RESEARCH COMMUNICATIONS
(An International Open Access, Peer Reviewed, Multidisciplinary Online Journal)
https://research-communications.cmpcollege.ac.in
C. M. P. DEGREE COLLEGE
(A Constituent P.G. College, University of Allahabad)

Volume-3, Issue-2, July-December 2025, pp 32-38 ISSN: 2584-1270
DOI: doi.org/10.65719/RC.3.2.2025.032

PRIVACY IN THE DIGITAL AGE: A CRITICAL STUDY OF THE DPDP ACT 2023 AND ITS IMPLICATIONS

Praveen Yadav[1] & Rajesh Yadav[2]

Research Scholars
Faculty of Law, University of Lucknow, U.P.
E-mail: *yadavrajpraveen@gmail.com & rydv371@gmail.com*

Abstract

The right to privacy has become one of the significant rights of the digital era and is strictly connected with human dignity, autonomy, and free choice. As the internet, artificial intelligence, and big data continue to grow at incredible rates, corporations, governments, and digital platforms are gathering, storing, and analysing personal data in scale. This has brought great concerns on the issue of surveillance, profiling and misuse of data. In India, the awareness of a right to privacy as a priority provided in the Constitution under Article 21 of the Constitution in Justice K.S. Puttaswamy v. Union of India (2017) developed a constitutional directive of a robust data protection framework. In reaction to this, the Digital Personal Data Protection Act, 2023 (DPDP Act) was made the first national law to deal exclusively with digital personal data. The Act provides rights of individuals, responsibilities of organizations and a Data Protection Board to oversee it. It also concerns questions such as consent, cross-border data transfer, and the penalties for violation. Nonetheless, it is left with loopholes, including broad government exemptions, no special protection of sensitive data, and worries about the independence of the regulator. In this work, the DPDP Act is critically analysed in comparison with international standards and discussed as to whether it is appropriate to balance privacy, state power, and digital innovations.

Keywords: *Privacy Rights, DPDP Act, Data Protection Board of India, Global Data Protection Frameworks, Surveillance and Profiling.*

Introduction

Privacy has always been associated with dignity and liberty however; in the context of time the meaning of privacy has changed. In contemporary theories, it is seen in three accounts, as the control of the personal information, the right of the human dignity not to be invaded, and as informational self-determination, the right to determine how personal data are gathered and used.[1] Online tracking, profiling, and biometric databases such as Aadhaar, among other challenges to privacy, are new risks in the digital world that increase the chances of surveillance and misuse. It evokes a grave concern regarding individual's freedom, autonomy and consent. Justice K.S. Puttaswamy has solidified the value of privacy in the case of Union of India 2017, where the Supreme Court had proclaimed it a fundamental right and a right under Article 21 of the Constitution. The Court believed that the chief element of dignity, liberty and freedom of choice lies in privacy. This historic judgment established the basis of enhanced privacy and established the constitutional imperative of the data protection legislation in India.[2]

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the first comprehensive privacy legislation in India influenced by the growing digital landscape and a series of data misuse scandals in the country, including the Aadhaar Privacy scandal, Cambridge Analytica and Pegasus spyware. The data breaches witnessed regularly in banks, telecom, and government databases further revealed the necessity to have a more robust protection. To counter this, the Justice B.N. Srikrishna Committee (2017) provided a

framework that accepted privacy as a basic right, and demanded an independent regulator. According to its report, the Personal Data Protection Bill, 2019 was proposed based on the GDPR of the EU and contained the following provisions: data fiduciaries, sensitive personal data, location of data and user rights including the right to be forgotten. The Bill was however criticized as allowing broad government exemptions, imposing high compliance costs, and leaving a regulator in the control of the state and was withdrawn in 2022.[3] It was followed by a simplified draft, the DPDP Bill, 2022, which abandons the strong focus on localization and the use of sensitive data categories but remains based on a consent-based model but offers far-reaching government authority. This eventually led to the adoption of the DPDP Act, 2023, a more friendly to the business and less extensive law than the 2019 draft, though still an important milestone in the privacy history of India. The DPDP Act, 2023 was introduced in Parliament on 3rd August 2023 and passed by both Houses within days and received Presidential assent on 11thAugust 2023. It is the first Indian digital personal data law which is specific and general. It goes online or digitized offline personal data and it is extraterritorial i.e. it is applicable to entities outside India so long as they offer services to people in India. It gives rights to people referred to as data principals to have access to their data, correct and delete the information. Data fiduciaries must be accurate, secure and report breaches as soon as possible. A Data Protection Board of India has been established to watch over the compliance and to settle disputes.[4]

The Act has its flaws despite these accomplishments. The critics note that the regulator is not independent in essence since he is closely linked to the central government. It does not cover non-digital personal information and only deals with digital information, which is a limitation to its scope as compared to international standards like the GDPR. The privacy protection has also been jeopardized by the fact that the government has received wide exemptions. The DPDP Act, 2023, in general, can be described as a long and controversial struggle by India to safeguard data scandals and make privacy a central right in the court, the 2019 Bill which was ambitious but did not succeed and a new, more straightforward law. Even though it is not a perfect solution and leaves the majority of the concerns untouched, it is a success of the India privacy system. It offers the constitutional right to privacy with a legal foundation and a point of departure in order to regulate the rapidly expanding digital economy in India. The implementation is the real test and the power of the law and subsequent amendments to seal the loopholes in the law to create a balance in the protection of individual rights, support of innovation and national security.

Conceptual and Legal Framework of Privacy

The Oxford dictionary defined the word 'privacy' as a state in which one is not observed or disturbed by other people, or the state of being free from public attention.[5]

Privacy has never been associated with anything less than human dignity and in the age of computer it has become a lot bigger. Priorly, it was primarily considered to be the privacy of personal life against external intrusion. However, the simplest online activities, such as a search, any purchase or a visit to the social media leave a digital footprint. This data is collected and analysed by companies, governments, and other parties without even the knowledge of individuals. This has resulted in as the surveillance capitalism where personal information is an important asset. The actions of the people or any individual in monitored by technology that displays a specific advertisement, affect their opinions, and even forecast or determine the decisions based on AI and large data. The legal progress of privacy in India started reluctantly. In M.P. Sharma v. Satish Chandra (1954)[6] and Kharak Singh. U.P. v. State of (1962)[7], the Supreme Court did refuse to recognize privacy as a right. This was altered in the case of Justice K.S. Puttaswamy v. Union of India (2017)[8], a nine-judge court decided to unanimously establish that privacy is a right of fundamental value under Article 21, which is central to dignity, liberty, and autonomy. The Court identified the various aspects of privacy, spatial, decisional, and informational, and established the test of proportionality on restrictions. It was a landmark decision that formed the basis of privacy jurisprudence in India and led to the Digital Personal Data Protection Act, 2023.[9]

The highest standards of privacy legislation globally are the EU GDPR, which provides high-level rights such as consent, access, erasure, and portability of the data, and imposes rigorous responsibilities on the

organization.[10] The U.S. is still fragmented, but it has legislation, such as the California Consumer Privacy Act (CCPA), but international bodies, such as the OECD Guidelines, and the APEC Privacy Framework, emphasize responsibility and cross-border data flows. Overall, nowadays, privacy is not only a personal right, which is based on dignity, but also a legal protection against intrusion. The digital age renders it more critical than ever not only as a personal preference but as a pillar of government, technology and human rights.[11]

Salient Features of the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the first explicitly comprehensive law in India to govern the collection, processing, storage, and use of digital personal data. The DPDP Act represents a significant change in the narrow protections of the Information Technology Act, 2000, to a modern and comprehensive privacy legislation. It is conducted on the principles of consent, accountability, transparency, and proportionality. The Act applies to all digital personal data in India, both online and subsequently digitized. It also extends to those not in India provided they process personal data and provides goods or services to individuals in India. Meanwhile, it excludes personal or household use of data, data released by the individual, and law-mandated processing. This extensive coverage guarantees that even foreign organizations that deal with the information of Indian citizens can be held accountable to law.[12]

The Act provides definitions so as to eliminate ambiguity. A data principal is the person to whom the personal data is associated and in the case of children or of people who are incapacitated, it pertains to parents or legal guardians. Any entity, be it a company, government agency, or individual is a data fiduciary that determines the purpose and method of processing personal data. Processing is defined in a broad sense to include all activities of collection and storage through to sharing, transfer and erasing. Such definitions bring clarity on the roles and responsibilities of the rest of the actors in the data ecosystem. The Act is based on consent. Personal data may only be processed by free, specific, informed and unambiguous consent of the data principal. The Act states that consent should be achieved by a clear communication in plain language, not a technical and legal one. Notably, the consent can be withdrawn any time and the termination should be equal to consent. In the case of children below 18 years, verifiable parental consent is compulsory. This framework gives persons meaningful control over their data and avert coercive or misleading consent systems such as pre-ticked boxes.[13]

Digital Personal Data Protection (DPDP) Act, 2023 proposes Significant Data Fiduciaries (SDFs)organizations that process high volumes of personal data or that process sensitive or more risky data with greater privacy implications. Government has an opportunity to designate SDFs according to their data volume, sensitivity, or impact on the country and those have to appoint Data Protection Officer (DPO), produce impact assessment and be audited. The Act permits cross-border data transfers, with the exception of countries which are deemed by the government, and data localization policies of the previous drafts without compromising on international trade and security. In order to keep the compliance, it puts massive fines up to 250 crores as a penalty in case of violations such as security lapses, breaches, or misuse. The existence of the Data Protection Board of India that is in charge of monitoring compliance and investigating violations and imposing fines leads to oversight. Nonetheless, its autonomy is undermined as its members are selected by the government, but its creation is one of the milestones in the Indian privacy policy.[14]

The Act gives a number of rights to individuals to protect the autonomy of their personal data. The data principals have the right to information regarding what personal data are being processed, the purpose and the sharing of the data also. They also can require correction of their personal information, its completion and updating. It is also worth noting that they have a right to erasure of the personal data as it is not required any longer or the right is withdrawn. The Act also provides individuals with the right of grievance redressal. They can also resolve their grievances with the data fiduciary and in case they are not satisfied with the resolution then they can go to the Data Protection Board of India. These rights give strength to the role of the individual in the digital ecosystem and responsibility. The Act also subjects data principals to some rights obligations as well as rights. False and frivolous complaints, submitting false

information, and misusing their rights through assuming the identity of another individual falls outside the rights of people. To ensure the law is not abused and a reasonable balance is provided to persons and data fiduciaries, the following are some of the intended roles. In the meantime, the Act imposes significant responsibility and liability on the data fiduciaries to protect personal data. They should make sure that the data processing is carried out so that it is possible only with the consent and that they have measured security measures that can prevent any kind of breach of information. In case of breach, they should inform not only the data principal who is affected by the breach but also the Data Protection Board of India. In order to effectively address complaints, it is also the duty of fiduciaries to post contact information of grievance redressal officer. Such responsibilities support the concept of accountability and make sure that fiduciaries cannot misuse data without accountability.[15]

Thus, the DPDP Act 2023 aligns India with the international standards of privacy and adapts the rules to the domestic requirements. The Act will create a comprehensive data protection regime by defining rights and responsibilities of individuals and organizations, creating a consent-based model, controlling cross-border transfers, and by establishing a Data Protection Board. Although some questions have been raised regarding government exemptions and regulatory autonomy, the Act is nonetheless a very important step of ensuring the privacy of more than a billion Indians during the digital age.[16]

Critical Analysis of the DPDP Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a catchword in the history of privacy and data regulation in India. It happens to be the first nationally-focused law on personal data protection to be enacted in years of debate, committee and draft bill deliberations. The Act is created in the era of digital technologies ruling the day, and the issue of surveillance, profiling, and misuse of data are the frequent concerns. Although it is a big step towards the right direction, the DPDP Act also poses relevant questions concerning the scope, protection, and enforcement. The solution of balancing both privacy and innovation and governance require a critical analysis of its strengths and weaknesses of the issue to have a balanced critical analysis. The initial strength of the DPDP Act is that it is the first act concerning data protection in India. Prior to its enactment, the protection of data in India was covered by the few scattered provisions of the Information Technology Act, 2000 and the Information Technology Act rules, which were insufficient to address the contemporary demands of an algorithmic profiling, cross-border data flows and data breaches at scale.[17] The Act, which creates a complex system of provisions, closes a long-term legislative loophole and provides a statutory support to the constitutional right to privacy identified in the case of Justice K.S. Puttaswamy v. Union of India (2017).[18]

The Act is based on the principle of data processing consent that must be free, informed, specific and revocable. The individuals who are referred as the data principals, still retain the meaningful control over the manner and location where their personal information is being collected and utilized. Children who are below 18 years would require the approval of their parents, which adds protection. These safeguards protect online users and prevent the use of vague consent forms. The act also gives key rights to the data principles to know how the data is used, corrected or deleted and can file a complaint. The rights are important in India, where privacy of data is not too strong and individuals lack power against large companies or the state. The Act is aimed at minimizing the power gap between data subjects and data fiduciaries by codifying these rights to provide greater safeguarding of personal autonomy.[19] The strength is a consent-based model, which is the same as world practices such as the General Data Protection Regulation (GDPR) in the EU.

The Act has also established the Data Protection Board of India to provide compliance enforcement, which is also not very independent. The Board might not be a strong and independent regulator since the members are appointed and regulated by the central government. To achieve effective protection of data, an effective independent body is needed, which is similar to the European Data Protection Board in the GDPR. The absence of independence in the Board poses a threat of regulatory capture and low accountability hence credibility. The Act does not also cover such crucial questions as profiling, algorithmic decision-making, and misuse of children data. The lack of algorithmic fairness and profiling rules is a significant gap with AI determining outcomes. Parental consent is mandatory to the data of

children; however, the Act does not control target advertising to minors and their security on the Internet.[20]

The DPDP Act, despite having strength, has various weaknesses. The most debated is Section 17, which grants the government broad exemptions for reasons like national security or foreign relations, raising concerns of mass surveillance and state overreach. The lack of distinction between sensitive and non-sensitive data, unlike the 2019 Bill, leaving high-risk data like health, biometrics, and finance less protected.[21] For businesses and startups, the Act is lighter than earlier drafts, removing strict data localization and sensitive data rules, which eases compliance and encourages investment. However, this comes at the cost of weakening privacy protections.

The dilemma arises in the need of maintaining the privacy rights without violating innovation.[22] The balance approach in the Act can also be observed in its efforts of cross-border data transfers. Instead of the blanket restrictions, it permits transfers to all jurisdictions except those that are signified by the government as restricted. This elasticity is favourable to business firms that are involved in international business but leaves much room to the government that could be subject to arbitrarily in decisions. The DPDP Act, 2023 is the first comprehensive data protection law that acknowledges the individual rights and complies with global standards on consent and accountability. But it still has gaps, particularly the government accountability, self-governing, and safeguarding against risks such as profiling and AI-based decision making. Its success will be determined by how well the laws are implemented and the strength of the Data Protection Board, outreach the information to the people and judicial control of government exemptions. When implemented effectively, the Act will be able to foster digital trust, individual empowerment, and innovation and economic development. Otherwise, it will become another symbolic law that does not offer anything significant as the protection in practice.[23]

Another significant difficulty consists of enforcement. India's digital ecosystem is vast and diverse, with large multinational companies, small startups, and informal digital service providers. Compliance on this spectrum will not be easy, particularly as smaller organizations are often not knowledgeable in the art of data protection. The Data Protection Board is unproven; thus, it is not clear how successful it will work in practice. The major problem of the DPDP Act, 2023 is that it tries to balance the right to privacy with other competing priorities like innovations, national security, and the development of the economy. Although the Act has the promise of protecting privacy, in that it acknowledges individual rights and data fiduciary responsibilities, its widely-seen state exemptions are heavily biased toward national security. This forms a conflict between the privacy rights assurance and the state power reality.

Implications of the DPDP Act, 2023

The Act is a major development in India's legal and digital sphere. The Act enhances the privacy rights and increases the issues of government surveillance. It makes businesses more expensive to comply with and assists in gaining consumer trust. To the government, it concentrates the power, which should be checked against excess. Its achievement relies on its enforcement, exemptions, and emphasizing individual rights over surveillance, innovations, and development. When done prudently it would give India a safe and privacy-conscious digital future.

The Act proposes the first system of protection of personal data in India, whose effectiveness requires the proper implementation of rights, obligations, and checks. It makes the citizens or the data principals in control as it grants them the right to access, correct and delete, as well as seek redress as a further means of controlling their online data. However, the Act is not risk free. The government with broad exemptions in the name of national security, civil order and other state interests as Section 17 provides. This introduces the threat of monitoring or intrusion, which will undermine the privacy promised otherwise. As citizens obtain means of exercising informational self-determination, the equilibrium between privacy and the state power is tenuous.[24] The Digital Personal Data Protection Act 2023 is a historic law which reforms the regulation of personal data in the digital era in India. It has different consequences and impacts on people, companies, government, and the digital economy as a whole.

The investment in the legal-tech solutions, infrastructure, and trained professionals will be required to build consent frameworks, grievance redressal systems, and cybersecurity measures. Although these

measures enhance accountability, they also render compliance to be expensive. On the one hand, the companies that would be complying would gain more consumer confidence and it is essential in the current data driven economy. The government is also greatly affected by the Act.

It enhances the possibility of the State as a data fiduciary since it mandates the legal and open data processing. Meanwhile, the Act also provides to the government with very broad discretionary powers in terms of which it can relieve its agencies of various obligations under Section 17.[25] The Act comes with both liabilities and issues to the companies that handle a significant number of personal information. Companies must comply with strict laws of information gathering, processing and storing such as receiving informed and explicit permission. They should also ensure that they are correct, security measures are in place and inform authorities and the affected persons in case of a data breach. Startups and small enterprises may find compliance that are of special concern.

This is a strong and controversial dual role. Although the State is justified to make exemptions in the interest of national security, sovereignty and public order, such power can also lead to the danger of its use to promote mass data collection and surveillance. With no robust checks and balances, there is the question of whether the State as such will be answerable to the law. The efficacy of the Data Protection Board which is a body consisting of the Central Government will then be critical in establishing how far the government agencies will be held accountable. At a larger level, the DPDP Act has an extensive implication on the digital economy of India.

The Act establishes confidence among people in online transactions by establishing a proper legal framework on personal data. This trust is topmost in the area of e-commerce, fintech, and digital healthcare where sensitive personal information is regularly shared. India is enhanced to comply with the international data protection regulations such as the GDPR. This would boost the cross-border data flows, investor confidence, and foreign business to pursue safe jurisdictions to pursue data with appropriate coordination. The compliance requirements shall consequently undermine innovation especially in scenarios where a small company has few resources. This will compel the policymakers to trade-off between privacy and business friendliness.[26]

Conclusion & Suggestions

Technological and digital advancements are happening at a much faster pace than relevant legislative and regulative initiatives. Privacy is one of the significant rights in this era, as it guarantees human dignity, autonomy, and freedom of choice. With the emergence of an era of surveillance capitalism, artificial intelligence and big data, personal information is being gathered and utilized more than ever before. The Digital Personal Data Protection Act, 2023 is a significant move towards India against this backdrop. The Act recognises privacy as a constitutional right, the people have the right to access, correct and delete data, and imposes obligations on firms using Data Protection Board. It is however undermined by wide government exemptions, absence of special protection to sensitive data and less independence in regulating bodies. It will succeed when the exemptions are enforced and checked well.

India should aim at creating a balance between security, innovation, and rights by continuing reforms, introducing an independent Data Protection Authority, and more restrictive government exemptions to stop mass surveillance. The protection against algorithmic profiling and AI-driven data processing should also be provided to India, because the technologies influence the most important areas of life, such as finance, healthcare, and employment, and otherwise can result in bias.

The other major factor is digital literacy, awareness and education will enable the people to know and practice their rights. India must consider updating the DPDP Act on a regular basis and aligning it with the international standards, as in the case of Europe, UK, and the U.S. to safeguard citizens and allow free digital trade and investments across the borders.

Thus, the DPDP Act is in the right direction but to be very effective, more independence, accountability and public awareness is required. Through continuous reforms, India can revert this law into a strong structure that will establish privacy in its online future.

References

1. Thapa, S. (2021). The evolution of right to privacy in India. *International Journal of Humanities and Social Science Invention, 10*(2), 53–58.
2. Rajput, S. (2025). Privacy, dignity, and liberty: A critical examination of the *Puttaswamy* case. *International Journal of Creative Research Thoughts (IJCRT), 13*(5), 306–312.
3. Dharod, V., & Tauro, K. (2023). Assessing India's Digital Personal Data Protection Act, 2023: A comparative study with the GDPR. *Indian Journal of Law and Legal Research, 6*(2), 1318–1329. https://www.ijllr.com/post/assessing-india-s-digital-personal-data-protection-act-2023-a-comparative-study-with-the-gdpr
4. Sengar, S. S. (2024). From pixels to policies: Analysing the provisions and navigating the complexities of the Digital Personal Data Protection Act, 2023. *SSRN Electronic Journal, 2*. https://doi.org/10.2139/ssrn.4547842
5. Oxford Dictionary. (2015). Oxford: Oxford University Press.
6. *M. P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
7. *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.
8. *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
9. Supra note 1.
10. Voronova, S. (2020). *Understanding EU data protection policy*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf
11. Boyne, S. M. (2018). Data protection in the United States. *American Journal of Comparative Law, 66*, 299.
12. Chaudhary, V. K., & Verma, D. (2023). The new frontier of data protection: Understanding India's DPDP rules and global compliance. *Global Compliance, 4*(22), 38–49.
13. Dalei, P. (2023). The digital personal data protection Act, 2023: A legal analysis in light of global data protection standards. *Law Journals, 11*(3), 127–131. www.lawjournals.org
14. Kalra, L. (2023, August). Decoding the Digital Personal Data Protection Act, 2023. *EY Shape the Future with Confidence*. https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023
15. Ibid.
16. Dalei, P. (2023). The Digital Personal Data Protection Act, 2023: A legal analysis in light of global data protection standards. *Law Journals, 11*(3), 127–131. www.lawjournals.org
17. Tandon, U., & Gupta, N. K. (2025). Informational privacy in the age of artificial intelligence: A critical analysis of India's DPDP Act, 2023. *Legal Issues in the Digital Age, 6*(2), 87–117. https://doi.org/10.17323/2713-2749.2025.2.87.117
18. Act, D. P., & Context, L. (2025, March). Tracing the constitutional journey of data privacy in India: From *Puttaswamy* to the draft DPDP rules, 2025—Introduction. *Journal/Working Paper*.
19. Bansal, A., & Goyal, G. (2021, December). Digital Personal Data Protection Act: A survey.
20. Purohit, N., & Elavarasi, V. B. A. (2025). Protecting children's personal data: India & beyond. *Atlantis Press SARL*. https://doi.org/10.2991/978-2-38476-426-6
21. Ibid.
22. Lakra, R., & Jha, N. (2024). Publicly available data in the DPDPA Act 2023: Interpretative, constitutional and comparative perspectives. *SSRN*. https://www.ssrn.com/abstract=4933252
23. Gajjar, N. T. (2024, May). Data privacy and protection in the digital age: Emerging trends and technologies. *International Journal of Engineering Applied Science and Management, 5*. ISSN 2582–6948. https://www.researchgate.net/publication/380721493
24. KPMG. (2023, August). Decoding the Digital Personal Data Protection Act, 2023. https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2023/08/decoding-the-digital-personal-data-protection-act-2023.pdf
25. Kumar, P., Deep, S., Raghuvanshi, S., & Kumar, V. (2025). India's new data frontier: A critical legal insight of the Personal Data Protection Act, 2023. *Library Progress International, 44*(3). www.bpasjournals.com
26. Border, & Protection, D. (2025, April). *International Journal of Scientific and Social Inquiry Research (IJSSIR), 14*(4), 124–139.