 DOI: https://doij.org/10.10000/IJLSI.116975

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 5

2025

Right to Privacy in the Digital Age: Legal Challenges and Emerging Trends in India

SANJANA CHATURVEDI[1]

ABSTRACT

The recognition of the right to privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) represents a watershed moment in Indian constitutional jurisprudence, firmly embedding privacy within the framework of dignity, autonomy, and liberty under Article 21 of the Constitution. The Supreme Court, speaking through a nine-judge bench, overruled earlier restrictive precedents and held that privacy is not merely a statutory protection but a constitutionally guaranteed intrinsic right forming part of the basic structure of human dignity.

This doctrinal transformation coincides with India's rapid digitalization, where personal data has become a core resource for governance, economic activity, and algorithmic decision-making. However, the transition from constitutional recognition to effective enforcement remains incomplete due to structural regulatory gaps, weak institutional independence, and expanding state and corporate surveillance.

The enactment of the Digital Personal Data Protection Act, 2023 introduces a consent-based regulatory model, yet it has been criticized for broad state exemptions and limited judicial oversight. This paper critically analyses the evolution of privacy jurisprudence in India, integrates comparative insights from foreign legal systems such as the EU's GDPR regime and US constitutional privacy doctrine, and examines emerging technological challenges including artificial intelligence, biometric surveillance, and blockchain systems.

It argues that India is entering a post-constitutional-privacy enforcement gap, where judicial recognition is strong but institutional safeguards remain underdeveloped.

Keywords: *Right to Privacy, Puttaswamy, DPDP Act 2023, Data Protection, Surveillance Law, GDPR, Digital Constitutionalism*

I. CONSTITUTIONAL EVOLUTION OF PRIVACY: DOCTRINAL TRANSFORMATION

M.P. Sharma v. Satish Chandra (1954)

The foundational position on privacy in early constitutional jurisprudence was firmly restrictive. In *M.P. Sharma v. Satish Chandra*, the Supreme Court categorically held that the

[1] Author is an Assistant Professor at Rabindranath Tagore University, Bhopal, Madhya Pradesh, India.

Constitution of India does not expressly recognize a right to privacy. The Court further ruled that privacy could not be inferred under Article 20(3), which protects against self-incrimination.[2]

The Court adopted a state-centric interpretative approach, prioritizing investigatory and enforcement powers over individual liberty. It reasoned that constitutional safeguards against search and seizure were deliberately absent in the text of the Constitution, thereby indicating that privacy was not intended to be a protected fundamental right. This reflected a post-colonial administrative continuity where state authority was given precedence over individual autonomy in matters of criminal investigation.

Kharak Singh v. State of Uttar Pradesh (1962)

In *Kharak Singh v. State of Uttar Pradesh*, the Supreme Court once again declined to recognize privacy as a constitutionally guaranteed right.[3] The majority opinion upheld certain forms of police surveillance, including periodic domiciliary visits, on the ground that they did not amount to physical restraint under Article 21.

However, the Court partially struck down aspects of surveillance that intruded excessively into personal liberty, signaling early discomfort with unchecked state intrusion. Although fragmented in reasoning, the judgment marked the beginning of judicial engagement with the concept of personal autonomy.

The most significant contribution came from **Justice Subba Rao's dissent**, which later became foundational to modern privacy doctrine. He powerfully articulated that personal liberty inherently includes protection against intrusive state surveillance, observing that:

"Personal liberty takes in not only freedom from physical restraint but also freedom from encroachments upon one's private life."

This dissent is widely regarded as the intellectual precursor to India's modern privacy jurisprudence, as it conceptually linked liberty with informational and spatial autonomy.

A. Expansion Phase: Privacy as an Element of Dignity

Gobind v. State of Madhya Pradesh (1975)

A gradual doctrinal shift emerged in *Gobind v. State of Madhya Pradesh*, where the Supreme Court cautiously acknowledged that the right to privacy may be inferred from Article 21.[4]

---

[2] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300
[3] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295
[4] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148

Unlike earlier decisions, the Court accepted that privacy could not be completely excluded from constitutional protection, particularly where state action interferes with personal liberty.

However, the Court also emphasized that privacy is not absolute and may be restricted where a **compelling state interest** exists. This case introduced an early balancing framework between individual liberty and state necessity, laying the groundwork for later proportionality analysis.

The Court's reasoning indicated an evolving understanding that privacy is essential to human dignity, but must coexist with legitimate governance objectives.

R. Rajagopal v. State of Tamil Nadu (1994)

A more structured recognition of privacy emerged in *R. Rajagopal v. State of Tamil Nadu*, where the Supreme Court explicitly acknowledged **informational privacy** in the context of freedom of speech and media law.[5]

The Court held that the publication of private facts without consent, even if true, may violate the right to privacy unless justified by public interest. This judgment significantly expanded the conceptual scope of privacy beyond physical intrusion to include control over personal information.

The Court further clarified important doctrinal principles:

- Privacy protects an individual's autonomy over personal identity and narrative.
- Public figures retain privacy rights, although the threshold for public disclosure is narrower.
- Unauthorized publication of private life constitutes a civil wrong unless justified by overriding public interest.

This case marked a decisive shift toward recognizing privacy as an aspect of dignity, reputation, and informational control.

B. Constitutional Breakthrough: Justice K.S. Puttaswamy (2017)

The most transformative development in Indian privacy jurisprudence occurred in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where a nine-judge bench unanimously declared privacy to be a fundamental right under Articles 14, 19, and 21 of the Constitution.[6]

The Court overruled earlier restrictive interpretations and held that privacy is intrinsic to life and personal liberty. It rejected the notion that fundamental rights should be narrowly construed

[5] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632
[6] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

in a technologically evolving society.

The judgment introduced a structured constitutional test for evaluating privacy infringements:

1. **Legality** – Any intrusion must be backed by valid law.
2. **Legitimate Aim** – The state objective must be legitimate and necessary.
3. **Proportionality** – The extent of interference must be proportionate to the need pursued.

This three-fold test now forms the doctrinal backbone of privacy adjudication in India.

The judgment contained significant concurring opinions that expanded the philosophical and legal scope of privacy:

Justice D.Y. Chandrachud

He emphasized that privacy is central to human dignity and constitutional identity, stating:

"Privacy is the constitutional core of human dignity."

He further clarified that privacy is not merely a negative right but also imposes positive obligations on the State to protect individuals from intrusion.

Justice Rohinton F. Nariman

Justice Nariman highlighted the limits of state authority, observing that:

"The State cannot intrude into the inner sanctum of human life without justification."

This reinforced the idea that the Constitution places strict limits on executive power in matters affecting personal autonomy.

Justice S.K. Kaul

Justice Kaul expanded the doctrine into the digital era by recognizing informational privacy, stating:

"Data protection is essential to autonomy in the digital age."

He explicitly linked privacy with control over personal data, thereby laying the foundation for modern data protection law in India.

II. Comparative constitutional perspectives

A. United States: Fourth Amendment Doctrine

The constitutional protection of privacy in the United States is primarily derived from the Fourth Amendment, which guards against "unreasonable searches and seizures." Unlike India's post-*Puttaswamy* framework, where privacy is expressly recognized as a fundamental right under Articles 14, 19, and 21, American privacy jurisprudence has developed in a more **case-driven and fragmented manner**, heavily dependent on judicial interpretation and sector-specific legislation.

A major doctrinal turning point occurred in *Katz v. United States (1967)*, where the U.S. Supreme Court fundamentally redefined the scope of privacy protection. The Court held that constitutional protection is not limited to physical spaces but extends to individuals wherever they have a **"reasonable expectation of privacy."** The Court famously stated:

"The Fourth Amendment protects people, not places."[7]

This marked a shift from property-based notions of privacy to a more person-centric approach. Justice Harlan's concurring opinion introduced the two-part test for determining privacy expectations: (1) whether an individual has exhibited a subjective expectation of privacy, and (2) whether society recognizes that expectation as reasonable. This test continues to guide American privacy law, particularly in cases involving surveillance and digital monitoring.

However, despite *Katz*, U.S. privacy law remains **non-unified and sectoral in nature**, governed by a patchwork of statutes such as the Electronic Communications Privacy Act (ECPA), Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA). Unlike India's constitutional model post-*Puttaswamy*, there is no single overarching constitutional doctrine explicitly guaranteeing informational privacy across contexts.

Digital Age Expansion: Carpenter v. United States (2018)

The limitations of traditional Fourth Amendment doctrine became increasingly apparent with technological advancement, particularly in relation to digital surveillance and metadata collection. In *Carpenter v. United States (2018)*, the U.S. Supreme Court significantly expanded privacy protections by holding that law enforcement access to historical cell-site location information (CSLI) constitutes a search under the Fourth Amendment.[8]

Chief Justice Roberts, writing for the majority, recognized that digital records generated by mobile phones reveal detailed and continuous information about an individual's movements, associations, and daily life. The Court rejected the argument that such data is excluded from constitutional protection merely because it is held by third-party service providers.

This judgment marked a critical doctrinal evolution by acknowledging that:

[7] *Katz v. United States*, 389 U.S. 347 (1967)
[8] *Carpenter v. United States*, 585 U.S. 296 (2018)

- Digital metadata can be deeply revealing of personal life patterns
- Traditional third-party doctrines are insufficient in the digital age
- Continuous surveillance raises heightened constitutional concerns

The Court emphasized that allowing unrestricted access to such data would effectively enable a form of **“near-perfect surveillance”**, incompatible with democratic values and individual liberty.

Comparative Assessment: India and the United States

A comparison between India and the United States reveals fundamental differences in constitutional design and privacy protection:

1. **Unified Constitutional Right vs. Fragmented Protection:** India recognizes privacy as a fundamental right under the Constitution after *Puttaswamy*, whereas the United States relies on the Fourth Amendment interpreted through judicial precedents and sectoral statutes.
2. **Proportionality vs. Reasonableness Standard:** India applies a structured proportionality test requiring legality, necessity, and balancing of interests. The U.S. employs the “reasonable expectation of privacy” test, which is less structured and more flexible but also less predictable.
3. **Data-Centric Privacy Evolution:** While both jurisdictions have adapted to digital surveillance concerns, India’s framework explicitly integrates informational privacy as a constitutional principle, whereas the U.S. continues to evolve through incremental judicial expansion, as seen in *Carpenter*.
4. **Institutional Design Differences:** India is moving toward statutory regulation through the Digital Personal Data Protection Act, 2023, whereas the U.S. maintains a decentralized, sector-based regulatory model.

Doctrinal Significance

The evolution of U.S. privacy jurisprudence demonstrates a gradual shift from physical-space protection to data-driven constitutional interpretation. However, compared to India’s post-*Puttaswamy* framework, the U.S. model remains less coherent in addressing comprehensive informational privacy.

The decisions in *Katz* and *Carpenter* collectively illustrate the judiciary’s attempt to adapt traditional constitutional protections to modern digital realities. Nevertheless, the absence of a unified constitutional privacy doctrine continues to generate gaps in protection, particularly in the context of large-scale data collection and algorithmic surveillance.

B. European Union: GDPR Model

The European Union's data protection framework, particularly the General Data Protection Regulation (GDPR), represents one of the most comprehensive and rights-based approaches to informational privacy globally. Unlike jurisdictional models that rely heavily on fragmented statutes or primarily judicial evolution, the EU adopts a codified and enforceable regulatory framework that treats data protection as a fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union.[9]

The GDPR is built upon core principles that structure all forms of personal data processing within the EU. These include data minimization, which requires that only data strictly necessary for a specified purpose be collected; purpose limitation, which restricts the use of data to the original stated objective; and lawfulness, fairness, and transparency, which ensure that individuals are clearly informed about how their data is used.[10] A central feature of the GDPR is explicit and informed consent, which must be freely given, specific, and unambiguous, thereby strengthening individual control over personal information.

Another defining element of the GDPR framework is the right to erasure, commonly referred to as the "right to be forgotten." This right empowers individuals to request deletion of personal data when it is no longer necessary, when consent is withdrawn, or when processing violates legal requirements. Unlike many other jurisdictions, the EU provides structured enforcement mechanisms through independent Data Protection Authorities (DPAs) in each member state, ensuring regulatory autonomy and compliance monitoring.[11]

Judicial Expansion: Google Spain v. AEPD (2014)

A landmark development in European privacy jurisprudence occurred in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (2014)*, where the Court of Justice of the European Union (CJEU) recognized the "right to be forgotten" within the broader framework of informational autonomy.[12]

The Court held that search engines qualify as "data controllers" and are therefore responsible for ensuring compliance with data protection principles. It ruled that individuals may request

[9] Charter of Fundamental Rights of the European Union art. 8, 2012 O.J. (C 326) 391
[10] Regulation 2016/679, General Data Protection Regulation, arts. 5–6, 2016 O.J. (L 119) 1 (EU)
[11] GDPR, arts. 15–22, 51–59, 2016 O.J. (L 119) 1 (EU)
[12] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI:EU:C:2014:317 (CJEU 2014)

the removal of links to personal information that is inadequate, irrelevant, or excessive in relation to the purposes for which it was processed. This decision significantly expanded the scope of informational privacy by recognizing that personal data dissemination through search engines can have long-term reputational consequences.

Importantly, the Court balanced privacy rights against the public's right to information, holding that removal is not absolute and must be assessed on a case-by-case basis depending on factors such as the individual's public role and the relevance of the information.

C. United Kingdom: Evolving Common Law Privacy

The United Kingdom does not recognize a standalone constitutional right to privacy in the same manner as India or many civil law jurisdictions. Instead, privacy protection has developed through a **gradual convergence of common law principles and human rights obligations**, particularly after the incorporation of the European Convention on Human Rights (ECHR) through the Human Rights Act 1998.[13] This has led to a distinctive model where privacy is protected indirectly through the tort of **misuse of private information**, rather than through a codified constitutional guarantee.

A landmark development in this evolution occurred in *Campbell v. MGN Ltd. (2004)*, where the House of Lords formally recognized **misuse of private information as an actionable tort**, thereby consolidating privacy protection within English common law.[14] The case involved the publication of details about supermodel Naomi Campbell's drug rehabilitation treatment. While the Court acknowledged that public figures have reduced expectations of privacy in certain contexts, it held that publication of private medical information without justification constituted a wrongful intrusion into private life.

The Court developed a structured balancing approach between two competing rights:

- The right to privacy under Article 8 of the European Convention on Human Rights (respect for private and family life)
- The right to freedom of expression under Article 10 of the ECHR

This proportionality-based balancing exercise became central to UK privacy jurisprudence. The Court emphasized that neither right has automatic priority, and that adjudication must depend on the facts of each case, particularly the degree of intrusion and public interest involved.

[13] Human Rights Act 1998, c. 42 (U.K.)
[14] *Campbell v. MGN Ltd.*, [2004] UKHL 22, [2004] 2 A.C. 457 (appeal taken from Eng.)

Following *Campbell*, UK courts have increasingly refined the doctrine of misuse of private information into a mature legal framework. The tort now involves a two-stage test:

1. Whether the claimant had a **reasonable expectation of privacy** in the information disclosed
2. Whether that expectation is outweighed by a **countervailing public interest**, including freedom of expression and media reporting rights

This framework has allowed UK courts to address modern privacy issues such as media intrusion, data disclosure, and digital surveillance while maintaining flexibility consistent with common law traditions.

Comparative Significance

The UK approach represents a **hybrid privacy model**, combining:

- Common law evolution (judge-made doctrine)
- Human rights integration (ECHR-based proportionality)
- Absence of a single constitutional privacy clause

Compared to India, the UK lacks an explicit constitutional declaration of privacy as a fundamental right. However, post-*Campbell* jurisprudence has effectively elevated privacy to a quasi-fundamental status through human rights interpretation.

Unlike the EU's GDPR framework, which provides comprehensive statutory regulation, the UK model remains primarily judicially driven and case-specific, offering flexibility but less structural uniformity. Nonetheless, the proportionality-based balancing approach closely aligns with both Indian constitutional doctrine post-*Puttaswamy* and European human rights standards.

Comparative Significance in Global Privacy Governance

The EU model under the GDPR is widely regarded as the global benchmark for data protection due to its comprehensive, rights-based, and enforceable structure. It differs significantly from both the United States and India in several respects:

- It treats data protection as a fundamental right, not merely a statutory protection.
- It establishes uniform regulatory standards across all member states, unlike the sectoral U.S. approach.
- It provides strong institutional enforcement mechanisms through independent supervisory authorities.

- It incorporates advanced rights such as data portability, restriction of processing, and automated decision-making safeguards.

In comparison, India's Digital Personal Data Protection Act, 2023 draws conceptual inspiration from the GDPR but lacks comparable institutional independence and detailed regulatory granularity. Similarly, the U.S. system remains fragmented and primarily reactive, relying on judicial interpretation and sector-specific statutes rather than a unified constitutional or regulatory framework.

Thus, the GDPR represents a mature model of constitutionalized data governance, where privacy is not only a legal right but also an enforceable regulatory obligation integrated into the digital economy.

III. DIGITAL EXPANSION AND STRUCTURAL PRIVACY CHALLENGES

India's rapid transition toward a digital governance ecosystem under the *Digital India* framework has significantly transformed the relationship between the State and citizens. Large-scale digitization of identity systems, welfare delivery mechanisms, financial services, and public administration has enabled improved efficiency, reduced leakage in subsidy distribution, and expanded access to essential services. However, this transformation has simultaneously produced a data-intensive governance structure, where personal information has become central to state functioning.

This shift raises fundamental constitutional concerns, particularly regarding informational autonomy, consent, and the risk of continuous profiling. The increasing dependence on centralized digital identity systems and interoperable databases has intensified fears of surveillance, function creep, and erosion of anonymity in everyday life. In such a system, the boundaries between governance efficiency and constitutional liberty become increasingly blurred, requiring strict judicial and legislative safeguards.

Aadhaar and Constitutional Tension

A critical constitutional turning point in India's digital privacy jurisprudence emerged in *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India (2018)*, where the Supreme Court upheld the validity of the Aadhaar scheme while simultaneously imposing significant constitutional limitations on its use.[15]The judgment represented a nuanced balancing of welfare efficiency against fundamental rights, particularly the right to privacy under Article 21.

The majority opinion upheld Aadhaar as constitutionally valid, emphasizing its role in targeted

[15] *K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.)*, (2019) 1 SCC 1 (India)

welfare delivery and financial inclusion. However, it read down several provisions to prevent disproportionate intrusion into privacy rights. Notably, the Court struck down provisions allowing mandatory linkage of Aadhaar with private-sector services such as bank accounts and mobile services, holding that such compulsory linkage violated the principle of proportionality.

The Court further emphasized three core safeguards that any Aadhaar-related data processing must satisfy:

- **Purpose limitation**: Data collected for Aadhaar cannot be used beyond welfare and state-authorized objectives.
- **Data minimization**: Only minimal necessary biometric and demographic data may be collected and stored.
- **Restriction on profiling**: Aadhaar data cannot be used to create behavioral or personal profiles of individuals.

These principles were intended to ensure that Aadhaar functions as an identity authentication system rather than a tool for pervasive surveillance or behavioural tracking.

However, the judgment was deeply divided. In his dissenting opinion, Justice D.Y. Chandrachud issued a strong warning regarding the structural implications of Aadhaar for constitutional democracy. He cautioned that:

"Aadhaar creates the architecture of a surveillance state."[16]

This dissent highlighted the potential for centralized biometric databases to enable continuous monitoring of individuals' activities across sectors, thereby fundamentally altering the balance between citizen and State.

Structural Privacy Concerns in Digital Governance

The Aadhaar framework illustrates broader structural tensions inherent in India's digital governance model:

1. **Centralization of Sensitive Data:** Large-scale biometric databases consolidate identity information, increasing risks of unauthorized access and systemic breaches.
2. **Function Creep:** Systems initially designed for welfare delivery risk expansion into law enforcement, commercial, or surveillance applications.

[16] Id. (Chandrachud, J., dissenting)

3. **Weak Institutional Oversight:** Concerns persist regarding limited independent regulation of data usage and security protocols.
4. **Consent Deficit in Welfare Systems:** In practice, individuals often lack meaningful choice when participation in digital identity systems becomes functionally mandatory for accessing essential services.
5. **Interoperability Risks:** Integration of Aadhaar with multiple databases increases the possibility of cross-platform profiling and aggregation of personal data.

These challenges demonstrate that digital governance is not merely a technological shift but a **constitutional transformation in the nature of state power**, requiring continuous judicial scrutiny under the proportionality standard established in *Puttaswamy*.

Doctrinal Significance

The Aadhaar judgment reflects a central tension in Indian privacy jurisprudence: the need to balance **welfare efficiency and constitutional liberty**. While the majority sought to preserve the legitimacy of large-scale digital governance, it simultaneously acknowledged the necessity of strict safeguards to prevent misuse of personal data.

The dissenting opinion, however, underscores a deeper constitutional anxiety—that digital identity systems, if insufficiently regulated, may fundamentally alter the architecture of governance by enabling pervasive surveillance capabilities.

This duality makes *Aadhaar* one of the most significant cases in India's privacy jurisprudence, as it operationalizes the abstract principles of *Puttaswamy* in a real-world digital governance context.

State Surveillance and Constitutional Limits

India's legal framework governing surveillance remains fragmented, colonial-era in origin, and technologically outdated, primarily anchored in the *Indian Telegraph Act, 1885* and the *Information Technology Act, 2000*.[17]These statutes empower the executive to intercept communications and access digital data under broadly defined grounds such as "public emergency," "public safety," and "national security," but they do not establish a comprehensive, transparent, or constitutionally robust surveillance regime.

A key structural concern is the absence of mandatory prior judicial authorization for interception or surveillance activities. Unlike several constitutional democracies, India largely

[17] Indian Telegraph Act, 1885, No. 13 of 1885; Information Technology Act, 2000, No. 21 of 2000.

 [ISSN 2581-9453]

relies on executive-led authorisation mechanisms, typically exercised through administrative orders. This creates significant risks of arbitrariness, lack of accountability, and potential overreach.

This framework sits uneasily with the constitutional principles articulated in *Justice K.S. Puttaswamy v. Union of India (2017)*, where the Supreme Court held that any infringement of privacy must satisfy the tests of legality, necessity, and proportionality.[18] However, in the absence of strong procedural safeguards and independent oversight, the operationalization of these principles in surveillance contexts remains limited

IV. GLOBAL CONSTITUTIONAL CONTRAST

A comparative perspective highlights how other constitutional systems have developed stronger safeguards against state surveillance:

Germany

Germany represents one of the most privacy-protective jurisdictions globally. The Federal Constitutional Court has consistently applied a **strict proportionality doctrine**, particularly after recognizing the concept of "informational self-determination" in its landmark census decision.[19] Surveillance measures must satisfy stringent necessity tests and are subject to strong constitutional review.

United States

In the United States, the Fourth Amendment requires that searches and surveillance generally be supported by a **judicial warrant based on probable cause**.[20] While exceptions exist (such as the third-party doctrine), recent jurisprudence has strengthened protections for digital data, particularly in *Carpenter v. United States (2018)*, which extended warrant requirements to location metadata.[21]

European Union

The EU provides a dual-layer protection regime:

- The **Charter of Fundamental Rights of the European Union (Article 7 & 8)** guarantees privacy and data protection as fundamental rights.[22]

[18] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1
[19] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 BVerfGE 1 (Germany Census Case)
[20] U.S. Const. amend. IV
[21] *Carpenter v. United States*, 585 U.S. 296 (2018).
[22] Charter of Fundamental Rights of the European Union arts. 7–8, 2012 O.J. (C 326) 391

- The **GDPR** imposes strict rules on data processing, consent, and state/corporate accountability.[23]

Together, these frameworks ensure that surveillance and data processing are tightly regulated and subject to independent oversight.

India's Position

In contrast, India's surveillance architecture remains executive-heavy and judicially under-institutionalized, relying on internal administrative authorisation rather than independent judicial scrutiny. While the *Puttaswamy* judgment imposes constitutional constraints, enforcement mechanisms remain weak and inconsistently applied in practice.

This raises critical constitutional concerns, particularly regarding:

- Lack of transparency in surveillance authorisation
- Absence of independent oversight mechanisms
- Risk of disproportionate intrusion into informational privacy
- Potential chilling effects on free speech and association

Thus, India's surveillance model reflects a continuing tension between national security imperatives and constitutional liberty protections.

V. PRIVATE SURVEILLANCE AND THE DATA ECONOMY

Beyond state surveillance, a parallel system of private-sector surveillance has emerged, driven by digital platforms, artificial intelligence systems, and data-driven advertising ecosystems. In this model, corporations act as data controllers and behavioural intermediaries, shaping user preferences, decisions, and even political behaviour.

A globally significant example of this phenomenon is the Facebook–Cambridge Analytica scandal, where personal data harvested from social media platforms was used for political profiling and targeted manipulation during electoral processes.[24] The scandal triggered worldwide regulatory scrutiny and revealed deep structural vulnerabilities in digital consent mechanisms.

Key implications of this incident include:

- **Illusory consent**: Users often agree to data policies without meaningful understanding

[23] Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU)
[24] *Facebook, Inc. v. Cambridge Analytica Scandal* (global regulatory investigations 2018)

- **Behavioural manipulation**: Data analytics can influence preferences and decision-making
- **Political microtargeting**: Personal data can be used to shape electoral outcomes

This phenomenon aligns with Shoshana Zuboff's theory of **"surveillance capitalism,"** which describes a system in which human experience is commodified, extracted as behavioural data, and monetized for predictive and commercial purposes.[25] In such a framework, privacy is not merely violated by the State but systematically transformed into an economic resource.

The convergence of state surveillance and private data extraction highlights a fundamental shift in the nature of privacy threats in the digital age. Unlike traditional violations, modern privacy risks are:

- Continuous rather than episodic
- Automated rather than manual
- Systemic rather than isolated
- Embedded in governance and market structures

This reinforces the relevance of the *Puttaswamy* proportionality doctrine, which must now be applied not only to state action but also to powerful private actors operating within the digital economy.

VI. DIGITAL PERSONAL DATA PROTECTION ACT, 2023: CRITICAL ASSESSMENT

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first consolidated legislative attempt to regulate the processing of digital personal data. It introduces a structured compliance framework grounded in consent-based processing, granting individuals (data principals) certain enforceable rights while imposing obligations on entities that process personal data (data fiduciaries).[26]

The Act also establishes the Data Protection Board of India, which is intended to function as the primary adjudicatory and enforcement body for data protection disputes and violations. In principle, the DPDP Act marks a significant shift from the earlier fragmented regime under the Information Technology Act, 2000.

However, despite its progressive intent, the Act has been widely critiqued for structural and substantive limitations that may weaken its effectiveness in safeguarding informational

[25]SHOSHANA ZUBOFF, *The Age of Surveillance Capitalism* (2019)
[26] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India)

privacy.

One of the most significant concerns is the broad exemption granted to the State, particularly under grounds such as national security, sovereignty, and public order. These exemptions are drafted in expansive terms, allowing wide executive discretion and limiting the scope of judicial or independent scrutiny.[27] This raises concerns about potential dilution of privacy protections in cases involving state surveillance or data-intensive governance systems.

Another major issue is the limited independence of the Data Protection Board. Although it is designed as an enforcement authority, its composition and functioning remain closely linked to executive control, raising questions about institutional autonomy and neutrality, especially in disputes involving government agencies.

The Act also provides limited safeguards for algorithmic accountability, despite the increasing use of artificial intelligence and automated decision-making systems in both public and private sectors. Unlike more developed frameworks, it does not impose strong transparency obligations regarding how automated systems process or profile individuals.

Furthermore, the DPDP Act does not explicitly incorporate a robust "right to be forgotten", instead offering limited rights to correction and erasure subject to prescribed conditions. This restricts an individual's ability to permanently remove personal data from digital environments.

Comparative Criticism: DPDP Act vs GDPR

When compared to the European Union's General Data Protection Regulation (GDPR), the DPDP Act reflects a more restrained regulatory approach.

The GDPR provides stronger protections in several key areas:

- **Data portability**, allowing individuals to transfer their data between service providers
- **Independent supervisory authorities**, ensuring regulatory autonomy
- **Strict enforcement mechanisms**, including substantial financial penalties
- **Detailed cross-border data transfer restrictions**, based on adequacy standards[28]

In contrast, the DPDP Act offers a more state-centric governance model with broader executive discretion and fewer structural safeguards for regulatory independence.

This difference highlights a fundamental divergence: while GDPR treats data protection as a deeply institutionalized fundamental-rights framework, the DPDP Act adopts a more

[27] Id. § 17 (Government exemptions and lawful access provisions)
[28] Regulation 2016/679, General Data Protection Regulation, arts. 44–50, 2016 O.J. (L 119) 1 (EU)

compliance-driven regulatory model.

VII. EMERGING GLOBAL TRENDS IN PRIVACY LAW

Artificial intelligence (AI) has emerged as one of the most transformative drivers of contemporary privacy challenges, primarily due to its dependence on vast datasets and often opaque decision-making processes. AI systems raise significant concerns relating to algorithmic bias, discriminatory outcomes, lack of transparency, and the increasing use of predictive analytics in areas such as policing and behavioural profiling. In response, the European Union has introduced the **EU AI Act (2024)**, which establishes a risk-based regulatory framework that classifies AI systems according to their potential harm and imposes stricter obligations on high-risk applications. This reflects a broader global shift toward proactive regulation of algorithmic systems rather than reactive legal intervention.

Biometric surveillance technologies, including facial recognition and fingerprint identification systems, are also expanding rapidly across governance and commercial sectors. While these technologies enhance identification and security capabilities, they simultaneously raise serious concerns regarding mass surveillance, continuous tracking, and identity misuse. Regulatory responses differ across jurisdictions: several cities in the United States have restricted or banned police use of facial recognition, while the European Union has introduced stringent limitations on high-risk biometric systems under its AI regulatory framework. These developments reflect growing recognition that biometric data is uniquely sensitive because it is permanent, non-revocable, and closely tied to individual identity.

Similarly, blockchain technology presents a structural challenge to conventional data protection principles due to its inherent immutability, which prevents easy modification or deletion of stored data. This creates direct tension with core privacy rights such as the right to be forgotten, the right to correction, and the principle of data accuracy. As a result, blockchain-based systems often conflict with established data protection frameworks, raising unresolved legal and regulatory questions about how technological design can be reconciled with individual privacy rights.

Finally, the emergence of the metaverse introduces a new and more immersive dimension of privacy risk. Unlike traditional digital platforms, metaverse environments collect highly detailed behavioural data, including physical movements, voice interactions, gestures, and emotional responses. This raises concerns about continuous behavioural tracking, identity manipulation through digital avatars, and large-scale cross-platform data integration. Together, these developments indicate that privacy risks are no longer limited to static data collection but increasingly extend to real-time surveillance within fully immersive digital ecosystems, significantly expanding the boundaries of informational control and autonomy.

VIII. CONCLUSION

The evolution of privacy jurisprudence in India reflects a deep and structural constitutional transformation, marking a shift from a traditional model of **state supremacy** toward a rights-based framework centred on **individual autonomy, dignity, and informational self-determination**. The landmark decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* decisively elevated privacy to the status of a fundamental right under the Indian Constitution, embedding it within the broader guarantees of Articles 14, 19, and 21. This judgment not only overruled earlier restrictive interpretations but also established a principled constitutional framework based on legality, necessity, and proportionality for evaluating any intrusion into personal liberty.

Despite this doctrinal clarity, the post-*Puttaswamy* era reveals a persistent and widening gap between constitutional recognition and practical enforcement. The rapid expansion of digital governance systems, surveillance technologies, and data-driven private platforms has created new forms of privacy vulnerability that were not fully anticipated within traditional legal frameworks. As a result, the protection of privacy today depends not only on judicial interpretation but also on the effectiveness of administrative institutions, regulatory design, and technological safeguards.

A comparative perspective further highlights India's transitional position in global privacy governance. Jurisdictions such as the European Union have developed comprehensive and enforceable regulatory ecosystems through instruments like the GDPR, supported by strong independent supervisory authorities and clearly defined individual rights. In contrast, India's framework, while constitutionally robust after *Puttaswamy*, remains in an evolving stage of institutional development. The Digital Personal Data Protection Act, 2023 represents an important legislative milestone in this direction, introducing principles of consent-based processing and data fiduciary accountability. However, its effectiveness is constrained by concerns regarding broad state exemptions, limited algorithmic regulation, and questions surrounding the independence and capacity of the Data Protection Board.

The analysis also demonstrates that contemporary privacy protection cannot be achieved solely through statutory enactments. Instead, it requires a multi-dimensional governance structure that integrates constitutional interpretation, legislative precision, institutional independence, and technological regulation. In particular, the growing influence of artificial intelligence, biometric surveillance, and data-driven behavioural profiling necessitates stronger mechanisms of transparency and accountability to ensure that technological advancement does not undermine constitutional liberties.

Ultimately, the future of privacy in India will depend on the development of a robust and adaptive regulatory ecosystem capable of responding to rapidly evolving digital realities. This includes the strengthening of independent regulatory institutions, continued judicial vigilance in applying the proportionality doctrine, and the introduction of clear standards for algorithmic accountability and data governance. Equally important is the need for global cooperation and harmonization of data protection standards, given the inherently cross-border nature of digital data flows.

In conclusion, privacy in the digital constitutional order is no longer merely a legal entitlement but a foundational requirement for preserving democratic values in a data-driven society. Only through a coordinated and multi-layered approach—combining constitutional interpretation, institutional strength, technological safeguards, and international alignment—can India fully realize the promise of *Puttaswamy* and ensure meaningful protection of individual autonomy in the digital age.

*****

 [ISSN 2581-9453]