INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

From Privacy to Profiling: Rethinking Constitutional Limits of State Surveillance in the Age of Datafication in India

APARAJITA GUPTA[*] AND DEEPAK YADAV[**]

ABSTRACT

The growing use of digital technologies has changed the way surveillance operates in India. While legal discussion continues to focus on privacy as the primary concern, recent developments suggest a deeper shift: from simple data collection to the large-scale profiling of individuals. Initiatives such as Aadhaar, together with controversies such as Pegasus, show that the State is increasingly capable not only of gathering data but also of analysing and predicting human behaviour. This paper examines whether the existing constitutional framework, centred on the right to privacy, is sufficient to address these developments. It argues that a privacy-based approach is limited, as it focuses on individual harm while overlooking broader concerns such as profiling, a lack of transparency and the misuse of aggregated data. This gap raises serious risks for individual autonomy and democratic accountability. Adopting a doctrinal and comparative methodology, the paper analyses Indian constitutional jurisprudence alongside global data-protection frameworks, particularly those of the European Union. It identifies the absence of clear safeguards against profiling in Indian law and highlights the need to move beyond privacy-centric thinking. The paper finds that current legal safeguards do not adequately address the risks posed by data-driven surveillance. It concludes by proposing greater transparency, stronger accountability mechanisms and clearer limits on profiling, so that technological advancement does not undermine constitutional values.

Keywords: *Digital surveillance; datafication; profiling; right to privacy; constitutional law*

I. INTRODUCTION

In recent years, digital technologies have become central to governance in India. From welfare-delivery systems to law-enforcement practices, the State increasingly relies on large-scale data collection and digital infrastructures. Programmes such as Aadhaar have created extensive databases linking identity, finance and services, while incidents such as Pegasus have raised concerns about the reach and depth of state surveillance. These developments suggest that

[*] Author is a Research Scholar at Banaras Hindu University (BHU), Varanasi, Uttar Pradesh, India.
[**] Author is a Research Scholar at Devi Ahilya Vishwavidyalaya (DAVV), Indore, Madhya Pradesh, India.

 [ISSN 2581-5369]

surveillance today is no longer limited to observing individuals but is gradually evolving into systems that process and interpret data at scale.

This shift marks an important change in how power operates. Surveillance is no longer confined to monitoring specific individuals; it now involves the aggregation of vast amounts of data to identify patterns, generate profiles and anticipate behaviour. Such systems function quietly and often without direct visibility, making their effects difficult to trace. As a result, individuals may be influenced or categorised without any clear point of intrusion.

Despite these changes, legal responses in India continue to be framed largely in terms of privacy. The recognition of privacy as a fundamental right has strengthened protections against arbitrary state action. However, this framework is primarily concerned with individual harm and identifiable violations. It does not fully engage with forms of surveillance that operate through data processing and profiling rather than direct intrusion.

This raises an important question: can a privacy-based constitutional framework adequately address data-driven surveillance, or is there a need to rethink how the law understands and regulates such practices? This paper approaches the question through a doctrinal and comparative analysis, examining Indian constitutional principles alongside global developments, particularly in the European Union.

It suggests that, while privacy remains essential, it cannot by itself address the challenges posed by profiling and datafication. A broader framework is required: one that focuses not only on the collection of data but also on its use and on the forms of power that emerge from it.

II. The constitutional framework of privacy in India

A. Evolution of privacy jurisprudence

The right to privacy in India has evolved through judicial interpretation rather than explicit constitutional recognition. In *M.P. Sharma v. Satish Chandra*, the Supreme Court rejected the existence of a fundamental right to privacy, holding that such a right was not protected under Part III of the Constitution.[1] This position was reaffirmed in *Kharak Singh v. State of U.P.*, although certain aspects of personal liberty were acknowledged.[2] A shift began in *Gobind v. State of M.P.*, where the Court cautiously recognised privacy as an implied right under Article 21.[3] This evolution culminated in *Justice K.S. Puttaswamy v. Union of India*, where a nine-judge bench unequivocally affirmed privacy as a fundamental right intrinsic to life and personal

[1] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).
[2] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India).
[3] *Gobind v. State of M.P.*, (1975) 2 SCC 148 (India).

 [ISSN 2581-5369]

liberty.[4] The Court emphasised that privacy is not merely a negative right but also a positive condition necessary for individual dignity and autonomy.[5]

B. Privacy as autonomy and individual-centric protection

Following *Puttaswamy*, privacy has been conceptualised as a core component of individual autonomy. It protects personal decision-making and enables individuals to exercise freedom without unwarranted interference. This understanding aligns with philosophical accounts of privacy that emphasise dignity and moral agency. Scholars such as Bloustein have argued that privacy is essential for preserving human dignity and individuality.[6] Similarly, Benn highlights that privacy is closely linked to respect for persons and the ability to exercise freedom meaningfully.[7]

In constitutional practice, this translates into an individual-centric framework, in which violations are assessed according to their impact on identifiable persons. While this approach strengthens protection against intrusive surveillance, it remains anchored in the assumption that harm is individual and arises from direct state action.

C. Judicial tests: legality, necessity and proportionality

To regulate state action, the Supreme Court has developed a structured test comprising legality, legitimate aim and proportionality. This test requires:

- Legality: the existence of a valid law authorising the action;
- Legitimate aim: the presence of a legitimate state objective; and
- Necessity and proportionality: the measure must be necessary and proportionate to the objective pursued.[8]

This framework reflects broader constitutional principles of balancing competing interests between individual rights and state power. The doctrine of proportionality ensures that state action is not excessive or arbitrary.[9]

In *Justice K.S. Puttaswamy v. Union of India*, the Court applied this test to assess the Aadhaar scheme, upholding its validity while imposing safeguards against the misuse of personal data.[10]

---

[4] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India), https://indiankanoon.org/doc/127517806/.
[5] *Id.*
[6] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962 (1964); ANITA L. ALLEN, UNPOPULAR PRIVACY (Oxford Univ. Press 2011).
[7] Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY 223 (Ferdinand D. Schoeman ed., 1984).
[8] T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 Yale L.J. 943 (1987).
[9] YUTAKA ARAI-TAKAHASHI, THE MARGIN OF APPRECIATION DOCTRINE AND THE PRINCIPLE OF PROPORTIONALITY IN THE JURISPRUDENCE OF THE ECHR (Intersentia 2002).
[10] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (India).

However, these tests are primarily designed to evaluate direct and identifiable intrusions into individual privacy.

D. Limits of the existing framework

Despite its doctrinal strength, the privacy framework exhibits significant limitations in addressing contemporary surveillance practices.

First, it is premised on identifiable individual harm. Privacy violations are recognised when there is a clear intrusion into a person's private sphere. However, modern surveillance often operates through aggregation and inference rather than direct intrusion.[11]

Second, the framework focuses largely on data collection rather than on the broader lifecycle of data use. Data-driven systems analyse and combine information to generate insights that extend beyond the original purpose of collection.

Third, it does not adequately address group-based harms. Algorithmic systems classify individuals into categories, producing consequences that affect communities rather than identifiable individuals.[12]

Scholars have highlighted how big data enables prediction and behavioural control, creating new forms of power that operate without direct visibility. These developments challenge the foundational assumptions of privacy law.[13]

Thus, while the privacy framework remains essential, it is conceptually tied to an earlier model of surveillance that no longer reflects current realities.

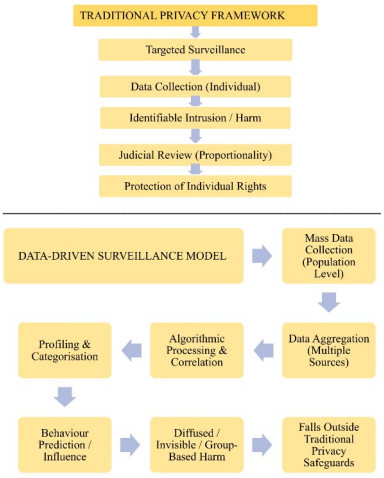

Figure 1: Traditional Privacy Framework vs Data-Driven Surveillance

[11] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012).
[12] danah boyd & Kate Crawford, *Critical Questions for Big Data*, 15 Info. Comm. & Soc'y 662, 666–68 (2012).
[13] *Id.*

III. From data collection to profiling: the changing nature of surveillance

A. Datafication and the shift in governance

Digital technologies have transformed governance by converting everyday activities into structured data. Transactions, mobility, communication and access to services are continuously recorded and integrated into interconnected systems. This process, often described as datafication, enables governance through data infrastructures rather than isolated records.[14]

Unlike earlier forms of surveillance that focused on observation, data-driven systems rely on aggregation and analysis. The ability to combine datasets allows institutions to generate insights about behaviour, preferences and patterns, thereby shifting governance from reactive monitoring to predictive assessment.[15]

B. The rise of profiling and predictive governance

A key consequence of datafication is the emergence of profiling. Profiling involves the automated processing of personal data to evaluate or predict individual behaviour, often without direct interaction or verification.[16]

In India, this shift is visible in predictive-policing practices. Systems developed in cities such as Delhi and Hyderabad rely on historical and demographic data to identify individuals or areas considered likely to be involved in future criminal activity. These practices move beyond traditional investigation, as decisions are increasingly based on statistical probabilities rather than proven conduct.[17]

As a result, governance shifts from responding to past events to anticipating future risks, expanding surveillance from specific individuals to broader populations.

C. Integrated data infrastructures: the Aadhaar ecosystem

Large-scale data infrastructures such as Aadhaar further reinforce this transformation. By linking identity with banking, telecommunications and welfare systems, Aadhaar enables data generated in one domain to be used across multiple contexts. This interconnected system creates

---

[14] danah boyd & Kate Crawford, *Critical Questions for Big Data*, 15 Info. Comm. & Soc'y 662 (2012), https://doi.org/10.1080/1369118X.2012.678878.

[15] *Id.*

[16] Lee A. Bygrave, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 Computer L. & Sec. Rev. 17 (2001).

[17] Ramachandran Murugesan, *Predictive Policing in India: Deterring Crime or Discriminating Minorities?*, LSE Hum. Rts. Blog (Apr. 16, 2021), https://blogs.lse.ac.uk/humanrights/2021/04/16/predictive-policing-in-india-deterring-crime-or-discriminating-minorities.

 [ISSN 2581-5369]

continuous visibility of individuals across institutional frameworks. Its consequences extend beyond identification to decision-making processes that determine access to services and entitlements.

Studies have shown that such systems can lead to exclusion from welfare benefits owing to authentication failures or data mismatches, demonstrating how harm can arise from the functioning of data systems rather than from direct state action.[18] These outcomes highlight the role of classification and processing in shaping administrative decisions.

D. From individual to group-based harm

A defining feature of data-driven surveillance is the shift from individual to collective impact. Profiling systems operate by grouping individuals according to shared characteristics, producing effects that extend beyond any single person. Predictive policing illustrates this dynamic: areas with historically higher crime rates, often associated with socio-economic disadvantage, are subjected to increased monitoring. This creates feedback loops in which surveillance reinforces existing patterns.[19]

Predictive policing and national identity databases do not necessarily produce direct harm to a single individual. Instead, they reshape decision-making processes and influence how groups are monitored and governed. This results in systemic and cumulative effects rather than isolated violations. Thus, while the law seeks a clearly identifiable victim, the actual harm lies in broader patterns of exclusion, classification and data-driven control.

E. Informational power and structural asymmetry

Data-driven governance has altered the balance of power between the State and individuals. The State possesses an extensive capacity to collect, aggregate and analyse data, while individuals have limited awareness of how their data is processed or used. This asymmetry transforms surveillance into a form of informational power. Decisions relating to policing, welfare and governance are increasingly shaped by opaque systems that remain inaccessible to those affected.[20]

Scholars have noted that such systems do not merely observe behaviour but actively structure and influence it, raising concerns about autonomy and democratic accountability.[21]

---

[18] Reetika Khera, *Impact of Aadhaar on Welfare Programmes*, 52(50) Econ. & Pol. Wkly. 43 (Dec. 16, 2017).
[19] ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (NYU Press 2017).
[20] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (Oxford Univ. Press 2019).
[21] Lee A. Bygrave, *supra* note 16.

 [ISSN 2581-5369]

IV. LIMITS OF THE PRIVACY-CENTRIC FRAMEWORK

The Digital Personal Data Protection Act, 2023 (DPDP Act) can be understood as a privacy-centric model that prioritises individual autonomy through consent, notice and purpose limitation. While this framework recognises informational privacy, it is increasingly insufficient to address contemporary data-driven surveillance. State data practices are often justified on grounds such as welfare, public order and national security, yet this framing obscures the growing asymmetry between the State and individuals. This is not merely a technical gap but a regulatory blind spot. By focusing narrowly on individual rights, the framework overlooks how large-scale data processing, aggregation and analytics reshape power structures.[22] The emphasis remains on procedural safeguards, particularly notice and consent, while insufficient attention is given to the consequences of profiling and algorithmic decision-making.[23]

A. Failure to regulate profiling

At first glance, the DPDP Act permits the processing of personal data for lawful purposes based on consent or legitimate use. The definition of processing under Section 2(x) is broad and includes various forms of data handling.[24] However, the Act does not impose specific safeguards against profiling.

Profiling is understood as the automated processing of personal data to evaluate behaviour or characteristics. In practice, therefore, profiling remains largely unregulated within the Indian framework.[25] What makes this more concerning is that it creates a significant gap, especially since state authorities increasingly rely on profiling in areas such as welfare distribution and law enforcement.

In the absence of clear limitations or accountability mechanisms, profiling can operate unchecked. This raises a deeper concern about arbitrariness and discrimination.

B. Limits of consent

[22] Navmi Joshi, *Emerging Challenges in Privacy Protection with Advancement in Artificial Intelligence*, 4 Int'l J.L. & Pol'y 55, 60 (2024).
[23] Alka Nanda Mahapatra & Harshita Gupta, *India's Data Protection Dilemma: Safeguarding Privacy or Silencing Voices*, CONST. L. SOC'Y, WBNUJS (Apr. 9, 2025), https://wbnujscls.wordpress.com/2025/04/09/indias-data-protection-dilemma-safeguarding-privacy-or-silencing-voices/.
[24] Digital Personal Data Protection Act, 2023, § 2(x) (India); MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, THE DIGITAL PERSONAL DATA PROTECTION BILL, 2023, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.
[25] Sonali Srivastava, *India: Decrypting Critical Concepts Under India's Digital Personal Data Protection Act, 2023 and Comparison with GDPR and PIPL*, IJLT BLOG (Mar. 21, 2024), https://forum.nls.ac.in/ijlt-blog-post/india-decrypting-critical-concepts-under-indias-digital-personal-data-protection-act-2023-and-comparison-with-gdpr-and-pipl/.

 [ISSN 2581-5369]

Consent is central to the privacy framework, yet its effectiveness is limited in practice. In many cases, access to essential services is contingent upon the submission of personal data, leaving individuals with little meaningful choice. This reflects a structural imbalance between the State and individuals. In effect, consent becomes a formality rather than a meaningful safeguard. Judicial recognition of unequal bargaining power in *Central Inland Water Transport Corporation Ltd. v. Brojo Nath Ganguly* highlights that consent cannot be considered valid where it undermines free will.[26]

Although the DPDP Act incorporates safeguards such as purpose limitation and data erasure, these measures do not adequately address the coercive conditions under which consent is often obtained.

C. Lack of transparency

A key limitation of the existing framework is the lack of transparency in data processing. Individuals may be informed about data collection, but they are rarely aware of how their data is analysed, combined or used in decision-making processes. This opacity becomes more concerning in the context of algorithmic governance, where decisions rest on data-driven inferences that remain inaccessible to those affected.[27] This lack of visibility makes it difficult for individuals even to realise that they are being affected.

D. Weak safeguards in the data-usage phase

The privacy framework places greater emphasis on data collection than on data use. Once collected, data is often shared across departments, repurposed or used for secondary purposes.

This phenomenon, commonly described as function creep, allows the expansion of data use beyond its original intent without adequate safeguards. In public data systems, such practices are often embedded within institutional processes, with limited oversight of retention, anonymisation or internal sharing.

E. Democratic risks: chilling effect and bias

The expansion of state surveillance raises broader concerns for democratic values. Continuous monitoring can alter individual behaviour, producing a chilling effect on freedom of expression and participation.[28]

At the same time, data-driven systems risk reinforcing existing biases, particularly when decisions are based on historical datasets. These dynamics affect not only individuals but also

[26] *Central Inland Water Transport Corp. Ltd. v. Brojo Nath Ganguly*, AIR 1986 SC 1571 (India).
[27] PHILIP E. AGRE & MARC ROTENBERG, TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (MIT Press 2001).
[28] Navmi Joshi, *supra* note 22.

 [ISSN 2581-5369]

communities, raising concerns about fairness, equality and accountability within democratic governance. Over time, this can reshape how people participate in public life.

V. Towards a framework beyond privacy: recommendations and conclusion

A. The need to move beyond privacy

The recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* marked a transformative moment in Indian constitutional jurisprudence. However, in the context of contemporary data governance, a purely privacy-centric framework is no longer sufficient. In practice, state practices of large-scale data collection and algorithmic processing extend well beyond issues of consent and lawful use. What is important here is that data-driven governance today affects not only informational privacy but also the autonomy, equality and democratic participation of people. As noted by the Srikrishna Committee, the objective of data-protection law must also include ensuring fairness and addressing the imbalance of power between individuals and the entities processing their data.[29] Thus, the regulatory focus must shift from protecting data alone to addressing how data is used to exercise power.

B. Recognition of profiling as harm

A critical step in this transition is recognising profiling as an independent source of harm. Profiling enables the State to evaluate and predict individual behaviour through automated processing, thereby influencing life chances and reinforcing structural inequalities. Article 4(4) of the European Union's General Data Protection Regulation defines profiling as follows:

> 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[30]

Thus, even when data collection is lawful, profiling can produce harms that are indirect, cumulative and difficult to detect.

These harms operate through opaque systems and inductive reasoning, leaving individuals with a limited ability to identify or challenge adverse outcomes. Recognising profiling as harm is therefore essential to developing an effective regulatory framework.

---

[29] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018), https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf.

[30] Regulation (EU) 2016/679, of the European Parliament and of the Council, art. 4(4), 2016 O.J. (L 119) 1, https://gdpr-info.eu/art-4-gdpr/.

C. Transparency and explainability

Transparency and explainability are central to regulating data-driven decision-making. Existing frameworks often confine transparency to data collection, without addressing how decisions are made using that data. A meaningful approach to transparency must include disclosure of the logic, criteria and consequences of automated decision-making processes. This is essential to enabling legal oversight, democratic accountability and judicial review.

However, as scholars such as Edwards and Veale have pointed out, the "right to explanation" alone may not be sufficient to address the complexities of algorithmic systems.[31] Transparency must therefore be accompanied by broader accountability mechanisms.

D. Comparative insight: the EU GDPR

The European Union's General Data Protection Regulation (GDPR) offers an important comparative model by addressing the risks associated with automated decision-making and profiling. Article 22 of the GDPR provides:

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[32]

Additionally, the GDPR incorporates principles such as data minimisation, purpose limitation and data-protection impact assessments, reflecting a shift towards regulating data use rather than mere collection.

While the Indian context is distinct, these provisions highlight the need for a framework that recognises profiling and automated decision-making as key regulatory concerns.

E. A suggested Indian approach

An effective Indian framework must move in a similar direction while remaining grounded in constitutional principles. First, profiling and algorithmic decision-making should be explicitly recognised as sources of harm. Second, the regulatory focus must shift from consent-based models to principles such as purpose limitation and proportionality. Third, transparency obligations must extend to the logic and consequences of data processing. Finally, stronger institutional mechanisms are needed to ensure accountability in state data practices.

---

[31] Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For*, 16 Duke L. & Tech. Rev. 1, 21 (2017).

[32] Regulation (EU) 2016/679, of the European Parliament and of the Council, art. 22, 2016 O.J. (L 119) 1, https://gdpr-info.eu/art-22-gdpr/.

 [ISSN 2581-5369]

The *Puttaswamy* judgment provides a constitutional foundation for such an approach. Building on it, India must move towards a model that regulates not only the collection of data but also the power exercised through it.

F. Conclusion

The recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* marked a significant constitutional shift. However, the existing framework remains limited to addressing direct and individual intrusions, and fails to capture contemporary state practices of data aggregation, profiling and automated decision-making. This paper has shown that surveillance has evolved from data collection to behavioural prediction. Systems such as Aadhaar-linked infrastructures and predictive policing demonstrate how individuals are increasingly subjected to classification and decision-making processes that operate beyond their awareness. The resulting harms are systemic and structural, and therefore fall outside the scope of traditional privacy protections.

In this context, the Digital Personal Data Protection Act, 2023 falls short, as its reliance on consent and procedural safeguards does not address profiling and algorithmic governance. There is, therefore, a need to recognise profiling as an independent source of harm and to regulate data use rather than mere collection. A reoriented framework grounded in transparency, accountability and the constitutional values of dignity and equality is essential. Ultimately, regulating data-driven power, rather than merely protecting data, is crucial to preserving democratic governance in the digital age.

*****

 [ISSN 2581-5369]