# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

# DISCLAIMER



The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

# ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

# *PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT*

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

# DATA PROTECTION AND PRIVACY RIGHTS UNDER INDIAN LAW

AUTHORED BY - DR K RAMA KRISHNA BABA
Faculty, Dr B R Ambedkar Department of Legal Studies
Acharya Nagarjuna University, Guntur, Andhra Pradesh

## ABSTRACT

*The Digital Personal Data Protection Act 2023 (DPDPA) represents a watershed moment in Indian privacy jurisprudence, formally establishing a statutory right to data protection for 1.4 billion citizens and aligning India with global data governance standards. This paper undertakes a comprehensive legal analysis of the DPDPA 2023 and its implications for the right to privacy as constitutionally enshrined by the Supreme Court of India in Justice K.S. Puttaswamy v Union of India (2017). The study traces the evolution of privacy law in India from the colonial era through the landmark Puttaswamy judgment, examining successive attempts to enact data protection legislation including the Personal Data Protection Bill 2019, the Data Protection Bill 2022, and the ultimately enacted DPDPA 2023. The paper critically analyses the DPDPA's provisions on consent architecture, data fiduciary obligations, data principal rights, cross-border data transfers, and the Data Protection Board of India. A comparative analysis with the EU General Data Protection Regulation (GDPR), Singapore's PDPA, and California's CCPA reveals both strengths and significant gaps in India's data protection regime. The paper concludes that while the DPDPA marks a significant legislative advance, critical concerns regarding governmental exemptions, data localisation, and enforcement adequacy remain unresolved.*

**Keywords:** *Data Protection, Privacy Rights, DPDPA 2023, GDPR, Data Fiduciary, Consent Architecture, Right to Privacy, India*

## 1. INTRODUCTION

Privacy, as a fundamental human right, has undergone profound transformation in the digital age. The capacity of digital technologies to collect, process, and monetise personal data at an unprecedented scale has created a structural asymmetry of power between data-collecting entities and the individuals whose data is being processed. In India, this asymmetry is

ISSN: 2582-6433

particularly acute given the scale of digital adoption, the relative weakness of digital literacy among large sections of the population, and the extensive collection of biometric and personal data through the Aadhaar programme, the Unified Payments Interface, the CoWIN vaccination platform, and numerous state-level digital governance initiatives.

The Supreme Court of India's landmark nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 constitutionally established privacy as a fundamental right under Article 21 of the Constitution. This judgment overruled the earlier decisions in M.P. Sharma v Satish Chandra (1954) SCR 1077 and Kharak Singh v State of U.P. (1963) 1 SCR 332 and created an urgent constitutional imperative for data protection legislation. After six years of legislative deliberation, multiple draft bills, and extensive public consultation, the Digital Personal Data Protection Act 2023 (DPDPA) received Presidential assent on 11 August 2023.

However, the DPDPA's journey to enactment was fraught with controversy. The original Personal Data Protection Bill 2019, drafted by a high-level committee under Justice B.N. Srikrishna, was withdrawn by the government in August 2022 after more than eighty parliamentary amendments were proposed. Critics have argued that the enacted legislation, while a significant advance, sacrifices privacy rights through overbroad state exemptions and inadequate enforcement mechanisms.

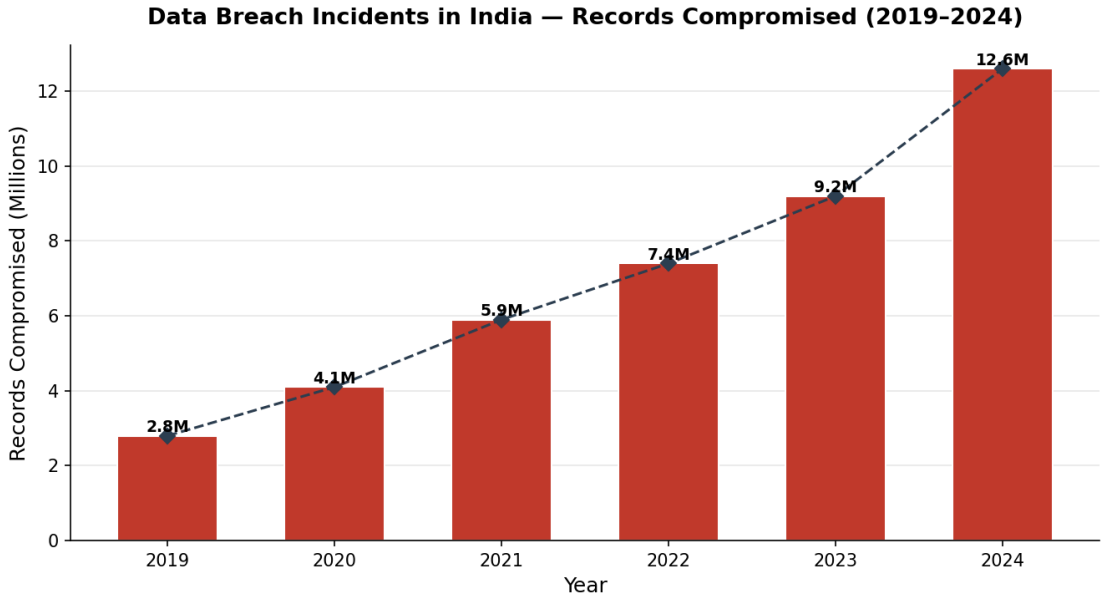


*Figure 1: Data Breach Incidents in India — Records Compromised (2019–2024) — Source: CERT-In Annual Reports & IBM Cost of Data Breach Report India 2024*

ISSN: 2582-6433

### 1.1 Research Objectives

- To trace the constitutional and legislative evolution of privacy and data protection law in India from independence to the DPDPA 2023.
- To critically analyse the key provisions of the DPDPA 2023 including consent architecture, data fiduciary obligations, and enforcement mechanisms.
- To undertake a comparative analysis of the DPDPA 2023 with the GDPR, Singapore PDPA, and California CCPA.
- To identify significant gaps, ambiguities, and constitutional concerns in the DPDPA 2023.
- To propose recommendations for strengthening India's data protection regime.

## 2. CONSTITUTIONAL FOUNDATION: THE RIGHT TO PRIVACY

### 2.1 The Puttaswamy Judgment: A Paradigm Shift

The Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v Union of India (2017) represents the most significant development in Indian privacy jurisprudence since the Constitution's adoption. The nine-judge constitutional bench unanimously held that privacy is a fundamental right intrinsic to life and liberty under Article 21 and that it inheres in all the fundamental rights in Part III of the Constitution. Writing for himself and four other justices, Justice D.Y. Chandrachud articulated an expansive conception of informational privacy, recognising that individuals must have the ability to control data about themselves and to prevent the surveillance of their actions by the state.

The Puttaswamy decision also laid down the proportionality test for the evaluation of state intrusions into privacy: any restriction on privacy must be: (i) sanctioned by law; (ii) in pursuance of a legitimate state aim; (iii) necessary for the achievement of that aim; and (iv) proportionate to the interference caused. This four-part test established a robust normative framework for evaluating data protection legislation.


*Figure 2: Evolution of Data Protection Law in India (2000–2025) — Source: Parliamentary Records & MeitY Notifications*

ISSN: 2582-6433

### 2.2 Pre-Puttaswamy Privacy Jurisprudence

Prior to the Puttaswamy judgment, Indian privacy jurisprudence was characterised by inconsistency and judicial restraint. The restrictive decisions in M.P. Sharma and Kharak Singh, which held that the Constitution did not guarantee a fundamental right to privacy, left citizens without constitutional protection against invasive state surveillance for over six decades. The enactment of the IT Act 2000 and Section 43A (inserted in 2008) requiring 'reasonable security practices' for sensitive personal data provided a weak statutory privacy protection framework.

## 3. THE DIGITAL PERSONAL DATA PROTECTION ACT 2023: A CRITICAL ANALYSIS

### 3.1 Structural Overview

The DPDPA 2023 is structured around seven key chapters addressing: definitions and interpretability; obligations of data fiduciaries; rights and duties of data principals; the Data Protection Board of India; appeals; offences, penalties and other matters; and miscellaneous provisions. The Act applies to the processing of digital personal data within India, whether processed online or offline after digitisation, and to processing outside India where it relates to offering goods or services to data principals in India.

### 3.2 Consent Architecture

The DPDPA 2023 establishes consent as the primary legitimate basis for personal data processing. Under Section 6, consent must be free, specific, informed, unconditional, and unambiguous. The Act introduces the concept of a 'Consent Manager' — a registered entity through which data principals may give, manage, review, and withdraw consent. The Act also recognises certain 'deemed consent' categories under Section 7, permitting data processing without explicit consent for purposes including the performance of state functions, compliance with legal obligations, and medical emergencies.

### 3.3 Rights of Data Principals

The DPDPA 2023 confers five principal rights upon data principals: (i) the right to access information about personal data processed (Section 11); (ii) the right to correction and erasure of personal data (Section 12); (iii) the right of grievance redressal against data fiduciaries (Section 13); (iv) the right to nominate a representative to exercise rights in case of death or

 ISSN: 2582-6433

incapacity (Section 14); and (v) the right to withdraw consent (Section 6(4)). Notably absent is an explicit right to data portability.

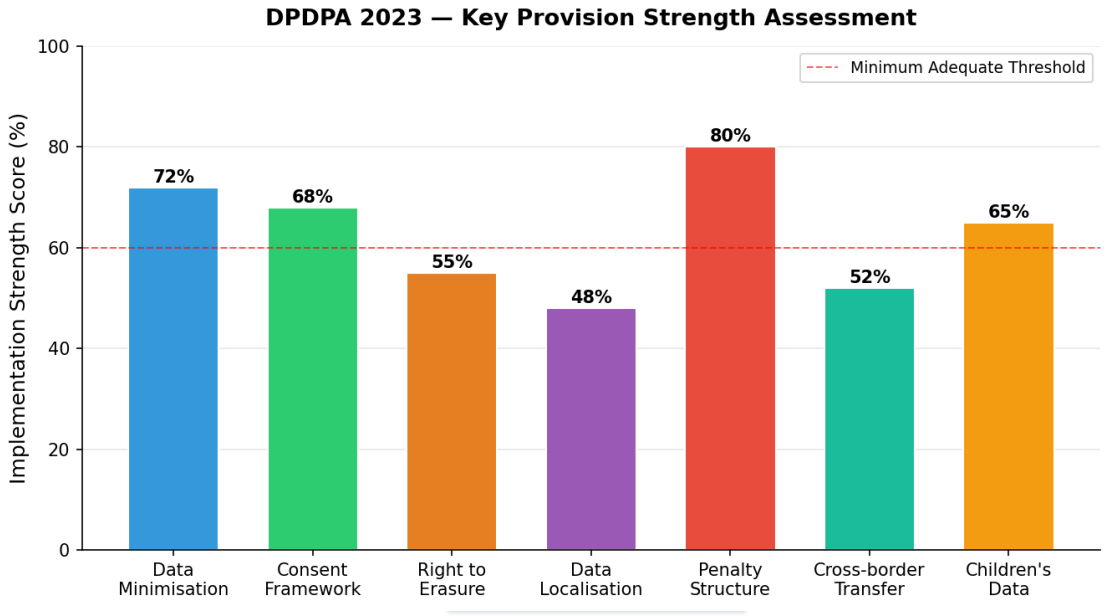


*Figure 3: DPDPA 2023 — Key Provision Strength Assessment — Source: Author's Analysis based on Parliamentary Debates & Legal Scholarship*

### 3.4 Obligations of Data Fiduciaries

Data fiduciaries — entities that determine the purpose and means of data processing — bear the primary compliance obligations under the DPDPA 2023. These include: (i) the duty to maintain security safeguards to prevent personal data breaches; (ii) the obligation to notify the Data Protection Board of India and affected data principals in the event of a personal data breach; (iii) the duty to appoint a consent manager or data protection officer as required; and (iv) the obligation to erase personal data upon withdrawal of consent or achievement of the specified purpose.

### 3.5 Government Exemptions: The Central Controversy

The most controversial provision of the DPDPA 2023 is Section 17, which grants the central government broad exemption powers. Clause 17(1) permits the government to exempt any government instrumentality from the Act's requirements in the interest of sovereignty, state security, friendly relations with foreign states, or public order. Privacy advocates have argued that these sweeping exemptions effectively immunise the state from data protection obligations, creating a surveillance state exemption incompatible with the Puttaswamy framework.

ISSN: 2582-6433

# 4. COMPARATIVE ANALYSIS WITH GLOBAL DATA PROTECTION REGIMES

## 4.1 General Data Protection Regulation (GDPR), European Union

The EU GDPR, in force since May 2018, is widely regarded as the global gold standard for data protection legislation. Its key features include: a comprehensive scope applying to all processing of personal data; six lawful bases for processing; expansive data subject rights including portability and the right not to be subject to automated decision-making; mandatory data protection impact assessments; and substantial penalties of up to €20 million or 4% of global annual turnover.

## 4.2 Personal Data Protection Act (PDPA), Singapore

Singapore's PDPA 2012 (as amended in 2020) provides a sectoral but comprehensive approach to data protection. The 2020 amendments significantly strengthened the PDPA by introducing mandatory data breach notification within three days, enhanced criminal penalties for egregious data misuse, a data portability obligation, and a deemed consent framework for legitimate interests.

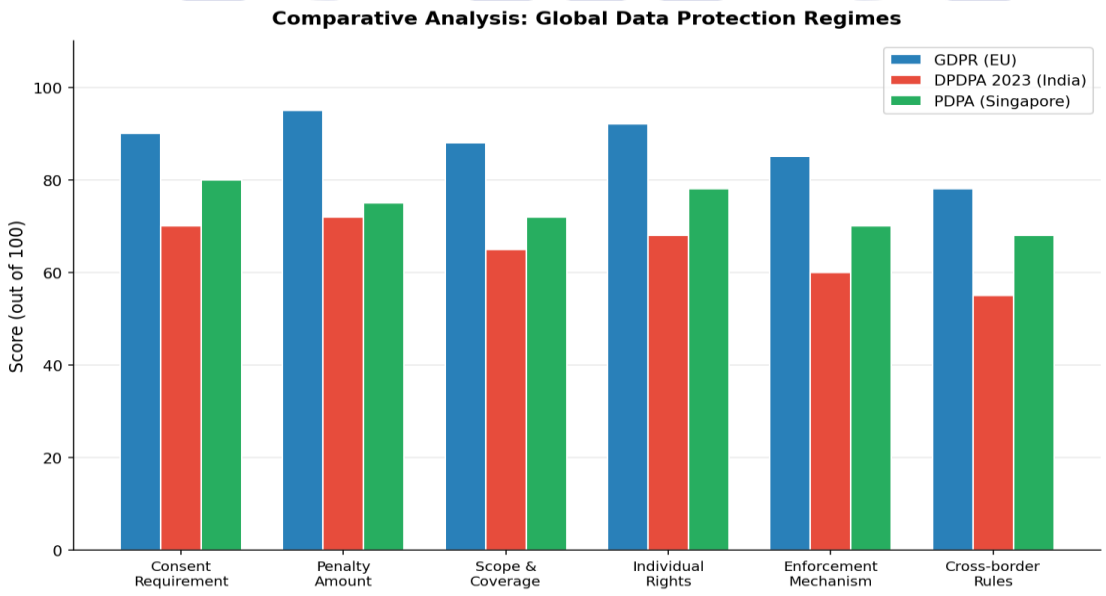


*Figure 4: Comparative Analysis — Global Data Protection Regimes (GDPR vs DPDPA 2023 vs PDPA Singapore)*

| Feature | GDPR (EU) | DPDPA 2023 (India) | PDPA (Singapore) | CCPA (California) |
|---|---|---|---|---|
| Consent Requirement | Explicit, granular | Free, specific, informed | Explicit / deemed consent | Opt-out basis |

ISSN: 2582-6433

| | | | | |
|---|---|---|---|---|
| Data Portability | Yes (Art. 20) | Absent | Yes (2020 Amendment) | Yes (limited) |
| Right to Erasure | Yes (Art. 17) | Yes (Sec. 12) | Yes (Sec. 24) | Yes (limited) |
| Max Penalty | €20M / 4% turnover | Rs.250 Crore per violation | SGD 1 Million | USD 7,500 per violation |
| Gov. Exemptions | Narrowly defined | Very broad (Sec. 17) | Limited | Limited |
| Enforcement Body | DPAs (independent) | DPBI (Govt. appointed) | PDPC (independent) | California AG / CPPA |

*Table 1: Comparative Analysis of Global Data Protection Regimes*

## 5. ENFORCEMENT ARCHITECTURE: THE DATA PROTECTION BOARD OF INDIA

The DPDPA 2023 establishes the Data Protection Board of India (DPBI) as the primary enforcement authority. The Board is empowered to receive and investigate complaints from data principals, impose financial penalties for violations, and direct data fiduciaries to take remedial actions. However, the Board's institutional design has attracted significant scholarly criticism. Unlike the GDPR's independent national supervisory authorities, the DPBI is constituted by the Central Government, raising concerns about the Board's ability to independently investigate and sanction government data fiduciaries.

### 5.1 Penalty Structure

The DPDPA 2023 establishes a tiered penalty structure: (i) up to Rs.250 crore for failure to implement adequate security measures; (ii) up to Rs.200 crore for failure to notify data breaches; (iii) up to Rs.150 crore for violation of obligations regarding children's data; and (iv) up to Rs.10,000 for violation of duties as a data principal. While these penalties represent a significant advance over the Rs.5 crore maximum under the IT Act 2000, they may be insufficient deterrents for large multinational corporations.

### 5.2 The Children's Data Framework

Section 9 of the DPDPA 2023 imposes specific protections for children's personal data. Data fiduciaries are required to obtain verifiable parental consent before processing children's data, and are prohibited from processing data in a manner likely to cause detrimental effects on

ISSN: 2582-6433

children's well-being or track their behaviour or target advertising at them.

## 6. SECTORAL PRIVACY CONCERNS IN INDIA

### 6.1 Aadhaar and Biometric Data

The Aadhaar scheme, which has enrolled over 1.3 billion Indians, represents perhaps the world's largest biometric database. The DPDPA 2023's relationship with Aadhaar remains ambiguous: while the Act in principle applies to Aadhaar data processing, the broad government exemptions in Section 17 effectively shield UIDAI operations from DPDPA scrutiny. The Aadhaar data breach incidents reported between 2018 and 2023, affecting hundreds of millions of records, underscore the urgency of robust enforcement.

### 6.2 Healthcare Data

The National Digital Health Mission (NDHM) and the Ayushman Bharat Digital Mission (ABDM) are creating a comprehensive digital health ecosystem for India. Health data represents perhaps the most sensitive category of personal data. The DPDPA 2023 does not specifically categorise health data as 'sensitive personal data' requiring heightened protection — a significant divergence from the GDPR and a cause for concern among healthcare privacy advocates.

## 7. CRITICAL GAPS AND RECOMMENDATIONS

### 7.1 Significant Legislative Gaps

- Absence of a right to data portability, limiting consumers' ability to switch service providers and exercise genuine data sovereignty.
- Overly broad governmental exemptions in Section 17 that effectively immunise state surveillance activities from data protection obligations.
- No prohibition on automated decision-making with legal effects, unlike GDPR's Article 22, leaving citizens unprotected from algorithmic discrimination.
- The absence of a requirement for Data Protection Impact Assessments (DPIAs) for high-risk processing activities.
- The lack of an independent enforcement body — the DPBI's structural dependence on the central government compromises its accountability function.

ISSN: 2582-6433

### 7.2 Policy Recommendations

- The DPDPA 2023 should be amended to introduce: a right to data portability; a prohibition on automated decision-making without human review in high-stakes contexts; and mandatory Data Protection Impact Assessments for Significant Data Fiduciaries.
- Section 17 should be substantially narrowed to comply with the proportionality test established in Puttaswamy, limiting governmental exemptions to narrowly defined national security situations subject to independent judicial oversight.
- The Data Protection Board of India should be reconstituted as a genuinely independent statutory authority with security of tenure for members, parliamentary accountability, and financial autonomy.
- India should pursue adequacy recognition from the European Commission, which would facilitate cross-border data flows and position India as a trusted data processing destination.

## 8. CONCLUSION

The Digital Personal Data Protection Act 2023 represents a historic milestone in India's journey towards establishing a comprehensive data protection framework. After decades of inadequate protection under the IT Act 2000, Indian citizens now possess statutory rights to access, correct, and erase their personal data, and data fiduciaries face meaningful penalties for non-compliance. The recognition of the right to privacy as fundamental under Puttaswamy and its legislative crystallisation through the DPDPA creates a new legal ecology for digital India.

Yet the Act's limitations are as significant as its advances. The broad governmental exemptions, the institutional fragility of the DPBI, the absence of key rights such as data portability and algorithmic accountability, and the delayed operationalisation through rules conspire to undermine the Act's transformative potential. As Justice Chandrachud reminded us in Puttaswamy, privacy is 'a constitutional core that cannot be bartered away.'

## REFERENCES

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India — Nine-Judge Bench).*
2. *Digital Personal Data Protection Act, 2023. (Act 22 of 2023). Government of India.*
3. *Personal Data Protection Bill, 2019. (Bill No. 373 of 2019). Ministry of Electronics*

ISSN: 2582-6433

*and Information Technology.*

4. *European Parliament & Council. (2016). General Data Protection Regulation (EU) 2016/679. Official Journal of the European Union.*
5. *Srikrishna Committee. (2018). A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians.*
6. *Internet Freedom Foundation. (2023). Analysis of the Digital Personal Data Protection Act 2023. IFF Working Paper No. 7.*
7. *M.P. Sharma v. Satish Chandra, (1954) SCR 1077 (Supreme Court of India).*
8. *Kharak Singh v. State of U.P., (1963) 1 SCR 332 (Supreme Court of India).*
9. *Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632 (Supreme Court of India).*
10. *CERT-In. (2023). Annual Report on Cyber Security Incidents. Indian Computer Emergency Response Team, MeitY.*
11. *Nariman, F., & Salve, H. (2023). Commentary on the Digital Personal Data Protection Act 2023. LexisNexis India.*
12. *Bhatia, G. (2023). Governmental Exemptions in the DPDPA: A Constitutional Critique. National Law School Journal, 22(1), 11-45.*
13. *Singapore Personal Data Protection Act 2012 (as amended 2020). Singapore Government.*
14. *California Consumer Privacy Act 2018 (CCPA), Cal. Civ. Code § 1798.100 et seq.*
15. *UIDAI. (2023). Annual Report 2022-23. Unique Identification Authority of India.*