SAFEGUARDING DIGITAL RIGHTS: COMPARING INDIA'S DPDP ACT, GDPR, AND CCPA

Amrita Verma*

ABSTRACT

The digital revolution across the globe has changed everything. Unlike ever before, personal data is being collected, stored, and processed. Therefore, data protection has become a worldwide legal issue of utmost consequence. Several Jurisdictions have responded to the increasing incidents of data misuse and breaches of privacy by enacting comprehensive data protection laws. The Digital Personal Data Protection Act, 2023 (DPDPA), offers an immense leap forward toward enacting a statutory regime for the protection of personal data and aligning India with global standards of privacy. This article compares and contrasts the DPDPA, 2023, with two influential international data protection laws, the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA) of the United States. The study begins with tracing the evolution of data protection laws at a global level, highlighting how privacy has changed from a moral concept to a legally enforceable right. It then examines the key features of the DPDPA, 2023, such as consent-based data processing, obligations of data fiduciaries, rights of data principals, and enforcement mechanisms. This is followed by a detailed comparative analysis of similarities and differences between the DPDPA, GDPR, and CCPA. Further, the article considers the implications of the DPDPA in India and also discusses the limitations of the Act. The article concludes with suggestions for a way forward to strengthen India's data protection regime and strike a balance between innovation, governance, and individual privacy.

Keywords: Data Privacy, Consent, Data Breach, Personal Data, Data Protection.

*BA LLB, SECOND YEAR, UNIVERSITY OF LUCKNOW, LUCKNOW.

INTRODUCTION

In today's digitally advanced world, technology has altered the generation, collection, and dissemination of information. Among those assets, personal data has grown into one of the most coveted ones, acting as the propeller of innovation, governance, and economic growth. From digital transactions to social platforms, e-governance systems, and digital healthcare systems, millions of individuals keep sharing their personal information beyond the boundaries with the help of digital technology. Although data-driven ecosystems make life easier, they pose far-reaching risks such as unauthorised video surveillance, identity theft, profiling, and misuse of personal information through data breaches. In view of all these concerns, governments around the world have enacted well-structured laws for personal data protection within the global digital ecosystem. Globally, the benchmark in data privacy regulation has been set and shaped through the influence of the General Data Protection Regulation (GDPR)[1] of the European Union and the California Consumer Privacy Act (CCPA)[2] of the United States. Inspired by these global developments and as the country with the second-most internet-using population, India too has enacted one such landmark law concerning individuals' privacy rights, namely, the Digital Personal Data Protection Act (DPDPA) of 2023.[3] The legal framework thus entails the processing, storage, and transferring of personal data by public or private data fiduciaries. The study focuses on the evolution of data protection laws in the country, analyses the key features of the DPDPA, 2023,[4] and offers a comparative perspective with the GDPR[5] and CCPA[6] to analyse India's standing in the global data protection scenario.

EVOLUTION OF DATA PROTECTION LAWS: GLOBAL OVERVIEW

Globally: International organisations and nation-states responded by formulating comprehensive data protection frameworks to regulate the collection, use, and disclosure of personal data and to impose penalties for non-compliance. According to the United Nations Conference on Trade and Development (UNCTAD), 137 out of 194 countries (roughly 71%) have legislated data protection or privacy legislation in some form. Region-wise adoption

[1] General Data Protection Regulation (EU) 2016/679
[2] California Consumer Privacy Act 2018
[3] Digital Personal Data Protection Act 2023
[4] ibid
[5] General Data Protection Regulation (EU) 2016/679
[6] California Consumer Privacy Act 2018

includes 44 of 45 countries in Europe, 34 of 60 in the Asia-Pacific region, 33 of 54 in Africa, and 26 of 35 in the Americas.[7]

The European Union set a major global benchmark through the enactment of the General Data Protection Regulation (GDPR) in 2018. Meanwhile, in the field of data protection, the requirements introduced in the United States through the California Consumer Privacy Act (CCPA) in 2018 became effective in 2020. Other frameworks include the OECD Guidelines on Personal Data Protection (1980, revised in 2013), the APEC Privacy Framework (2005), the Personal Information Protection Law (PIPL) of China, Singapore's Personal Data Protection Act (PDPA), Canada's Bill C-27, and the United Kingdom's Data Protection Act, 2018. This is gradually indicating the process of becoming globalised in reconciling the consideration of data protection as a fundamental regulatory requirement in the digital economy.[8]

In coordination with international policy and business affairs, India has realised the need to enact a data protection act for its people. Also, being an emerging superpower, our country is attracting various kinds of global businesses trying to get established in the vast Indian market. In the process of conducting online business, the personal data of Indian citizens remains at stake. To safeguard the privacy of the Indian masses and to understand the scope of privacy law, the Government of India introduced the Digital Personal Data Protection Act,2023 (DPDPA).[9]

India: The history of the development of data protection laws in India has been a slow one, extremely influenced by constitutional interpretations and judicial recognition of privacy. The judiciary has played a conspicuous role in fostering the concept of privacy as an enforceable right, particularly in light of the absence of an explicit mention in the Constitution.

The earliest recorded judicial consideration of privacy can be traced to M.P. Sharma v. Satish Chandra (1954),[10] wherein the Supreme Court declared that there was no express guarantee of privacy under the Constitution, especially with respect to search and seizure. This notion was

[7] iPleaders, 'Digital Personal Data Protection Act, 2023: A Comprehensive Analysis' iPleaders Blog https://blog.ipleaders.in/digital-personal-data-protection-act-2023-a-comprehensive-analysis/ accessed 16 January 2026
[8] iPleaders, 'Digital Personal Data Protection Act, 2023: A Comprehensive Analysis' iPleaders Blog https://blog.ipleaders.in/digital-personal-data-protection-act-2023-a-comprehensive-analysis/ accessed 16 January 2026
[9] Digital Personal Data Protection Act 2023
[10] M.P. Sharma v Satish Chandra AIR 1954 SC 300 (SC)

pondered upon to a limited extent in Kharak Singh v. State of Uttar Pradesh (1963),[11] wherein the SC emphasised that surveillance measures which authorise "domiciliary visits" violated Article 19[12] and 21[13] of the Indian Constitution. The Court held that such an invasive police surveillance action would violate the personal liberty guaranteed in Article 21,[14] but it chose not to declare privacy as a free-standing fundamental right.

Developments in this regard had occurred in Govind v. State of Madhya Pradesh (1975),[15] wherein the Court accepted that privacy could be implicitly read into Article 21,[16] subject to overriding state interests and reasonable restrictions, while introducing a compelling state interest test from the case of Griswold vs Connecticut and Roe vs Wade, which were decided by the Supreme Court of the US.[17]

In India is PUCL v. Union of India (1997),[18] popularly known as “the telephone tapping case”. For the first time in that ruling, the Supreme Court held that an individual has a privacy interest in respect of his telephonic conversations, and unauthorised interception of such would violate Article 21[19] right to privacy. The Court held that any privacy invasion would need a procedure established by law and laid down stringent checks to avoid arbitrary surveillance by the executive. The judgment proved instrumental in linking privacy with control of personal information and communication data, thereby providing a stronger basis for future data protection standards.

The jurisprudential evolution finally culminated in the landmark judgment of Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017),[20] which recognised that the right to privacy is a fundamental right under Article 21[21] of the Indian Constitution. The Court recognised this informational privacy as an integral part of dignity and autonomy, giving rise to a constitutional mandate for a comprehensive data protection regime.

[11] Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295 (SC)
[12] Constitution of India 1950, art 19
[13] Constitution of India 1950, art 21
[14] ibid
[15] Govind v State of Madhya Pradesh AIR 1975 SC 1378 (SC)
[16] Constitution of India 1950, art 21
[17] Anurag Sourot and Deepali Kushwaha, ‘Critical Analysis of the Digital Personal Data Protection Act, 2023’ (2024) VII Indian Journal of Law and Legal Research 7356, 7362
[18] People’s Union for Civil Liberties v Union of India (1997) 1 SCC 301 (SC)
[19] Constitution of India 1950, art 21
[20] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (SC)
[21] Constitution of India 1950, art 21

From a legislative standpoint, early initiatives regarding data protection were disjunctive and mainly dealt with under the Information Technology Act, 2000.[22] The provisions of Section 43A[23] and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,[24] incidentally imposed a few obligations with respect to data security and protection of sensitive personal data, largely concerning corporate entities. Nonetheless, these provisions would distinctly lack a comprehensive rights-based framework and an efficacious enforcement mechanism. But SC's judgement in Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017)[25] case, which declared the right to privacy a fundamental right under the Indian Constitution, led to the establishment of the Justice B. N. Shrikrishna Committee, which was set up by the Ministry of Electronics and Information Technology (MeitY), Government of India.[26] Following this, several drafts of the Personal Data Protection Bill were introduced, beginning with the PDP Bill 2018, followed by the Personal Data Protection Bill 2019 and the Digital Personal Data Protection Bill 2022. These earlier versions faced challenges and were withdrawn after extensive public consultation. Finally, in August 2023, the Digital Personal Data Protection Act (DPDPA)[27] was passed, marking a significant milestone in India's data protection journey.[28]

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Scope of the Act: The Digital Personal Data Protection framework applies to the processing of digital personal data in India as well as to any entity outside India which deals with the personal data of Indian citizens, thus guaranteeing protection irrespective of the place of processing of data. It includes both data that originates in digital form and non-digital data that has been digitised. However, the provisions would not apply to personal data that is processed by an individual for purely personal or domestic use, nor will it apply to personal data that has been made public or deliberately disclosed to the public.[29]

[22] Information Technology Act 2000
[23] Information Technology Act 2000, s 43A
[24] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011
[25] Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (SC)
[26] Anurag Sourot and Deepali Kushwaha, 'Critical Analysis of the Digital Personal Data Protection Act, 2023' (2024) VII Indian Journal of Law and Legal Research 7356, 7362
[27] Digital Personal Data Protection Act 2023
[28] Aishwarya Agrawal, 'Digital Personal Data Protection Act, 2023' LawBhoomi https://lawbhoomi.com/digital-personal-data-protection-act-2023/ accessed 16 January 2026
[29] Digital Personal Data Protection Act 2023, s 3

Rights of Data Principles: Data principals, "the people whose data is being processed,"[30] have several rights to control and protect their information. These include the right to know what data is being collected about them, for what purposes it was collected, and how it is being used.[31] A data principal shall have the right to rectify any processing of information that may seem inaccurate or misleading, complete any information deemed incomplete, update its personal data, and have its personal data deleted where applicable, namely upon expiry of the initial purpose.[32] In addition, they can object to certain data processing, especially when their data is being processed for purposes beyond the requested person. They may also seek the intervention of the DPB-I in cases of violation or failure on the part of the data fiduciary or the consent manager to justify the exercise of these rights.[33] If a person is unable to exercise his or her rights due to death, mental incapacity, or physical infirmity, then such a person may nominate another individual to manage his or her data on his or her behalf.[34]

Duties of a Data Fiduciary: The duties and obligations of a data fiduciary," any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data,"[35] are specified under the Digital Personal Data Protection Act, 2023,[36] for the benefit of the Data Principal. The Data Fiduciary must obtain the consent of the Data Principal for the processing of his/her data; such consent has to be free, informed, specific, unconditional, and unambiguous, given by a clear affirmative action, and relating to lawful purpose/s for which consent was given or to certain legitimate purposes. The Data Principal may grant consent, manage consent, review consent, or withdraw consent through a Consent Manager, "a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform"[37] designated for this purpose. However, consent is not a prerequisite for processing for recognised legitimate interests, for instance, supplying government services or in case of medical emergencies. According to this law, the State or its instrumentalities may process personal data to provide specified subsidies, benefits, services, certificates, licenses, or

[30] Digital Personal Data Protection Act 2023, s 2(j)
[31] Digital Personal Data Protection Act 2023, s 11
[32] Digital Personal Data Protection Act 2023, s 12
[33] Digital Personal Data Protection Act 2023, s 13
[34] Digital Personal Data Protection Act 2023, s 14
[35] Digital Personal Data Protection Act 2023, s 2(i)
[36] Digital Personal Data Protection Act 2023
[37] Digital Personal Data Protection Act 2023, s 2(g)

permits. Such processing must either be based on explicit consent or on data lawfully obtained from notified government databases, in accordance with applicable data protection laws.[38]

In the case of children or persons with disabilities, consent must be given by a competent parent or guardian. For processing children's data, the Act under Section 9[39] requires verifiable parental consent, prohibits harmful processing, and bans targeted advertising directed toward children under the age of 18. A Data Fiduciary would also be barred from processing personal data in a way that is likely to be detrimental to a child's interests unless a notification is made by the Central Government providing for an age limit beyond which certain obligations would not apply, provided the processing is implemented in a verifiably safe manner.[40]

In the event of a data breach, the Data Fiduciary shall also notify the Data Protection Board and the affected individuals of the breach within 72 hours.[41] In addition, it must implement appropriate technical and organisational measures to safeguard personal data against unauthorised access, disclosure, alteration, or destruction and must destroy personal data once the purpose of its collection is fulfilled or the legal basis for its retention ceases to exist.

SDFs: Under Section 10[42] of Digital Personal Data Protection Act, 2023, Significant Data Fiduciaries (SDFs) process large amounts of personal data or sensitive personal data and are therefore under heightened obligations. The Central Government may declare some Data Fiduciaries to be SDFs depending upon the nature and scale of their data processing activities. Such organisations are required to appoint a Data Protection Officer and an independent auditor to ensure compliance with the provisions of the Act. In addition, SDFs must carry out Data Protection Impact Assessments at regular intervals to assess and mitigate any risks to the privacy and security of the personal data they process in order to comply with the statutory requirements and safeguard the rights of the Data Principals.[43]

[38] Digital Personal Data Protection Act 2023, s 6
[39] Digital Personal Data Protection Act 2023, s 9
[40] Drishti IAS, 'DPDP Act 2023 and DPDP Rules 2025' Drishti IAS Daily News Analysis https://www.drishtiias.com/daily-updates/daily-news-analysis/dpdp-act-2023-and-dpdp-rules-2025 accessed 16 January 2026
[41] Aishwarya Agrawal, 'Digital Personal Data Protection Act, 2023' LawBhoomi https://lawbhoomi.com/digital-personal-data-protection-act-2023/ accessed 16 January 2026
[42] Digital Personal Data Protection Act 2023, s 10
[43] Aishwarya Agrawal, 'Digital Personal Data Protection Act, 2023' LawBhoomi https://lawbhoomi.com/digital-personal-data-protection-act-2023/ accessed 16 January 2026

DPBI: The Digital Personal Data Protection Act, 2023,[44] establishes an independent Body to be named the Data Protection Board of India (DPBI) and is to be the central regulatory authority for the implementation of the Act. The Board will ensure monitoring of compliance, inquire into data breaches and violations, penalize organizations for their non-compliance, and adjudicate in cases of data protection. Members of the DPBI shall be appointed by the Central Government for a period of two years, which may be renewed at the discretion of the Government.[45] As the primary grievance redressal and regulatory forum, the Board is a vital cog in the enforcement machinery of the Act, securing the rights of Data Principals. Appeals against the decisions of DPBI shall lie before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).[46]

Penalties: It must be known that the Digital Personal Data Protection Act of 2023 has provided for very strict penalties regarding non-compliance with the Act to bring about some form of accountability among Data Fiduciaries.[47] Noncompliance with adequate security measures may be penalised up to ₹250 crore (USD 30 million). Noncompliance with the specified time frame in notifying data breaches entails a massive penalty of up to ₹200 crore ($24 million). Similar penalties apply for noncompliance with the protection of children's personal data under the provisions of the Act. Failure to meet the additional obligations under the Act would attract a fine of up to ₹150 crore (approximately $18 million) for Significant Data Fiduciaries. The measures highlight the regulatory emphasis on strong data protection practices, along with the judicial or other government intervention in protecting the rights of Data Principals.[48]

COMPARATIVE ANALYSIS: DPDPA VS GDPR VS CCPA

A comparative assessment[49] of the Digital Personal Data Protection Act, 2023, with the GDPR and the CCPA reveals divergent legislative approaches to data protection, reflecting variations in constitutional values, regulatory philosophy, and the balance between individual privacy and economic interests:

[44] Digital Personal Data Protection Act 2023
[45] Digital Personal Data Protection Act 2023, s 18
[46] Ishwar Ahuja and Sakina Kapadia, 'Digital Personal Data Protection Act, 2023 – A Brief Analysis' Bar and Bench https://www.barandbench.com/view-point/digital-personal-data-protection-act-2023-a-brief-analysis accessed 16 January 2026
[47] Digital Personal Data Protection Act 2023, s 10
[48] Aishwarya Agrawal, 'Digital Personal Data Protection Act, 2023' LawBhoomi https://lawbhoomi.com/digital-personal-data-protection-act-2023/ accessed 16 January 2026
[49] Alfahive, 'A Comparative Analysis of DPDPA, GDPR and CCPA' Alfahive Blogs https://www.alfahive.com/blogs/a-comparative-analysis-of-dpdpa-gdpr-and-ccpa accessed 16 January 2026.

Aspect	DPDPA	GDPR	CCPA
Jurisdiction	India	European Union + EEA (has global reach for entities handling EU residents' data)	California, USA (applies to businesses worldwide handling Californian consumers' data)
Personal Data Definition	A broad definition of personal data, excluding non-digital data	Extensive, including all personal and sensitive	Focus on consumer personal data, limited to certain categories
Data Subject Rights	Right to Access, Correct, Port, and Erase data	Access, Rectification, Erasure, Restriction, Portability, Objection	Right to Know, Delete, Opt-out of Sale, Non-discrimination
Penalties for Non-Compliance	Up to ₹250 crore for serious breaches	Up to €20 million or 4% of global annual turnover (whichever is higher)	Up to $7,500 per intentional violation, and $2,500 for unintentional
Data Breach Notification	To be defined in future rules requires prompt notification	Notify within 72 hours of awareness of a breach	Must notify without unreasonable delay

Cross-border data transfers	Provisions on international transfers exist, but not in detail	allowed only with adequate safeguards (e.g., standard contractual clauses)	No specific provisions or restrictions exist on the sale of personal data
Sensitive Personal Data	Includes Financial data, health data, biometrics, etc.	Special category data: race, religion, health, etc.	No strict category; some protections in place
Enforcement Authority	Data Protection Board of India (yet to be fully operational)	Data Protection Authorities (DPAs) in each EU member state	California Attorney General, California Privacy Protection Agency (CPPA)
Applicability Threshold	Applicable to entities processing large amounts of personal data, specifics pending	Covers all entities processing personal data of EU residents	Applies to businesses with gross annual revenue > $25 million or handling > 50,000 consumers' data
Consent Requirements	Requires Explicit consent with limited exceptions	Explicit, informed consent required	Opt-out model; explicit consent for minors (<16 years)

LIMITATIONS

Unlimited Power and no Liability of the State: The Central Government has the authority to fix dates for enforcing various provisions of the Act. Again, the state has the power to use

citizens' personal digital information in the interest of sovereignty and integrity of India, which can be misused by government agencies in the name of national security. Similarly, under Sections 40,[50] 42[51] and 43[52] of the new law, the power of the Central Government to make rules regarding different provisions, to amend the schedule, as well as to remove difficulties in the practical implementation of the Act, could be misused for political gains by controlling large amounts of public information. Also, the Central Government is granted an entirely unfettered power to regulate and exempt major data fiduciaries without being bound to give a rationale for doing so. In a similar vein, one can presume that, if former members slack, the current Central Government would appoint and 'reappoint' members of the Data Protection Board.

No Limit on Cross-Border Data Flow: It allows personal data to be transferred without hindrance to most countries, leaving it up to the government to constrain it from this itself, raising security and sovereignty concerns.

Classification of Offences: The Act has not classified different types of online offences and the degree of offences. For example, if a data fiduciary steals digital personal data for financial gain and another data fiduciary steals it to commit a more serious crime. Will they receive the same punishment?

Ambiguity in Child Consent and Protection Mechanisms: The DPDP Act 2023[53] provides that parental consent shall be a prerequisite for processing a child's data, but the act lacks obvious clarity in relation to the manner of ascertaining that consent. Additionally, the Act permits the Central Government to declare some entities exempt from the threshold age under the child consent requirement, which dilutes the safeguards accorded to minors. Guidelines regarding age-verification/enforcement are not well-defined or completely lacking, resulting in ambiguous compliance and a potential for the misuse of data relating to children.

Gap for Lack of Awareness: One of the most significant gaps for effective implementation concerning the DPDP Act would be due to limited awareness on the part of people, parents, as well as Data Fiduciaries, about their rights and responsibilities under this law. A lot of Data Principals do not know the requirements of consent, remedies available, and grievance redressal mechanisms, while parents might not be properly aware of their role in gaining and

[50] Digital Personal Data Protection Act 2023, s 40
[51] Digital Personal Data Protection Act 2023, s 42
[52] Digital Personal Data Protection Act 2023, s 43
[53] Digital Personal Data Protection Act 2023

managing consent for children's data. This absence of awareness creates a risk of poor compliance and bad enforcement with increased chances of misuse of personal data, particularly for children and other vulnerable users.

WAY FORWARD

Curbing Excessive State Powers: The Act providing a check on the discretionary powers of the Central Government, as mentioned above, should provide for greater judicial or parliamentary oversight. The Act should clearly set out guidelines as to how personal data may be used for national security purposes; transparency in rule-making and appointments to the Data Protection Board is needed to secure its independence.

Strengthening Cross-Border Data Transfer Rules: Cross-border data flow should be regulated by clear and objective standards, rather than depending on the unilateral discretion of the government. Adoption of adequacy studies, data localisation for sensitive data, and international safeguards will go a long way toward ensuring users' privacy and data sovereignty.

Classification of Offences and Proportional Punishments: The Act must define offences in terms of seriousness and motivation clearly. With this, further equity and deterrence safeguard provisions would be given by the scaling of penalties to distinguish lesser violations from serious data misuse.

Improved Protection of Children's Data: Some definitional clarity should be provided on age verification, and perhaps stricter limits should be set on exemptions relating to children's data to ensure uniform and effective protection of minors**.**

Further Enforcement and Awareness: Any capacity building of the Data Protection Board must go hand in hand with awareness programs organised for citizens and organisations for effective compliance and enforcement.

CONCLUSION

The Digital Personal Data Protection Act, 2023,[54] serves as a significant step forward in strengthening the data protection framework in the country for the digital age. It operationalises

[54] Digital Personal Data Protection Act 2023

the constitutional right to privacy in a statutory setting through consent-based processing, defines the rights of Data Principals, and defines the obligations of Data Fiduciaries. An exercise in comparative assessment vis-à-vis the GDPR[55] and CCPA[56] reveals that while the DPDPA[57] is in keeping with the international standards in data protection, with respect to how individual privacy is governed and public interest considerations. This is an Indian way of framing things.

However, there are certain shortcomings in terms of undue discretion exercised by the state, lack of clear classification of offences, unrestricted trans-border flow of data, ambiguity with respect to the child consent mechanism, and finally, the gaps arising out of the limited awareness. Stronger and clearer rules, institutional independence, and improved awareness are necessary elements for effective implementation. Continuous edification and ensuring strong enforcement, the DPDPA[58] has the potential to evolve into a balanced and effective data-protected regime that equally does justice to individual privacy and does so under India's digital growth.

[55] General Data Protection Regulation (EU) 2016/679
[56] California Consumer Privacy Act 2018
[57] Digital Personal Data Protection Act 2023
[58] ibid