ISSN: 3048-8702(O)

LLRJ

LEX LUMEN RESEARCH JOURNAL

VOLUME 2 - ISSUE 1

2025

LEX LUMEN RESEARCH JOURNAL-ISSN:3048-8702
Open Access-Peer Reviewed Law Journal, Licensed by-CC BY-NC-SA- © 2025
Editor-in-Chief: Prof. (Dr). Razit Sharma, Publisher: Mrs. Rachana

Volume-2, Issue-1 ***Pages:220-228***

WATCHING THE WATCHERS: BALANCING PRIVACY AND SURVEILLANCE IN THE AI ERA

By- **Sooraj K.R**[1]

ABSTRACT

The expansion of state surveillance in the digital era, driven by artificial intelligence and advanced data analytics, has intensified debates surrounding the right to privacy. While national security remains a legitimate state interest, unregulated monitoring risks undermining constitutional liberties. This article examines the evolution of privacy as a fundamental right in India, particularly post-K.S. Puttaswamy v. Union of India, and evaluates the legal framework governing surveillance. It analyses the proportionality principle as a constitutional safeguard, compares global regulatory models, and proposes measures for ensuring accountability and transparency. The study underscores the need for a balanced approach where technological tools enhance security without eroding democratic freedoms.

KEYWORDS: Right to Privacy, State Surveillance, Artificial Intelligence, National Security, Proportionality, K.S. Puttaswamy v. Union of India, Data Protection.

INTRODUCTION

In the digital age, the relationship between personal liberty and state power is undergoing unprecedented strain. Rapid advancements in artificial intelligence, biometric identification, and real-time data analytics have armed governments with

[1]Student, Government Law College Thrissur.

Volume-2, Issue-1 *Pages:220-228*

sophisticated tools for monitoring individuals. While such technologies can strengthen national security and help combat threats ranging from terrorism to cybercrime, they also carry the potential to intrude deeply into citizens' private lives. The challenge lies in striking a balance where security imperatives do not overshadow the constitutional promise of individual dignity and autonomy.

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*[2] laid the groundwork, but more recent rulings such as *Anuradha Bhasin v. Union of India*,[3] have reaffirmed and expanded privacy's scope by linking it to free expression and access to information in the context of internet restrictions. This article examines the constitutional, statutory, and comparative dimensions of the tension between privacy and surveillance, proposing a proportionality-based framework to reconcile individual rights with legitimate state interests in the age of AI.

BACKGROUND

The recognition of the right to privacy in India is the result of a gradual judicial evolution. Early rulings such as *Kharak Singh v. State of Uttar Pradesh*[4] and *Justice K.S. Puttaswamy (Retd.) v. Union of India*[5] laid the doctrinal foundation by affirming privacy as intrinsic to dignity and liberty. However, in recent years, the Supreme Court has extended and applied this principle in the context of modern technological realities.

In *Anuradha Bhasin v. Union of India*,[6] the Court connected privacy to freedom of speech and access to information, holding that indefinite internet restrictions are impermissible and must meet necessity and proportionality standards. Similarly, in

[2] Supra note 1
[3] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637
[4] Kharak Singh v. State of U.P. & Ors., 1963 AIR 1295, 1964 SCR (1) 332 (India)
[5] Supra note 1
[6] Supra note 3

Volume-2, Issue-1 *Pages:220-228*

Manohar Lal Sharma v. Union of India,[7] that is the Pegasus spyware case where the Court underscored that surveillance without statutory backing or judicial oversight threatens both privacy and democratic freedoms, appointing an independent committee to investigate the allegations.

The surveillance regime in India remains anchored in older laws like the Indian Telegraph Act, 1885,[8] and the Information Technology Act, 2000,[9] which empower interception under specified grounds. While procedural safeguards exist, critics highlight the absence of independent authorisation and robust accountability mechanisms.

The integration of Aadhaar-linked biometric databases with emerging tools such as facial recognition, predictive policing algorithms, and AI-driven analytics has amplified the state's monitoring capacity. These developments have prompted judicial scrutiny in cases like *Internet Freedom Foundation v. Union of India*[10] where concerns were raised over the deployment of facial recognition in public spaces without a clear legislative framework. This ongoing shift reflects the judiciary's increasing engagement with privacy concerns in the face of rapid technological change, setting the stage for a more nuanced legal response to state surveillance in the AI era.

CURRENT LEGAL FRAMEWORK IN INDIA

India's constitutional protections for personal liberty and expression Articles 21[11] and 19[12] now operate against a more intrusive technological backdrop. The Supreme Court

[7] Manohar Lal Sharma v. Union of India, (2021) 10 SCC 275
[8] Indian Telegraph Act, No. 13 of 1885, INDIA CODE (1885).
[9] Information Technology Act, No. 21 of 2000, India Code (2000)
[10] Internet Freedom Foundation v. Union of India, Writ Petition (Civil) No. 44 of 2019 (India)
[11] India Consti art.21
[12] India Consti art.19

Volume-2, Issue-1 *Pages:220-228*

has repeatedly insisted that restrictions on digital freedoms and communications must satisfy tests of legality, necessity and proportionality. In *Anuradha Bhasin v. Union of India*[13] the Court held that indefinite or blanket internet suspensions cannot stand and must be measured against necessity and proportionality, thereby bringing internet access within the scope of fundamental rights scrutiny.[14]

Statutory interception and surveillance powers remain grounded in older enactments: the Indian Telegraph Act, 1885,[15] and the Information Technology Act, 2000,[16] together with rules thereunder that permit interception, monitoring and blocking under specified grounds. These statutes provide the legal architecture for lawful interception but have been criticised for outdated drafting, vague grounds for action and limited independent authorization. The Supreme Court's post-2020 scrutiny has exposed this gap between modern surveillance capacity and existing legal safeguards.[17] Recent litigation has made these tensions explicit. The Pegasus-related proceedings in *Manohar Lal Sharma v. Union of India*[18] prompted the Court to probe allegations of state-sponsored or state-enabled spyware use and highlighted the lack of clear statutory, judicial or parliamentary frameworks for intrusive digital surveillance. The Court's response, including appointment of independent fact-finding mechanisms, signals judicial insistence on stronger procedural safeguards and transparency when

[13] Supra note 3
[14] Global Freedom of Expression, Case Law Database, https://globalfreedomofexpression.columbia.edu/ (last visited Aug. 11, 2025).
[15] Supra note 8
[16] Supra note 9
[17] India Code, Digital Personal Data Protection Act, 2023, Ministry of Law and Justice, https://www.indiacode.nic.in/handle/123456789/24501.
[18] Supra note 7

surveillance affects fundamental rights.[19] AI and Surveillance Technologies, capabilities, risks, biases

Artificial intelligence multiplies the state's surveillance reach. Systems combining biometric databases, facial recognition, location metadata, and behavioural analytics allow mass identification, pattern recognition and predictive inferences at scale. These tools promise efficiency for law enforcement (faster identification, automated flagging), but they also increase the risk of false positives, discrimination, and opaque decision-making, problems that are magnified where datasets are biased or poorly audited. Independent technical audits, transparency about training data, and explainability are therefore not mere technical niceties but constitutional safeguards.[20] AI tools tend to be "black boxes": proprietary models and complex pipelines make it difficult for affected persons (or courts) to understand how a particular identification or risk score was produced. This opacity undermines meaningful judicial review and remedies in cases of wrongful surveillance. Bias in facial recognition systems, particularly poor accuracy for women and certain ethnic groups, further aggravates the risk of discriminatory state enforcement. Given these harms, courts and regulators are increasingly treating AI surveillance not merely as a technical problem but as a legal one requiring rule-making, oversight, and enforceable standards.[21]

CONSTITUTIONAL LIMITATIONS & THE PROPORTIONALITY TEST — DEEP CASE LAW ANALYSIS

[19] Indian Kanoon, https://indiankanoon.org/ (last visited Aug. 11, 2025). Supreme Court Observer, https://www.scobserver.in/ (last visited Aug. 11, 2025).
[20] Artificial Intelligence Act, Regulation (EU) 2024/1689, O.J. (L 1689) 2024/1689 (July 12, 2024) (E.U.), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 (last visited Aug. 11, 2025).
[21] Morrison & Foerster LLP, https://www.mofo.com (last visited Aug. 11, 2025).

Volume-2, Issue-1 *Pages:220-228*

Since *Puttaswamy*[22] established proportionality as the touchstone for privacy intrusions, post-2020 decisions have tested how proportionality functions against digital surveillance. *Anuradha Bhasin*[23] reinforced that measures restricting communications must be necessary and proportionate — a principle directly applicable to AI-enabled mass surveillance.[24] The Pegasus litigation in *Manohar Lal Sharma*[25] took that principle further: the Court treated allegations of covert intrusion as potentially unconstitutional in the absence of clear statutory authorization, independent oversight, or post-fact remedies. The Court's insistence on an independent probe and strict judicial scrutiny indicates a judicial posture that will not accept unregulated surveillance merely because it is technologically feasible or claimed to be for security.[26] Applied to AI surveillance, the proportionality inquiry requires (a) a clear legal basis (parliamentary statute or rules), (b) demonstrable necessity for the specific objective, (c) least-intrusive means, and (d) safeguards, independent oversight, periodic review, notice/ redress where possible, and transparency measures (audit trails, impact assessments). Post-2020 jurisprudence shows courts demanding these elements before validating intrusive digital tactics; absent them, the risk of judicial intervention is high.[27]

COMPARATIVE PERSPECTIVE — EU, US AND UK MODELS

International approaches offer important design cues. The European Union, through the GDPR and its jurisprudence, has emphasised data-protection principles such as

[22] Supra note 1
[23] Supra note 3
[24] Global Freedom of Expression, Columbia University, https://globalfreedomofexpression.columbia.edu (last visited Aug. 11, 2025).
[25] Supra note 7
[26] Indian Kanoon, https://indiankanoon.org (last visited Aug. 11, 2025).
Supreme Court Observer, https://www.scobserver.in (last visited Aug. 11, 2025).
[27](https://globalfreedomofexpression.columbia.edu/cases/investigatory-powers-act-2016/)

Volume-2, Issue-1 *Pages:220-228*

purpose limitation, data minimisation and the right to meaningful explanation. The Schrems II judgment[28] famously invalidated the European Union-United States Privacy Shield because of systemic foreign surveillance concerns, underscoring how national surveillance programs can disrupt cross-border data frameworks. More recently, the European Union's AI ACT, adopts a risk-based approach that places strict controls or bans on high-risk biometric identification in public spaces, a regulatory posture that foregrounds rights protection over unfettered technological deployment.[29] The United States anchors protections in the Fourth Amendment; while doctrinal debates about digital searches continue, recent rulings and lower-court decisions (and ongoing legislative proposals) reflect heightened scrutiny of warrantless access to digital devices and location data. The U.S. experience suggests that strong constitutional text plus robust judicial remedies can check executive excess, but gaps remain where legislation fails to address modern data practices.[30] The United Kingdom's Investigatory Powers Act 2016,[31] created a centralized statutory framework with judicial oversight mechanisms (the "double-lock" for the most intrusive warrants) and an independent Investigatory Powers Commissioner, a model that balances investigatory needs with external authorization and review. Recent UK amendments and debates over oversight show how legislative design and institutional review can either strengthen or weaken privacy protections depending on political choices.[32]

[28] Data Protection Commissioner v. Facebook Ireland Ltd. & Maximillian Schrems (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).
[29](Artificial Intelligence Act, Regulation (EU) 2024/1689, O.J. (L) 2024/1689 (July 12, 2024) (E.U.), available at EUR-Lex (accessed Aug. 11, 2025); see also summary, Wikipedia.)
[30]American Constitution Society, https://www.acslaw.org. The Verge, https://www.theverge.com.
[31] Investigatory Powers Act 2016, c. 25 (UK)
[32] Legislation.gov.uk, https://www.legislation.gov.uk (last visited Aug. 11, 2025).
Investigatory Powers Commissioner's Office (IPCO), https://www.ipco.org.uk (last visited Aug. 11, 2025).

Volume-2, Issue-1 *Pages:220-228*

CRITICAL ISSUES & CHALLENGES

Though India recognises privacy as a fundamental right, legal protections remain incomplete. The Digital Personal Data Protection Act, 2023,[33] while a step forward, contains exemptions that permit government surveillance without independent oversight. The lack of a clear statutory framework for surveillance creates ambiguity and risks misuse. The Justice B.N. Srikrishna Committee Report, which laid the groundwork for data protection reform, had emphasised strong independent oversight and limited government exemptions, elements yet to be fully realised.[34]

Lack of effective grievance redressal and inadequate penalties further undermine protections. The Pegasus spyware controversy, examined in *Manohar Lal Sharma v. Union of India*[35] demonstrated gaps in legal safeguards against covert surveillance and the need for enforceable remedies. Furthermore, limited public awareness and weak cyber security infrastructure exacerbate risks of data breaches and misuse. Without strong laws and oversight, both state and private actors may wield disproportionate control over personal data, endangering rights to privacy and free expression.

WAY FORWARD

India requires a comprehensive data protection law with minimal exemptions for government surveillance, ensuring all interception and monitoring are subject to prior judicial authorisation and independent oversight. The Justice B.N. Srikrishna

[33] Digital Personal Data Protection Act, 2023, No. XX of 2023, Acts of Parliament, India (2023)
[34] Justice B.N. Srikrishna Committee Report (2018), A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics & IT, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
[35] Supra note 7

Volume-2, Issue-1 *Pages:220-228*

Committee's recommendations for a powerful, autonomous Data Protection Authority must be implemented to empower enforcement and safeguard rights.[36]

Oversight should include mandatory transparency reports from government agencies and corporations detailing surveillance activities. Technology infrastructure must adopt a privacy-by-design approach, mandating data minimisation, encryption, and regular privacy impact assessments as recommended by the Ministry of Electronics and Information Technology (MeitY's) draft Data Protection Rules.[37]

Public awareness initiatives should inform citizens of their digital rights and the means to seek redress. India can also align its framework with international standards like the EU's GDPR and judicial decisions such as *Schrems II*, which underscore the importance of safeguarding data during cross-border transfers.[38]

CONCLUSION

India stands at a crossroads in protecting privacy in the digital age. While judicial rulings such as *K.S. Puttaswamy (Retd.) v. Union of India*[39] affirm privacy as fundamental, existing laws and oversight are insufficient to guard against unchecked surveillance. Robust legal reforms, independent regulatory bodies, and technological safeguards are essential. Building a culture that values privacy alongside educating citizens about their rights will strengthen democracy and personal freedom. With coordinated efforts, India can establish a framework balancing security needs and individual dignity, securing a resilient digital future.

[36] Supra note 34
[37] Ministry of Electronics and IT, Draft Data Protection Rules, 2023, https://meity.gov.in/writereaddata/files/MeitY_Data_Protection_Rules_2023.pdf
[38] Supra note 22
[39] Supra note 1