HUMAN RIGHTS AND DIGITAL PRIVACY IN INDIA: CONSTITUTIONAL CHALLENGES AND JUDICIAL RESPONSES

Dr. Suruchi, Assistant Professor, Patna Law College, Patna University, Patna

ABSTRACT

The expansion of digital technologies and state-supported information architectures has transformed the landscape of civil liberties in India. E-governance platforms, biometric identification systems, data-driven welfare schemes, artificial intelligence, and widespread use of social media have collectively led to the unprecedented collection and processing of personal data. In this environment, digital privacy has emerged as a core component of human rights, intimately connected with dignity, autonomy and personal freedom. The recognition of the right to privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India marked a turning point in Indian constitutional law. The decision clearly affirmed that informational privacy control over personal data is protected under Article 21 of the Constitution. However, the legal and institutional response to technological change remains incomplete and uneven.

This article examines the evolving relationship between human rights and digital privacy in India by analysing constitutional provisions, judicial decisions, legislative developments and comparative international standards. It considers the impact of the Digital Personal Data Protection Act, 2023, surveillance practices, and the growing influence of private digital platforms on individual autonomy. While the Indian judiciary has articulated important principles relating to proportionality, necessity and legality, practical concerns persist regarding weak oversight of surveillance, broad executive discretion, opaque data-sharing arrangements and limited public awareness.

The paper adopts a doctrinal and analytical approach, mapping key cases, statutes and policy debates. It also draws brief comparisons with models like the European Union's GDPR and international human rights instruments to identify possible directions for reform. The central argument advanced is that safeguarding digital privacy is not an obstacle to governance or security but an essential condition for a rule-of-law based digital state. The article concludes that India must strengthen institutional safeguards, clarify accountability structures and promote digital literacy to ensure that

technological innovation advances, rather than undermines, the protection of human rights.

Keywords: Human Rights; Digital Privacy; Article 21; Surveillance; Data Protection; Puttaswamy; Constitutional Law.

INTRODUCTION

The progressive digitalisation of governance and everyday life has brought citizens into constant interaction with electronic systems. From identity verification and banking to education, healthcare and communication, most activities leave behind a trail of data. This transformation has created new opportunities for service delivery and transparency, but it has also exposed individuals to risks of profiling, misuse of information and pervasive surveillance.[1]

In a constitutional democracy such as India, technology cannot be allowed to dilute the guarantees of liberty, equality and dignity.[2] The central concern of this article is to examine how digital privacy fits within the broader framework of human rights, and how Indian constitutional law has attempted to respond to the challenges posed by contemporary technologies.[3]

HUMAN RIGHTS AND DIGITAL PRIVACY: CONCEPTUAL FRAMEWORK

Human rights are inherent, inalienable and universal claims that flow from the dignity of the human person.[4] Traditionally, discussions on privacy focused on protection from physical or spatial intrusions. However, in the digital era, privacy increasingly concerns:

- control over personal information;
- protection against unauthorised data collection and surveillance;[5]
- autonomy in digital decision-making; and
- the right to develop one's personality without constant monitoring.

[1] UN Human Rights Committee, *General Comment No. 16: Right to Privacy (Art. 17)* (1988).
[2] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[3] Alan F. Westin, *Privacy and Freedom* 7 (1967).
[4] *Universal Declaration of Human Rights*, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).
[5] UN Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy)* (1988).

Digital privacy may be described as the right of an individual to decide when, how and to what extent personal data is communicated to others, including the State and private entities.[6] It links closely with other rights such as freedom of expression, association, thought and movement. A citizen who is constantly watched or profiled may hesitate to speak, dissent or participate fully in public life. Therefore, digital privacy is not a luxury; it is integral to meaningful enjoyment of basic freedoms.[7]

CONSTITUTIONAL FOUNDATIONS OF DIGITAL PRIVACY IN INDIA

The Constitution of India does not explicitly mention the term "privacy". For a long time, judicial opinion was divided on whether a general right to privacy could be read into Article 21, which protects life and personal liberty. Earlier decisions showed some hesitation, but with time, a more rights-oriented approach evolved.[8]

The matter was conclusively settled in Justice K.S. Puttaswamy (Retd.) v. Union of India, where a nine-judge Bench of the Supreme Court unanimously held that the right to privacy is a fundamental right under Part III.[9] The Court recognised that privacy has multiple facets spatial, decisional and informational and that it is closely tied to dignity and autonomy.[10]

The judgment laid down three essential conditions for any State intrusion into privacy:

1. Legality – existence of a law;
2. Legitimate aim – the law must pursue a legitimate State purpose;
3. Proportionality and procedural safeguards – the extent of interference must be necessary and proportionate, with appropriate protections against abuse.[11]

These parameters are directly relevant for assessing State conduct in the digital sphere, including data collection, surveillance and data-sharing.[12]

---

[6] Alan F. Westin, *Privacy and Freedom* 7 (1967).
[7] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[8] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (illustrating early judicial hesitation).
[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[10] Id.
[11] *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353 (for proportionality test).
[12] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

JUDICIAL EVOLUTION: FROM TELEPHONE TAPPING TO DATA PROTECTION

Even before Puttaswamy, Indian courts had expressed concerns about intrusive surveillance. In People's Union for Civil Liberties v. Union of India, the Supreme Court examined the legality of telephone tapping and stressed the need for procedural safeguards to prevent arbitrary interception.[13] The Court linked privacy with the freedom of speech and expression.

Post-Puttaswamy, several decisions have further developed the contours of digital rights:

- In the Aadhaar cases, the Court examined whether the large-scale collection of biometric data for welfare schemes violated privacy. While upholding Aadhaar with restrictions, the Court emphasised data minimisation, purpose limitation and security safeguards.[14]

- In Anuradha Bhasin v. Union of India, the Supreme Court held that indefinite internet shutdowns are impermissible and that restrictions must meet the tests of necessity and proportionality.[15]

These decisions collectively signal that the judiciary expects the State to justify digital restrictions and data practices on constitutional grounds, rather than treating technology policy as a purely administrative matter.[16]

LEGISLATIVE FRAMEWORK: DATA PROTECTION AND SECTORAL LAWS

For many years, India relied primarily on scattered provisions of the Information Technology Act, 2000 and related rules to address data protection.[17] The growing complexity of digital ecosystems prompted calls for a dedicated data-protection law.

The Digital Personal Data Protection Act, 2023 is the first comprehensive statute aimed at regulating the processing of personal data.[18] It introduces concepts such as:

[13] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
[14] *K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1.
[15] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
[16] Id.
[17] *Information Technology Act*, No. 21 of 2000, India Code (2000); see also Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[18] *Digital Personal Data Protection Act*, No. 22 of 2023, Gazette of India, Aug. 11, 2023.

- obligations of data fiduciaries;
- consent and legitimate uses;
- duties of data principals (individuals); and
- penalties for non-compliance.

However, the Act has attracted critique on several grounds. First, it grants wide powers to the Central Government to exempt its agencies from compliance on grounds such as national security, public order or prevention of offences.[19] Secondly, much of the detailed framework is left to delegated legislation, raising concerns about executive overreach.[20] Thirdly, the degree of independence of the proposed Data Protection Board has been questioned.[21]

Thus, while the Act is a significant step, it does not fully resolve anxieties about unchecked State surveillance or corporate misuse of data. Its effectiveness will depend heavily on how powers are exercised and how robustly safeguards are implemented.[22]

SURVEILLANCE, NATIONAL SECURITY AND THE PROPORTIONALITY TEST

Security agencies increasingly rely on digital tools for intelligence gathering, crime detection and border protection. At the same time, unregulated or secretive surveillance risks creating a "panopticon effect", where citizens cannot know when and how they are being watched.[23]

Puttaswamy and later judgments suggest that any surveillance framework must satisfy the proportionality test:

- there must be a clear, accessible law authorising the measure;
- the measure must pursue a legitimate aim;
- there must be a rational connection between the measure and the aim;

[19] Id. § 17 (Government exemptions).
[20] Id. § 40 (rule-making powers).
[21] See parliamentary critiques and expert comments noting lack of independence: Internet Freedom Foundation, *Analysis of the DPDP Act 2023* (2023).
[22] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (emphasising necessity of safeguards in data processing).
[23] Jeremy Bentham's metaphor applied to modern surveillance: Shoshana Zuboff, *The Age of Surveillance Capitalism* 339 (2019).

- there must not be a less restrictive alternative; and
- adequate procedural safeguards, including independent oversight, must be ensured.[24]

In practice, India's surveillance system relies on executive authorisation, with limited judicial or parliamentary scrutiny. This leaves scope for arbitrary or disproportionate use of powers, which may chill dissent and undermine democratic accountability.[25]

ROLE OF PRIVATE PLATFORMS AND THE DATA ECONOMY

Digital privacy is not only a matter of State power. Private corporations, especially large digital platforms, collect and monetise vast quantities of personal data. Targeted advertising, algorithmic profiling and behavioural nudging have become central to their business models.[26]

From a human rights perspective, such practices raise questions about:

- informed and meaningful consent;
- the right to explanation in algorithmic decision-making;
- discrimination and exclusion based on data profiles; and
- cross-border data transfers without adequate protection.

While the data protection law attempts to regulate private entities, effective enforcement will require a vigilant regulator, sector-specific guidelines and active civil-society engagement. Without these, corporate data extraction may continue in ways that silently erode individual autonomy.[27]

COMPARATIVE PERSPECTIVES AND INTERNATIONAL STANDARDS

Globally, rights-based data protection regimes, such as the European Union's General Data Protection Regulation (GDPR), stress core principles like lawfulness, fairness and

[24] *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353 (proportionality test); applied in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[25] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (noting dangers of unchecked surveillance and requiring safeguards).
[26] Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019) (discussion of behavioural profiling and data monetisation).
[27] UN Human Rights Council, *Guiding Principles on Business and Human Rights*, U.N. Doc. A/HRC/17/31 (2011).

transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity, confidentiality and accountability.[28] International human rights instruments and soft-law documents emphasise that any restriction on privacy must be lawful, necessary and proportionate.[29] These principles provide useful benchmarks for evaluating India's legal framework and for interpreting domestic laws consistent with international commitments.

International human rights instruments and soft-law documents emphasise that any restriction on privacy must be lawful, necessary and proportionate. These principles provide useful benchmarks for evaluating India's legal framework and for interpreting domestic laws consistent with international commitments.

KEY CHALLENGES IN THE INDIAN CONTEXT

Despite significant jurisprudential advances, several challenges remain:

1. Institutional Weakness – Regulatory bodies may lack independence, resources or expertise.[30]

2. Opaque Practices – Citizens often do not know when their data is collected, shared or analysed.[31]

3. Digital Divide – Limited digital literacy and language barriers make it difficult for many individuals to understand consent forms or exercise their rights.[32]

4. Delegated Legislation – Excessive reliance on rules and notifications can dilute legislative scrutiny.[33]

5. Overlap of Laws and Agencies – Multiple authorities with overlapping jurisdiction can create confusion and reduce accountability.[34]

Unless these structural issues are addressed, the promise of privacy as a fundamental right may

[28] *Regulation (EU) 2016/679 (General Data Protection Regulation)*, 2016 O.J. (L 119) 1.
[29] U.N. Human Rights Committee, *General Comment No. 16: Right to Privacy (Art. 17)* (1988).
[30] Internet Freedom Foundation, *Analysis of India's Data Protection Landscape* (2023).
[31] Id.
[32] UNESCO, *Digital Literacy for the 21st Century* (2018).
[33] *Digital Personal Data Protection Act*, No. 22 of 2023, § 40.
[34] NITI Aayog, *Data Governance Framework for India* (2020).

remain largely on paper.[35]

SUGGESTIONS AND THE WAY FORWARD

To reconcile technological progress with constitutionalism, the following measures may be considered:

- Strengthening Oversight: Establish truly independent regulatory and oversight bodies with clear mandates, transparent appointment procedures and adequate resources.[36]
- Comprehensive Surveillance Law: Enact a dedicated law on surveillance practices that incorporates judicial authorisation, periodic review, and reporting obligations to the legislature.[37]
- Rights-Based Interpretation of the Data Protection Act: Apply Puttaswamy principles consistently while framing rules and exercising powers under the Act.[38]
- Enhanced Digital Literacy: Promote awareness about privacy rights through educational curricula, public campaigns, and legal-aid programmes.[39]
- Corporate Accountability: Impose strict obligations on digital platforms regarding transparency, algorithmic fairness and respect for user rights.[40]
- Judicial Vigilance: Continue robust constitutional scrutiny of digital policies to ensure that efficiency or security is not used as a blanket justification for rights-intrusive measures.[41]

CONCLUSION

Digital technologies are now inseparable from governance and everyday life. The challenge before India is not whether to adopt such technologies, but how to do so in a manner consistent

[35] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[36] Id.
[37] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
[38] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[39] UNICEF India, *Digital Literacy and Child Rights* (2021).
[40] U.N. Human Rights Council, *Guiding Principles on Business and Human Rights*, U.N. Doc. A/HRC/17/31 (2011).
[41] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

with the Constitution's vision of dignity, liberty and equality. The recognition of privacy as a fundamental right has created a strong normative foundation. However, constitutional promises must be matched by concrete institutional safeguards and genuine public participation.[42]

Protecting digital privacy is essential for maintaining citizens' trust in the State, encouraging free expression and safeguarding democratic values. If constitutional principles guide technological governance, digital innovation can become a vehicle for empowerment rather than a tool of control. The task, therefore, is not to choose between human rights and technology, but to ensure that technology operates within the framework of human rights.[43]

[42] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[43] Shoshana Zuboff, *The Age of Surveillance Capitalism* 339 (2019).