International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Consumer Privacy Vs. Business Interests: Evaluating Data Protection in India's Digital Marketplaces

Ms. Farhat Yunus[1], Mr. Manish Kumar Attry[2]

[1]PhD Student, Raffles University
[2]Professor, Raffles University

Abstract

Indian e-commerce has been expanding at an exponential rate, which is both fantastic news for online commerce and a big source of concern for consumers' privacy rights and the protection of their personal data. This article does an analytical analysis of the evolving legal framework governing data management and privacy in India's e-commerce industry. In light of the Digital Personal Data Protection Act, 2023 (DPDPA), the research evaluates the current regulatory framework to see if it effectively addresses concerns about data processing, consent management, online platform accountability procedures, and cross-border transfers. It contrasts the Indian framework with foreign standards such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) of the EU in order to assess parallels, divergences, and possible areas of harmonisation. The study specifically explores how the monetisation of customer data and profit-driven targeted advertising in e-commerce generate an inherent conflict with customers' rights. Using doctrinal and comparative legal research approaches, the study looks at court rulings, policy documents, and corporate compliance practices. Its objective is to identify the regulatory gaps that impede efficient enforcement. Although India's data protection law is a significant step in the right direction, the paper argues that the law will only be effective if the Data Protection Board is institutionally independent, data-driven business models are more transparent, and the law is strictly implemented. To foster confidence, accountability, and sustained expansion in India's e-commerce industry, the article concludes by proposing a compromise legal approach that safeguards consumer privacy while fostering digital innovation.

Keywords: Digital Personal Data Protection Act, Data Protection Board, Right to privacy, Consumer's Rights, Protection Law and Digital Innovation

Introduction

The right to keep one's personal relationships and other private matters private is the most basic definition of privacy, according to beginners. While the concept of privacy was formally recognised in the nineteenth and twentieth centuries, one might argue that the necessity and significance of privacy have persisted for the whole history of humanity. Though the term "privacy" may be lacking in concrete proof in Hindu and Islamic literature, it would be a colossal mistake to think that such a socially engaged nation as India would reject the concept. The distinction between what is explicitly protected by law and what is just

believed to be private has recently gained considerable acceptance.[1] Despite the fact that the European Court of Human Rights and many researchers have concluded that defining privacy is difficult because of its vast dimensions, it is vital to educate the public about this distinction so that their legal rights can be protected. A handful of seminal international documents in the late 20th century was the first to recognise the right to safety as a basic human right; following governments swiftly followed suit. Several international accords and conventions have reiterated the importance of protecting individuals' right to privacy. Various international texts have made this clear, such as the Universal Declarations of Human Rights, the European Charter of Fundamental Rights, the International Covenant on Civil and Political Rights, and the European Convention on Human Rights. 11. It is quite evident from all of these treaties that everyone has the right to live in peace and safety, which includes the right to an individual's home, communications, and freedom from illegal invasion.

It is necessary to have the right to privacy in order to have a good life. There are several forms of cybercrime that are prevalent in contemporary culture. Some examples of these include phishing, malware, ransomware, hacking, and spamming. For the purpose of mitigating these dangers and protecting the personal information of individuals, data protection rules need to be quite stringent. Laws pertaining to data protection are an all-encompassing collection of regulations, procedures, and policies that are intended to reduce the possibility of individuals whose privacy has been violated as a result of the occurrence of data breaches. In this context, the processing, collecting, and disclosure of personally identifiable information (PII) refer to facts that allow for the identification of a particular individual. This is true regardless of whether the information is collected by a private corporation or a governmental agency. It is imperative that consumers and citizens alike have access to the resources that will enable them to exercise their right to privacy and safeguard their personal information from being misused. The right to privacy has been repeatedly upheld by both international and provincial court judgements and regulations, and the protection of personal information is a crucial component of effectively safeguarding this right. During the process of collecting, processing, and storing an individual's personal information, it is necessary to have a set of rules and regulations in place to protect that information.[2]

Business activities and public policy are both affected by and controlled by laws intended to protect personal information. These regulations empower individuals to protect data from potential exploitation. In the lack of such regulations, institutions have demonstrated a tendency to gather, assess, and retain all data without divulging much to the individuals concerned. In today's technology-driven society, data protection policies are crucial for preserving privacy and empowering individuals with control over their personal data.

Present Indian Regulations Regulating Online Trade in India

Customer data security is paramount while doing business online. Despite some scholars defining "Information Privacy" as "the idea of controlling how one's personal information is acquired and used in ecommerce transactions," it seems that consumers do not have control over the gathering and utilisation of their information. This is because websites (companies) use web bugs, cookies, and other unauthorised methods to gather information without consumers' knowledge or consent. We want to know what people

[1] Bhardwaj, U., & Pabbi, B. (2024). E-commerce and consumer protection laws in India. JournalNX: A Multidisciplinary Peer Reviewed Journal, 10(4), 127–132. https://doi.org/10.26662/rcn5ms04.

[2] Sharma, S. P. M., & Philip, C. E. (2025). Balancing e-commerce and data privacy in India – An analytical study. Journal of Information Systems Engineering and Management, 10(54s).

want, so we're breaking the law to get it. Then, we'll use that knowledge to strategically market our website. The two main problems with online purchasing are (a) the need for companies to obtain personal information from consumers in order to operate their marketing efforts and (b) the perception among consumers that this violates their privacy. Consumers' reluctance to part up personal information on commercial websites is understandable given the pros and cons of e-commerce companies' data collection tactics and the possibility of losing control over how their data is stored, processed, shared, and used.

There are rules and regulations in place on a global and national scale to deal with issues of online privacy and to promote the use of legal power to safeguard personal information during online transactions. The proposed amendments (IT) Act of 2000 by the Ministry of Communications and Information Technology is an example of such an endeavour. The proposed amendments to the IT (Amendment) Act of 2008 included important provisions like Section 43A, which deals with the disclosure of information in violation of legal contracts, and Section 72A, which stresses the importance of implementing reasonable security practices to protect sensitive data. Just so you know, new regulations called the Privacy Rule were put in place because of these proposed amendments. However, they are still not fully incorporated into the present Act.[3]

Furthermore, the National Association of Software and Computer Companies (NASSCOM) has established the Information Security Council of India, which is a self-regulatory body with the objective of establishing industry standards for data privacy and security. Additionally, it serves as a venue for professionals to discuss their perspectives and experiences in this particular field. In addition, the National Do Not Call Registers were established by the Telecom Regulatory Authority of India (TRAI) in response to concerns over unsolicited calls and the privacy of telephone numbers.[4] These registers allow users to reject unwanted calls and increase their level of privacy. These steps are a demonstration of India's proactive approach to data protection in an era that is characterised by growing web-based activities and interconnectedness. This approach is particularly pertinent given the quickly expanding digital landscape. While doing so, they ensure the protection of individuals while also cultivating an atmosphere that is favourable to scientific advancement and trust, both of which are necessary for the economic and technological development of the nation. In the process of continuing to adjust to the digital world, these aggregate forecasts expect that India will discover a method to strike a balance between the essential of preserving people's personal data and the data-driven growth that the country is experiencing.[5]

DPDPA, 2023 and e-commerce websites

Based on who makes the decisions about why and how personal data is processed, Data Principals have various rights under the Act, and Data Fiduciaries have several obligations to protect and limit data processing.[6]

[3] Harikumar, P., Balasubramanian, J., Padmanabhan, S., Bathia, A., Chheda, K., & Nikam, K. (2025). Digital privacy laws – Evolution and consumer perceptions among online users in India. Journal of International Commercial Law and Technology, 6(1), 427–436.

[4] 82% of Indian consumers prioritize data protection for trust: Survey. (2024, July 12). ET Retail. Retrieved from https://retail.economictimes.indiatimes.com/news/industry/82-of-indian-consumers-prioritize-data-protection-for-trust-pwc-survey/111674399.

[5] Kumar, V. (2025). Data privacy and consent in e-commerce transactions: A legal examination of the Digital Personal Data Protection Act, 2023 and its impact on online consumers. International Journal of Applied Research, 11(10), 388–399. https://doi.org/10.22271/allresearch.2025.v11.i10e.12969.

[6] Personal data protection and e-commerce. (2025). Indian Journal of Law and Legal Research. Retrieved from https://www.ijllr.com/post/personal-data-protection-and-e-commerce.

Online retailers frequently handle vast quantities of user data in the course of processing transactions, developing targeted marketing campaigns, and delivering customer service. All data processing operations must comply with state legal standards as mandated by the Data Protection and Privacy Act of 2023. Some examples of such legal requirements includes:

- Not processing personal information without first obtaining consent from data principals.
- Ensuring that all processed data is accurate, complete, and up-to-date.
- Request for Personal Information and Itemised Notice; • Appropriate channels for Data Principals to resolve complaints or get in touch with the data protection officer via the designated representative.
- Additional duties related to the processing of data pertaining to children, including the need to get parental approval and restrict behavioural monitoring.
- Organisations should evaluate their data practices to ensure compliance and avoid heavy fines.

This law has given people more say over their personal data. There should be no hiccups for customers when it comes to data access, deletion, transfer, or correction while shopping online. According to the DPDPA, a Data Principal can use a Consent Manager to control who has access to their data and how they can use it. This includes the ability to provide, review, withdraw, or manage consent.[7] A Data Protection Board-registered individual can assist Data Principals in managing their consent. The Consent Manager is responsible to the Data Principal and has the responsibility to provide the Data Principal remedy for grievances. As a result, people's rights have been expanded in India by the DPDP Act. Data minimisation, storage limits, and accuracy are of the utmost significance according to the DPDPA 2023. Online merchants should check their data processing methods to make sure they are gathering the right information, not losing any details, and preserving it for the right period of time. According to the DPDPA, all data must be accurate, current, and thorough.[8]

In accordance with the provisions of the Act, the Data Principal may also withdraw consent at any moment or when the initial purpose of the data is no longer justified. The implementation of these principles could necessitate revisions to data retention regulations, forms used for collecting information, and storage technology. Further safeguards for overseas transfers of personal data are introduced by DPDPA, 2023. The DPDPA enables the Central Government to bind personal data transfers outside of India to a specific area or nation upon notice. Certain nations' laws and regulations require a higher level of security and may ban the transfer of personally identifiable information (PII).[9] Online retailers are within their rights to do so, provided the US government does not announce any limitations on the transmission of personal information over international borders. It is not mandatory for all data fiduciaries to designate a data protection officer (DPO) under the DPDP Act. But it's mandatory for some e-commerce companies who are considered Significant Data Fiduciaries. The DPDPA, 2023 deals with this. Compliance, data protection authorities, and data protection strategies will all fall within the purview of DPOs according to the DPDP Act. In addition to having DPOs on staff, significant data fiduciaries are required to hire an independent auditor, perform data protection impact assessments on a regular basis, and conduct data audits.[10]

[7] Adanyin, A. (2024). Ethical AI in retail: Consumer privacy and fairness. arXiv. https://arxiv.org/abs/2410.15369.
[8] *Comparative analysis of privacy and data protection laws in e-commerce*. (2025). *Indian Journal of Law and Legal Research*. Retrieved from https://www.ijllr.com/post/comparative-analysis-of-privacy-and-data-protection-laws-in-e-commerce.
[9] Ley de Protección de Datos Personales Digitales de 2023. (2025). Retrieved from https://es.wikipedia.org/wiki/Ley_de_Protecci%C3%B3n_de_Datos_Personales_Digitales_de_2023.
[10] Singh, A. (2025). Recalibrating consumer rights in the digital marketplace. International Journal of Law, Social Sciences and Security Studies, 3(2), 386–399.

Indian Laws vs International Legislation

With the adoption of the Digital Personal Data Protection Act, 2023 (DPDPA), a new statutory framework for data protection has developed in India. This approach seeks to safeguard personal information while permitting lawful data processing. The Act delineates the concepts of data fiduciary duty, purpose limitation, and consent-based data utilisation. Concerns exist over the autonomy and independence of the Data Protection Board of India in its activities; yet, it is designated as the principal enforcement authority. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, together with the Information Technology Act, 2000, offer limited protections, primarily focussing on corporate responsibility and sensitive data. Online platforms are supposed to be transparent and have processes in place to handle issues according to the Consumer Protection (E-Commerce) Rules, 2020, which are supplementary to these.[11]

Significant discrepancies become obvious when contrasted with international regulations like the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA). The General Data Protection Regulation (GDPR) is regarded as the global benchmark due to its extensive user rights, such as data portability and the right to be forgotten, alongside its stringent consent requirements and the establishment of independent regulatory authorities. The CCPA, while less rigorous, aims to empower consumers by providing them with the rights to access, delete, and opt out of the sale of their data. Both models have clearly-defined roles and responsibilities for processors and controllers as well as robust enforcement mechanisms. Conversely, the DPDPA in India may undermine privacy safeguards because to its more permissive permission requirement and the extensive powers it grants the federal government to exempt firms. Indian method likewise rely on government-notified transfer lists, in contrast to the General Data Protection Regulation's (GDPR) comprehensive cross-border data safeguards supplied by adequacy decisions and standard contractual terms. In comparison to global best practices on institutional independence, user autonomy, and enforcement authority, the Indian regime is deficient. Nonetheless, it is a significant advancement.[12]

Conclusion and Suggestions

The Digital Personal Data Protection Act, 2023 (DPDPA) in India is a pivotal stage in the nation's legislative history regarding privacy and data protection. The analysis indicates that the Act remains inadequate compared to the comprehensive and enforceable safeguards established by international standards like the General Data Protection Regulation (GDPR). Despite advancements in law concerning data fiduciary responsibilities and consent, challenges persist over inadequate institutional autonomy, broad governmental exemptions, and limited individual rights. Transitioning from a compliance-centric framework to a rights-based and enforcement-oriented structure is essential for the DPDPA to effectively protect persons in the digital age.

A. Ensure Institutional Independence: The Data Protection Board must be restructured to operate autonomously, free from executive interference, therefore ensuring equitable enforcement and accountability.

[11] Chawla, N., & Kumar, B. (2022). E-commerce and consumer protection in India: The emerging trend. Journal of Business Ethics, 180. Retrieved from https://ideas.repec.org/a/kap/jbuset/v180y2022i2d10.1007_s10551-021-04884-3.html.

[12] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India). Retrieved from https://en.wikipedia.org/wiki/Information_Technology_Act%2C_2000.

B. Restrict the Scope of Exemptions: To prevent misuse, the government's power to exempt entities must be exercised judiciously and overseen by the judiciary or legislature.
C. Enhance User Rights: To align with global standards, it is essential to incorporate extra rights such as data portability, the right to be forgotten, and the right to contest machine learning.
D. Establish Clarity in Cross-Border Data Transfers: To facilitate secure international data exchanges while safeguarding user security, implement transparent adequacy standards and bilateral agreements.
E. Enhance Compliance and Awareness: Implement regular audits, industry-specific standards, and educational campaigns to encourage organisations to manage data ethically.

Implementing these measures would enable India to establish a data protection framework that safeguards individual privacy, fosters innovation, and enhances consumer trust in online enterprises, therefore bridging the divide between legal objectives and tangible outcomes.