

RIGHT TO PRIVACY IN THE DIGITAL ERA: CONSTITUTIONAL CONTOURS AND STATUTORY SAFEGUARDS IN INDIA

DR. BHANUPRIYA KUMAWAT¹ & DR. PHALGUN PUROHIT²

ABSTRACT

The advent of the digital age has fundamentally recalibrated the normative and doctrinal understanding of privacy. This article examines the evolution of the right to privacy in India from a judicially developed concept to an expressly recognised fundamental right under Article 21 of the Constitution of India³. It analyses the landmark decision in Justice K.S. Puttaswamy (Retd.) v. Union of India⁴ and its three-fold test of legality, necessity, and proportionality. The article further critically evaluates the Digital Personal Data Protection Act, 2023, assessing its adequacy in addressing contemporary challenges posed by state surveillance, data capitalism, artificial intelligence, and cross-border data flows. A comparative analysis with the European Union's General Data Protection Regulation and other global frameworks is undertaken to identify legislative gaps. The authors argue that while India has established a constitutional and statutory foundation for digital privacy, the expansive exemptions for the State, absence of surveillance reform, and limited data principal rights necessitate further jurisprudential and legislative intervention to align with international standards of informational self-determination.

Keywords: Right to Privacy; Article 21; Puttaswamy; Digital Personal Data Protection Act 2023; Informational Privacy; Proportionality

I. INTRODUCTION

Privacy as a legal concept has traversed a complex trajectory from its early articulation as the “right to be let alone”⁵ to its contemporary recognition as a multifaceted right encompassing spatial, decisional, and informational autonomy. The digital transformation of society, marked by pervasive datafication, algorithmic governance,

¹ Dr. Bhanupriya Kumawat, Assistant Professor of Law, Pacific Law School, Pacific University, Udaipur

² Dr. Phalgun Purohit, Assistant Professor of Law, Pacific Law School, Pacific University, Udaipur

³ 1. INDIA CONST. art. 21.

⁴ (2017) 10 SCC 1

and platform capitalism, has rendered traditional conceptions of privacy inadequate. In India, the constitutional silence on privacy until 2017 necessitated judicial creativity to locate the right within the interstices of Part III of the Constitution. The unanimous nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India fundamentally altered India's constitutional landscape by declaring privacy a fundamental right intrinsic to life and liberty under Article 21.

This article seeks to undertake a doctrinal analysis of the right to privacy in the digital era. Part II traces the constitutional evolution of privacy jurisprudence. Part III examines the legislative response through the Digital Personal Data Protection Act, 2023.⁶ Part IV analyses judicial application post-Puttaswamy. Part V identifies contemporary challenges in the digital ecosystem. Part VI provides a comparative perspective, and Part VII suggests reforms. The central thesis posits that while India has achieved constitutional recognition and statutory codification of digital privacy, the framework remains State-centric and inadequately addresses the asymmetry of power between individuals and data-processing entities.

II. CONSTITUTIONAL EVOLUTION: FROM DENIAL TO RECOGNITION

The Constitution of India, as adopted in 1950, did not enumerate privacy as a fundamental right. Early jurisprudence reflected judicial reticence. In *M.P. Sharma v. Satish Chandra*⁷, an eight-judge bench held that the power of search and seizure was not subject to a fundamental right of privacy. This position was affirmed in *Kharak Singh v. State of U.P.*, where the majority declined to recognize privacy as a guaranteed right, though Justice Subba Rao's dissent characterized it as an essential facet of personal liberty under Article 21.

The doctrinal inflection point arrived in Justice K.S. Puttaswamy (Retd.) v. Union of India. The Supreme Court overruled *M.P. Sharma* and *Kharak Singh*⁸ to the extent

3. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

5. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

⁷ AIR 1954 SC 300.

⁸ AIR 1963 SC 1295

they held that privacy was not constitutionally protected⁹. The Court identified three elements of privacy: (i) spatial privacy denoting the sanctity of the physical body and spaces; (ii) decisional privacy concerning intimate personal choices; and (iii) informational privacy relating to control over personal data.¹⁰ The judgment formulated a three-fold requirement for permissible State intrusion: (i) legality, which postulates the existence of law; (ii) legitimate State aim; and (iii) proportionality, ensuring a rational nexus between the objects and the means adopted to achieve them.¹¹ The Court further situated privacy within the Golden Triangle of Articles 14, 19, and 21, holding that it was not an elitist construct but a postulate of human dignity. Justice Chandrachud observed that privacy is the constitutional core of human dignity. Justice Nariman traced the right to the preambular values of liberty and fraternity, while Justice Kaul emphasized its connection to the right to self-determination.

III. LEGISLATIVE FRAMEWORK: THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Puttaswamy judgment¹² catalysed legislative action, culminating in the Digital Personal Data Protection Act, 2023, which received Presidential assent on 11 August 2023. The Act applies to digital personal data¹³ processed within India and to processing outside India if in connection with offering goods or services to Data Principals within India.

A. CORE PRINCIPLES AND OBLIGATIONS

Section 4 mandates that personal data may be processed only for a lawful purpose with consent or for certain legitimate uses.¹⁴ Section 6 requires consent to be free, specific, informed, unconditional, and unambiguous through clear affirmative action. Data Fiduciaries must provide an itemised notice specifying the personal data and purpose.

Sections 8 to 10 impose obligations on Data Fiduciaries to ensure compliance, implement reasonable security safeguards, ensure accuracy and completeness of data, and erase personal data upon withdrawal of consent or upon the purpose being

⁹ (2017) 10 SCC 1.

¹⁰ Id. at para 122.

¹¹ Id. at para 131.

¹² at 1326 (Subba Rao, J., dissenting).

¹³ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

¹⁴ The Digital Personal Data Protection Act, 2023, 4.

fulfilled. Significant Data Fiduciaries are subject to additional obligations, including data protection impact assessments and appointment of Data Protection Officers.

B. RIGHTS OF DATA PRINCIPALS

Chapter III confers enforceable rights: right to access information about processing, right to correction and erasure, right of grievance redressal¹⁵, and right to nominate. Notably, the Act does not recognise the right to data portability or the right to be forgotten, which exist under the EU GDPR.¹⁶

C. EXEMPTIONS AND STATE POWER

Section 17¹⁷ provides broad exemptions for the State and its instrumentalities for purposes including sovereignty, security, public order, and prevention of offences. The Central Government may, by notification, exempt any Data Fiduciary or class thereof. Such exemptions are subject only to the procedure established by law and not to independent judicial oversight, raising proportionality concerns under the Puttaswamy test.

D. ENFORCEMENT MECHANISM

Section 18 establishes the Data Protection Board of India as an adjudicatory body with powers to impose penalties up to two hundred and fifty crore¹⁸ rupees. Appeals lie to the Telecom Disputes Settlement and Appellate Tribunal and thereafter to the Supreme Court. The Board lacks the structural independence of a statutory regulator, as its members are appointed by the Central Government.

IV. POST-PUTTASWAMY JUDICIAL APPLICATION

The Supreme Court has applied Puttaswamy across domains. In *Anuradha Bhasin v. Union of India*,¹⁹ the Court held that indefinite internet shutdowns violate Articles 19 and 21, recognising that access to the internet is integral to freedom of speech and trade. In *Internet and Mobile Association of India v. Reserve Bank of India*, the Court

¹⁵ Id. ch. III.

¹⁶ GDPR, *supra* note 4.

¹⁷ The Digital Personal Data Protection Act, 2023, 17.

¹⁸ Id. 18.

¹⁹ (2020) 3 SCC 637.

struck down the RBI's circular prohibiting banking services to virtual currency exchanges, applying the proportionality standard.

In the Aadhaar litigation²⁰, Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J), the Court upheld the Aadhaar Act but invalidated mandatory linking of Aadhaar with bank accounts and mobile numbers, holding that such linkage failed the proportionality test. The Court read down Section 57 to prohibit private entities from demanding Aadhaar.

V. CONTEMPORARY CHALLENGES IN THE DIGITAL ECOSYSTEM

A. STATE SURVEILLANCE

India lacks a comprehensive surveillance law. Interception is governed by Section 69 of the Information Technology Act, 2000²¹ and the Indian Telegraph Act, 1885²², which permit interception without prior judicial authorisation. The Central Monitoring System, NATGRID, and deployment of Facial Recognition Technology operate without statutory basis or oversight. The Pegasus spyware investigation revealed extra-legal surveillance of journalists, activists, and constitutional functionaries.

B. PRIVATE SECTOR DATA EXPLOITATION

The digital economy operates on surveillance capitalism, characterised by behavioural advertising, dark patterns, and consent fatigue. Data Fiduciaries routinely employ bundled consent and opaque privacy policies, vitiating the free and informed elements of consent under Section 6²³ of the DPDP Act. ²⁴Algorithmic profiling enables price discrimination and exclusion without transparency.

²⁰ (2020) 10 SCC 274 (2019) 1 SCC 1.

²¹ The Information Technology Act, 2000, 69, No. 21, Acts of Parliament, 2000 (India).

²² The Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).

²³ Id. 16. Id. 9.

²⁴ The Digital Personal Data Protection Act, 2023, 6.
Id. 7(a).

C. ARTIFICIAL INTELLIGENCE AND AUTOMATED DECISION-MAKING

Automated processing under Section 7(a) of the DPDP Act permits processing for employment purposes without consent. AI-driven credit scoring, predictive policing, and social media content moderation lack algorithmic accountability mechanisms. The Act contains no provision for explanation of automated decisions or human review, unlike Article 22 of the GDPR.

D. CROSS-BORDER DATA FLOWS

Section 16 permits transfer of personal data to countries notified by the Central Government, departing from the adequacy framework under GDPR. This approach prioritises geopolitical considerations over data protection standards and risks undermining Data Principal rights upon transfer to jurisdictions with weak safeguards.

E. PROTECTION OF CHILDREN

Section 9 prohibits tracking, behavioural monitoring, and targeted advertising directed at children, and mandates verifiable parental consent. However, the Act delegates age-verification mechanisms to rules, and the absence of a statutory definition of detrimental effect creates interpretational ambiguity.

VI. COMPARATIVE PERSPECTIVE

The EU General Data Protection Regulation, 2016 ²⁵establishes a high-watermark for data protection, emphasising lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and accountability. It recognises the right to erasure, right to data portability, and right to object to automated processing. The California Consumer Privacy Act, 2018 ²⁶grants rights to know, delete, and opt-out of sale. Brazil's Lei Geral de Protecao de Dados ²⁷adopts GDPR principles with adaptation for the Global South.

²⁵ GDPR, supra note 4.

²⁶ Cal. Civ. Code 1798.100 et seq. (2018).

²⁷ Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.08.2018 (Brazil).

India's DPDP Act converges with these frameworks on consent and security but diverges on State exemptions, absence of data portability, and limited institutional independence of the enforcement body. The legislative choice reflects a policy preference for State sovereignty and ease of doing business over maximalist individual autonomy.

VII. THE PROPORTIONALITY STANDARD AND BALANCING OF INTERESTS

The right to privacy is not absolute. Puttaswamy adopted the European doctrine of proportionality, as elaborated in *Modern Dental College v. State of M.P.*²⁸. The four-pronged test requires: (i) legitimate goal; (ii) suitable means; (iii) necessity, denoting the least restrictive measure; and (iv) balancing or proportionality *stricto sensu*.

Applying this to digital governance, blanket data retention under Section 67C of the IT Act, mandatory facial recognition in public spaces, and unfettered exemptions under Section 17 of the DPDP Act merit strict scrutiny. The Supreme Court in *Ritesh Sinha v. State of U.P.*²⁹, permitted collection of voice samples, emphasising that privacy must be balanced against compelling State interests. However, such balancing cannot become a judicial imprimatur for surveillance overreach.

VIII. RECOMMENDATIONS AND WAY FORWARD

First, India must enact a comprehensive surveillance reform legislation instituting prior judicial authorisation, necessity, and time limits for interception, as recommended by the B.N. Srikrishna Committee.³⁰

Second, the Data Protection Board must be conferred with structural independence, security of tenure, and financial autonomy to ensure impartial adjudication.

Third, the DPDP Act should be amended to incorporate the right to data portability, right to explanation of automated decisions, and a qualified right to be forgotten, subject to freedom of expression and public interest.

²⁸ (2016) 7 SCC 353.

²⁹ (2012) 6 SCC 571.

³⁰ B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Report of the Committee of Experts on Data Protection (2018).

Fourth, algorithmic accountability must be mandated through algorithmic impact assessments and audit requirements for Significant Data Fiduciaries deploying AI systems.

Fifth, public awareness and digital literacy programmes are essential to enable Data

IX. CONCLUSION

The digital era has reconfigured the relationship between the individual, the State, and the market. Puttaswamy elevated privacy from a common law derivative to a fundamental right, and the DPDP Act, 2023 provides the statutory architecture for data governance. Nevertheless, the framework remains incomplete. Expansive State exemptions, absence of surveillance safeguards, and weak institutional design dilute the promise of informational self-determination.

Privacy in the twenty-first century is not merely a negative right against intrusion but a positive right to control one's informational persona. As Justice Kaul cautioned, the right to privacy is inextricably bound up with all exercises of human liberty.³¹ The realisation of constitutional privacy in cyberspace requires constant vigilance, legislative refinement, and judicial innovation to ensure that technological advancement does not subvert human dignity. The Indian legal system stands at a critical juncture where it must choose between a surveillance State and a digital democracy. The choice will determine whether the right to privacy remains a constitutional promise or becomes a lived reality.

³¹ (2017) 10 SCC 1 at para 542 (Kaul, J.)