INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

DIGITAL SOVEREIGNTY AND THE RIGHT TO PRIVACY: GLOBAL PERSPECTIVES WITH A CRITICAL STUDY OF INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - LOVELEEN KAUR[1]

Abstract

This research paper investigates the growing tension between how states are increasingly asserting their digital sovereignty and, on the other side, the way individuals continue to demand protection of their right to privacy, especially in today's globalised world. The central focus here is on India's new law, the Digital Personal Data Protection Act, 2023 (DPDPA), but the discussion does not stop there.[2] The paper tries to place India's approach within a much larger international setting, by comparing it with some of the most influential global models — particularly the European Union's General Data Protection Regulation (GDPR), the sectoral and more market-driven approach followed in the United States, and the much more sovereignty-driven system that is visible in China's legal framework.[3]

The argument put forward in this work is that while India's 2023 Act clearly tries to strike a balance between competing concerns — namely the economy, national security, and privacy rights — its actual structure and the kinds of exemptions it allows for the state may, in practice, lean more in favour of government control rather than individual freedoms. In making this assessment, the paper relies on various sources: constitutional judgments like Justice K.S. Puttaswamy v. Union of India (2017), key international human rights documents, important comparative statutes, and even landmark cases such as the Schrems II ruling in the European Court of Justice.[4] Based on these, it finally offers some policy suggestions and reforms — operational, institutional, and normative — that could help India move towards a more privacy-friendly framework. while still respecting the legitimate role of state sovereignty. Main sources referred to include Digital Personal Data Protection Act, 2023; Justice K.S.

[1] School of Law, Lovely Professional University, Jalandhar, Punjab, India.
[2] The Digital Personal Data Protection (DPDP) Act, 2023," Law Journals (vol. article) (2025).
[3] Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL, IJLT (April 10, 2024).
[4] K.S. Puttaswamy & Anr. v. Union of India & Ors., (2017) 10 SCC 1, AIR 2017 SC 4161 (Constitution Bench).

ISSN: 2582-6433

Puttaswamy v. Union of India (2017); GDPR; Schrems II decision of the ECJ; and the Justice Srikrishna Committee Report.)

Keywords: *Digital Sovereignty, Right to Privacy, Data Protection Act in India, GDPR, DPDPA 2023, Justice K.S. Puttaswamy v. Union of India (2017), Schrems II decision of the ECJ and the Justice Srikrishna Committee Report.*

I. Introduction

In July 2020, the Court of Justice of the European Union (CJEU) rendered its ruling in the iconic Schrems II case. Within that ruling, the court invalidated the EU–US Privacy Shield framework because it believed the agreement did not actually safeguard European residents information after it transferred to the United States, where public agencies had access to it too readily.[5] This result shook the world to its core. Large technology firms, regulators and even governments worldwide suddenly had to hit pause and rethink how they were approaching cross-border data transfers. The case set forth, in very stark terms, the fundamental tension of the digital age: nations wish to use their sovereign prerogatives to control data or even exploit it for national defense, yet at the same time people anticipate that their personal information will be secure and preserved, wherever it may go.

It is within this broader global context that India enacted its Digital Personal Data Protection Act, 2023 (DPDPA).[6] The legislation is intended to establish guidelines for processing digital personal data, and it also specifies some rights for those individuals, referred to as data principals, whose data is being gathered. It also discusses mechanisms for compliance. Nevertheless, the Act has sparked controversy since it holds some exceptions that allow the State a significant amount of leeway to act upon, which many are worried will permit additional state power over information than is good for a system based on the right to privacy. So, the question remains: does this legislation actually succeed in balancing the concept of digital sovereignty with the right to privacy? This research paper attempts to investigate that by comparing India's Act with the GDPR and also by examining a few prominent global cases and experiences.[7]

[5] Max Schrems v. Data Protection Commissioner ("Schrems II"), Case C-311/18, Judgment of the Court (Grand Chamber), 16 July 2020.
[6] India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison, Global Privacy Blog (13 December 2023)
[7] Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with

ISSN: 2582-6433

II. Conceptual and normative foundations

- ***Digital sovereignty***

  Digital sovereignty is the ability of a state to exert influence over digital infrastructure, platforms, and data in its territory. It involves legal and policy options like data localisation, limitations on cross-border transfers, and regulation in the home country by domestic authorities of foreign digital service providers. Digital sovereignty tends to be based on state interests (political control, economic policy, security) and is expressed differently in jurisdictions: protective economic nationalism in some states, or regulatory harmonisation with international norms in others. The Srikrishna Committee advised India to create a personal data framework that safeguards citizens but allows for a free and fair digital economy — thereby implicitly accepting the sovereign aspect of data rule.[8]

- ***Right to privacy in international law***

  The right to privacy is a firmly established human right. Article 12 of the Universal Declaration of Human Rights safeguards people against "arbitrary interference" in privacy.[9] Article 17 of the International Covenant on Civil and Political Rights (ICCPR) enshrines the right to privacy and the obligation of states to ensure legal protection against such interference.[10] International human rights mechanisms, and follow-up General Comments, insist that privacy protections are effective and proportionate, even when weighed against legitimate state interests like security or public order. GDPR as a normative benchmark.[11]

- **GDPR as a normative benchmark**

  The EU's General Data Protection Regulation (GDPR) is the most impactful contemporary data protection tool. Its design prioritises individual rights (consent, access, rectification, erasure, portability), legal bases for processing, accountability by design, and strong oversight by independent supervisory authorities. GDPR has an influence felt well beyond Europe, numerous jurisdictions look to its principles as a benchmark for their laws and standards.[12]

GDPR and PIPL, IJLT (April 10, 2024).

[8] Justice B.N. Srikrishna Committee, Report of the Committee of Experts on Data Protection Framework for India (2018).

[9] Universal Declaration of Human Rights, 10 Dec. 1948, G.A. Res. 217 A (III), U.N. Doc. A/810 (1948).

[10] International Covenant on Civil and Political Rights, Art. 17, 16 Dec. 1966, 999 U.N.T.S. 171, entered into force 23 Mar. 1976.

[11] Data-Protection Laws and Obligation of Data Fiduciaries, IJLMH (2025).

[12] Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL, IJLT (April 10, 2024).

ISSN: 2582-6433

III. Methodology and scope

It is a doctrinal and comparative analysis on the basis of primary legal documents (DPDPA 2023, GDPR, ICCPR, UDHR), seminal judicial rulings (Puttaswamy, Schrems II), influential policy reports (Srikrishna Committee), and chosen academic commentary and policy reviews. The article synthesises statutory rules and case law, subsequently evaluating the DPDPA by applying normative tests gleaned from international human rights law and comparative experience. The comparative framework looks at the GDPR (subject-centric approach) and state-centred approaches (most notably China's PIPL and attendant data security legislation) in order to identify divergent efforts toward addressing the sovereignty–privacy paradox.

IV. Literature review — global and Indian perspectives

- **Global literature**

  Scholars and policy experts have characterised three wide regulatory paradigms: (i) the individual rights-based regime (GDPR), (ii) the market/sectoral approach (United States), and (iii) the sovereignty-first approach (China and several other states) in which state control and security concerns prevail. The literature emphasises recurring issues: the tension between free data flow and national security; market concentration and platform power; the technical difficulty of enforcement across borders; and the necessity of international cooperation to balance privacy rights with legitimate government interests. Comparative studies (e.g., Green leaf's comparative mapping of global privacy laws) substantiate that states adapt solutions by political economy and strategic agenda.[13]

- **Indian literature**

  Indian scholarship has grappled intensively with the constitutional foundation of privacy after Puttaswamy (2017), which constitutionally protected informational privacy under the right to life and personal liberty under Article 21.[14] The Srikrishna Committee's report in 2018 gave a detailed roadmap to India's regime of personal data,

[13] See Trilemma and Tripartition: The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU, the U.S. and China, 43 Computer L. & Sec. Rev. (Nov. 2021) 105610 (contrasting EU GDPR-style rights-based, U.S. sectoral, and China's security/sovereignty-first approaches); Sungjin Lim & Junhyoung Oh, Navigating Privacy: A Global Comparative Analysis of Data Protection Laws, 2025, IET Information Sec. 1 (analysing tensions between free data flow, enforcement, market power, national security across EU, U.S., China and others); Graham Greenleaf, Asian Data Privacy Laws: Trade & Human Rights Perspectives (Oxford 2014); Graham Greenleaf, Global Data Privacy Laws: Forty Years of Acceleration, 2011; Graham Greenleaf, "Global Data Privacy Laws 2025: 172 Countries, Twelve New in 2023/24" (Apr. 2, 2025).

[14] K.S. Puttaswamy & Anr. v. Union of India & Ors., (2017) 10 SCC 1, AIR 2017 SC 4161 (Constitution Bench)

ISSN: 2582-6433

with a focus on consent, limitation of purpose, and a light-touch regulatory framework tailored to India's socio-economic realities. Post-2019 discussions—such as parliamentary committee examinations—prioritised state exceptions, independent regulators, and ensuring clarity on cross-border flows and legal bases of processing.[15] Opponents (civil society and lawyers) claim successive drafts and the resultant 2023 Act water down some protection and grant wide powers to the state.

V. The Digital Personal Data Protection Act, 2023 — architecture and key features

- **Scope and definitions**

  DPDPA covers processing of online or offline digitised digital personal data in India, and certain overseas processing while providing services to Indian data principals. It prescribes categories like data fiduciary, data principal, and processing—using a terminology that is harmonized with international practice.[16]

- **Rights of data principals**

  The Act identifies rights such as confirmation and access, correction, erasure, data portability, and notice. These rights reflect GDPR characteristics; however, their performance is contingent upon the regulatory framework and the Data Protection Board enforcement posture.[17]

- **Lawful processing and exemptions**

  The DPDPA enumerates permissible grounds for processing (consent, contractual obligation, compliance with law, public interest categories), with significant state-facing exceptions.[18] The Act authorises processing for purposes of national security, crime prevention, and performance of tasks under law—provisions which are common in other systems but must be carefully shielded from abuse.

- **Governance and enforcement**

  The Act provides for a Data Protection Board with investigatory and punitive powers. Issues raised in legislative debate focused on the Board's autonomy, appointment

[15] Justice B.N. Srikrishna Committee, Report of the Committee of Experts on Data Protection Framework for India (2018)
[16] The Digital Personal Data Protection (DPDP) Act, 2023, Law Journals (Vol. 11, Issue 3, 2025).
[17] Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL, IJLT (April 10, 2024).
[18] Anirudh Burman, Understanding India's New Data Protection Law, Carnegie Endowment for International Peace (October 3, 2023).

ISSN: 2582-6433

processes, and budgetary allocations—factors that define its ability to impose rights effectively. The Srikrishna Committee had suggested an independent regulator with explicit procedural protections; observers record slippage from that initial conception to the resultant statutory makeup.

VI. Comparative examination: DPDPA (India) and GDPR (EU) against sovereign models.

- **Rights orientation and autonomy of the individual**

  GDPR prioritizes autonomy of the individual via consent and a set of enforceable rights, accompanied by independent supervisory bodies with robust correctional powers. DPDPA has equivalent rights in theory, however, the existence of sweeping exemptions (notably for public purposes) will undermine effective enjoyment of these rights. In brief: formal compatibility is present, but functional shortfall exists.

- **State exemptions, surveillance, and proportionality**

  The structure of GDPR allows public authority processing but anchors it to legal bases and protections, EU human rights law priorities proportionality and judicial review.[19] The DPDPA's broader government use carve-outs and few publicly available ways to keep an eye on things show that it favours sovereign privilege. Comparative scholarship warns that such carve-outs risk mission creep—eroding privacy unless firmly bounded and transparently regulated.

- **Cross-border data flows and localisation**

  Data localisation has long been an object of India's policy discourse as a tool of digital sovereignty. The DPDPA governs cross-border transfers and allows conditions for transfer, but India's wider regulatory environment (sectoral policies, pre-notification localisation rules in certain sectors) shows continued leaning towards localisation. The Schrems II jurisprudence, through emphasis on national security access risk in the destination country, has prompted regulators around the world to scrutinise adequacy and protection for transfers rigorously.[20] The consequence: regulated flows must balance sovereignty with interoperability to prevent trade frictions and innovation expense.

[19] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), 4 Nov. 1950, 213 U.N.T.S. 221, entered into force 3 Sept. 1953.
[20] Max Schrems v. Data Protection Commissioner ("Schrems II"), Case C-311/18, Judgment of the Court (Grand Chamber), 16 July 2020

ISSN: 2582-6433

- **Independence of institutions and ability to enforce**

  The supervisory bodies of the GDPR are independent and can give out big fines. The Data Protection Board of the DPDPA can investigate things, but there are worries about how the board is set up and how independent it really is. Rights are meaningless without strong, independent enforcement. Policy analyses (including by think tanks and consultancies) highlight that building regulatory capacity is necessary for the law to have actual impact.

VII. Constitutional and rights-based evaluation: India's legal framework

- **Puttaswamy and the constitutional benchmark**

  The Puttaswamy judgment of the Supreme Court laid a strong constitutional basis for privacy in India. Any legislation curbing privacy must meet the threefold test outlined in Puttaswamy: legality, legitimate state interest, and proportionality (necessity and minimal invasion). So, when looking at the DPDPA's exemptions and state processing, you need to keep this constitutional standard in mind.[21]

VIII. Exemptions and proportionality in the DPDPA

Broad or general exemptions may be impervious to proportionality if they permit arbitrary or disproportionate interference. The use of executive notification and undefined standards for some exceptions under the Act requires strong procedural guarantees (judicial review, transparency, independent oversight) to pass constitutional scrutiny. The lack of clear judicial or parliamentary oversight mechanisms for particular state uses is a normative gap.

IX. Policy implications and critiques

- **Economic and innovation trade-offs**

  Data localisation and restrictive transfer regimes can safeguard domestic control and potentially drive domestic data service industries. They, however, enhance compliance costs for companies, reduce global cloud service efficiencies, and can inhibit foreign investment and research partnerships. Comparative research warns that proportionate, risk-based solutions can protect citizens without disproportionately curbing innovation.

- **Risk of mission creep and surveillance**

  Historical and current controversies (Aadhaar litigation, Pegasus allegations, and

[21] K.S. Puttaswamy & Anr. v. Union of India & Ors., (2017) 10 SCC 1, AIR 2017 SC 4161 (Constitution Bench).

ISSN: 2582-6433

sectoral data uses) serve to demonstrate the danger of mission creep—where data collection for legitimate public ends becomes a means of extensive surveillance if left unchecked. The DPDPA must then be placed within a broader framework of governance with robust checks and remedies.

- **Interoperability around the world and coordination between diplomats**

  Schrems II shows that allowing destination states to access data makes transfer adequacy worse. India needs bilateral and multilateral agreements (adequacy agreements, standard contractual mechanisms, and mutual legal assistance arrangements) that balance sovereignty, security, and privacy. Taking part in talks about global norms and interoperability will help keep knowledge from getting scattered and the law from being unclear

Recommendations

Toward a balanced sovereignty based on rights the following suggestions try to make digital sovereignty fit with strong privacy protection by using India's constitutional duties and best practices from other countries :-

1. Give the Data Protection Board more freedom: Open hiring processes, financial independence, and strong protections against political interference. (GDPR supervisory bodies are a good example.)
2. Improve and narrow down state exceptions: Specify legitimate objectives, subject mass collection, or invasive processing to first judicial or legislative scrutiny and incorporate end clauses for emergency powers. This will help meet Puttaswamy's test of proportionality.
3. Risk-based transboundary approach: As your first option, apply adequacy findings, standard terms of contracts and technical protection features such as encryption and pseudonymization. Localisation should be done only in some, and very few high-risk areas. Negotiations of bilateral adequacy: You can work on them when you can.
4. Open procedures and provide more choice in seeking assistance: the government must be made to make demands of access to open, and it should not censor sensitive and working data unless it is unavoidable. Empower the citizens to demand justice and the courts to exercise control.
5. was easier to enforce: Instead, provide the regulator and courts with more money so that they can enhance their technical, legal and forensic capabilities. This will assist them to make key decisions on data protection cases. Cooperate with foreign institutions

ISSN: 2582-6433

in order to train and support in technical terms.

6. The participation of the masses and civil society: It should become a standard feature of the rule-making process to include the stakeholders, in particular, to ensure that the exemptions are transparent and algorithms are held accountable. The Srikrishna Committee placed high value on inclusive design—this recommendation reaffirms it.

Conclusion

Digital sovereignty and a right to privacy are not necessarily conflicting aims; they can be complementary if policy tools are carefully framed. India's DPDPA 2023 is a significant achievement which acknowledges data rights but relies not just on statutory language but on institutional autonomy, open procedures, and consistent judicial protection consonant with constitutional commands like Puttaswamy. Comparative lessons from the GDPR and judicial evolution such as Schrems II recommend against simplistic localisation or unfettered state exemptions. To serve as a model for the Global South, India needs to further safeguard individual autonomy while forging pragmatic, interoperable solutions to legitimate state interests in the digital era.