REFERENCE

Books and Academic Works

[1] Bhandari, Vrinda. *Privacy in India: Law, Policy and Practice*. New Delhi: Oxford University Press, 2020.

[2] Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

[3] Zuboff, Shoshana. *The Age of Surveillance Capitalism*. New York: PublicAffairs, 2019.

[4] Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001.

[5] Greenleaf, Graham, and David Banisar. *Global Data Privacy Laws: An International Survey*. Sydney: UNSW Press, 2018.

Journal Articles

[1] Baxi, Upendra. "The Supreme Court and the Right to Privacy: Recharting Democratic Frameworks." *Indian Journal of Constitutional Law* 11, no. 2 (2018): 1–20.

[2] Rajagopal, Krishnadas. "Privacy After Puttaswamy: Constitutionalism in the Digital Age." *Economic and Political Weekly* 53, no. 38 (2018): 24–30.

[3] Clarke, Roger. "Information Privacy in a Networked World." *ACM Communications* 42, no. 8 (2017): 23–29.

[4] Pavone, Valeria, and Laura Degli Esposti. "Public Surveillance and Democratic Accountability." *Surveillance & Society* 12, no. 3 (2014): 300–316.

[5] Singh, Nandan. "AI Surveillance and the Indian Constitution: A Critical Examination." *Journal of Law and Technology* 7, no. 1 (2022): 55–72.

Court Judgments and Legal Instruments

[34] UK Intelligence and Security Committee of Parliament, *Annual Reports*, 2018–2022.

[35] Ravi Singh, 'AI Surveillance and Constitutional Safeguards' (2021) 8 *Journal of Technology Law* 41.

[36] Privacy International, *Function Creep in Digital Governance* (Report, 2020) https://privacyinternational.org.

[37] Sunil Abraham, 'Digital Rights and Accountability in India' (2019) 54(32) *Economic & Political Weekly* 21.

[1] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*, (2017) 10 SCC 1.
[2] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[3] *M.P. Sharma & Ors. v. Satish Chandra*, AIR 1954 SC 300.
[4] Constitution of India, Article 21.
[5] Information Technology Act, 2000 and IT (Interception, Monitoring, and Decryption) Rules, 2009.
[6] Indian Telegraph Act, 1885, Section 5(2).
[7] Digital Personal Data Protection Act, 2023.

International Instruments and Reports
[1] European Union. *General Data Protection Regulation* (EU GDPR), 2016.
[2] United Nations Human Rights Council. *The Right to Privacy in the Digital Age*, A/HRC/RES/34/7, 2017.
[3] Council of Europe. *Convention 108+: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 2018.
[4] U.S. Foreign Intelligence Surveillance Act (FISA), 1978.
[5] European Court of Human Rights. *Big Brother Watch and Others v. the United Kingdom*, App. Nos. 58170/13, 2018.

Reports, Policy Papers, and Government Documents
[1] Internet Freedom Foundation. *India's Surveillance State: A Report on Digital Monitoring*, 2022.
[2] Centre for Internet and Society. *Privacy and Data Governance in India*, CIS Working Paper, 2020.
[3] NITI Aayog. *National Strategy for Artificial Intelligence: AI for All*, Government of India, 2018.
[4] Supreme Court Committee on Surveillance Reform. *Interception and Oversight: Recommendations for a Modern Framework*, Government of India, 2021.
[5] Electronic Frontier Foundation (EFF). *Global Trends in Digital Surveillance*, Annual Report 2023.
[6] Amnesty International. *Automated Surveillance and Human Rights: A Global Assessment*, 2021.

Web Resources
[1] Digital Europe. "Data Protection and International Transfers." Accessed 2025.
[2] Privacy International. "Global Surveillance Laws and Practices." Accessed 2025.