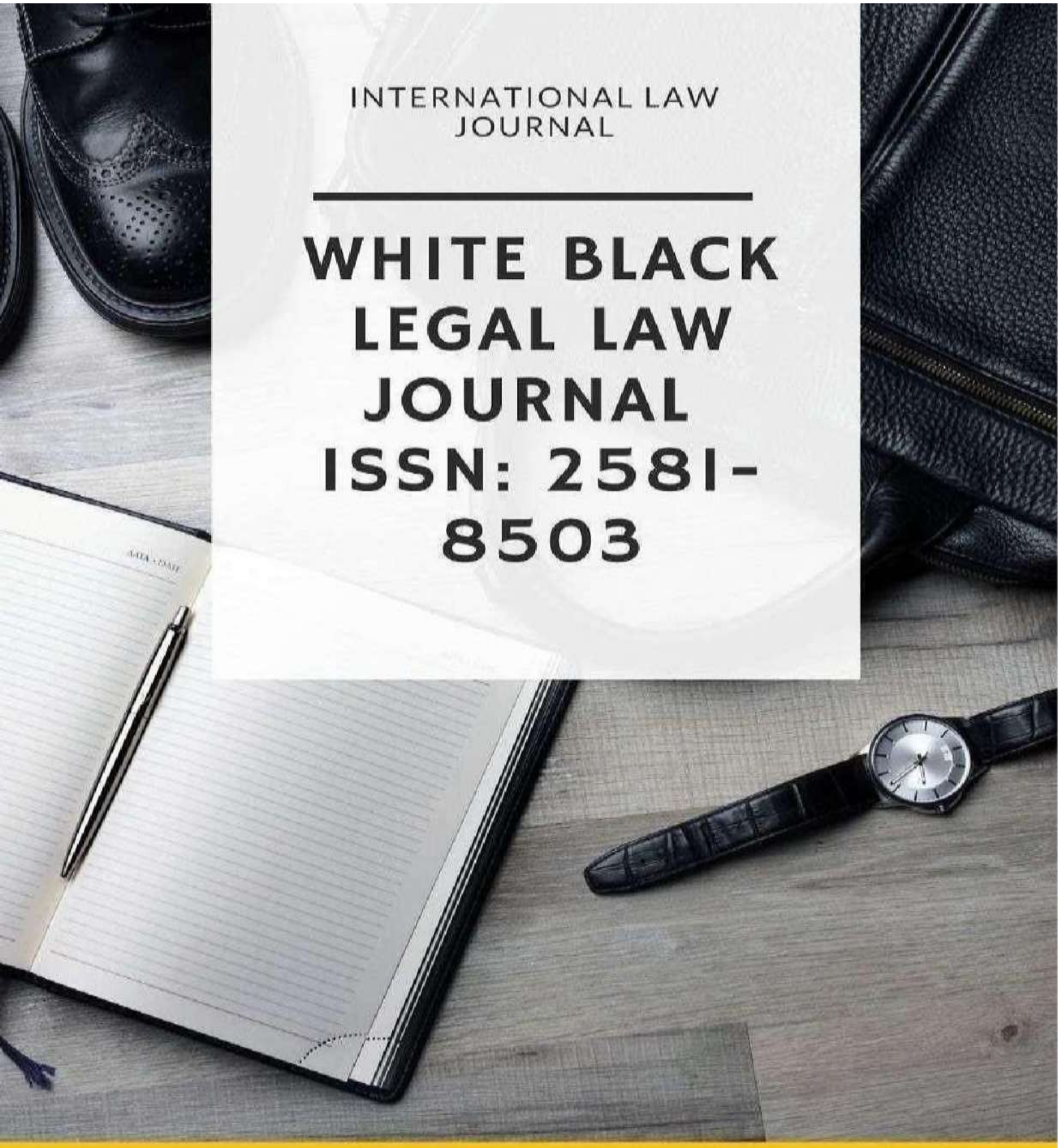


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 6 | April 2026 ISSN: 2581-8503

CONSENT FATIGUE AND LEGAL GAPS: A CRITICAL STUDY OF PRIVACY SAFEGUARDS IN INDIA

AUTHORED BY - SUKHSAGAR MISRA & RIDDHI TRIPATHI
Faculty of Juridical Sciences, Rama University, Kanpur, India

Abstract

India's digital ecosystem has experienced rapid expansion, accompanied by growing dependence on technologies powered by data. The DPDP Act, 2023 represents a significant legislative effort to regulate personal data processing through a consent-based framework. However, the effectiveness of this model is undermined by consent fatigue is a situation in which people are overwhelmed by repetitive and complex consent requests, resulting in uninformed decision-making. This paper critically examines the limitations of consent-centric privacy protection in India and identifies key legal and institutional gaps within the existing framework. Drawing upon constitutional jurisprudence, particularly the landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the study argues for a shift toward accountability-based and design-oriented privacy safeguards. The paper concludes by proposing reforms to strengthen India's data security laws in a manner that ensures meaningful user autonomy and robust enforcement.

Keywords: consent fatigue, data protection, privacy law, India, DPDP Act, Puttaswamy, digital governance.

1. Introduction

The growth of India's digital infrastructure has transformed personal data into a central component of economic and administrative systems. Digital platforms, e-governance initiatives, and artificial intelligence applications increasingly depend on the gathering and handling of personal data. The legislature created a statutory framework for data governance in response to these advances by passing the Digital Personal Data Protection Act, 2023.

A key feature of this framework is its reliance on user the main legal foundation for data processing is consent. Although consent has historically been seen as a mechanism for

protecting individual autonomy, its practical application in complex digital environments raises serious concerns. Users are frequently required to engage with lengthy privacy policies and repetitive consent requests, often leading to mechanical acceptance rather than informed choice.

This research paper looks at the limitations of consent-based privacy regulation in India, focusing on the concept of consent fatigue and the existence of legal gaps within the current framework. It further situates these issues in the larger constitutional framework of the right to privacy.

2. India's Constitutional Basis for Privacy

The constitutional one of the biggest developments in India is the acknowledgment of privacy in fundamental rights jurisprudence. Unlike some jurisdictions where privacy is explicitly guaranteed, a "right to privacy" is not specifically mentioned in the Indian Constitution. Instead, this right has emerged through judicial interpretation, particularly under Article 21, which protects individual liberty and the right to life. The judiciary has gradually broadened the definition of Article 21 to encompass many aspects of human dignity, leading to the official acknowledgement of privacy as a basic right.

2.1 Early Judicial Approach: Absence of Explicit Recognition

During the early years after independence, the SC adopted a limiting interpretation of fundamental rights, refusing to acknowledge privacy as a right guaranteed by the Constitution. In *M.P. Sharma v. Satish Chandra* (1954 SCR 1077), An eight-judge panel ruled that a broad right to privacy was not recognized by the Constitution. The case concerned search and seizure, and the Court determined that there was no comparable protection in India by comparing Indian constitutional provisions with the Fourth Amendment of the US Constitution.

Similarly, in *Kharak Singh v. State of Uttar Pradesh* (1963 AIR 1295), the Court considered whether police surveillance was lawful. The majority rejected privacy as a basic right even though it declared domiciliary visits to be unlawful. But Justice Subba Rao's opinion stood out since it clearly stated that privacy is a crucial aspect of individual freedom. Later on, this dissent had a significant impact on the development of subsequent jurisprudence.

2.2 Gradual Expansion: From Liberty to Privacy

In subsequent decades, the Supreme Court began to adopt a more broad reading of Article 21, gradually laying the groundwork for privacy protection.

In *Gobind v. State of Madhya Pradesh* (1975 2 SCC 148), the Court cautiously admitted that certain aspects of privacy could fall within the ambit of personal liberty. However, it stopped short of declaring the unalienable right to privacy and instead treated it as a limited and case-specific interest.

The development continued in *R. Rajagopal v. State of Tamil Nadu* (1994 6 SCC 632), commonly referred to as the "Auto Shankar case." In this case, the Court upheld people's right to privacy about their private lives and acknowledged the right to be left alone.

Further, in *PUCL v. UOI* (1997 1 SCC 301), the Court addressed the tapping of phones and concluded that unlawful interception of communications violates the right to privacy. Additionally, it established procedural protections to stop the abuse of surveillance powers.

These decisions collectively indicated a shift toward recognizing privacy, even though it had not yet been firmly established as a FR.

2.3 The Transformative Moment: Justice K.S. Puttaswamy Case

The constitutional status of privacy was definitively settled in *UOI v. Justice K.S. Puttaswamy (Retd.) (2017 10 SCC 1). The Supreme Court's nine-judge panel unanimously ruled that the right to privacy is a fundamental right safeguarded under* Part III of the Constitution.

2.3.1 Essential Ideas Established

The ruling stated a number of foundational ideas:

- **Intrinsic to Article 21:** The Privacy is an essential aspect of the right to life and individual freedom.
- **Interconnected Rights:** Privacy is associated with autonomy and dignity, the freedom of choice.
- **Horizontal and Vertical Application:** It applies not just against the government but also has implications for private players.
- **Informational Privacy:** The Court recognized the significance of safeguarding personal information in the digital era.

2.3.2 Overruling Earlier Judgments

The rulings in M.P. Sharma and Kharak Singh were expressly overturned by the Court (to the extent that they denied privacy as a basic right), marking a decisive shift in constitutional interpretation.

2.3.3 Threefold Test

The Court established a tripartite examination for any infringement of privacy:

1. **Legality**- the existence of a valid law
2. **Necessity**- the legitimate state aim
3. **Proportionality**- the logical relationship between means and goal

This test has since become central to evaluating state actions affecting privacy.

2.4 Developments After Puttaswamy

Following the landmark judg-ment, several cases have further elaborated the contours of privacy.

2.4.1 Aadhaar Judgment

In *K.S. Puttaswamy (Aadhaar-5J.) v. UOI* (2019 1 SCC 1), the Supreme Court upheld the constitutional validity of the Aadhaar scheme but imposed limitations on its use. The Court emphasized data protection, purpose limitation, and safeguards against misuse, reflecting the growing importance of informational privacy.

2.4.2 Anuradha Bhasin Case

In *Anuradha Bhasin v. UOI* (2020 3 SCC 637), the Court addressed internet closers in Jammu and Kashmir. While primarily focused on freedom of speech, the judgment indirectly reinforced the importance of digital access and its connection to privacy and autonomy.

2.4.3 Navtej Singh Johar Case

In *Navtej Singh Johar v. UOI* (2018 10 SCC 1), the Court recognized privacy as a fundamental component of personal identity and dignity and decriminalized consenting same-sex relationships.

2.4.4 Joseph Shine Case

In *Joseph Shine v. UOI* (2019 3 SCC 39), the Court struck down the offense of adultery, emphasizing decisional autonomy and privacy within personal relationships.

2.5 Dimensions of Privacy Recognized by the Courts

Indian constitutional jurisprudence now recognizes several aspects of privacy:

a) **Bodily Privacy**- Protection against physical intrusions
b) **Informational Privacy**- Control over personal data and information
c) **Decisional Privacy**- Freedom to make intimate personal choices

These dimensions reflect a comprehensive understanding of privacy as essential to human dignity.

2.6 Privacy and the Digital Age

The recognition of informational privacy in *Puttaswamy* has particular relevance in the context of digital technologies. The increasing use of data analytics, artificial intelligence, and surveillance systems has intensified concerns regarding data misuse and profiling.

The Court acknowledged that informational privacy requires a robust data protection regime, thereby influencing laws like the DPDP, Act of 2023.

2.7 Challenges and Unresolved Issues

Despite significant progress, several challenges remain:

- **Balancing Privacy and State Interests:** National security and public order often justify restrictions on privacy.
- **Regulation of Private Entities:** Increasing data collection by private corporations raises concerns about accountability.
- **Implementation Gaps:** Judicial recognition alone is insufficient without effective enforcement mechanisms.

3. Conceptualizing Consent Fatigue

3.1 Definition and Characteristics

Consent fatigue refers to the diminished ability of individuals to make informed decisions due to repeated exposure to consent requests. In digital environments, users are often confronted with multiple notifications seeking permission for data collection and processing.

3.2 Illusion of Choice

Although consent mechanisms are designed to empower users, they frequently result in an illusion of control. Users may lack the time, expertise, or alternatives necessary to make meaningful choices, leading to routine acceptance of terms.

3.3 Structural Drivers

Consent fatigue arises from systemic factors, including:

- Information asymmetry between users and data processors
- Complexity of privacy policies
- Lack of standardization in consent interfaces

4. The Digital-Personal Data-Protection Act, 2023

4.1 Key Elements

The DPDP Act establishes a framework based on:

- Lawful processing through consent
- Principal data Rights (access, correction, deletion)
- Obligations of data fiduciaries
- Establishment of a Data Protection Board
- Provision for consent managers

4.2 Consent-Centric Model

The Act emphasizes "free, informed, specific, and unambiguous" consent. However, it does not sufficiently address the practical challenges associated with obtaining such consent in digital ecosystems.

5. Legal Gaps in the Existing Framework

5.1 Overdependence on Consent

The reliance on the main legal foundation for data processing is consent fails to account for real-world user behavior. Consent obtained under conditions of fatigue or coercion cannot be considered genuinely informed.

5.2 Broad Government Exemptions

The DPDP, Act provides exemptions for state agencies for reasons including public order and national security. While such although exclusions can be required, its wide reach concerns questions regarding possible misuse and lack of accountability.

5.3 Institutional Limitations

The Board for Data Protection structure and functioning raise questions regarding independence and enforcement capacity. Effective regulation requires a strong and autonomous authority.

5.4 Weak Redress Mechanisms

Users may encounter difficulties in enforcing their rights due to procedural complexities and limited awareness.

5.5 Absence of Strong Accountability Measures

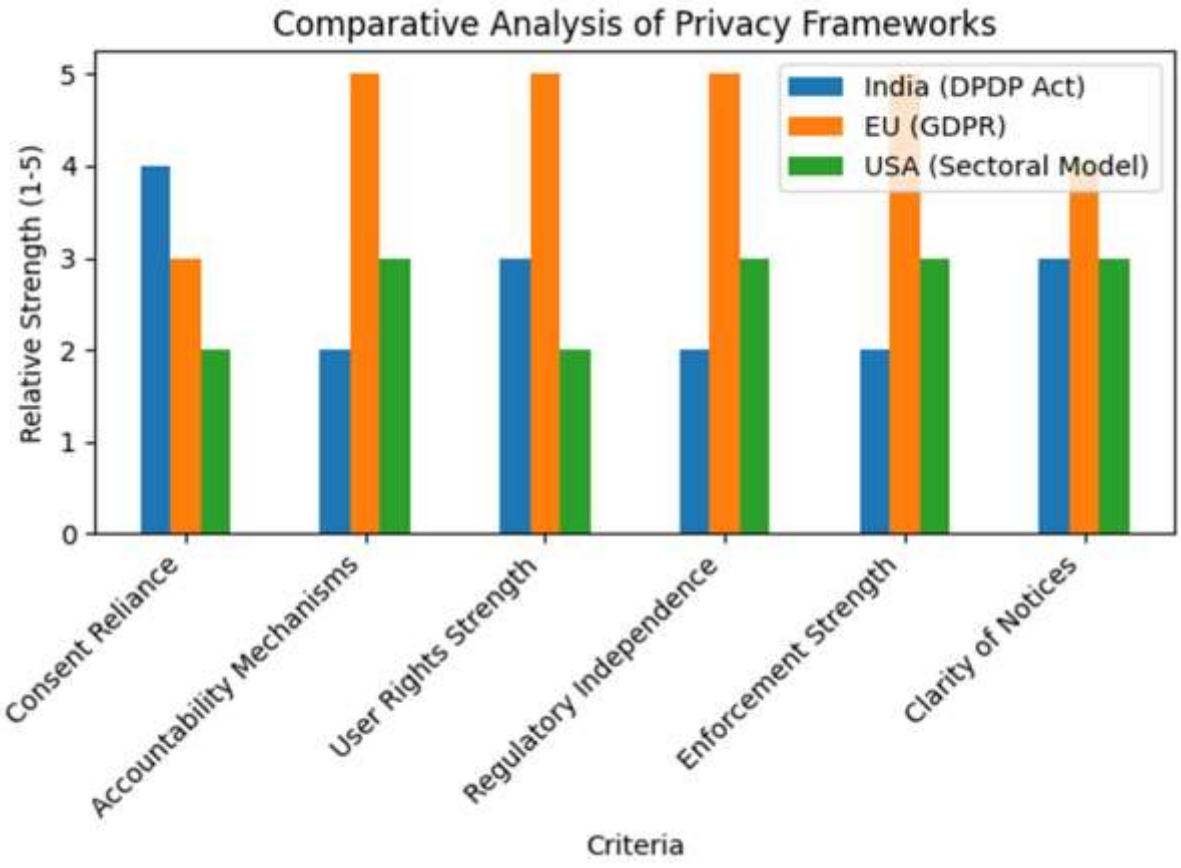
Compared to global frameworks, the Act places less emphasis on proactive accountability measures including independent audits and required impact assessments.

6. Comparative Analysis

International data protection laws, especially the General Data-Protection Regulation (GDPR) of the European-Union, adopt a more balanced approach by combining consent with accountability concepts like purpose limitation and data minimization. This comparative perspective highlights the need for India to strengthen non-consent-based safeguards.

Comparative Analysis of Privacy Frameworks

To critically evaluate consent fatigue and legal gaps, a comparative analysis was conducted between the sectoral approach in the US, the GDPR in the EU, and the Digital Personal Data Protection framework in India as shown in the below figure.



The comparison is based on key dimensions such as consent reliance, accountability, enforcement, and user rights as shown below in the table.

Criteria	India (DPDP Act)	EU (GDPR)	USA (Sectoral Model)
Consent Reliance	High	Moderate	Low
Accountability Mechanisms	Limited	Strong	Moderate
User Rights Strength	Moderate	Strong	Limited
Regulatory Independence	Limited	Strong	Moderate
Enforcement Strength	Developing	Strong	Moderate
Clarity of Notices	Moderate	High	Moderate

Interpretation:

The analysis reveals that India's framework places **significant reliance on user consent**, which contributes directly to the problem of consent fatigue. In contrast, the GDPR adopts a **balanced approach**, combining consent with strong accountability mechanisms such as data audits, impact assessments, and strict penalties.

India's relatively lower scores in **regulatory independence and enforcement strength** highlight institutional gaps that may weaken the practical implementation of privacy safeguards. Meanwhile, the US follows a sector-specific strategy, leading to disjointed protections and inconsistent user rights.

7. Toward a More Effective Privacy Framework

7.1 Accountability Centric Regulation

Accountability-centric regulation shifts the burden of data protection from individuals to organizations. Instead of relying mainly on user consent, it requires data handlers to justify how and why personal data is used. This approach emphasizes internal responsibility, regular audits, risk assessments, and strict consequences for misuse. By making organizations answerable for their practices, it ensures that privacy protection is proactive rather than dependent on user vigilance.

7.2 Design-Based Privacy

Privacy by Design involves integration data protection measures directly into the development of technologies and systems. Instead of putting privacy last, it is integrated from the initial stages of design. This includes minimizing data collection, ensuring secure storage, and limiting access. Such an approach reduces the need for constant user intervention and helps create systems that inherently respect user privacy.

7.3 Simplified Consent Mechanisms

Simplified consent mechanisms aim to make privacy choices clearer and more accessible for users. Instead of lengthy and complex policies, information is presented in concise, easy-to-understand formats. Layered notices, visual cues, and straightforward language enable users to quickly grasp key details. This reduces confusion and helps ensure that consent, when given, is more meaningful and informed.

7.4 Strengthening Regulatory Institutions

Effective privacy protection depends on strong and independent regulatory bodies. Strengthening such institutions involves improving their autonomy, resources, and enforcement powers. A well-equipped regulator can monitor compliance, address violations promptly, and build public trust. Clear procedures and transparency in decision-making further enhance their effectiveness in safeguarding data rights.

7.5 Enhancing Digital Literacy

Enhancing digital literacy emphasizes equipping people having the expertise and abilities required to navigate digital platforms responsibly. It includes understanding how personal data is collected, recognizing potential privacy risks, and making informed choices while interacting online. A digitally aware user is less likely to give uninformed consent and more capable of managing privacy settings effectively.

This can be achieved through education, awareness programs, and simplified communication by digital service providers. When users are better informed, they are more confident in exercising their rights, which in turn encourages organizations to adopt more transparent and responsible data practices.

8. Conclusion

The recognition of privacy as an essential right in *Puttaswamy* establishes a strong constitutional basis for safeguarding data in India. However, the effectiveness of statutory frameworks depends on their ability to translate these principles into practical safeguards.

The current reliance on consent as the foundation of data security is increasingly inadequate in the face of complex digital ecosystems. Consent fatigue undermines user autonomy, while legal and institutional gaps weaken enforcement.

A shift toward accountability-driven and design-based approaches is essential to guarantee that privacy protection in the India is both meaningful and effective. Such reforms would align the legal framework with constitutional principles and the digital age's reality.

References:

[1] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

[2] Digital Personal Data Protection Act, 2023 (India).

[3] *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.

[4] Greenleaf, G. (2014). Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report*, 133, 10–13.

[5] *Joseph Shine v. Union of India*, (2019) 3 SCC 39.

[6] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

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

[8] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

[9] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

[10] *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1.

[11] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

[12] Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880–1903.