INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

PROTECTION OF CONSUMER PERSONAL DATA IN E-COMMERCE TRANSACTIONS: A STUDY UNDER THE DPDP ACT, 2023

AUTHORED BY - PALAK KAPOOR

ABSTRACT

The exponential rise of the digital economy in India has made personal data a vital economic resource, especially in the e-commerce sector, and hence, the concerns regarding privacy, autonomy, and governance have escalated. This research article will analyze the development of data protection law in India, culminating in the enactment of the Digital Personal Data Protection Act, 2023, and its effectiveness in governing the processing of personal data in e-commerce transactions. The research paper will outline the historical development of data protection law in India in three phases: the commerce-oriented regime established under the Information Technology Act, 2000; the recognition of privacy as a fundamental right under the Constitution in the case of K.S. Puttaswamy v. Union of India; and the present regime of statutory regulation, established by the DPDP Act, 2023.The article critically evaluates the conceptual framework of e-commerce data governance, emphasizing the dual character of personal data as both an enabler of e-commerce and a source of potential harm to privacy. It rigorously evaluates the set of core obligations imposed on e-commerce actors as "data fiduciaries," such as consent-based processing, purpose limitation, data minimization, storage limitation, security measures, and accountability. Additionally, the research conducts a comparative analysis of the DPDP Act, 2023 and the General Data Protection Regulation (GDPR), pointing out the most important differences in scope, legal basis of processing, rights of data subjects, independence of the regulatory authority, and state exemptions. Although the DPDP Act, 2023 is a major paradigm shift towards the structured data governance framework in India, the research argues that some of its limitations, such as the broad exemptions granted to the government and the issues of autonomy of the regulatory authority, may potentially impact its long-term sustainability.

INTRODUCTION

"Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect"[1] as quoted by Bruce Schneier an American author meaning thereby privacy is neither a legal privilege nor a means of concealment, rather it is a fundamental necessity for every individual. The author emphasizes that the capacity to manage one's own information is indivisible from personal liberty. Privacy act as a guardian of dignity as it protects the individual from transparent object of surveillance, ensuring that individuals are respected as independent beings with a right to boundary between their private life and the outside world. Data has always been closely associated with every type of governance but slowly and gradually with the advent of digitalization in tools, its usage has increased rapidly, assisting everyone while hindering many. Data collection is not a new concept, it has been continuing from many centuries even before the development of digital technologies used in collection and distribution of data. Even Mahatma Gandhi in his first Satyagraha agitated against the kind of data collection led by Britishers for Asian ethnics.[2] In today's era digital forms of governance are being used in phenomenal surge due to which government faces various challenges in combating the new dimensions (like e-commerce transactions) by using traditional techniques and hence analyzed the need to transform the government system in order to provide efficient and cost- effective services through information and communication technologies. Development in information and communication technologies led to the formation of E-government that facilitates electronic transactions.

As India moves towards a digital economy, both public and private sectors handle personal data as a routine activity. The inherent value of data increases rapidly due to which efficiency is enhanced. In current scenario almost every act of individual includes exchange of data which has led to the emergence of new marketplaces that are focused on managing and utilizing personal data.[3]

For India to play a significant role in shaping the digital future of the 21st century, it needs to establish a legal framework for protecting personal data that might set an example for other developing countries. Thus, it can be said that securing personal information is necessary for promoting growth, empowerment, advancement and creativity. There's an intrinsic understanding to develop a legal framework concerning personal data and it should be designed in a way so as to

cover all the concerns and objectives that individuals have around their personal data.

In 2017, Supreme Court affirmed privacy as a fundamental right under the constitution. After six years of recognizing privacy as a fundamental right, the nation has introduced a substantial piece of legislation related to data protection i.e the Digital Personal Data Protection Act of 2023 (DPDP Act).[4] It plays a significant role in protecting personal data. It contains concepts that are similar to General Data Protection Regulation (GDPR)[5] of the European Union that includes rights related to notification, access, erasure and limitations. The Act deals with the processing of personal data in India, along with the data digitally collected or subsequently digitized data. Additionally it applies to data outside the territory of India it it relates to the provision of goods and services within India.

HISTORICAL EVOLUTION OF DATA PROTECTION LAWS

The historical development of legislation related to data protection in India can be defined as a path of statutory silence to constitutional primacy and it can be classified into three phases. The first phase (2000-2011) deals with commerce-centric approach where privacy was purely an incidental concern under the Information Technology Act 2000. The second phase (2012-2022) represents a significant constitutional shift, as judiciary intervenes and declares privacy as a fundamental right. The third phase (2023-present) highlights the era of formal codification and enactment of a comprehensive, principle-based statute i.e Digital Personal Data Protection (DPDP) Act 2023.

Phase 1: The Reactive Era (2000-2011)

- **Information Technology Act (2000)-** The 1990's marked a technological revolution at a global level. Due to the rapid development in the domain of computer technology, software development and telecommunications internet usage has increased at a higher rate.[6] Slowly and gradually India emerged as a global center for IT services as commercial and governmental activities shifted their approach from traditional to digital by emphasizing on the activities like digital storage and transmission of data, e-contracts, e-mail communication etc. However, the existing legal framework like Indian Evidence Act 1872

and Indian Penal Code 1860 were inadequate in dealing with such changes as these were drafted in pre-digital era and relied mainly on physical documents and handwritten order to provide legal recognition to electronic records and digital signatures and thus Parliament enacted Information Technology Act 2000 enforced on October 17, 2000.

- **The Information Technology Rules, 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) –** Despite the existence of a robust IT Act 2000 it has been observed that cyber incidents were rapidly increasing, in order to curb the inefficiencies of the existing framework, an amendment has been done in 2008 in which section 43A is introduced which paved the way for 2011 rules. Section 43 A requires the body corporate to adopt "reasonable security practices"[7] while dealing with any sensitive personal data. As per Rule 3 of 2011 Rules sensitive personal data includes information related to passwords, credit/debit card information, any biometric information that are used for authentication purposes.

Phase 2: The Constitutional Era (2012-2022)

- **Justice A.P Shah Committee, 2012-** Shah Committee was established by the government of India in January 2012 in order to address the challenges posed by The Information and Technology Act, 2000 regarding privacy, data protection and surveillance and to examine the national privacy principle in the context of the emerging issues at a global level. The committee in its report recommended the framework for privacy legislation in India by suggesting five salient features namely –
    1. Technology neutrality and interoperability with international standards.
    2. Multi-dimensional privacy
    3. Horizontal applicability to state and non-state entities
    4. Conformity with privacy principles
    5. A co-regulatory enforcement regime.
- **K.S Puttaswamy Judgement, 2017- "**A 9 Judge bench unanimously declared that right to privacy is an intrinsic part of right to life and personal liberty under Article 21 of the Indian Constitution." The then honourable Chief Justice of India, Justice Dhananjaya Yeshwant Chandrachud stated that "Privacy is concomitant of the right of an individual to exercise

control over his or her personality. It finds an origin in the nation that there are certain rights that are natural to or inherent in human beings."[8]

- **Justice B.N Shrikrishna Committee, 2018-** The 2017 judgement, declaring privacy as a fundamental right prompts an immediate need for a robust personal data protection law and in consideration to that Government of India constituted a committee under the leadership of Justice (Retd.) B.N Shrikrishna to draft a suitable data protection law for India. One of the main aspect of the report is the individual consent in relation to their personal data and obligations of fiduciaries including states and entities. The committee has also proposed a draft of Personal data Protection Bill.
- **Personal Data Protection Bill, 2019-** In 2019, Personal Data Protection Bill was introduced in Lok Sabha by the Minister for Electronics and Information Technology and incorporates several changes from 2018 draft to include social media intermediaries as prominent data fiduciaries.[9]
- **Joint Parliamentary Committee Report, 2021-** The significant conflict between the proposed mandates of the Personal Data Protection Bill, 2019 and the interest of the global tech companies led to the bill's referral to Joint Parliamentary Committee. The committee recommended and renamed "Personal Data Protection Bill" to "Data Protection Bill" while broadening its scope to include non-personal data as well. The Personal Data Protection Bill was withdrawn from the Parliament after the JPC report in 2022. The draft of "Digital Personal Data Protection Bill" was released and made open for public opinion, suggestions and recommendations.

Phase 3: The Codified Era (2023-Present)

- **Digital Personal Data Protection Act, 2023-** Following discussions and recommendations in 2023, the draft of Digital Personal Data Protection Act was introduced in Parliament. It was approved by both the houses and received the assent of President on 11th August, 2023. The Act lays down the foundation for processing digital personal data and acknowledges individual's right to protect their personal data. The Digital Personal Data Protection Rules, 2025 were formally came into effect on 13th November, 2025. The rules enforce the Digital Personal Data Protection Act, 2023 and provides operational

guidance with respect to certain provisions of the Act.

CONCEPTUAL FRAMEWORK: E-COMMERCE AND PERSONAL DATA

- **E-COMMERCE, PERSONAL DATA AND REGULATORY CONTEXT UNDER THE DPDP ACT, 2023**

  E-commerce can be defined as business transactions that occur online. This type of trade includes all the types of business transactions as that of conventional businesses including buying, selling and payments. It can be said that e-commerce contains all the information and services ranging from pre-purchase information to after sale services. [10]In E-commerce, companies typically establish a virtual store that includes a detailed description of a product. It requires no physical interaction between the buyer and seller since purchases are done online. Customers can directly add items to their shopping cart and use their debit or credit card to complete the payment process. To facilitate such transactions effectively, these platforms gather, process and store vast amount of personal data or information that can be plausibly attributed to an individual. Personal data in case of e-commerce would consist of names, addresses, phone numbers, e-mail addresses, payment details, transaction history, browsing history etc. The importance of personal data in the context of digital commerce highlights its importance as not only an operational requirement, but also a commercial resource, which is a part of user experience optimization, personalization of services and targeted marketing.

  Personal data in e-commerce assumes a special significance since it is gathered not only at one moment but constantly at various touchpoints of the users. Data collection begins from the initial stage of account registration and is accumulated by further interaction with the user, such as login authentication, search history, product views and purchase decisions. Through such aggregation, e-commerce platforms can create comprehensive user profiles and use advance analytics to serve the commercial purposes. However such massive data processing poses inherent privacy threats such as potential misuse, sharing with third parties and security breaches. These risk highlights a need of a robust legal framework to solve the structural conflict in digital markets- the dual nature of personal data as a facilitator of commerce and as a possible cause of privacy damage.

The first comprehensive attempt by the Indian Parliament towards processing of digital personal data is the enactment of Digital Personal Data Protection Act, 2023 that acknowledges the right of individual to protect their personal data and the legitimate need to process such data for lawful purposes. The DPDP Act formalizes the important ideas that influence data governance in e-commerce ecosystems. It defines "data principal as the individual to whom personal data relates"[11] and "data fiduciary as any person (including state, company or organization) who determines the purpose and means of processing personal data".[12] The act mandates the lawful and consent-based processing that requires data fiduciaries to collect and process personal data only after obtaining the free consent of data principal. These guidelines highlight the data protection norms, which requires that data should be strictly used for specified purposes for which it is collected.

- **CORE OBLIGATIONS OF E-COMMERCE ENTITIES UNDER DPDP ACT, 2023**

The DPDP Act provides a methodical approach to the collection, analysis and storage of personal data in order to respect and protect individual's privacy. It is a first data protection law in a country that deals with emerging trends of data protection especially in e-commerce.[13] The Act categorized e-commerce companies as "data fiduciaries" since they frequently handle vast volumes of consumer personal data. Therefore, they are subject to several legal obligations aimed at ensuring safe, equitable and secure processing of individual's personal data.

One of the primary obligation imposed on e-commerce entities is the necessity of lawful purpose and consent- based processing.[14] As per section 6 of the Act, personal data may only be used for legitimate purposes after obtaining a free consent of the data principal. In the context of e-commerce, it requires the platforms to inform the consumers regarding the nature of data collected, reason behind its processing and the duration of its retention.

Another significant obligation is highlighted under the section 8 of the DPDP Act as it requires Data fiduciaries to execute suitable organizational and technical safeguards to prevent breach of personal data. To prevent unauthorized access, misuse of consumer data e-commerce organizations must have strong cybersecurity protections, encryption protocols and access restrictions. Furthermore, DPDP provides severe penalties for non-

compliance, which serves as an endorsement for data protection.

THE EFFICACY OF THE DPDP ACT, 2023 IN REGULATING E-COMMERCE

The Digital Personal Data Protection Act, 2023 signifies a paradigm shift in the approach to safeguard online identities by highlighting people's right to privacy, security and autonomy in the digital realm. As we navigate the intricacies of an increasingly digitalized world, this regulation plays a crucial role in ensuring that our online personas stay unaltered. The Act provides clear guidelines for the collection, use and storage of personal data, it seeks to give people greater control over their digital identities. This is particularly crucial in a country where digital platforms are integrated into every aspect of our life, from social interactions to financial transactions.

The DPDP Act, 2023 is framed around several fundamental pillars that provides a detailed legal framework for data protection in India.

1. **Consent and lawful purpose (Section 4)-** It creates a binary framework for processing data in an authorized manner. As per 4(1), "a person may process the personal data of data principal for lawful purposes in 2 cases-
   -for which the data principal has given her consent or
   -for certain legitimate uses.
   4(2) defines lawful purpose as "any purpose which is not expressly forbidden by law".[15]
2. **Data minimization and purpose limitation (section 5 and 6)-** Companies must only collect and use personal data as needed to fulfill the goals for which it is intended. By following the data minimization principle, the likelihood of excessive data collection is reduced and personal information is used for legitimate and approved purposes.
3. **Storage limitation (section 8)-** Personal data should only be stored as long as it is required to achieve the original purpose or until the consent is withdrawn, whichever comes first. Data must be securely deleted after completion in order to mitigate the risk associated with data hoarding and illegal access.[16]
4. **Security measures and accountability (section 9 and 10)-** It require fiduciaries to implement strong security measures, such as encryption, access control, and prompt breach

reporting. Accountability entails preserving compliance documentation, going through audits, minimizing vulnerabilities, and enhancing the organization's reputation for safeguarding personal information.[17]

5. **Cross border data transfer –** Cross-border data exchanges are common in increasing globalized digital economy. The DPDP Act ensures that personal data is adequately protected regardless of its location by establishing clear guidelines and safeguards for these type of transfers.

COMPARATIVE ANALYSIS OF INDIA'S DPDP ACT, 2023 AND EU's GDPR

The Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation (GDPR) are the two most well-known contemporary legislative frameworks governing personal data. Both aim to safeguard individual privacy and provide accountability for organizations handling personal data, which is crucial in e-commerce transactions because consumer data is frequently collected, examined, shared and monetized. The GDPR sets a strict bar for others to follow and is a global beacon of excellent data protection and privacy standards.[18] In comparison, India's DPDP Act is a landmark piece of legislation for a fast digitally transformed economy, offering a tailored solution that respects its own socio-economic fabric.

At the outset, the two frameworks differ in several parameters-

1. **Scope and applicability-** The GDPR applies to all personal data including digital and non-digital belonging to individuals within the EU and also extends extraterritorially to organizations outside EU that handle data belonging to individuals. On the other hand, the DPDP Act applies to companies who sell products or services to Indian citizens regardless of where they are located and expressly regulates digital personal data, including data that is initially obtained offline but is later converted to digital form. While GDPR's wider ambit encompasses both domains, its more narrowly defined scope reflects India's emphasis on digital ecosystem governance while simultaneously excluding non-digital data until it is digitized.[19]
2. **Legal basis for processing personal data-** In order to provide flexibility for e-commerce operations like contract fulfillment or direct marketing under legitimate interest, GDPR

recognizes a number of legal basis including consent, contractual necessity, legal obligation, vital interest, public interest and legitimate interest. In contrast, DPDP Act is notably consent-centric approach and requires free, specific, informed, and unambiguous authorization for processing with only a narrow list of "legitimate uses" (such as compliance, medical crises, and employment) are allowed without consent under the DPDP Act. This constrains Indian e-commerce businesses by prohibiting non-consensual explanations that could otherwise facilitate data flows for commercial utility.

3. **Data subject rights-** Both GDPR and DPDP grant core rights such as access, rectification and erasure and both offer procedures for grievance resolution and consent withdrawal. However, GDPR provides certain additional rights that enhance consumer control including data portability, restriction of processing and objection to automated decision making. In contrast, DPDP Act provides a smaller set of individual rights because it does not expressly provide data portability or robust objection rights against automated processing.
4. **Exemptions and State power-** One of the major shortcomings of the DPDP Act is that it provides wide exemptions to state and government activities. The law permits the processing of personal data that does not need consent based on the sovereignty, public order or security, without the explicit necessity and proportionality test. The exemptions of national security in the GDPR should be subjected to strict conditions, and the rights of the data subject may be restricted under the strict necessity and proportionate reasons. The lack of such protections in the DPDP Act is dangerous to weaken privacy privileges and institutionalize a higher level of discretion of the state in its data access.
5. **Independence of the regularity authority-** The GDPR mandates complete independence of the supervisory authorities, free of exclusive influence, with enforcement powers including audits and binding orders. The DPDP Act's enforcement body, the Data Protection board of India is nominated and dominated by the central government, which casts doubt on institutional independence, objectivity and strength of enforcement. This concentration of power may undermine the capacity of the Board to resolve conflicts where the involved parties are strong, whether private corporations or state actors.

SUGGESTIONS AND RECOMMENDATIONS

In light of the foregoing analysis, the independence and functional autonomy of the Data Protection Board should be reinforced to ensure impartial enforcement, particularly in cases that involve powerful corporate entities or state authorities.[20] The scope of data principal rights may be expanded to incorporate protections such as data portability and safeguards against automated decision-making, which are more in line with global standards as reflected in the General Data Protection Regulation.

E-commerce entities should be made mandatory to implement privacy by design principles[21], perform periodic data protection impact assessments, and establish grievance redressal mechanisms, and the legislature should introduce more specific guidelines on cross-border data flows to ensure that the data of Indian citizens is adequately protected. Finally, the data protection framework needs continuous legislative scrutiny and increased digital literacy efforts to ensure that the framework is adaptive, participatory, and responsive to the dynamic nature of the digital economy.

CONCLUSION

The development of data protection laws in India has represented a transformative shift from a position of statutory silence to constitutional recognition and, finally, to legislative codification. Starting from the commerce-oriented regime of the Information Technology Act, 2000, in which privacy considerations were merely incidental, the legal framework has developed through judicial activism, most notably in the historic decision of K.S. Puttaswamy v. Union of India,[22] in which privacy was recognized as a fundamental right under Article 21 of the Indian Constitution. This constitutional shift provided the normative basis for the DPDP Act, 2023, which represents the formal codification of data protection norms in India.

In the e-commerce context, the DPDP Act assumes special importance. Digital marketplaces function on the basis of the continuous and large-scale processing of consumers personal data, which makes such data both an operational necessity and a commercial resource. The DPDP Act seeks to address this tension by establishing a consent-driven framework, establishing specific

obligations for data fiduciaries, and providing for specific rights of data principals. Norms such as lawful purpose, data minimization, storage limitation, and accountability establish a framework for responsible data management in digital marketplaces. A comparison with the General Data Protection Regulation (GDPR) shows that, while the DPDP Act is in line with the international standards in principle, it has a more flexible and state-oriented approach, which is in line with the socio-economic vision of India. While this is perfectly valid in the context of a developing digital economy, the long-term viability of this approach will depend on its ability to strike a balance between innovation, economic development, and the constitutional imperatives of privacy and dignity.

In conclusion, The DPDP Act, 2023 marks the beginning of a new era in the development of data protection in India's burgeoning e-commerce sector. However, its transformative power will be realized only when it is strictly enforced and interpreted in accordance with the constitutional vision of India.

[1] Bruce Schneier, *Schneier on Security* 69 (John Wiley & Sons, 2009).
[2]Divya Dwivedi, *Data Privacy And Public Service Delivery In India : A Critical Legal Study* (2024) (Unpublished Ph.D. thesis, Dr. Ram Manohar Lohiya National Law University).
[3]Ryan Moshell, "And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Towards Comprehensive Data Protection Framework," 37 Tex. Tech L. Rev. 357 (2005).
[4]The Digital Personal Data Protection Act ,2023 (NO. 22 OF 2023)
[5] GDPR.eu What is GDPR? *available at*: https://gdpr.eu/what-is-gdpr/ (last visited on Feb 6, 2026)
[6]Information Technology Act, 2000: Evolution, Genesis and Necessity, *available at*: https://thelegalhubb.com/1-information-technology-act-2000-evolution-genesis-and-necessity/ (last visited on Feb 6, 2026)
[7]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information), *available at*: https://ssrana.in/articles/information-technology-reasonable-security-practices-and- procedures-and-sensitive-personal-data-or-information/ (last visited on Feb 12, 2026).
[8] (2017) 10 SCC 1.
[9]Renjith Mathew,"Personal data Protection Bill,2019-Examined through the Prism of Fundamental Right to Privacy-A Critical Study", SCC online (2020).
[10]UNCTAD E-Commerce Week 2017- connecting the dots for sustainable development, *available at*: UNCTAD E-Commerce Week 2017 - connecting the dots for sustainable development | UN Trade and Development (UNCTAD)(last visited on Feb 14, 2026).
[11] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
[12] Ibid
[13] Sowmya Sharma PM, Dr. Chanjana Elsa Philip, "Balancing E-Commerce and Data Privacy in India- An Analytical Study" *Journal of Information Systems Engineering and Management* (2025).

[14]Shejal Verma, "India's New Digital Personal Data Protection Law- The Digital Personal Data Protection Act, 2023" *NO&T Asia Legal Review* 69 (2023).
[15]*Supra* note 11, s.4
[16]Minal Purwar, "DPDP Rules, 2025: A Guide to Digital Personal Data Protection", (2025).
[17] Ibid
[18]*Supra* note 2, chapter 5 at 2.
[19]Anahad Narain, "Difference between DPDP Act & GDPR"(2026).
[20] The General Data Protection Regulation, 2018, art.52.
[21]Id, art.25.
[22]*Supra* note 8