Page: 150-167 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.155

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)
To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript Click here

PRIVACY, SURVEILLANCE AND DATA PROTECTION IN THE DIGITAL PUBLIC SPHERE

Arun Jaijeev[1] & Chilakala Aswini[2]

I. ABSTRACT

The enactment of India's Digital Personal Data Protection Act, 2023 arrives at a critical juncture following the Supreme Court's historic affirmation in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). Justice K.S. Puttaswamy was a retired judge of the Karnataka High Court, and the judgment recognised privacy as an intrinsic facet of the constitutional right to life and liberty. This paper undertakes a critical examination of whether the statutory framework governing data protection effectively upholds privacy entitlements against state-initiated surveillance operations within India's evolving digital ecosystem. Employing a doctrinal research methodology, the study scrutinises two particularly contentious features of the legislation: Section 36, which confers upon the government broad authority to compel data fiduciaries and intermediaries to disclose information, and the graduated exemption regime under Section 17, which largely absolves national security apparatuses from compliance with core statutory obligations. The analysis demonstrates that these provisions encounter substantial difficulties when subjected to the four-pronged proportionality test articulated in Puttaswamy. Specifically, the legislative scheme lacks robust procedural checks such as pre-authorisation by judicial authorities, fails to establish that sweeping data access represents the least restrictive means available, and extends beyond recognised legitimate state interests to encompass routine administrative functions. The absence of independent oversight institutions, combined with gag provisions that prevent individuals from discovering when the state has accessed their personal information, effectively nullifies the right to informational self-determination and the right to erasure. The paper additionally considers real-world manifestations of these vulnerabilities, including the Pegasus spyware episode and the

[1] BBA LL. B, 6th Semester, Student at Christ Academy Institute of Law, Hullahalli, Begur Koppa Road, Bengaluru, Karnataka (India). Email:arunjaijeev@gmail.com
[2] BBA LL. B, 6th Semester, Student at Christ Academy Institute of Law, Hullahalli, Begur Koppa Road, Bengaluru, Karnataka (India). Email: chilakalaaswini123@gmail.com

© 2026. LawFoyer International Journal of Doctrinal Legal Research (ISSN: 2583-7753)

Sanchar Saathi mandate controversy, before offering reform recommendations drawn from comparative legal frameworks in the European Union and United States

II. KEYWORDS

Informational Self-Determination, State Monitoring, Proportionality Analysis, Constitutional Compliance, Digital Liberty.

III. INTRODUCTION

The rapid expansion of digital infrastructure in India, reflected in the exponential growth of internet penetration and platform-based communication, has significantly reshaped how individuals engage in public discourse and governance.[3] This transformation has sharpened a constitutional tension between two competing imperatives: the state's assertion of enhanced surveillance powers in the name of national security, and the individual's right to privacy, which remains integral to democratic participation.[4] This tension invites closer scrutiny of the permissible limits of state authority, the evolving meaning of liberty under constitutional law, and the normative framework governing digital rights in India.[5]

The recognition of privacy as a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1 constitutes a pivotal development in Indian constitutional jurisprudence.[6] The nine-judge bench unequivocally affirmed that privacy is intrinsic to the right to life and personal liberty under Article 21.[7] Significantly, the Court formulated a four-part test to evaluate state intrusion into privacy: legality, legitimate state aim, proportionality, and the presence of procedural safeguards.[8] This framework has since become the constitutional benchmark for assessing surveillance-related measures.

[3] Internet & Mobile Ass'n of India, *Digital in India Report 2023*.
[4] Gautam Bhatia, *Privacy in the Age of the Internet*, 4 NUJS L. Rev. 127 (2011).
[5] Julie E. Cohen, *Between Truth and Power* (2019).
[6] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[7] Id. at ¶ 297.
[8] Id. at ¶¶ 180–181.

Notwithstanding this doctrinal clarity, the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) has generated sustained scholarly and policy debate regarding its compatibility with these constitutional standards.[9] Analyses of the Act, particularly in light of the Justice B.N. Srikrishna Committee Report (2018), suggest a departure from a rights-centric model toward one that expands executive discretion in accessing personal data.[10] The breadth of exemptions and the absence of robust oversight mechanisms have raised concerns about the emergence of a surveillance framework insufficiently constrained by constitutional safeguards.[11]

A. Research Objectives

The present study seeks to critically evaluate the constitutional and statutory framework governing privacy, surveillance, and data protection in India's digital public sphere. Specifically, the research aims to:

1. Examine the constitutional foundations of the right to privacy in India, particularly following Justice K.S. Puttaswamy (Retd.) v. Union of India.
2. Analyse the provisions of the Digital Personal Data Protection Act 2023 that enable state access to personal data.
3. Assess the compatibility of these provisions with the proportionality standard and procedural safeguards mandated under constitutional jurisprudence.
4. Evaluate the implications of surveillance practices on democratic freedoms, including freedom of expression and press autonomy.
5. Propose reforms to strengthen accountability, oversight, and constitutional compliance within India's data protection framework.

B. Research Questions

[9] Apar Gupta & Udbhav Tiwari, *The DPDP Act: A Critique*, Internet Freedom Found. (2023).
[10] Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy* (2018).
[11] Anupam Chander, *Data Protection in India*, 8 Nat'l L. Sch. Rev. 45 (2023).

1. To what extent does the Digital Personal Data Protection Act, 2023 conform to the constitutional standards established in Justice K.S. Puttaswamy (Retd.) v. Union of India?
2. Whether the surveillance-related powers granted under the DPDP Act satisfy the requirements of legality, necessity, proportionality, and procedural safeguards?
3. How do broad governmental exemptions and data access provisions affect informational privacy and democratic freedoms in the digital public sphere?
4. What lessons can India derive from comparative data protection and surveillance frameworks in jurisdictions such as the European Union and the United States?
5. What legal and institutional reforms are necessary to ensure a constitutionally compliant balance between national security and privacy rights?

C. Research Methodology

This study adopts a doctrinal research methodology based upon constitutional interpretation, statutory analysis, and judicial precedent. The research critically examines the Digital Personal Data Protection Act, 2023 in light of the constitutional principles articulated in Justice K.S. Puttaswamy (Retd.) v. Union of India. The study further incorporates comparative analysis of international data protection and surveillance frameworks, particularly those operating within the European Union and the United States, alongside relevant academic and policy-oriented scholarship to evaluate the adequacy of existing safeguards and propose constitutional reforms.

IV. THE CONSTITUTIONAL FOUNDATIONS OF PRIVACY

A. The Trajectory of Privacy Jurisprudence in India

The evolution of privacy as a constitutional right in India has been gradual and marked by doctrinal shifts. In *Kharak Singh v. State of Uttar Pradesh* AIR 1963 SC 1295, the Supreme Court declined to explicitly recognise a right to privacy, although it invalidated certain

intrusive police practices as inconsistent with personal liberty.[12] This early hesitation resulted in a fragmented approach to privacy protection.[13]

Subsequently, in *R. Rajagopal v. State of Tamil Nadu* (1994) 6 SCC 632, the Court acknowledged aspects of privacy within Article 21, particularly in the context of protection against unauthorised publication of personal information.[14] However, these developments remained limited until the authoritative pronouncement in *Puttaswamy*, which conclusively established privacy as a fundamental right.[15]

B. The Puttaswamy Framework

The *Puttaswamy* judgment conceptualised privacy as encompassing bodily autonomy, decisional freedom, and informational self-determination.[16] The recognition of informational privacy is especially significant in the digital era, where personal data is continuously generated, processed, and stored by both state and non-state actors.[17]

The Court's four-pronged test requires that any restriction on privacy must satisfy:

1. Legality: Existence of a valid statutory basis
2. Legitimate Aim: Pursuit of a constitutionally permissible objective
3. Proportionality: Rational connection and necessity of the measure, with minimal intrusion
4. Procedural Safeguards: Institutional mechanisms to prevent abuse

Importantly, the Court emphasised that proportionality entails substantive judicial scrutiny[18], aligning Indian jurisprudence with comparative constitutional standards, including European data protection principles.[19]

---

[12] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
[13] M.P. Jain, *Indian Constitutional Law* (8th ed. 2018).
[14] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
[15] *Puttaswamy*, supra note 4.
[16] Id.
[17] Paul M. Schwartz, *Information Privacy in the Digital Age*, 94 Mich. L. Rev. 1463 (1996).
[18] *Puttaswamy*, supra note 4.
[19] Id.

C. Privacy as a Precondition for Democratic Participation

Privacy functions not only as an individual right but also as a structural condition for democratic governance.[20] Judicial observations in *Puttaswamy* underscore that autonomy in thought and expression depend upon freedom from unwarranted surveillance.[21] Empirical and theoretical scholarship on surveillance further indicates that perceived monitoring can lead to behavioural modification[22] and self-censorship, thereby constraining open discourse.

In the contemporary digital environment, where communication is mediated by private platforms and generates persistent data trails, the risks associated with surveillance are amplified. This necessitates a regulatory framework that addresses both direct state surveillance and indirect access facilitated through private intermediaries.

D. Surveillance And the Digital Public Sphere

Prior to the enactment of the Digital Personal Data Protection Act, 2023, the principal statutory framework governing state surveillance in India was contained in Section 5(2) of the Indian Telegraph Act, 1885 and Section 69 of the Information Technology Act, 2000. Section 5(2) authorises interception of communications on grounds such as public emergency and public safety, while Section 69 empowers the Central and State Governments to direct interception, monitoring, or decryption of electronic information in the interests of sovereignty, integrity, defence, security of the State, public order, or prevention of offences. These provisions collectively constitute the operational architecture for lawful interception and digital surveillance in India.

In People's Union for Civil Liberties v. Union of India, the Supreme Court recognised that telephone tapping constitutes a serious infringement of privacy and laid down procedural safeguards governing interception under Section 5(2) of the Telegraph Act. The Court mandated that interception orders must ordinarily be authorized by the Union

[20] Neil Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013).
[21] *Puttaswamy*, supra note 4.
[22] Id.; Richards, supra note 20.

or State Home Secretary, be limited in duration, and remain subject to periodic review by a Review Committee. The judgment established that surveillance powers cannot operate in an unregulated manner and must remain constrained by procedural accountability mechanisms.[23]

The absence of procedural safeguards is perhaps the most glaring deficiency. The *Puttaswamy* Court emphasized that procedural safeguards are not optional but essential components of a valid privacy-limiting law. This deficiency becomes particularly significant when contrasted with the safeguards recognised in People's Union for Civil Liberties v. Union of India, where the Supreme Court required Home Secretary authorization, periodic review, and procedural accountability in cases of telephone interception under the Telegraph Act. In comparison, the DPDP Act's framework for governmental access to data lacks comparable institutional checks and independent oversight mechanisms.

V. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: PROMISE AND PERIL

A. Legislative Context and Objectives

The DPDP Act, 2023 represents a significant legislative milestone in India's data governance framework.[24] However, a comparative reading with the Justice B.N. Srikrishna Committee Report (2018) reveals a shift away from the Committee's emphasis on accountability and user rights.[25] Notably, recommendations concerning judicial oversight and limitations on state access to data have not been fully incorporated into the final legislation.

1. Section 36: The Surveillance Provision

[23] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[24] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[25] Srikrishna Committee Report, supra note 8.

Section 36 empowers the Central Government to require "any information" from data fiduciaries, intermediaries[26], and the Data Protection Board. The absence of definitional limits on this power raises concerns regarding its potential overreach[27] and susceptibility to expansive interpretation.

The Digital Personal Data Protection Rules, 2025 (notified on 13 November 2025) extend the scope of such requests through Rule 23 and the Seventh Schedule, which permit information requests for purposes including national security, compliance with legal obligations, and specified regulatory functions.[28] This formulation presents three key constitutional concerns:

- **Overbreadth:** The reference to "any law" lacks specificity, enabling data access beyond narrowly defined objectives.
- **Absence of Necessity Requirement:** There is no obligation to demonstrate that less intrusive alternatives are inadequate.
- **Limited Transparency:** The absence of notification mechanisms restricts the ability of individuals to challenge data access.[29]

2. Tiered Exemptions and the Right to Be Forgotten

Section 17(2)(a) provides broad exemptions for government agencies[30] on grounds of national security and public order. These exemptions extend to core obligations such as data minimisation, purpose limitation, and user rights.[31]

From a constitutional perspective, such blanket exemptions are difficult to reconcile with the proportionality standard, which requires narrowly tailored restrictions. Furthermore,

[26] DPDP Act, § 36.
[27] Gupta & Tiwari, supra note 7.
[28] The Digital Personal Data Protection Rules, 2025 (India).
[29] Chander, supra note 9.
[30] DPDP Act, § 17(2)(a).
[31] Bhatia, supra note 2.

exemptions relating to investigative functions limit the applicability of notice and erasure rights, thereby undermining the right to be forgotten as recognised in *Puttaswamy.*[32]

VI. SURVEILLANCE AND THE DIGITAL PUBLIC SPHERE

1. **The Pegasus Revelations and Systemic Vulnerabilities:** The Pegasus spyware disclosures in 2021, supported by forensic analyses conducted by Amnesty International's Security Lab, highlighted potential instances of unauthorised digital surveillance tools[33] targeting journalists and public figures. The Supreme Court's subsequent constitution of a technical committee underscores the seriousness of these concerns.[34] While definitive attribution remains contested, the episode revealed structural vulnerabilities in India's surveillance framework, particularly the absence of independent oversight and clear accountability mechanisms.
2. **The Sanchar Saathi Controversy:** The proposal to mandate pre-installation of the Sanchar Saathi application raised important constitutional questions regarding proportionality and user autonomy. Critics argued that compulsory installation would constitute a disproportionate intrusion into privacy, especially in the absence of informed consent or adequate safeguards. The eventual withdrawal of the proposal illustrates the role of public scrutiny in constraining executive overreach.
3. **Implications for Press Freedom and Democratic Expression:** The implications of surveillance for press freedom are significant. Journalists depend on secure communication channels to protect sources and conduct investigations.[35] The possibility of state access to such communications may deter investigative reporting and weaken democratic accountability. Judicial observations have

[32] *Puttaswamy*, supra note 4.
[33] Amnesty Int'l, *Pegasus Project Report* (2021).
[34] *Manohar Lal Sharma v. Union of India*, AIR 2021 SC 5396.
[35] Int'l Fed'n of Journalists, *India Press Freedom Report* (2023).

acknowledged that surveillance measures can produce a chilling effect, thereby indirectly restricting freedom of expression.

VII. COMPARATIVE PERSPECTIVES

A. The European Union Framework

The European Union's data protection framework, centred on the General Data Protection Regulation (GDPR) and supplemented by the Law Enforcement Directive, provides a useful comparative reference point[36]. The GDPR establishes a comprehensive rights-based framework that applies to both public and private sector data processing, with limited exceptions for national security activities.[37]

Crucially, the GDPR's exceptions for law enforcement and national security are subject to the requirements of necessity and proportionality and are accompanied by independent supervisory authorities with powers to investigate and sanction violations. The Court of Justice of the European Union has consistently held that indiscriminate data retention is incompatible with the Charter of Fundamental Rights, requiring that surveillance measures be targeted and subject to prior judicial authorization.[38]

The United Kingdom's Data Protection Act 2018 (DPA), which implements the GDPR's principles while providing for national security exemptions, offers a more nuanced model. Under the DPA, intelligence agencies seeking exemption from data protection provisions must obtain a National Security Certificate from a minister of the crown, and the grant of such certificate is subject to appeal before a tribunal.[39] Moreover, even exempted agencies must still abide by principles of security and lawfulness, ensuring that the exemption is not a complete blank cheque.

---

[36] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1; Directive (EU) 2016/680, 2016 O.J. (L 119) 89.
[37] GDPR, supra note 35, arts. 5, 6, 23.
[38] Cases C-203/15 and C-698/15, Tele2 Sverige AB v. post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, ECLI:EU:C:2016:970 (Grand Chamber, 21 December 2016); Charter of Fundamental Rights of the European Union arts. 7, 8, 52, 2012 O.J. (C 326) 391.
[39] Data Protection Act 2018, c. 12 (UK) §§ 26–28.

The contrast with India's DPDP Act is striking. Where the DPA requires agencies to declare the extent and purpose of data required, the DPDP Act contains no such requirement. Where the DPA allows for appeal of national security certifications, the DPDP Act provides no mechanism for challenging government notifications under Section 17(2)(a). Where the DPA requires notification to data subjects of data processing activities, the DPDP Act exempts government agencies from this requirement entirely.[40]

B. The United States Framework

The United States framework, while different in structure, similarly incorporates procedural safeguards that are absent from India's DPDP Act. The Fourth Amendment's requirement that searches and seizures be reasonable has been interpreted to require warrants based on probable cause for most government access to personal data.[41] The Electronic Communications Privacy Act and the Foreign Intelligence Surveillance Act establish statutory frameworks for government surveillance that include judicial authorisation requirements and oversight mechanisms.[42]

The comparison is not to suggest that the US framework is without flaws—indeed, it has been subject to significant criticism, particularly in light of revelations about warrantless surveillance programs. However, the existence of judicial authorisation requirements, even if imperfectly implemented, represents a meaningful constraint on executive power that the DPDP Act lacks.[43]

VIII. ANALYSIS AND EVALUATION

A. The Failure of the Proportionality Standard

[40] Digital Personal Data Protection Act, No. 22 of 2023, §§ 17(2)(a), 36 (India).
[41] U.S. Const. amends. IV; *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[42] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523; Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c.
[43] ACLU, *Reforming the Surveillance State: Section 702 and Beyond* (2021); see also Laura K. Donohue, *The Future of Foreign Intelligence Surveillance*, 62 Am. U. L. Rev. 575 (2013).

Applying the Puttaswamy proportionality framework to the DPDP Act's surveillance provisions reveals fundamental constitutional infirmities.[44] The requirement of legality is satisfied, as the provisions are contained in a statute enacted by Parliament.[45] However, the remaining three requirements are legitimate aim, necessity, and procedural safeguards pose significant difficulties.

With respect to legitimate aims, while national security and crime prevention are unquestionably legitimate state interests, the Act's provisions extend beyond these aims[46]. The Seventh Schedule's reference to "performance of any function under any law" could encompass a vast range of governmental activities, many of which have no connection to security or criminal justice. The absence of limiting language means that the government could invoke Section 36 to demand personal data for routine administrative purposes, without any showing of necessity.[47]

The necessity requirement is even more problematic. Under the Puttaswamy framework, the state must demonstrate that the means employed are the least intrusive available to achieve the legitimate aim. The DPDP Act does not make such showing. It does not explain why less intrusive alternatives such as targeted data requests based on reasonable suspicion, judicial authorization requirements, or data minimization principles would be inadequate. Instead, it authorizes broad, potentially indiscriminate data collection without any threshold requirement.[48]

The absence of procedural safeguards is perhaps the most glaring deficiency. The Puttaswamy Court emphasized that procedural safeguards are not optional but essential components of a valid privacy-limiting law. Yet Section 36 contains no requirement for judicial authorization, no mechanism for affected persons to challenge data requests, no

[44] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶¶ 180–181 (India).
[45] Digital Personal Data Protection Act, No. 22 of 2023, §§ 17(2)(a), 36 (India).
[46] Gautam Bhatia, *The Transformative Constitution and the Limits of State Power*, 9 Nat'l L. Sch. Rev. 45 (2022).
[47] Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy* (2018).
[48] Paul M. Schwartz & Daniel J. Solove, *The PII Problem*, 86 N.Y.U. L. Rev. 1814 (2011).

independent oversight body, no time limits on data retention, and no requirement that the government demonstrate necessity before accessing data.[49]

B. The Surveillance Intermediary Problem

The DPDP Act's provisions requiring data fiduciaries and intermediaries to furnish information to the government raise additional concerns about the role of private entities in the surveillance architecture.[50] Technology companies, including telecom operators and OTT platforms, are increasingly positioned as surveillance intermediaries required to collect and retain data that can subsequently be accessed by government agencies.

This arrangement creates a form of indirect surveillance that avoids many of the constitutional constraints that would apply to direct state collection of information. Where the state itself would be required to demonstrate necessity and obtain judicial authorisation, it can instead compel a private intermediary to collect and retain data, then access that data through administrative demand.

The scale of this phenomenon is substantial. Meta's Government Requests for User Data Report indicates that India is the second-largest source of government data requests globally, accounting for approximately 21 percent of all requests across major technology platforms. This reflects both the scale of digital adoption in India and the intensity of governmental interest in accessing citizen data.[51] Telecom operators and OTT platforms, which process continuous streams of metadata including location data, communication patterns, and behavioural profiles, face particular exposure to government demands for information.

C. The Democratic Deficit

Beyond the specific constitutional violations, the DPDP Act's surveillance provisions reflect a broader democratic deficit in the legislative process. The Justice B.N. Srikrishna Committee's draft Bill had included provisions for judicial authorisation and

[49] Anupam Chander, *Data Protection in India*, 8 Nat'l L. Sch. Rev. 45 (2023).
[50] Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013).
[51] Meta Platforms, Inc., *Government Requests for User Data Report* (2023).

independent oversight, but these were omitted in the final legislation without adequate explanation. The Act was passed without the robust parliamentary debate that a measure affecting fundamental rights would warrant.

The result is a framework that prioritises administrative convenience over constitutional rights, treating governmental discretion as a substitute for procedural safeguards. As one commentator has observed, the DPDP Act seems to treat exemption as the norm and the right as the exceptional position that stands in direct contradiction to the constitutional architecture established by the Supreme Court.

IX. SUGGESTIONS AND RECOMMENDATIONS

1. **Strengthening Judicial Oversight:** The most urgent reform required is the introduction of meaningful judicial oversight for government access to personal data. Drawing on comparative models, the DPDP Act should be amended to require that any request for information under Section 36 be authorized by a judicial officer based on a showing of reasonable suspicion or probable cause, depending on the nature and sensitivity of the data sought.[52] Judicial authorization serves multiple functions: it provides an independent check on executive power, creates a record of surveillance activities that can be reviewed, and ensures that the necessity requirement is meaningfully enforced. The experience of other democracies demonstrates that judicial oversight is compatible with effective law enforcement and national security protection.[53]
2. **Establishing Independent Oversight:** In addition to judicial authorization for individual data requests, the framework should establish an independent oversight body with powers to review government surveillance activities generally. This body would have access to classified information and would be empowered to investigate complaints, conduct audits, and report publicly on compliance with legal requirements. The oversighting body should be

[52] Christopher Kuner et al., *The GDPR: A Commentary* (Oxford Univ. Press 2020).
[53] International Commission of Jurists, *Surveillance and the Right to Privacy in the Digital Age* (2019).

structurally independent of the executive branch, with members appointed through a process that ensures diverse representation and security of tenure. Its reports should be made public, with appropriate redactions for genuinely sensitive information, to enable democratic accountability.

3. **Data Minimization and Retention Limits:** The DPDP Act should incorporate data minimization principles, requiring that government agencies collect only the data that is strictly necessary for the specified purpose and that data be deleted when no longer required. The current framework's absence of meaningful retention limits is inconsistent with the Puttaswamy requirement of proportionality. Legislative amendments should specify maximum retention periods for different categories of data, require periodic review of retained data, and mandate deletion of data that no longer serves a legitimate purpose. Exceptions for ongoing investigations should be narrowly defined and subject to periodic judicial review.
4. **Transparency and Notification:** Individuals whose data has been accessed by the government should have a right to be notified of such access, unless a judicial officer determines that notification would compromise an ongoing investigation. This notification requirement creates accountability by enabling affected people to challenge unlawful access and by creating a deterrent against arbitrary surveillance. The current framework's non-disclosure obligations, which permit the government to restrict disclosure indefinitely, are inconsistent with this principle. Amendments should provide that non-disclosure orders are exceptional, time-limited, and subject to judicial review.
5. **Reforming the Exemption Framework:** The blanket exemption for national security agencies under Section 17(2)(a) should be replaced with a more nuanced framework that balances security needs with constitutional rights. Agencies should be required to demonstrate that specific data processing activities are necessary for legitimate national security purposes, and these determinations should be subject to independent oversight. Even national security agencies

should be required to comply with basic data security standards and should be subject to audit and oversight. The current framework's assumption that national security requires complete exemption from legal constraints is both constitutionally dubious and practically unnecessary, as demonstrated by the experience of other democracies that conduct effective intelligence operations within legal frameworks.

X. CONCLUSION

The DPDP Act, 2023 represents an important step in India's data governance landscape but does not fully satisfy constitutional standards for privacy protection. Its surveillance-related provisions fall short of the proportionality requirements articulated in *Puttaswamy*, particularly in relation to necessity and procedural safeguards.

These shortcomings have broader implications for democratic governance. As digital technologies increasingly mediate public discourse, unchecked surveillance risks undermining both individual autonomy and institutional accountability.

The challenge is not to prioritize privacy over security, but to design a legal framework in which both coexist within constitutional limits. Ensuring that surveillance powers remain subject to meaningful oversight is essential to preserving the democratic character of the digital public sphere.

XI. REFERENCES

A. Statutes and Rules

1. The Constitution of India, 1950.
2. The Indian Telegraph Act, 1885.
3. The Information Technology Act, 2000.
4. The Digital Personal Data Protection Act, 2023.
5. Digital Personal Data Protection Rules, 2025 (Notified on 13 November 2025).

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
7. Data Protection Act 2018 (United Kingdom).
8. Electronic Communications Privacy Act, 1986 (United States).
9. Foreign Intelligence Surveillance Act, 1978 (United States).

B. Cases

1. Indian Cases

- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
- *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
- *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
- *Manohar Lal Sharma v. Union of India*, W.P. (Crl.) No. 314 of 2021, AIR 2021 SC 5396.

2. European Union Cases

- *Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v. post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, ECLI:EU:C:C:2016:970 (Grand Chamber, 21 December 2016).

C. Committee Reports and Government Documents

1. Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).
2. Government of India, Ministry of Electronics and Information Technology, *Digital Personal Data Protection Rules, 2025 Notification* (2025).
3. Meta Platforms, Inc., *Government Requests for User Data Report* (2023).
4. Internet & Mobile Association of India, *Digital India Report* (2023).

D. Journal Articles, Books and Scholarly Works

1. Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins India 2019).
2. Upendra Baxi, "Human Rights in a Posthuman World: Critical Essays" (Oxford University Press 2007).
3. Daniel J. Solove, "A Taxonomy of Privacy," 154 University of Pennsylvania Law Review 477 (2006).
4. Neil M. Richards, "The Dangers of Surveillance," 126 Harvard Law Review 1934 (2013).

.