
PRIVACY IN THE DIGITAL ERA: A JURISPRUDENTIAL STUDY OF ARTICLE 21 AND DATA PROTECTION FRAMEWORKS

Bandana Devi Thokchom, Ph.D. Research Scholar, Manipur International University

Prof. S. James, Dean, Department of Law, Manipur International University

ABSTRACT

The digital revolution has profoundly reshaped the architecture of governance, commerce, and human interaction, creating unprecedented opportunities for connectivity while simultaneously intensifying the tension between privacy and surveillance. In India, the constitutional foundation of privacy is firmly anchored in **Article 21 of the Constitution**, which guarantees the right to life and personal liberty. Judicial interpretation, most notably in *Justice K.S. Puttaswamy v. Union of India (2017)*, has elevated privacy to the status of a fundamental right, intrinsic to dignity, autonomy, and democratic participation. This recognition situates privacy not merely as a defensive entitlement against intrusion but as a proactive guarantee enabling individuals to engage securely in digital society. The doctrinal analysis undertaken in this paper explores the jurisprudential evolution of Article 21, tracing its expansion from a narrow procedural safeguard to a dynamic repository of substantive rights. By situating privacy within Article 21's broad guarantee, the study demonstrates how constitutional interpretation has bridged domestic law with international human rights frameworks, drawing upon instruments such as the ICCPR and the ECHR. Yet, the digital era presents challenges that transcend traditional boundaries: algorithmic profiling, biometric surveillance, and cross-border data flows expose the fragility of privacy protections when technological innovation outpaces legislative and judicial responses. Comparative analysis highlights divergences between India's **Digital Personal Data Protection Act (DPDP) 2023** and global benchmarks such as the **General Data Protection Regulation (GDPR)** in the European Union and the **California Consumer Privacy Act (CCPA)**. While GDPR operationalizes privacy through expansive rights, independent regulators, and algorithmic accountability, India's DPDP Act remains narrower, centralized, and limited in enforcement scope. This doctrinal gap underscores the need for harmonization between Article 21's constitutional guarantee and statutory frameworks that can effectively safeguard individual rights in the digital age. The findings reveal three critical dimensions: first, the doctrinal adequacy of Article 21 as a

constitutional anchor for privacy; second, the enforcement gaps and legislative inertia that weaken India's statutory framework; and third, the socio-political realities—national security surveillance, corporate data commodification, and limited public awareness—that complicate operationalization of privacy rights. The study argues that privacy must be reconceptualized as a **non-derogable enabling right**, empowering individuals to participate freely in democratic, economic, and social life.

Keywords: Privacy, Article 21, Data Protection, Digital Rights, Surveillance, Social life.

Introduction

The concept of privacy has long been recognized as a cornerstone of human dignity and autonomy, yet its contours have been continually reshaped by technological progress and socio-political realities. In the digital era, privacy is no longer confined to the sanctity of the home or correspondence; it extends to the vast and complex ecosystem of online interactions, data flows, and algorithmic decision-making. The rise of surveillance capitalism, state monitoring, and cross-border data transfers has blurred the boundaries between legitimate governance and arbitrary intrusion, raising urgent questions about the adequacy of existing legal frameworks.

At the constitutional level, **Article 21 of the Indian Constitution** provides the foundational guarantee of life and personal liberty. Though originally framed as a procedural safeguard, judicial interpretation has expanded its scope to encompass substantive rights, including privacy. The landmark judgment in *Justice K.S. Puttaswamy v. Union of India (2017)* elevated privacy to the status of a fundamental right, affirming its intrinsic connection to dignity and autonomy. This doctrinal recognition situates privacy within the architecture of constitutional democracy, compelling legislative action to operationalize its guarantees in the digital age.

India's enactment of the **Digital Personal Data Protection Act (DPDP) 2023** represents a statutory attempt to codify privacy rights. While progressive in introducing a framework for data protection, its scope, enforcement mechanisms, and rights afforded to individuals remain narrower compared to global benchmarks such as the **General Data Protection Regulation (GDPR)** in the European Union. The divergence highlights the challenge of aligning Article 21's expansive constitutional guarantee with statutory provisions that often prioritize administrative convenience or economic feasibility over individual rights.

This paper situates privacy within the dual framework of constitutional law and comparative data protection regimes, while critically examining the adequacy of contemporary legislation. It argues that privacy in the digital era must be reconceptualized as a dynamic and enabling right, one that empowers individuals to participate freely and securely in digital society. By analyzing doctrinal foundations, comparative legislation, and empirical case studies of surveillance and data misuse, the study seeks to bridge the gap between normative ideals and operational realities.

The introduction thus sets the stage for a deeper inquiry into three core objectives: (i) evaluating the adequacy of Article 21 in addressing digital privacy challenges, (ii) assessing the effectiveness of current data protection laws in safeguarding individual rights, and (iii) proposing policy recommendations for harmonizing constitutional guarantees with international norms. In doing so, the research underscores the imperative of treating privacy not merely as a defensive shield against intrusion, but as a proactive guarantee of freedom, dignity, and democratic participation in the digital age.

Doctrinal Analysis of Article 21

1. Normative Foundation

Article 21 of the Indian Constitution declares that “No person shall be deprived of his life or personal liberty except according to procedure established by law.” Initially interpreted narrowly as a procedural safeguard, judicial creativity has transformed Article 21 into a repository of substantive rights. Privacy, as affirmed in *Justice K.S. Puttaswamy v. Union of India* (2017), is intrinsic to dignity and autonomy, thereby situating privacy within the architecture of constitutional democracy. This doctrinal expansion underscores the dynamic nature of Article 21, enabling it to adapt to evolving technological and societal contexts.

2. International Human Rights Influence

Although Article 21 is a domestic constitutional provision, its evolution has been influenced by international human rights instruments. The **International Covenant on Civil and Political Rights (ICCPR)** and the **European Convention on Human Rights (ECHR)** articulate privacy as a universal entitlement. Indian courts have drawn upon these frameworks to interpret Article 21 expansively, ensuring that constitutional guarantees resonate with global standards.

This comparative borrowing demonstrates how Article 21 bridges domestic jurisprudence with international norms.

3. Indian Constitutional Jurisprudence

The recognition of privacy as a fundamental right in *Puttaswamy* marked a watershed moment in Indian constitutional law. The Supreme Court held that privacy is intrinsic to life and liberty under Article 21, affirming its centrality to dignity, autonomy, and democratic participation. This doctrinal recognition compelled legislative action, culminating in the **Digital Personal Data Protection Act (DPDP) 2023**. Yet, the Act's narrower scope compared to global benchmarks reveals the challenge of translating judicial ideals into statutory safeguards.

4. Comparative Doctrinal Developments

The **General Data Protection Regulation (GDPR)** operationalizes privacy rights through expansive entitlements such as erasure, portability, and informed consent, enforced by independent regulators with significant sanctioning powers. In contrast, India's DPDP Act centralizes enforcement under the Data Protection Board, with limited autonomy and narrower rights. This divergence highlights the doctrinal challenge of aligning Article 21's broad constitutional guarantee with statutory frameworks that prioritize administrative feasibility.

5. Doctrinal Gaps in the Digital Era

Despite Article 21's robust foundation, its application faces challenges in the digital age:

- a. **Surveillance:** Mass monitoring by states often exceeds proportionality standards.
- b. **Corporate misuse:** Data harvesting and profiling undermine autonomy.
- c. **Cross-border enforcement:** Fragmented regimes weaken global privacy protection.

These gaps reveal the fragility of privacy protections when technological innovation outpaces legislative and judicial responses.

6. Policy Implications

The doctrinal analysis suggests that privacy must be reconceptualized as a **non-derogable**

right under Article 21. States must harmonize domestic laws with constitutional guarantees, ensuring independent oversight, algorithmic transparency, and effective remedies for violations. Embedding privacy into the architecture of digital governance strengthens resilience against technological exploitation and affirms dignity as the core of constitutional democracy.

Comparative Analysis: GDPR vs. DPDP Act 2023

1. Scope and Applicability

The **General Data Protection Regulation (GDPR)**, enacted by the European Union in 2018, is widely regarded as the gold standard of data protection. Its extraterritorial scope ensures that any entity processing the personal data of EU citizens, regardless of location, is bound by its provisions. In contrast, India's **Digital Personal Data Protection Act (DPDP) 2023** is primarily domestic in focus, applying to data processing within India and to foreign entities only if they deal with Indian citizens' data. This divergence reflects differing priorities: the EU emphasizes global accountability, while India balances privacy with economic and administrative feasibility under Article 21's constitutional umbrella.

2. Rights of Data Subjects

GDPR grants individuals expansive rights, including the **right to erasure** ("right to be forgotten"), data portability, and explicit consent requirements. The DPDP Act, while recognizing consent as central, provides narrower rights, with limited scope for erasure and portability. This doctrinal gap raises concerns about whether Article 21's guarantee of dignity and liberty is fully realized in India's framework.

3. Enforcement Mechanisms

GDPR establishes independent supervisory authorities across member states, empowered to impose significant fines (up to 4% of global annual turnover). India's DPDP Act centralizes enforcement under the **Data Protection Board of India**, which has limited autonomy and narrower sanctioning powers. This centralization risks undermining independence and effectiveness, particularly in politically sensitive cases.

4. Transparency and Accountability

GDPR mandates transparency in algorithmic decision-making and requires data controllers to conduct **Data Protection Impact Assessments (DPIAs)**. The DPDP Act does not impose equivalent obligations, leaving gaps in accountability for automated profiling and AI-driven data processing.

5. Policy Implications

The comparative analysis reveals that while India’s DPDP Act marks progress in codifying privacy rights under Article 21, it remains doctrinally weaker than GDPR. Harmonization requires strengthening individual rights, enhancing regulatory independence, and embedding transparency obligations into law.

Comparative Table: GDPR vs DPDP Act 2023

Aspect	GDPR	DPDP Act 2023
Scope	Extraterritorial, applies globally	Primarily domestic, limited extraterritorial reach
Rights of Individuals	Erasure, portability, informed consent, objection	Consent-based, limited erasure & portability
Enforcement	Independent regulators, heavy fines (up to 4% turnover)	Centralized Data Protection Board, limited penalties
Transparency	Mandatory DPIAs, algorithmic accountability	No equivalent obligations
Strengths	Strong rights, global influence	First statutory privacy law in India
Weaknesses	Complex compliance burden	Narrow rights, weaker enforcement

Findings & Discussion

1. Doctrinal Adequacy of Article 21

The analysis reveals that while **Article 21** provides a robust constitutional foundation for privacy, its application in the digital era remains limited. Drafted in a pre-digital context,

Article 21 does not explicitly address algorithmic profiling, biometric surveillance, or cross-border data transfers. Courts have attempted to extend its scope through interpretative creativity, but doctrinal clarity is still evolving. The absence of explicit statutory recognition of these modern threats weakens the operational strength of Article 21's guarantee.

2. Enforcement Gaps in India's DPDP Act 202

The **Digital Personal Data Protection Act (DPDP) 2023** represents India's first statutory attempt to codify privacy rights under Article 21. However, findings indicate several enforcement gaps:

- i. **Limited autonomy** of the Data Protection Board, raising concerns about independence.
- ii. **Narrower rights** compared to GDPR, particularly in erasure and portability.
- iii. **Absence of DPIAs**, weakening accountability for algorithmic profiling.

These gaps suggest that India's framework does not fully harmonize with Article 21's constitutional guarantee of dignity and liberty.

3. Judicial Activism vs. Legislative Inertia

The Indian Supreme Court's recognition of privacy as a fundamental right in *Puttaswamy* demonstrates judicial activism in advancing privacy jurisprudence. Yet, legislative inertia has slowed the translation of this doctrinal recognition into comprehensive statutory safeguards. The DPDP Act, while progressive, reflects compromises between individual rights and administrative convenience. This tension underscores the need for Parliament to align statutory law more closely with Article 21's expansive interpretation.

4. Global Lessons from GDPR Enforcement

Comparative findings highlight the effectiveness of GDPR's independent regulators and heavy sanctions in deterring violations. The EU's insistence on transparency and accountability has created a culture of compliance among corporations. India's DPDP Act, by contrast, risks being perceived as a compliance formality rather than a substantive rights-based framework. Aligning enforcement mechanisms with Article 21's spirit requires stronger independence and proportionate penalties.

5. Socio-Political Factors Shaping Privacy

Privacy enforcement in India is deeply influenced by socio-political realities:

- a) **Surveillance justified by national security** often exceeds proportionality standards, eroding trust in governance.
- b) **Corporate data misuse** driven by economic incentives commodifies personal information, undermining autonomy.
- c) **Limited public awareness** reduces demand for accountability, allowing both state and corporate actors to operate with minimal resistance.

These factors complicate the operationalization of Article 21 in practice, demonstrating that privacy protections must be reinforced not only through law but also through civic literacy and societal engagement.

6. Reconceptualizing Privacy as an Enabling Right

The discussion underscores the need to reconceptualize privacy under Article 21 not merely as a defensive shield against intrusion but as an enabling right. In the digital era, privacy empowers individuals to participate securely in democratic processes, economic activities, and social interactions. Treating privacy as a non-derogable right aligns with Article 21's spirit and strengthens resilience against technological exploitation.

Conclusion & Recommendations

1. Reconceptualizing Privacy in the Digital Era

Privacy in the digital age must be reconceptualized as more than a defensive shield against intrusion; it should be understood as an enabling right that empowers individuals to participate securely in democratic, economic, and social life. Under **Article 21 of the Indian Constitution**, privacy is intrinsic to dignity and liberty, and therefore must be treated as a **non-derogable entitlement**. The traditional conception of privacy as protection of the home or correspondence is insufficient in an era dominated by algorithmic profiling, biometric surveillance, and cross-border data flows. Reconceptualization requires embedding privacy

into the architecture of digital governance, ensuring autonomy, transparency, and effective remedies against misuse.

2. Harmonization of International and Domestic Norms

Comparative analysis reveals significant divergence between the **GDPR** and India's **DPDP Act 2023**. While GDPR operationalizes privacy through expansive rights and independent enforcement, India's framework remains narrower and centralized. Harmonization with Article 21 requires bridging this gap by embedding stronger rights and independent oversight into domestic law. This alignment ensures that constitutional guarantees resonate with global standards and protect citizens against arbitrary intrusion.

3. Strengthening Enforcement Mechanisms

Effective privacy protection depends on robust enforcement. India must strengthen the autonomy of the **Data Protection Board**, ensuring independence from political influence. Penalties should be proportionate to violations, mirroring GDPR's deterrent fines. Independent regulators are essential to uphold Article 21's guarantee against arbitrary interference, transforming privacy compliance from a procedural formality into a substantive safeguard.

4. Embedding Transparency in Technology

Algorithmic decision-making and AI-driven profiling pose unique threats to privacy. Mandatory **Data Protection Impact Assessments (DPIAs)** and algorithmic transparency obligations should be incorporated into domestic law. This ensures accountability in automated systems and aligns with Article 21's spirit of protecting individuals from arbitrary intrusion.

5. Enhancing Cross-Border Cooperation

Privacy violations often transcend national boundaries. India must engage in cross-border cooperation with international data protection authorities to combat cybercrime, regulate multinational corporations, and enforce privacy rights globally. Such cooperation strengthens the universality of Article 21 in the digital era and ensures that constitutional guarantees remain resilient in a globalized digital economy.

6. Policy Recommendations

To strengthen privacy protections in the digital era, policy must move beyond doctrinal recognition toward enforceable safeguards:

- a. **Independent regulators** with judicial oversight.
- b. **Algorithmic transparency** and accountability in AI systems.
- c. **Expanded individual rights** including erasure, portability, and objection.
- d. **Public awareness campaigns** to strengthen demand for enforcement.
- e. **Cross-border collaboration** for harmonized privacy standards.

In sum, the jurisprudential evolution of **Article 21** demonstrates India's constitutional commitment to safeguarding privacy as an inseparable component of life and liberty. Yet, the digital era exposes the fragility of this safeguard when statutory frameworks lag behind technological realities. Bridging doctrinal ideals with operational enforcement requires not only legislative refinement but also civic literacy, institutional independence, and international cooperation. By treating privacy as a **non-derogable enabling right**, India can ensure that technological progress enhances human dignity, democratic participation, and trust in governance. This conclusion reaffirms that privacy under Article 21 is not a peripheral entitlement but a central pillar of constitutional democracy in the digital age.

References

1. Bennett, Colin J. *The Privacy Advocates: Resisting the Spread of Surveillance*. MIT Press, 2008.
2. Bygrave, Lee A. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Kluwer Law International, 2002.
3. California Consumer Privacy Act (CCPA), 2018. State of California, USA.
4. Digital Personal Data Protection Act, 2023. Government of India.
5. European Convention on Human Rights (ECHR), 1950. Council of Europe.
6. General Data Protection Regulation (GDPR), 2016. European Union.
7. International Covenant on Civil and Political Rights (ICCPR), 1966. United Nations.
8. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. Supreme Court of India.
9. Solove, Daniel J. *Understanding Privacy*. Harvard University Press, 2008.
10. Swire, Peter & Ahmad, Robert. *Foundations of Privacy and Data Protection*. IAPP, 2019.
11. Universal Declaration of Human Rights (UDHR), 1948. United Nations.
12. Warren, Samuel D., & Brandeis, Louis D. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193–220.
13. Westin, Alan F. *Privacy and Freedom*. Atheneum, 1967.
14. Whitman, James Q. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale Law Journal*, 2004.
15. Zuboff, Shoshana. *The Age of Surveillance Capitalism*. Public Affairs, 2019.