RESEARCH COMMUNICATIONS
(An International Open Access, Peer Reviewed, Multidisciplinary Online Journal)
https://research-communications.cmpcollege.ac.in
ISSN: 2584-1270
Volume: 2, Issue: 2, July-December 2024, pp. 25-32

A Comprehensive Analysis of Data Privacy Evolution in India and Digital Personal Data Protection Act, 2023

Raje & Dr. Radheshyam Prasad

[1]*Raje, Research Scholar, Faculty of Law, University of Lucknow, Uttar Pradesh, India*
E-mail: *rajeraopwa@gmail.com*

[2]*Dr. Radheshyam Prasad, Associate Professor, Faculty of Law, University of Lucknow, U.P., India*
E-mail: *radheshyampd@gmail.com*

Abstract

The article provides a thorough exploration of India's journey in shaping data privacy regulations and the pivotal introduction of the Digital Personal Data Protection Act (herein after in as to DPDP Act 2023). Beginning with a foundational understanding of data privacy, it delves into the historical progression of data protection laws in India, tracing significant milestones and prior legislative endeavours. Highlighting the necessity for a contemporary approach to data privacy, it scrutinizes the shortcomings of existing laws, prompting the emergence of the DPDP Act 2023. This comprehensive legislation aims to address these gaps by delineating its objectives, core features and the potential ramifications for both businesses and individuals. By meticulously dissecting the Act and drawing comparative insights from global data protection frameworks such as the GDPR, the article elucidates its impact on the operational landscape of businesses and the rights it bestows upon consumers. However, amid its significance, the Act is not devoid of challenges. The article navigates through anticipated hurdles in its implementation and explores critiques from diverse perspectives, paving the way for discussions on potential areas for refinement. Looking forward, the article prognosticates the trajectory of data privacy in India, envisioning the Act's influence on the national landscape and contemplating future amendments or advancements. It culminates with a call for heightened data privacy awareness and compliance, underlining the Act's role as a pivotal milestone in India's evolving data protection narrative.

Keywords: *Digital Data Protection, Right to Privacy, Fundamental Right, Protection*

1. Introduction

India's journey toward data privacy has been a compelling one, shaped by historical principles, constitutional interpretations, and pivotal legal cases. The right to privacy, now recognized as an essential part of personal liberty, has emerged through landmark judgments and legal milestones. This progression paves the way for a deeper exploration of India's evolving data privacy framework, culminating in the enactment of the DPDP Act.

Privacy, deeply rooted in historical values and constitutional frameworks, was initially expressed in ancient Indian laws and texts, gaining prominence through constitutional interpretations. Despite the limited historical recognition, the judiciary's engagement with privacy matters

intensified, leading to landmark cases that laid the foundation for acknowledging privacy as a fundamental right.

The landscape further unfolded with cases such as ***People's Union for Civil Liberties (PUCL)* v. *Union of India***,[i] highlighting the commitment of the judiciary towards the protection of privacy rights in different contexts, such as unauthorized tapping of telephone calls and disclosure of medical records. During this legal evolution, the watershed moment arrived with the case of ***J. K. S. Puttaswami* v. *Union of India***[ii], where the Court pointed out that the right to privacy is a fundamental right.

Then comes the narrative of how the laws related to data protection evolved in India, beginning with the Information Technology Act, 2000 (IT Act) and further moving with the introduction of the Personal Data Protection Bill. It finally culminated in the DPDP Act of 2023, which marks a gigantic leap forward for India on its way to ensuring proper data privacy.

The DPDP Act, 2023, with its overarching objectives, addresses the challenges posed by evolving technologies. It replaces the outdated IT Act, offering a comprehensive legal infrastructure to regulate online activities, protect consumer rights, and adapt to emerging technologies like artificial intelligence (AI) and blockchain.

This law introduces important provisions, such as child rights and rights of individuals with disabilities, informed consent, and establishing a regime for cross-border transfers of personal data. The law also establishes the board named the Data Protection Board of India, which shall oversee compliance and impose penalties and remedies in cases of non-compliance.

In the dynamic journey of data privacy in India, the DPDP Act is testimony to the commitment of this nation towards safeguarding rights in the digital era. This delves into the intricacies of this legislative journey, peeling away layers to explain the intricate balance between privacy, technological advancement, and the collective well-being of society.

2. Evolution of Data Privacy in India

Privacy, considered a fundamental aspect of human existence, has a rich historical evolution, and is deeply ingrained in the constitutional foundations of nations. It reflects the innate desire to shield oneself from public scrutiny and the entitlement to maintain confidentiality in personal affairs. This societal value has transcended civilizations, finding roots even in ancient Indian laws like Dharmashastras and Hindu texts such as Hitopadesha, which underscored the importance of protecting specific matters from disclosure.

The Apex Court, by interpreting the term "Personal Liberty, in its broad sense, derived the Right to Privacy as an essential component of the Right to Life and Personal Liberty. Article 21 clearly states that no person shall be deprived of any right conferred on him except according to procedure established by law. Expanding from this basic provision, the Supreme Court noted that those charged with taking away peoples' liberties in performing their functions have to be bound strictly by law. Thus, the Court concluded that "Personal Liberty" could be understood as a life devoid of abuses that cannot be tolerated in the sight of the law.

Since the advent of the Constitution, the Indian judiciary has resolved privacy-related issues either as part of fundamental rights jurisprudence or through common law jurisprudence. However, privacy has not had a very long history with regard to recognition compared to other rights that fall within the umbrella of fundamental rights. The engagement by the judiciary on privacy issues is relatively recent and less seasoned in the experience of cases dealing with privacy rights. Decisions are case-sensitive.

In ***MP Sharma** v. **Satish Chandra,*** the challenge to the authority's power and seizure provision is allegedly one violating the privacy right. However, the superior judicial body pointed out that the Constitutional Framers were not seeking to abrogate the power to search and seize as violating

basic privacy rights. Besides, the Supreme Court clarified that the MP Sharma case had not settled the questions whether Right to Privacy is a Fundamental Right within Part III of the Constitution. Hence, it could not be established that Right to Privacy is a Fundamental Right within the Constitution.[iii]

In **Kharak *Singh* v. *State of Uttar Pradesh***.[iv] In this landmark case, the Court was tasked with determining the legality of police surveillance on individuals with criminal records, including domiciliary visits. The case involved an individual who faced intrusion by the police during nighttime visits, authorized under Regulation 236(b) [v] of UP Police Regulation, allowing domiciliary visits at night.

An aggrieved individual went to court and challenged the actions arguing that they violated his liberty as guaranteed under Article 21's 'right to personal liberty.' The majority of the judges, however contended that the right to privacy was not explicitly provided for within the fundamental rights that the Constitution gave to its citizens. On the other hand, however they acknowledged that the right to privacy would fall within the ambit of common law rights applicable to citizens.

Interestingly, only two out of the seven judges concurred that regardless of the absence of an explicit mention of the right to privacy in the Constitution, it remained a fundamental right intrinsic to personal liberty. Justice Subba Rao, in his opinion, asserted, "It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty." This divergence in opinion laid the groundwork for subsequent developments in recognizing the right to privacy in the legal landscape of India.[vi]

In ***Govind* v. *State of Madhya Pradesh***.[vii] Here, the petitioner contested certain police actions, asserting that they infringed his right to privacy. Once again, the bench reflected a split opinion, with only three judges inclined to interpret the matter through the lens of the right to privacy.

Among the judges, one judge argued that individuals should be free from government interference unless there is a reasonable basis for it. Justice Mathew expressed this, stating, "Rights and freedoms in the Constitution ensure that individuals and their personal matters are free from official interference, except where justified." This view, echoing Professor Corwin's idea of "liberty against government," highlights how many fundamental rights contribute to protecting privacy from undue governmental intrusion. Despite the divided stance, these discussions laid the groundwork for evolving interpretations of privacy rights in subsequent legal proceedings and set the stage for the eventual recognition of the right to privacy as a fundamental right in later landmark judgments.

In ***R. Rajagopal* v. *State of Tamil Nadu***[viii], There was a clash between the right to privacy and freedom of speech when a Tamil Nadu news magazine wanted to publish the autobiography of a death row convict 'Auto Shankar.' The state wanted to stop it because of its revelations regarding the nexus of criminals with the police. The Court confronted a basic question: Can a citizen prevent the publication of his or her life story? Does free speech allow the press to print unauthorized accounts, and if so, under what conditions? The Court ruled that although free speech is constitutionally protected under Article 19(1)(a), it cannot be absolute and must be balanced against the right of privacy. The judgment underlined the fact that people have the rights to control the diffusion of personal information, and it marks the watershed in defining the privacy boundaries and press freedom boundaries. The Court explained that the "Right to life and personal liberty" under Article 21 would include the right to privacy, meaning the "right to be let alone." Individuals could protect personal matters like marriage and family from unauthorized disclosure, which would infringe on the right to privacy and cause legal consequences. In contrast, information in the public domain via verifiable records or legal proceedings is no longer private and may be discussed without infringing on rights to privacy.

The Supreme Court's case of **Mr. 'X' v. Hospital 'Z'** addressed the privacy of blood donors' medical records. The court acknowledged the inherently private nature of medical records but

acknowledged exceptions in cases where non-disclosure might jeopardize public health and safety. The case highlighted the delicate balance between privacy and public interest, particularly in criminal cases or health-risk situations.

The court decisively ruled that such inspections amounted to a clear violation of the principles outlined in Article 14[ix], 19, and 21[x] of the Constitution, as they failed the test of reasonableness.

The SC articulated that any test pertaining to constitutionality should meet three essential criteria, as established in ***Maneka Gandhi* v. *Union of India***[xi]. These three tests, collectively known as the triple test:

- The procedure in question should be well-established.
- The process should ideally align with the fundamental rights outlined in Article 19 that are applicable to the specific context.
- The procedure must also undergo scrutiny under the principles outlined in Article 14.

paramount importance, the Court elucidated that the term privacy refers to the citizen itself and not a place. Therefore, be it at home or bank, the simple fact that financial data is about a private citizen would always have the data under protection as a matter of national law. The case law, thus, focused on the fact that provided that data refers to the citizens then, the data would definitely fall under the protection of citizens' right to privacy, provided it does.

In ***J. K. S. Puttaswamy* v. *Union of India***[xii], "The right to privacy is protected as an inherent facet of the right to life and personal liberty under Article 21, and is an integral part of the rights enshrined in Part III of the Constitution." This landmark judgment established the constitutional basis for the right to privacy in India, acknowledging its essential role in upholding fundamental human rights.

3. Evolution of the Digital Data Protection Act in India

India's journey towards data privacy protection has been a gradual one, evolving from fragmented regulations to the current comprehensive framework. Here is a timeline of key milestones:

Before the advent of information technology (IT), there were minimum legal safeguards for data protection in India. Privacy rights were mostly protected under common law principles. Unfortunately, there was no specific data protection laws existed. In 2000 the IT Act was passed. This Act was a pivotal step, providing legal recognition to electronic records and facilitating e-commerce. However, it lacked comprehensive provisions for data protection, leading to concerns about the vulnerability of personal information. Furthermore, in 2011, The Information Technology defined sensitive personal data and outlined additional security measures for its handling. In 2017, The Court declared privacy like fundamental right, paving the way for a comprehensive framework. Further Srikrishna Committee has been constituted for the advancement of data protection and it submitted its Report in 2018 in response to growing concerns, the Indian government constituted the Justice B.N. Srikrishna-led committee to draft a comprehensive data protection law.

The committee's report laid the groundwork for the subsequent legislation. The first draft of the PDP Bill was introduced, setting the stage for a more robust data protection regime.[xiii] Further in 2019 The PDP Bill was revised and reintroduced, facing several rounds of public consultations and industry critiques. Finally, in 2023 the DPDP Act was passed, marking a landmark moment in India's data privacy journey.

4. Digital Personal Data Protection Act, 2023

This is a landmark legislation designed to safeguard personal data while balancing individual rights and organizational responsibilities. It establishes a robust framework for the processing, storage, and transfer of personal data in India.

4.1. Objective of the Act

To craft adaptable regulations that align with evolving technological trends and can be revised as per the requirements of the country's digital infrastructure. An easily accessible adjudicatory mechanism for online civil and criminal offences is to be established, ensuring swift remedies, resolution of cyber disputes, and the enforcement of the law on the internet. A legislative framework will be designed with overarching governing principles to ensure compliance.

4.2. The salient feature of the Act

The Digital Information Act (DIA) is set to replace the IT Act, which, after two decades, no longer adequately addresses the evolving challenges and opportunities presented by the dynamic growth of the internet and emerging technologies.

- The framework of the DIA will centre on crucial elements such as online safety, trust, and accountability. It aims to ensure an open internet while also regulating new-age technologies like AI and blockchain.
- Together with the other related Acts and policies, including but not limited to DPDP Act, Digital India Act Rules, National Data Governance Policy, and amendments into Indian Penal Code for Cyber Crimes, DIA provides complete legal infrastructure.
- The DIA is set to review the 'safe harbour' rule, which currently protects platforms like Twitter and Facebook from being held responsible for content created by their users.
- With a focus on enhancing consumer protection, the DIA introduces stringent Know Your Customer (KYC) requirements for wearable devices utilized in retail sales. Non-compliance may result in criminal law sanctions and penalties.
- Crucially, the DIA aligns with the Digital India Goals for 2026, aiming to establish a USD 1 trillion digital economy and actively contribute to shaping the future of global technologies.

The DPDP Act 2023 encompasses a comprehensive set of laws delineating the inherent rights of individuals and the corresponding obligations of data fiduciaries. Here are some pivotal provisions and objectives encapsulated in this groundbreaking legislation:

- **Definition of Child**[xiv]

The legislation considers anyone under the age of 18 as a child. It emphasizes the importance of safeguarding the personal data of children and individuals with disabilities, recognizing their unique vulnerabilities.[xv]

- **Restriction on Applicability and Publicly Available Data**

The Act limits the scope further by excluding data that, through a legal obligation, is made public by a Data Principal or any other person. This provision is intended to limit the scope of applicability of the Act where the information is not available in the public domain as a result of legal obligations.[xvi]

- **Consent Request and Notice Mandate**

The Act provides that any consent request made to a Data Principal under Section 6 is required to be accompanied by notice issued by the Data Fiduciary. Notice should state the purpose of processing, explain how the data principal may exercise his rights in sections 6(4) and 138, and explain how to complain to the Data Protection Board.[xvii]

- **Specifics on Consent**

The outlines the requisites for obtaining consent, specifying that it must be "free, specific, informed, unconditional, and unambiguous," requiring a clear affirmative action from the Data Principal. The provision further emphasizes the right of the Data Principal to withdraw consent at any time. Importantly, it clarifies that the withdrawal of consent does not preclude the processing of personal data if allowed by the Act even after consent withdrawal.[xviii]

- **Government Bypass of Consent Requirements:**

This Act provides the government with the authority to circumvent consent requirements in situations where a beneficiary of government services has previously consented to receive any other benefit from the state. While streamlining the process for obtaining the personal information of beneficiaries to deliver government services, it also raises concerns about the potential aggregation of government databases.[xix]

- **Verifiable Consent for Children:**

This Act imposes the obligation on a Data Fiduciary to obtain verifiable consent from the parent or lawful guardian of a child or person with a disability before processing their data. Violations attract significant penalties, up to 200 crore rupees. However, the specific details of the verification process and conditions for potential exemptions granted to businesses are left unspecified in the provision.[xx]

- **Transfer of Personal Data to Other Countries:**

This Act permits the transfer of personal data by a Data Fiduciary to another country, subject to restrictions imposed on certain countries through notification. However, the criteria for selectively imposing such restrictions are not explicitly stated. This leaves ambiguity about the circumstances and considerations that would warrant restrictions on data transfer to specific countries.[xxi]

- **Exemption for Processing Activities Related to Law Enforcement:**

According to this Act, notice and consent requirements are waived for processing activities related to the prevention, detection, investigation, or prosecution of any offence or violation of any law.[xxii]

- **Comprehensive Exemption for Government Agencies:**

This Act grants a comprehensive exemption from the entire legislation to any government agency officially informed by the government to safeguard sovereignty, security, integrity, and public order. This provision reflects the intention to entirely exempt certain government agencies from the implementation of the Act.[xxiii]

- **Exemption for Certain Data Fiduciaries:**

This Act empowers the government to exempt specific Data Fiduciaries from the provisions of the Act, including the requirement to give notice for consent to data principals as mandated by Section 5. This exemption raises concerns as it undermines an individual’s right to data protection and privacy. The exemptions for state instrumentalities, based on vague grounds, may potentially result in unchecked state surveillance.[xxiv]

- **Government Authorization to Exclude Firms or Enterprises:**

The government is authorized to exclude any firm or group of enterprises from applying specific provisions of the law within five years from its initiation. The provision lacks clarity on the duration and guidelines for implementing this exemption, posing a risk of undermining the legislation's intended objective. This provision may be susceptible to misuse, potentially compromising the overarching goals of the law.[xxv]

- **Constitution, Powers, and Functions of the Data Protection Board of India (DPBI):**

Chapter Five provides a comprehensive overview of the establishment, powers, and functions of the DPBI. The Board's functions encompass ensuring compliance with the law and the authority to impose penalties.[xxvi]

- **Qualifications for Chairperson and Members:**

Outlines the qualifications for the Chairperson and Members of the Board. While the provision requires expertise in legal matters for at least one member, it could benefit from more specificity in delineating qualifications. The current mandate, albeit ensuring legal expertise, could be enhanced by explicitly stating the desired qualifications and expertise required for other members as well. This would contribute to a more robust and specialized composition of the Board, fostering a diverse range of skills and knowledge necessary for effective governance in the realm of data protection.[xxvii]

- **Authority of the DPB Chairperson:**

Additionally, the DPB Chairperson is vested with the authority to delegate any board member the capacity to perform "any of the functions of the board and conduct any of its proceedings." This provision grants flexibility in assigning responsibilities among board members.

- **Withholding Authorization for the Legal Member:**

However, it is noteworthy that the chairperson is empowered to withhold authorization for the legal member of the board to oversee the proceedings leading to the imposition of a penalty. This aspect may raise questions regarding the potential impact on the impartiality and independence of the legal member in executing their role. Clarity on the circumstances under which such withholding is permissible and the safeguards in place to ensure fair proceedings would be essential for maintaining transparency and the integrity of the DPB's functions.

5. Suggestions

In the light of foregoing discussion, it is suggested to-

1. Conduct a data mapping exercise to identify personal data collected, stored, and processed across departments.
2. Develop a data governance framework with policies for data handling, consent mechanisms, data minimization, and retention schedules.
3. Implement robust security measures to safeguard personal data from unauthorized access, loss, or damage.
4. Train employees on data privacy responsibilities and compliance with the Act.
5. Appoint a Data Protection Officer (DPO) to oversee data protection compliance.
6. Stay updated on regulatory developments and adapt practices to comply with guidelines.
7. Become familiar with your rights under the DPDP Act, 2023, including access, rectification, and erasure of data.

6. Conclusion

In conclusion, the journey of data privacy in India has been a nuanced evolution, weaving through historical principles, constitutional interpretations, and landmark legal cases. From ancient laws to constitutional battles, the right to privacy gradually unfolded, culminating in the DPDP Act, 2023.

The legal landscape navigated through pivotal cases like Kharak Singh, Govind, and R. Rajagopal, establishing the delicate balance between individual privacy and governmental actions. The watershed moment arrived with the Puttaswamy case, where the Supreme Court declared privacy

as a fundamental right. The evolution extended to data protection laws, leading to the comprehensive the Act.

This Act addresses challenges posed by evolving technologies. It introduces crucial provisions, defining rights, emphasising informed consent, and establishing a framework for cross-border data transfer. As India strides through this dynamic data privacy landscape, the Act stands testament to the nation's commitment to safeguarding individual rights in the digital era. The journey, intricate in its details, highlights the delicate balance between privacy, technological advancements, and societal well-being.

References

[i]1997 1 SSC 30.

[ii]AIR 2017 SC 4161

[iii]*MP Sharma v. Satish Chandra,* (1954 AIR 300, 1954 SCR 1077).

[iv]AIR 1963 SC 1295.

[v]UP Police Regulation, 1860, Para 236(b) stipulates that the state's endorsement of domiciliary visits is considered unconstitutional, as it goes against the provisions of Article 21 and lacks a legal foundation to legitimize the actions taken by the state.

[vi]Kharaksingh V. State Of Uttar Pradesh (1964) SCR (1) 332.

[vii]AIR 1975 SC 1378.

[viii]1994 SCC (6) 632.

[ix]Constitution of India, 1950, Art. 14.

[x]*Ibid.*

[xi]AIR 1978 SC 597.

[xii]AIR 2017 SC 4161.

[xiii]Justice BN Srikrishna Committee Submits Data Protection Report, available at https://www.drishtiias.com/daily-news-analysis/justice-bn-srikrishna-committee-submits-data-protection-report, last visited on 12 January 2024.

[xiv]The Digital data Protection Act, 2023, Sec. 2(f).

[xv]*Ibid,* Section 2(f).

[xvi]*Ibid*, Section 3(c)(ii)(B).

[xvii]*Ibid,* Section 5.

[xviii]*Ibid,* Section 6.

[xix]*Ibid,* Section 7(b).

[xx]*Ibid,* Section 9.

[xxi]*Ibid,* Section 16.

[xxii]*Ibid,* Section 17(1)C).

[xxiii]*Ibid,* Section 17(2)(a).

[xxiv]*Ibid,* Section 17(3).

[xxv]*Ibid,* Section 17(5).

[xxvi]*Ibid,* Chapter five.

[xxvii]*Ibid,* Section 19(3).