JURIS NEXUS: JOURNAL OF LAW & MULTIDISCIPLINARY STUDIES
(An Online Referred Peer-Reviewed Journal)
ISSN: XXXX-XXXX I PIF: X.XX I VOL. 01 I Mar. I 2026
Website – www.JNJLMS.com Emai Id - contact@JNJLMS.com

RIGHT TO PRIVACY IN THE DIGITAL AGE: EVOLVING CONSTITUTIONAL PROTECTIONS AND EMERGING DIGITAL RIGHTS IN INDIA

Shruti Kapoor
Research Scholar, Faculty of Law, Banaras Hindu University, Varanasi.
Sachin Singh
Assistant Professor at Department of Law, B.S.A. P.G. College, Mathura

ABSTRACT

The rapid expansion of digital technologies has fundamentally transformed the contours of the right to privacy, necessitating a re-evaluation of traditional legal frameworks. In India, the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India marked a constitutional milestone, yet its application in the digital ecosystem remains complex and evolving. This article critically examines the intersection between the right to privacy and emerging digital rights, focusing on data protection, informational self-determination, surveillance, and platform governance. The study analyses key legislative developments, including the Digital Personal Data Protection Act, 2023, and explores global standards such as the GDPR to assess India's regulatory position. It further evaluates challenges posed by artificial intelligence, big data analytics, and state surveillance practices. Through doctrinal and comparative analysis, the article highlights gaps in enforcement, issues of consent, and the tension between national security and individual liberties. The article argues for a rights-based, technology-sensitive legal framework that balances innovation with constitutional safeguards. It concludes by proposing reforms aimed at strengthening accountability, enhancing data subject rights, and ensuring robust judicial oversight in the digital age.

KEYWODRS: *Artificial Intelligence, Fundamental Right, Digital Technologies, The Digital Personal Data Protection Act, 2023, Digital Age and etc.*

INTRODUCTION

The right to privacy has emerged as one of the most significant constitutional and human rights concerns in the digital age, where personal data has become a central element of economic, social, and political interactions. Traditionally understood as the "right to be let alone," privacy has evolved beyond its classical conception to encompass informational autonomy and control

over personal data in an increasingly digitized environment.[1] The proliferation of digital technologies, including artificial intelligence, big data analytics, and ubiquitous internet connectivity, has intensified concerns regarding the collection, processing, and dissemination of personal information by both state and non-state actors.[2]

In India, the recognition of privacy as a fundamental right under Article 21 of the Constitution in *Justice K.S. Puttaswamy v. Union of India* marked a transformative moment in constitutional jurisprudence.[3] The Supreme Court unequivocally affirmed that privacy is intrinsic to life and personal liberty and is essential for the protection of dignity, autonomy, and individual choice. However, while *Puttaswamy* laid down a robust constitutional foundation, the practical realization of privacy in the digital ecosystem continues to face significant challenges, particularly in the context of mass surveillance, data breaches, and the expanding powers of digital intermediaries.[4]

The emergence of "digital rights" as an extension of traditional human rights further complicates the legal landscape. Digital rights encompass a broad spectrum of entitlements, including the right to data protection, the right to be forgotten, and the right to secure and equitable access to digital infrastructure.[5] These rights are increasingly recognized as indispensable in ensuring meaningful participation in the digital society. However, their enforcement remains fragmented, particularly in jurisdictions like India, where regulatory frameworks are still evolving.

The enactment of the Digital Personal Data Protection Act, 2023 represents a significant legislative step toward addressing data privacy concerns in India. Nevertheless, concerns persist regarding its effectiveness, especially in light of broad exemptions granted to the State and the absence of a fully independent regulatory authority.[6] At the same time, global developments such

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 193 (1890).
[2] Shoshana Zuboff, *The Age of Surveillance Capitalism* 8-12 (2019).
[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[4] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* 180-85 (2019).
[5] United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/RES/34/7 (Mar. 23, 2017).
[6] Digital Personal Data Protection Act, No. 22 of 2023, §§ 7, 17 (India).

as the European Union's General Data Protection Regulation (GDPR) have set higher standards for data protection, thereby influencing domestic legal reforms and policy debates.[7]

This article seeks to critically examine the intersection between the right to privacy and digital rights in the Indian context. It aims to analyze whether existing legal frameworks adequately safeguard individual privacy in the face of rapid technological advancements. The study adopts a doctrinal and comparative methodology, drawing upon constitutional jurisprudence, statutory frameworks, and international standards. It further evaluates emerging challenges such as algorithmic governance, data monopolies, and state surveillance practices.

The central argument of this article is that while India has made significant progress in recognizing privacy as a fundamental right, there remains a considerable gap between constitutional ideals and regulatory realities. Bridging this gap requires a comprehensive, rights-based, and technologically informed legal framework that balances innovation with individual liberties.

CONCEPTUAL FRAMEWORK OF PRIVACY AND DIGITAL RIGHTS

Privacy, as a legal and philosophical concept, has undergone significant transformation over time. Initially conceptualized as the "right to be let alone," it has evolved into a multifaceted right encompassing several dimensions, including physical, decisional, and informational privacy.[8] Physical privacy relates to bodily integrity and protection against intrusive searches, while decisional privacy safeguards personal choices such as reproductive autonomy and family life. Informational privacy, however, has gained paramount importance in the digital era, where vast amounts of personal data are continuously collected, processed, and shared.[9]

The notion of informational privacy is closely linked to the concept of "informational self-determination," which originated in German constitutional jurisprudence and emphasizes an

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[8] Alan F. Westin, *Privacy and Freedom* 7 (1967).
[9] Daniel J. Solove, *Understanding Privacy* 102-10 (2008).

individual's right to control the disclosure and use of personal data.[10] This principle recognizes that unchecked data processing can lead to profiling, surveillance, and manipulation, thereby undermining individual autonomy and democratic participation. In the Indian context, the Supreme Court in *Puttaswamy* acknowledged informational privacy as a core component of the right to privacy, particularly in relation to data protection and digital identity systems.[11]

a. Digital Rights: An Emerging Jurisprudence

Digital rights have emerged as an extension of traditional human rights in response to the growing influence of digital technologies. These rights are not entirely new but represent the adaptation of existing rights such as freedom of expression, privacy, and access to information to the digital environment.[12] Among the most prominent digital rights is the right to data protection, which ensures that individuals have control over their personal information and are protected against misuse by both public and private entities.

Another significant dimension is the "right to be forgotten," which allows individuals to seek the removal of personal information from digital platforms under certain circumstances.[13] This right reflects the need to balance privacy with the public's right to information in an era of permanent digital memory. Additionally, the recognition of access to the internet as a fundamental right in certain jurisdictions underscores the importance of digital inclusion as a prerequisite for the exercise of other rights.[14]

The rise of artificial intelligence and algorithmic decision-making has further expanded the scope of digital rights to include protection against automated profiling and algorithmic bias. These developments highlight the necessity of ensuring transparency, accountability, and fairness in digital governance frameworks.[15]

[10] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1 (Ger.).
[11] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, pp 297-98 (India).
[12] Molly Land, Toward an International Law of the Internet, 54 Harv. Int'l L.J. 393, 398-402 (2013).
[13] Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, 2014 E.C.R. I-317.
[14] *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637 (India).
[15] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3-15 (2015).

b. Relationship between Privacy and Digital Rights

The relationship between privacy and digital rights is both foundational and symbiotic. Privacy serves as the bedrock upon which many digital rights are constructed, particularly those relating to data protection and informational autonomy. Without robust privacy protections, digital rights risk becoming ineffective, as individuals would lack meaningful control over their personal data and digital identities.[16]

At the same time, digital rights extend and reinforce privacy by addressing new challenges posed by technological advancements. For instance, data protection laws operationalize the right to privacy by establishing mechanisms for consent, accountability, and redress. Similarly, rights related to cyber security and protection from surveillance contribute to safeguarding privacy in the digital domain.[17]

However, tensions often arise between privacy and other competing interests, such as national security, public order, and economic innovation. The challenge lies in achieving a balance that preserves the essence of privacy while accommodating legitimate state and commercial interests. The proportionality framework articulated in *Puttaswamy* provides a useful tool for resolving such conflicts, emphasizing legality, necessity, and proportionality as guiding principles.[18]

In sum, the conceptual framework of privacy and digital rights reflects an evolving legal landscape shaped by technological change and normative developments. Understanding this framework is essential for assessing the adequacy of existing legal protections and for formulating effective regulatory responses in the digital age.

CONSTITUTIONAL RECOGNITION OF THE RIGHT TO PRIVACY IN INDIA

The constitutional journey of the right to privacy in India reflects a gradual but profound evolution from judicial skepticism to unequivocal recognition as a fundamental right. Initially,

[16] Orla Lynskey, *The Foundations of EU Data Protection Law* 45-50 (2015).
[17] Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814, 1820-25 (2011).
[18] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶ 325 (India).

the Indian Constitution did not explicitly guarantee a right to privacy, and early judicial interpretations were reluctant to read such a right into Part III. In *M.P. Sharma v. Satish Chandra*, the Supreme Court held that the Constitution did not recognize a general right to privacy, particularly in the context of search and seizure under criminal law.[19] Similarly, in *Kharak Singh v. State of Uttar Pradesh*, the majority opinion rejected the existence of a constitutional right to privacy, although Justice Subba Rao's dissent laid the foundation for its future recognition by emphasizing personal liberty and dignity.[20]

Despite these early limitations, subsequent judicial developments gradually expanded the scope of Article 21 of the Constitution. The Court began to interpret the "right to life and personal liberty" in a more expansive manner, incorporating various derivative rights essential for a dignified existence. In cases such as *Gobind v. State of Madhya Pradesh* and *R. Rajagopal v. State of Tamil Nadu*, the Court acknowledged privacy interests in specific contexts, including surveillance and protection against unauthorized publication of personal information.[21] These decisions marked a shift toward recognizing privacy as an implicit constitutional value, albeit without a definitive articulation of its status as a fundamental right.

The constitutional position was conclusively settled in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where a nine-judge bench of the Supreme Court unanimously affirmed that the right to privacy is a fundamental right protected under Article 21 and other facets of Part III.[22] The Court overruled the earlier decisions in *M.P. Sharma* and *Kharak Singh* to the extent that they denied the existence of a constitutional right to privacy. It held that privacy is intrinsic to life and personal liberty and is essential for the realization of dignity, autonomy, and individual freedom.

A significant contribution of the *Puttaswamy* judgment lies in its articulation of the normative foundations of privacy. The Court recognized privacy as encompassing multiple dimensions, including bodily privacy, informational privacy, and decisional autonomy.[23] Importantly, the

[19] *M.P. Sharma v. Satish Chandra*, A.I.R. 1954 S.C. 300, 302 (India).
[20] *Kharak Singh v. State of Uttar Pradesh*, A.I.R. 1963 S.C. 1295, 1305 (India) (Subba Rao, J., dissenting).
[21] *Gobind v. State of Madhya Pradesh*, (1975) 2 S.C.C. 148, 155-56 (India); *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 S.C.C. 632, 649 (India).
[22] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, pp 3, 180 (India).
[23] Id. pp 248-49.

judgment emphasized informational privacy in the context of the digital age, acknowledging the risks posed by data collection, profiling, and surveillance. The Court also underscored the need for a robust data protection regime to safeguard individual interests against both state and non-state actors.

Furthermore, *Puttaswamy* introduced a structured proportionality test to evaluate restrictions on the right to privacy. According to this framework, any infringement of privacy must satisfy four key requirements:

(i) legality, which mandates the existence of a valid law;
(ii) legitimate state aim;
(iii) necessity, ensuring a rational nexus between the means and the objective; and
(iv) proportionality, which requires that the measure adopted is the least restrictive alternative.[24]

This test has since become a cornerstone in adjudicating privacy-related disputes in India.

Post-*Puttaswamy*, the Supreme Court has continued to develop privacy jurisprudence in various contexts. In *Aadhaar (K.S. Puttaswamy v. Union of India, 2018)*, the Court upheld the constitutional validity of the Aadhaar scheme but imposed limitations to ensure data protection and prevent misuse.[25] Similarly, in *Anuradha Bhasin v. Union of India*, the Court recognized the importance of internet access for the exercise of fundamental rights, thereby indirectly reinforcing the digital dimension of privacy and liberty.[26]

Despite these advancements, challenges remain in translating constitutional principles into effective legal protections. The absence of a comprehensive and consistently enforced data protection framework, coupled with increasing state surveillance capabilities, raises concerns about the practical realization of privacy rights. Moreover, the tension between privacy and competing interests such as national security and technological innovation continues to test the boundaries of constitutional interpretation.

[24] Id. 325.
[25] *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 S.C.C. 1, pp 447-48 (India).
[26] *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637, pp 68-70 (India).

In essence, the recognition of privacy as a fundamental right marks a transformative shift in Indian constitutional law. However, its effectiveness ultimately depends on the development of coherent legal frameworks and vigilant judicial oversight to address the complexities of the digital age.

LEGAL FRAMEWORK GOVERNING DIGITAL PRIVACY IN INDIA

The recognition of privacy as a fundamental right in *Puttaswamy* necessitated the development of a comprehensive statutory framework to regulate the collection, processing, and protection of personal data. In response, India has gradually evolved a multi-layered legal regime comprising the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and various sector-specific regulations. However, despite these developments, concerns persist regarding the adequacy, coherence, and enforcement of these legal mechanisms.

a. Digital Personal Data Protection Act, 2023

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant step toward establishing a dedicated data protection regime in India.[27] The Act seeks to regulate the processing of digital personal data while balancing the rights of individuals with the legitimate interests of the State and private entities. It introduces key concepts such as "data principal" and "data fiduciary," thereby aligning Indian law with global data protection terminology.

One of the central features of the DPDP Act is its emphasis on consent-based data processing. Section 6 of the Act mandates that personal data may be processed only for lawful purposes upon obtaining free, informed, specific, and unambiguous consent from the data principal.[28] Additionally, the Act provides certain rights to individuals, including the right to access information about data processing, the right to correction and erasure, and the right to grievance redressal.[29] These provisions reflect an attempt to operationalize informational privacy in line with constitutional principles articulated in *Puttaswamy*.

[27] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[28] Id. § 6.
[29] Id. §§ 11-14.

However, the DPDP Act has been subject to significant criticism. A major concern relates to the broad exemptions granted to the State under Section 17, which permit the processing of personal data for purposes such as national security, public order, and prevention of offenses without stringent safeguards.[30] Such provisions raise questions about the potential for excessive state surveillance and the dilution of privacy protections. Furthermore, the absence of a fully independent Data Protection Board, coupled with extensive rule-making powers vested in the executive, has led to concerns regarding regulatory independence and accountability.

b. Information Technology Act, 2000 and Allied Rules

Prior to the DPDP Act, the primary legal framework governing data protection in India was the Information Technology Act, 2000 (IT Act) and the rules framed thereunder. Section 43A of the IT Act imposes liability on body corporates for negligence in implementing reasonable security practices and procedures in handling sensitive personal data.[31] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) further elaborate on the obligations of entities collecting and processing personal data.

While these provisions provided an initial framework for data protection, they suffer from several limitations. The SPDI Rules apply only to body corporates and do not cover government agencies, thereby creating a regulatory gap. Moreover, the definition of "sensitive personal data" is narrow and outdated, failing to adequately address contemporary issues such as biometric data, behavioral data, and metadata generated through digital interactions.[32] As a result, the IT Act regime has been widely regarded as insufficient to address the complexities of modern data processing practices.

c. Intermediary Regulations and Platform Governance

The role of digital intermediaries, including social media platforms and online service providers, has become increasingly significant in the context of digital privacy. The Information

[30] Id. 17.
[31] Information Technology Act, No. 21 of 2000, § 43A (India).
[32] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence obligations on intermediaries, including requirements for content moderation, user grievance redressal, and traceability of messages in certain cases.[33]

While these rules aim to enhance accountability, they have also raised concerns regarding privacy and freedom of expression. The requirement of traceability, particularly for encrypted messaging platforms, has been criticized for potentially undermining end-to-end encryption and exposing users to surveillance risks.[34] This highlights the ongoing tension between regulatory objectives and fundamental rights in the digital ecosystem.

d. Sectoral Regulations

In addition to general data protection laws, various sectoral regulators have issued guidelines addressing privacy and data protection concerns. For instance, the Reserve Bank of India (RBI) has introduced data localization requirements for payment systems, while the Telecom Regulatory Authority of India (TRAI) has issued recommendations on data ownership and privacy in the telecommunications sector.[35] These sector-specific measures reflect an increasing recognition of the importance of data protection across different domains.

However, the multiplicity of regulatory frameworks has led to fragmentation and inconsistency. The lack of a unified approach to data protection creates compliance challenges for businesses and undermines the effectiveness of privacy safeguards. This underscores the need for greater harmonization and coordination among regulatory authorities.

Despite the progress made through the DPDP Act and related regulations, India's legal framework for digital privacy remains a work in progress. Key concerns include the concentration of regulatory power in the executive, insufficient safeguards against state surveillance, and limited enforcement mechanisms. Additionally, the emphasis on consent as the

[33] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).
[34] Internet Freedom Foundation, *Analysis of the Information Technology (Intermediary Guidelines) Rules, 2021* (2021).
[35] Telecom Regulatory Authority of India, *Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector* (July 16, 2018); Reserve Bank of India, *Storage of Payment System Data*, RBI/2017-18/153 (Apr. 6, 2018).

primary basis for data processing may not adequately address issues such as information asymmetry and the lack of meaningful choice for users in digital environments.

COMPARATIVE PERSPECTIVE: GLOBAL STANDARDS ON DIGITAL PRIVACY

The evolution of digital privacy law across jurisdictions reflects differing regulatory philosophies, institutional capacities, and socio-political priorities. A comparative analysis of global frameworks particularly the European Union (EU) and the United States (US) provides valuable insights into the strengths and limitations of India's emerging data protection regime.

a. European Union: The GDPR Model

The European Union's General Data Protection Regulation (GDPR) is widely regarded as the global benchmark for data protection law.[36] It establishes a comprehensive and rights-based framework governing the processing of personal data, grounded in principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, and accountability.[37] The GDPR provides robust rights to data subjects, including the right to access, rectification, erasure (right to be forgotten), restriction of processing, and data portability.[38]

A distinctive feature of the GDPR is its emphasis on accountability and enforcement. Data controllers and processors are required to implement appropriate technical and organizational measures to ensure compliance, and supervisory authorities are empowered to impose substantial penalties for violations.[39] Additionally, the GDPR applies extraterritorially, covering entities outside the EU that process the data of EU residents, thereby extending its global influence.[40]

The GDPR also incorporates safeguards against automated decision-making and profiling, requiring transparency and human oversight in algorithmic processes.[41] This aspect is particularly relevant in the age of artificial intelligence, where decisions affecting individuals are increasingly made by automated systems.

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[37] Id. art. 5.
[38] Id. arts. 12-22.
[39] Id. arts. 24, 83.
[40] Id. art. 3.
[41] Id. art. 22.

b. United States: Sectoral and Market-Oriented Approach

In contrast to the EU's comprehensive framework, the United States follows a fragmented, sector-specific approach to data protection. Privacy regulation in the US is governed by a combination of federal and state laws, such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the California Consumer Privacy Act (CCPA) for consumer data.[42]

The US model is largely market-driven and emphasizes consumer protection rather than a fundamental rights-based approach. While recent developments, including the California Privacy Rights Act (CPRA), have strengthened individual rights, the absence of a unified federal data protection law creates inconsistencies and regulatory gaps.[43]

Moreover, the US framework places significant reliance on self-regulation and corporate compliance, which has been criticized for inadequately addressing issues such as data monopolies and surveillance capitalism.[44] Nevertheless, the US approach is often seen as more conducive to innovation and technological growth, highlighting the trade-offs between regulation and economic development.

c. Lessons for India

India's data protection framework, particularly under the Digital Personal Data Protection Act, 2023, reflects elements of both the EU and US models but does not fully align with either. While the DPDP Act adopts certain GDPR-inspired concepts, such as consent-based processing and data subject rights, it lacks the same level of regulatory independence and enforcement rigor.[45]

One key lesson from the GDPR is the importance of a strong, independent supervisory authority to ensure effective enforcement. India's current framework, which vests significant powers in the executive, may undermine regulatory autonomy and accountability. Additionally, the GDPR's

[42] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199.
[43] California Privacy Rights Act of 2020, Cal. Civ. Code §§ 1798.100-1798.199 (as amended).
[44] Shoshana Zuboff, *The Age of Surveillance Capitalism* 93-100 (2019).
[45] Digital Personal Data Protection Act, No. 22 of 2023 (India).

emphasis on transparency and purpose limitation could inform improvements in India's consent mechanisms, which often suffer from opacity and information asymmetry.

From the US model, India can draw insights into fostering innovation and maintaining regulatory flexibility. However, excessive reliance on market mechanisms without adequate safeguards may lead to exploitation of personal data and erosion of privacy rights. Therefore, a balanced approach that integrates rights-based protections with innovation-friendly policies is essential.

The comparative analysis underscores that there is no one-size-fits-all model for data protection. Each jurisdiction must tailor its legal framework to its constitutional values, institutional structures, and socio-economic context. For India, the challenge lies in developing a coherent and effective data protection regime that upholds the fundamental right to privacy while accommodating the demands of a rapidly evolving digital economy.

KEY CHALLENGES IN PROTECTING DIGITAL PRIVACY

Despite the constitutional recognition of privacy as a fundamental right and the enactment of statutory frameworks such as the Digital Personal Data Protection Act, 2023, the effective protection of digital privacy in India continues to face significant challenges. These challenges arise from the increasing complexity of technological ecosystems, the expanding role of state and corporate actors, and structural limitations in regulatory enforcement.

a. State Surveillance vs. Individual Privacy

One of the most pressing concerns in the digital age is the tension between state surveillance and individual privacy. Governments increasingly rely on digital technologies for purposes such as national security, law enforcement, and governance. While such measures may be justified on legitimate grounds, they often risk encroaching upon fundamental rights if not subject to adequate safeguards.

In India, controversies surrounding programs such as Aadhaar and allegations of spyware usage, including the Pegasus surveillance scandal, have raised serious concerns regarding unauthorized

intrusion into personal privacy.[46] The absence of a comprehensive surveillance law, coupled with broad statutory powers under legislations such as the Information Technology Act, 2000 and the Telegraph Act, 1885, creates the potential for misuse and arbitrary state action.[47]

The Supreme Court in *Puttaswamy* emphasized that any infringement of privacy must satisfy the test of legality, necessity, and proportionality.[48] However, in practice, the lack of transparency and judicial oversight in surveillance mechanisms undermines the effective application of this standard. This highlights the urgent need for a robust legal framework governing surveillance activities.

b. Big Tech and Data Exploitation

The dominance of large technology companies has transformed personal data into a valuable economic resource. Corporations routinely collect, analyze, and monetize user data, often without meaningful consent or awareness. This phenomenon, described as "surveillance capitalism," raises concerns about exploitation, manipulation, and erosion of individual autonomy.[49]

Users frequently consent to data collection through complex and opaque privacy policies, leading to what scholars describe as the "consent paradox," where formal consent exists without genuine understanding.[50] Moreover, the concentration of data in the hands of a few corporations creates asymmetries of power, enabling targeted advertising, behavioral profiling, and even political influence.

The existing legal framework in India struggles to address these challenges effectively. While the DPDP Act emphasizes consent and accountability, it does not adequately tackle issues such as data monopolies, cross-border data flows, and algorithmic transparency. This underscores the

[46] *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 S.C.C. 1 (India); see also N. Ram et al., *The Pegasus Project*, Forbidden Stories (2021).
[47] Indian Telegraph Act, No. 13 of 1885, § 5(2) (India); Information Technology Act, No. 21 of 2000, § 69 (India).
[48] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶ 325 (India).
[49] Shoshana Zuboff, *The Age of Surveillance Capitalism* 8-12 (2019).
[50] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880, 1883-85 (2013).

need for stronger regulatory mechanisms to ensure corporate accountability and protect user interests.

c. Artificial Intelligence and Privacy Risks

The rapid adoption of artificial intelligence (AI) and machine learning technologies has introduced new dimensions to privacy concerns. AI systems rely on large datasets for training and decision-making, often involving the processing of sensitive personal information. This raises issues related to data security, algorithmic bias, and lack of transparency.

Automated decision-making processes can significantly impact individuals, particularly in areas such as credit scoring, employment, and law enforcement. The opacity of AI systems often referred to as the "black box" problem makes it difficult to assess whether decisions are fair, accurate, or discriminatory.[51] Furthermore, facial recognition technologies and predictive policing tools pose serious risks to civil liberties and may lead to mass surveillance.

Although global frameworks such as the GDPR incorporate safeguards against automated decision-making, India's legal regime lacks comprehensive provisions addressing AI-specific privacy concerns. This regulatory gap highlights the need for a forward-looking approach that integrates privacy protections into the design and deployment of emerging technologies.

d. Enforcement and Institutional Weaknesses

A critical challenge in the protection of digital privacy is the lack of effective enforcement mechanisms. Even where legal provisions exist, their implementation is often hindered by institutional limitations, resource constraints, and lack of technical expertise.

The DPDP Act establishes a Data Protection Board to oversee compliance and adjudicate disputes. However, concerns have been raised regarding its independence and capacity, given that its composition and functioning are significantly influenced by the executive.[52] This raises questions about the impartiality and effectiveness of regulatory oversight.

[51] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3-15 (2015).
[52] Digital Personal Data Protection Act, No. 22 of 2023, § 18 (India).

Additionally, the absence of a strong culture of compliance among organizations further exacerbates enforcement challenges. Data breaches and privacy violations often go unreported or inadequately addressed, leaving individuals with limited avenues for redress. The lack of awareness among users regarding their digital rights also contributes to the weak enforcement of

e. Structural and Socio-Economic Challenges

Beyond legal and institutional issues, broader structural factors also impact the protection of digital privacy in India. The digital divide, characterized by unequal access to technology and varying levels of digital literacy, affects individuals' ability to understand and exercise their rights.[53] Vulnerable populations are particularly at risk of exploitation due to limited awareness and bargaining power.

Moreover, the rapid pace of technological innovation often outstrips the development of legal frameworks, resulting in regulatory lag. This creates a dynamic where laws struggle to keep up with emerging risks, leaving gaps in protection. Addressing these challenges requires not only legal reforms but also investments in digital literacy, institutional capacity, and public awareness.

The challenges outlined above demonstrate that the protection of digital privacy is not merely a legal issue but a complex, multidimensional problem requiring coordinated efforts across legal, technological, and institutional domains. While India has made significant progress in recognizing privacy as a fundamental right, the effectiveness of this right depends on its practical enforcement in an increasingly data-driven society.

EMERGING ISSUES IN DIGITAL RIGHTS

The rapid evolution of digital technologies has given rise to new and complex issues that extend beyond traditional notions of privacy and data protection. These emerging concerns reflect the dynamic nature of digital rights and underscore the need for adaptive legal and regulatory frameworks capable of addressing novel challenges.

[53] United Nations Development Programme, *Human Development Report 2021-22* (2022).

a. Right to Be Forgotten

The "right to be forgotten" has gained prominence as an essential component of digital privacy, enabling individuals to seek the removal of personal information from online platforms under certain circumstances. This right seeks to address the problem of perpetual digital memory, where personal data, once published, remains accessible indefinitely, potentially affecting an individual's reputation and dignity.[54]

In India, the recognition of this right remains nascent and largely judicially driven. Courts have, in certain cases, acknowledged the need to balance the right to privacy with the right to freedom of speech and expression, particularly in the context of online content.[55] However, the absence of explicit statutory provisions in the Digital Personal Data Protection Act, 2023 creates ambiguity regarding the scope and enforceability of this right. This highlights the need for a clearer legal framework to reconcile competing interests.

b. Data Localization And Cross-Border Data Flows

Data localization has emerged as a significant policy issue in India, driven by concerns related to national security, data sovereignty, and regulatory control. Localization mandates require certain categories of data to be stored and processed within the territorial boundaries of the country.[56]

While such measures may enhance governmental access and oversight, they also raise concerns regarding increased surveillance, trade barriers, and the fragmentation of the global internet. Critics argue that excessive localization may hinder innovation and increase compliance costs for businesses, particularly in a globalized digital economy.[57]

The DPDP Act adopts a relatively flexible approach by allowing cross-border data transfers to notified countries, reflecting a shift toward balancing sovereignty concerns with economic considerations. Nevertheless, the lack of clarity regarding the criteria for such transfers remains a point of concern.

[54] Jeffrey Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88, 88-92 (2012).
[55] *X v. Registrar General, High Court of Karnataka*, 2021 SCC OnLine Kar 424 (India).
[56] Reserve Bank of India, *Storage of Payment System Data*, RBI/2017-18/153 (Apr. 6, 2018).
[57] Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677, 682-85 (2015).

c. Cyber security and Privacy Intersection

The relationship between cyber security and privacy is increasingly significant in the digital age. While cyber security measures are essential for protecting data from unauthorized access and breaches, they can also conflict with privacy rights if implemented without adequate safeguards.

For instance, measures such as mass data retention, surveillance systems, and intrusive security protocols may compromise individual privacy in the name of security.[58] At the same time, inadequate cyber security frameworks can expose individuals to risks such as identity theft, financial fraud, and data breaches.

In India, the absence of a comprehensive cybersecurity law, coupled with fragmented regulatory measures, limits the effectiveness of both privacy protection and data security. This underscores the need for an integrated approach that harmonizes privacy and cybersecurity objectives.

d. Digital Divide and Inequality

The digital divide remains a critical issue affecting the realization of digital rights. Unequal access to technology, internet connectivity, and digital literacy creates disparities in individuals' ability to exercise their rights effectively. In developing countries like India, marginalized communities often face significant barriers to accessing digital resources, thereby exacerbating existing socio-economic inequalities.[59]

The recognition of internet access as integral to the exercise of fundamental rights in *Anuradha Bhasin v. Union of India*[60] underscores the importance of digital inclusion. However, ensuring equitable access requires sustained policy interventions, infrastructure development, and public awareness initiatives.

e. Emerging Technologies and Future Risks

Emerging technologies such as block chain, the Internet of Things (IoT), and generative artificial intelligence present new challenges for digital rights. These technologies often operate in decentralized and data-intensive environments, complicating issues of accountability, consent,

[58] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* 15-20 (2015).
[59] World Bank, *World Development Report 2021: Data for Better Lives* (2021).
[60] *Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637, pp 68-70 (India).

and data control. For example, IoT devices continuously collect and transmit data, often without explicit user awareness, raising concerns about pervasive surveillance. Similarly, generative AI systems can process and reproduce personal data in ways that are difficult to regulate, posing risks to privacy and intellectual property rights.[61]

The existing legal framework in India is not fully equipped to address these emerging risks, highlighting the need for proactive and technology-neutral regulation. Policymakers must anticipate future challenges and design flexible frameworks that can adapt to evolving technological landscapes. The emerging issues in digital rights demonstrate that privacy is no longer a static concept but a dynamic and evolving right shaped by technological innovation. Addressing these issues requires a forward-looking approach that goes beyond traditional legal doctrines and incorporates interdisciplinary perspectives.

A key challenge lies in balancing competing interests privacy, innovation, security, and economic growth without compromising constitutional values. The development of a coherent and adaptive legal framework, supported by strong institutional mechanisms and public awareness, is essential to ensure that digital rights are effectively protected in the years to come.

CONCLUSION

The recognition of the right to privacy as a fundamental right marks a defining moment in India's constitutional and digital jurisprudence. Through its landmark decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court firmly established privacy as intrinsic to dignity, liberty, and autonomy, thereby laying a robust normative foundation for the protection of individual rights in the digital age.^80 However, as this article has demonstrated, the journey from constitutional recognition to effective realization remains incomplete.

The emergence of digital technologies has fundamentally altered the nature of privacy, transforming it from a predominantly physical concept into one deeply embedded in data, algorithms, and networked systems. In this context, digital rights such as data protection, informational self-determination, and the right to be forgotten have become indispensable for

[61] Frank Pasquale, *The Black Box Society* 218-25 (2015).

safeguarding individual autonomy. While legislative initiatives like the Digital Personal Data Protection Act, 2023 represent important steps forward, they fall short in addressing critical concerns related to state surveillance, regulatory independence, and corporate accountability. A central challenge lies in reconciling competing interests: the need for national security and technological innovation on one hand, and the protection of fundamental rights on the other. The proportionality framework articulated in *Puttaswamy* provides a valuable constitutional tool for navigating this tension, but its effective application requires strong institutional mechanisms, transparent governance, and vigilant judicial oversight. Furthermore, the comparative analysis of global frameworks underscores the importance of adopting a balanced and context-specific approach. While the European Union's rights-based model offers valuable lessons in terms of accountability and enforcement, and the United States' market-oriented approach highlights the importance of innovation, India must chart its own path that aligns with its constitutional values and socio-economic realities.

Ultimately, the protection of privacy and digital rights cannot be achieved through legal reforms alone. It requires a holistic strategy encompassing institutional strengthening, technological accountability, public awareness, and international cooperation. As digital technologies continue to evolve, the law must remain dynamic and responsive, ensuring that fundamental rights are not eroded in the face of rapid innovation.

In conclusion, the future of privacy in India depends on the development of a coherent, rights-based digital governance framework that bridges the gap between constitutional ideals and regulatory practice. Only through such an approach can the promise of privacy as a fundamental right be meaningfully realized in the digital era.