INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 3 [2025] | Page 634 - 637

THE RIGHT TO PRIVACY IN INDIA'S DIGITAL ERA: A POST-PUTTASWAMY PERSPECTIVE

- Drishti Singh

INTRODUCTION

In a nation of over 800 million internet users, India stands at the forefront of the digital revolution. Yet, this transformation has brought unprecedented challenges to individual privacy, with state surveillance, private-sector data collection and emerging technologies like artificial intelligence reshaping personal liberties. The landmark *Justice K.S. Puttaswamy v. Union of India* (2017) judgment declared the right to privacy a fundamental right under Article 21 of the Indian Constitution, setting a new benchmark for legal protections. However, the rapid digitization of governance and commerce raises critical questions about the adequacy of India's legal framework in safeguarding privacy. This blog examines the evolution of privacy rights in India, the impact of digital technologies, the strengths and limitations of the Digital Personal Data Protection Act, 2023 (DPDP Act) and the delicate balance between individual rights and state interests.

THE EVOLUTION OF PRIVACY RIGHTS IN INDIAN JURISPRUDENCE

The recognition of privacy as a legal right in India has been a gradual and contested process. Early judicial interpretations offered limited protection. In *Kharak Singh v. State of UP* (1963), the Hon'ble Supreme Court struck down domiciliary visits by police as a violation of personal liberty but explicitly denied privacy as a standalone right under Article 21. Similarly, *Gobind v. State of MP* (1975) acknowledged a narrow right to privacy, derived from Articles 19 and 21, but subjected it to reasonable restrictions for public interest. These rulings reflected a state-centric approach, prioritizing security over individual autonomy.

The *Justice K.S. Puttaswamy v. Union of India* (2017) case marked a watershed moment. A nine-judge bench unanimously declared privacy a fundamental right, encompassing informational, decisional and bodily autonomy. The Court emphasized that privacy is intrinsic to human dignity and liberty, protected under Article 21. It introduced a three-pronged test for state actions infringing privacy:

legality (backed by law), necessity (serving a legitimate aim) and proportionality (least intrusive means). This ruling not only redefined constitutional jurisprudence but also provided a framework to scrutinize digital surveillance and data practices. Post-*Puttaswamy*, courts have applied this test in cases like *Aadhaar v. Union of India* (2018), reinforcing privacy's centrality in India's legal system.

DIGITAL TECHNOLOGIES: OPPORTUNITIES AND THREATS

India's digital landscape, with initiatives like Digital India and Aadhaar, has transformed governance and connectivity. Aadhaar, the world's largest biometric database, links over 1.3 billion citizens to welfare services, banking and taxation. While it streamlines access, its mandatory linkages and data breaches have sparked privacy concerns. In *Aadhaar v. Union of India* (2018), the Supreme Court upheld Aadhaar's constitutionality but struck down its mandatory use in private transactions (e.g., bank accounts, mobile SIMs), citing the *Puttaswamy* proportionality test. The Court emphasized that blanket data collection without a legitimate purpose violates privacy rights.

Private-sector practices further complicate the privacy landscape. Social media platforms, e-commerce giants and mobile apps collect vast amounts of personal data, often with vague consent mechanisms. The 2021 WhatsApp privacy policy controversy, which involved data sharing with Meta, triggered public outcry and legal challenges. Users feared that their personal communications could be exploited for commercial purposes, highlighting the need for transparent data policies. Emerging technologies, such as facial recognition and artificial intelligence, exacerbate these risks. For instance, facial recognition systems deployed in smart cities and by law enforcement raise concerns about mass surveillance and profiling, often without legal safeguards.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL ANALYSIS

Enacted in August 2023, the DPDP Act is India's first comprehensive data protection legislation, inspired by the *Puttaswamy* judgment and the Justice B.N. Srikrishna Committee Report (2018). The Act mandates informed consent for data collection, data minimization and purpose limitation, ensuring that entities collect only necessary data. It imposes hefty penalties up to ₹250 crore for data breaches and establishes a Data Protection Board to oversee compliance. The Act applies to both government and private entities, addressing concerns about unchecked data practices.

Despite these strengths, the DPDP Act has notable shortcomings. First, it grants the government broad exemptions for "state security" and "public order," terms that are vaguely defined and prone to misuse. This undermines the *Puttaswamy* proportionality test, as state agencies like the Central Monitoring System (CMS) can access personal data without judicial oversight. Second, unlike the EU's General Data Protection Regulation (GDPR), which empowers individuals with rights like data portability and erasure, the DPDP Act offers limited user control. Third, the Data Protection Board's government-appointed structure raises concerns about independence, unlike GDPR's autonomous regulators. Critics argue that the Act prioritizes state and corporate interests, leaving individuals vulnerable to data exploitation.

BALANCING PRIVACY AND STATE INTERESTS

The tension between individual privacy and state security is a global challenge, acutely felt in India's surveillance framework. Programs like CMS and the National Intelligence Grid (NATGRID) enable real-time monitoring of communications and financial transactions, often without transparent legal checks. The *Puttaswamy* judgment requires that such measures meet the proportionality standard, yet vague legislative exemptions weaken accountability. The 2021 Pegasus spyware controversy, where journalists, activists, and politicians were allegedly targeted, exposed the risks of unchecked surveillance. The Hon'ble Supreme Court's formation of a technical committee to investigate Pegasus underscores the judiciary's role in safeguarding privacy.

Another flashpoint is the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which mandate traceability of messages on platforms like WhatsApp. This requirement threatens end-to-end encryption, a cornerstone of digital privacy. In *WhatsApp v. Union of India* (pending), the Delhi High Court is examining whether traceability violates *Puttaswamy*'s principles. These cases highlight the need for a balanced framework that respects both security imperatives and individual rights.

COMPARATIVE INSIGHTS: LEARNING FROM GLOBAL FRAMEWORKS

A comparative analysis with global frameworks offers valuable lessons. The EU's GDPR, implemented in 2018, is a gold standard for data protection, emphasizing user rights like data portability, erasure ("right to be forgotten") and strict consent protocols. GDPR's independent supervisory authorities ensure robust enforcement, a model India could emulate to strengthen the

DPDP Act's Data Protection Board. In contrast, the US lacks a comprehensive federal privacy law, relying on sector-specific regulations like the California Consumer Privacy Act (CCPA). This fragmented approach has led to inconsistent protections, a pitfall India must avoid.

India can adopt GDPR's focus on transparency and accountability while tailoring it to local contexts. For instance, addressing Aadhaar's unique scale requires specific provisions for biometric data protection. Strengthening judicial oversight of surveillance, as seen in Canada's Privacy Act, could align India's framework with *Puttaswamy*'s standards.

RECOMMENDATIONS FOR A ROBUST PRIVACY FRAMEWORK

To uphold privacy in the digital era, India must address gaps in its legal framework. First, the DPDP Act should be amended to limit government exemptions and define "state security" narrowly, ensuring compliance with the *Puttaswamy* proportionality test. Second, establishing an independent Data Protection Board, insulated from government influence, is critical for impartial enforcement. Third, introducing user-centric rights like data erasure and portability would empower citizens, aligning the DPDP Act with global standards. Fourth, mandatory judicial oversight of surveillance programs like CMS and NATGRID would enhance accountability.

Finally, public awareness campaigns can educate citizens about their data rights, fostering a culture of privacy consciousness.

CONCLUSION

The *Puttaswamy* judgment redefined privacy as a cornerstone of India's constitutional framework, but the digital age demands continuous legal evolution. The DPDP Act, 2023, is a significant step toward protecting privacy, yet its limitations government exemptions, limited user rights and lack of independent oversight highlight the need for reform. As India navigates its digital future, balancing individual liberties with state interests requires a robust legal framework, informed by global best practices and rooted in *Puttaswamy*'s principles. By strengthening laws, ensuring accountability and empowering citizens, India can uphold privacy as a pillar of its democratic ethos in the digital era.