© NOV 2025 | IRE Journals | Volume 9 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I5-1712357

Finding A Middle Ground Between Consumer Privacy and Business Needs: An Examination of Data Protection Policies in India's Online Marketplaces

FARHAT YUNUS[1], MANISH KUMAR ATTRY[2]
[1, 2]*Raffles University*

Abstract- ***Indian e-commerce has been growing at an exponential rate, which is both great news for digital trade and a major cause for worry about customers' right to privacy and the security of their personal information. An analytical examination of the changing legislative framework controlling privacy and data management in India's e-commerce sector is undertaken in this article. The study analyses the present legislative framework in light of the Digital Personal Data Protection Act, 2023 (DPDPA) and determines if it adequately handles issues related to online platform accountability mechanisms, data processing, cross-border transfers, and consent management. In order to evaluate similarities, differences, and potential areas of harmonisation, it compares the Indian framework to international norms like the General Data Protection Regulation (GDPR) of the EU and the California Consumer Privacy Act (CCPA). In particular, the research delves at the ways in which e-commerce's profit-driving tailored advertising and the monetisation of customer data create an inherent contradiction with consumers' rights. The study examines policy papers, court declarations, and business compliance procedures using doctrinal and comparative legal research methodologies. Its goal is to find the regulatory loopholes that prevent effective enforcement. While the data protection law in India is a major step in the right direction, the paper contends 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 vigorously enforced. In order to promote trust, accountability, and long-term growth in India's e-commerce sector, the essay finishes by suggesting a middle ground legislative strategy that protects consumer privacy without limiting digital innovation.***

Index Terms- ***Digital Personal Data Protection Act, Data Protection Board, Right to privacy, Consumer's Rights, Protection Law and Digital Innovation***

I. INTRODUCTION

A beginner's understanding of privacy is the right to secrecy regarding one's own relationships and other private affairs. Although the notion of privacy was officially acknowledged in the 19th and 20th centuries, it is safe to argue that the need for it and the importance of privacy have been there for as long as humans have.[1] It would be completely incorrect to assume that in a socially active country like India, privacy was an alien idea, even though the phrase may not find any clear evidence in either Hindu or Islamic literature. It is now widely acknowledged that there is a difference between what is legally guaranteed as private and what is perceived as private. Therefore, it is pertinent to educate the public about this difference in order to protect their legal rights, even though the European Court of Human Rights and numerous research scholars have determined that defining privacy is impossible due to its broad contours. The right to safety was first acknowledged as a fundamental human right in a small number of high-ranking international texts in the late 20th century, and subsequent states quickly followed suit. The right to privacy has been recognised as an essential human right in a number of international treaties and agreements. This is stated in several international documents, including the International Covenant on Civil and Political Rights, the Universal Declarations of Human Rights, the

Charter of Fundamental Rights of the European Union, and the European Convention on Human Rights. 11. All of these accords make it clear that everyone has the right to a private and secure existence, including the right to have one's home and communications respected, as well as the right to be free from unlawful intrusion.[2]

Living a decent existence requires the right to privacy. Many types of cybercrime, including phishing, viruses, ransomware, hacking, and spamming, are visible in our culture. Data protection laws must be strict in order to reduce these threats and safeguard people's private information. Data protection laws are an all-encompassing set of rules, processes, and policies designed to lessen the likelihood of breaches in the privacy of persons who have been affected by Regardless of whether it is obtained by a private company or a public agency, the processing, collection, and disclosure of personally identifiable information (PII) in this context relate to facts that permit the identification of a specific individual. Consumers and citizens alike must have access to the resources that will allow them to exercise their right to privacy and protect their personal information from misuse. International and provincial court rulings and laws have consistently affirmed the right to privacy, and data protection is an essential part of protecting this right. Protecting an individual's personal information during its collection, processing, and storage requires a system of laws and regulations.[3]

Legislation enacted to safeguard personal information must control and impact business practices and public policy alike. People are given the power to safeguard data from possible exploitation by these policies. Institutions have shown a propensity to collect, evaluate, and keep all data without disclosing much to the people involved in the absence of such rules. To maintain privacy and give people agency over their own data in our tech-driven world, data protection regulations are essential.

Current Indian Laws surrounding E-commerce in India – 800 words

When conducting business online, protecting customer data is of the utmost importance. Although "Information Privacy" has been defined differently by various scholars as "the idea of controlling how one's personal information is acquired and used in ecommerce transactions," it would appear that consumers do not have control over the gathering and utilisation of their information since websites (companies) utilise web bugs, cookies, and other unauthorised methods to gather information without consumers' knowledge or consent. The purpose of this unlawful access and collection is twofold: first, to understand what people want, and second, to promote our website in a strategic way using the information we acquire. One big issue with online shopping is that: (a) businesses can't run their marketing campaigns without collecting personal information from customers and site visitors; and (b) customers see this as an infringement on their right to privacy when it comes to their own information. Customers are understandably wary about disclosing sensitive information on commercial websites due to the double-edged sword of e-commerce websites' data collection practices and the potential loss of control over their data's storage, processing, dissemination, and use.[4] Concerns about personal data security were shown to be the biggest problem for online shoppers in a 2005 empirical study by Wang and Emurian. So, customers' ability to manage the gathering, processing, and sharing of their personal data makes them feel more at ease while shopping online, which in turn encourages more e-commerce.[5]

At both the national and international levels, legal laws and regulations have been put in place to address the concerns around online privacy and to encourage the exercise of legal authority over the protection of personal information during electronic transactions. An example of such an endeavour is The Ministry of Communications and Information Technology's proposed revisions (IT) Act of 2000 is one such noteworthy initiative. Important provisions such as Section 43A, which addresses the disclosure of information in violation of legal contracts, and Section 72A, which emphasises the importance of implementing reasonable security practices for the protection of sensitive data, were introduced into the IT (Amendment) Act of 2008 as a result of these proposed amendments. Be advised that the Privacy Rule, new rules, has been put in place as a result of

these proposed revisions, but they have not yet been completely integrated into the current Act.

In addition, NASSCOM has set up the Information Security Council of India, which is a self-regulatory organisation that aims to create industry standards for data privacy and security and provides a forum for experts to share their insights and experiences in this area. The National Do Not Call Registers, which customers may use to reject unwanted calls and improve their privacy, were also put in place by the telecom regulatory body of India (TRAI)[6] in response to concerns about unsolicited calls and telephone number privacy. These measures demonstrate India's proactive approach to data protection in an era defined by increased web-based activities and interconnection, which is particularly relevant given the rapidly evolving digital landscape. They protect people's safety while also fostering an environment that is conducive to progress and tech trust, which is essential for the country's economic and technological growth. These aggregate projections anticipate that India will find a way to balance data-driven growth with the fundamental of protecting people' personal data as the country continues to adapt to the digital era.

DPDPA, 2023 and e-commerce websites

Data Principals have several rights under the Act, and Data Fiduciaries have many responsibilities to safeguard and restrict the processing of data, depending on who decides why and how personal data is processed.[7]

When it comes to processing transactions, creating personalised marketing campaigns, and providing customer care, e-commerce companies often deal with massive amounts of user data. The Data Protection and Privacy Act of 2023 mandates that all data processing operations adhere to state legal standards. Among these mandates from the law are:

- Acquiring Data Principals' consent before processing their personal information.
- All processed data must be current, full, and correct.
- Request for Personal Information and Itemised Notice;
- Authorised representative to provide Data Principals with adequate grievance redressal processes or data protection officer contact information.
- Extra responsibilities for the processing of child data, such as obtaining parental consent and limiting behavioural monitoring.
- To stay in compliance while evading huge fines, businesses will need to take stock of their data procedures.

People now have greater control over their own data thanks to this law. Online retailers must be prepared to address customer concerns over data access, deletion, transfer, and correction. A Consent Manager also allows Data Principals to manage their consent—whether it's to grant, evaluate, withdraw, or manage it—to the Data Fiduciary, as per the DPDPA. Data Principals can manage their consent with the help of a Consent Manager, who is someone registered with the Data Protection Board. A Data Principal has the right to grievance redressal offered by the Consent Manager, and the Consent Manager is liable to the Data Principal. Therefore, the DPDP Act in India has broadened the scope of individuals' rights. Extreme importance on data minimisation, storage limitation, and accuracy is managed by the DPDPA 2023. Companies that deal with online transactions need to review their data processing procedures to ensure they are collecting relevant data, keeping it accurate, and storing it for an appropriate amount of time. Accurate, up-to-date, and comprehensive data is required under the DPDPA.[8]

Furthermore, the Data Principal may revoke consent at any time or when the data's original intended use is no longer justified, as per the Act's requirements. Changes to data retention policies, information collection forms, and storage technologies may be necessary to put these ideas into action. In addition, DPDPA, 2023 adds more checks and balances for personal data transfers abroad. Upon notice by the Central Government, the DPDPA allows for the binding of personal data transfers outside of India to a certain area or nation.[9] The export of personally identifiable information (PII) may also be limited in certain countries due to laws and regulations that mandate a greater level of security. So long as the

federal government doesn't notify any restrictions on cross-border data transfers, e-commerce companies can legally do so. According to the DPDP Act, not all Data Fiduciaries are required to appoint a Data Protection Officer (DPO). However, certain e-commerce organisations that have been designated as Significant Data Fiduciaries are required to do so. This is addressed in the DPDPA, 2023. As a result of the DPDP Act, DPOs will be responsible for overseeing data protection strategy, data protection authorities, and compliance. Significant Data Fiduciaries are obligated to do more than just employ DPOs; they must also conduct periodic data audits, data protection impact assessments, and engage an independent auditor.

Indian Laws vs International Legislation

With the passing of the Digital Personal Data Protection Act, 2023 (DPDPA), a new legislative framework for data protection has emerged in India. This framework aims to secure personal information while allowing for legitimate data processing.[10] The ideas of data fiduciary responsibility, purpose restriction, and consent-based data usage are laid forth in the Act. There are also doubts about the Data Protection Board of India's autonomy and independence in its operations, but it does establish it as the primary enforcement body. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and the Information Technology Act, 2000[11] both provide minimal protections, with the main emphasis being on corporate accountability and sensitive data. Online platforms are required to be transparent and have systems in place to resolve grievances according to the Consumer Protection (E-Commerce) Rules, 2020, which are complementary to these.

Significant differences become apparent when contrasted with international laws like the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA). Due to its comprehensive user rights, including data portability and the right to be forgotten, as well as its strict permission requirements and the formation of independent regulatory bodies, the General Data Protection Regulation (GDPR) is seen as the worldwide standard. Although it is less stringent, the CCPA seeks to empower consumers by granting them the rights to know, remove, and opt out of data selling. Both models include well-defined roles and responsibilities for processors and controllers as well as strong enforcement mechanisms.[12] On the other hand, the DPDPA in India might weaken privacy protections since it uses a more lenient consent threshold and gives the federal government broad authority to exclude companies. Indian approach also depends on government-notified transfer lists, in contrast to the General Data Protection Regulation's (GDPR) robust cross-border data protections provided by adequacy rulings and standard contractual provisions. When compared to the world's best practices in terms of institutional independence, user autonomy, and the power of enforcement, the Indian regime lags behind. Nevertheless, it is still a huge step forward.[13]

How well the new data protection strategy in India compares to international standards?

However, when compared to other prominent international standards like the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act, India's new data protection strategy, the Digital Personal Data Protection Act, 2023 (DPDPA), falls short in terms of framework comprehensiveness. In line with the General Data Protection Regulation's (GDPR) focus on data minimisation and transparency, the DPDPA establishes fundamental principles such as legitimate processing, purpose limitation, and user permission. On the other hand, data fiduciaries have more leeway to interpret the DPDPA broadly, in contrast to the General Data Protection Regulation (GDPR), which requires clear, informed, and revocable permission. Data portability and the right to be forgotten are fundamntal to the user-empowerment concept of the General Data Protection Regulation (GDPR), yet they are not included in the Act, even though data principals have access, rectification, and grievance redressal rights.[14]

The Data Protection Board in India is responsible for ensuring compliance, but it is still subordinate to the federal government, which calls into doubt its autonomy in contrast to the decentralised regulatory bodies required by the General Data Protection

Regulation (GDPR). Further complicating matters for international e-commerce operations is the fact that, instead of adequacy assessments or contractual terms, India's regulations for cross-border data transmission depend on official announcements. On the other hand, the CCPA requires openness in data monetisation processes and provides more clarity on consumer rights to opt out of data sharing, despite its more market-oriented orientation. In spite of this, the DPDPA acknowledges the necessity for legislative flexibility in light of India's quickly developing digital economy and aims to strike a balance between economic progress and individual privacy. While the data protection law in India is a big improvement over its predecessor, it is far from meeting the stringent privacy and accountability requirements set out by the General Data Protection Regulation (GDPR). This calls for further changes to make enforcement stronger, user rights better, and institutions more independent.

The current regulatory loopholes and challenges

A number of legal gaps and implementation issues have persisted since the DPDPA's passage in 2023, rendering India's data protection system inadequate. The extensive exemption powers given to the federal government raise serious issues since they allow for the possible exclusion of specific businesses or types of data processing from the law's jurisdiction. Concerns about possible abuse and the erosion of privacy protections on a global scale are heightened by this discretion, which is particularly problematic in situations involving governmental monitoring. The absence of a separate regulating body is another key drawback.[15] The GDPR establishes independent data protection authorities in the European Union; however, the Data Protection Board in India is subject to executive authority, which might undermine its independence and capacity to implement data protection laws. In addition, there aren't enough protections against the "dark patterns" or manipulative data gathering tactics employed by e-commerce platforms, and the DPDPA's consent standards are somewhat lax, permitting implicit permission in some situations. To further undermine user agency, the legislation does not protect data subjects' rights to data portability and the right to be forgotten.[16] International commerce and digital firms face uncertainty due to unclear cross-border data transfer regulations. In these cases, judgements are made entirely based on government notifications, without explicit adequacy requirements. Not to mention that automated decision-making, algorithmic profiling, and sensitive data categories—all of which are essential to contemporary data processing in e-commerce—are not adequately addressed by the Act. There is still a lack of a solid plan for monitoring compliance or providing consumers with recourse, and the enforcement procedures are inadequate, with fines only imposed. Taken as a whole, these holes show that DPDPA is still in its early stages of development, despite being a historic reform in India. In order for the framework to provide a data protection ecosystem that is really responsible and centred around user rights, it needs more robust institutional independence, expanded user rights, and clear cross-border data standards.[17]

II. CONCLUSION AND SUGGESTIONS

Finally, the Digital Personal Data Protection Act, 2023 (DPDPA) in India is a watershed moment in the country's history of privacy and data protection legislation. The research shows, however, that the Act is still not up to the level of thorough and enforceable protections provided by international standards such as the General Data Protection Regulation (GDPR). Although there has been some improvement in the legislation with relation to data fiduciary duties and consent, there are still issues with insufficient institutional autonomy, extensive government exclusions, and restricted individual rights.[18] Moving away from a framework focused on compliance and towards a system driven by rights and enforcement is necessary if the DPDPA is to successfully safeguard individuals in the digital era.

III. RECOMMENDATIONS

1. Establish Institutional Independence: The Data Protection Board has to be reorganised so it can act autonomously, without influence from the executive branch, guaranteeing fair enforcement and responsibility.
2. Limit the Range of Exemptions: In order to avoid abuse, the government's authority to exempt entities should be used with great caution and

subjected to monitoring by the courts or parliament.

3. Elevate User Rights: In order to be in line with global standards, it is necessary to integrate additional rights such data portability, the right to be forgotten about, and the right to object to machine learning.
4. Make Cross-Border Data Transfers Clear: To ensure safe international data flows without compromising user security, set up transparent adequacy criteria and bilateral agreements.
5. Raise Compliance and Awareness: Consistent audits, sector-specific standards, and education initiatives should be put in place to inspire companies to handle data responsibly.

By putting these steps into action, India can create a data protection ecosystem that protects individuals' privacy, promotes innovation, and boosts consumers' faith in online businesses, closing the gap between regulatory goals and actual results.

NOTES

[1] Agarwal, R., & Singh, M. (2024). Data Protection and Privacy Laws in India: Evolving Challenges and Future Directions. New Delhi: Eastern Book Company.

[2] Banerjee, A. (2022). Regulating Data in the Digital Age: The Indian Approach to Privacy Protection. Indian Journal of Law and Technology, 18(1), 45–67.

[3] Chatterjee, S. (2021). Data Localization and Cross-Border Data Flow: Policy Perspectives from India. Journal of Cyber Policy, 6(2), 198–215.

[4] Mitra, T. (2020). The Evolution of Data Protection in India: From IT Act to Personal Data Protection Bill. NUJS Law Review, 13(1), 1–25.

[5] Sharma, P. (2023). E-Commerce and Consumer Privacy: The Regulatory Paradigm in India. International Journal of Law and Policy Review, 12(2), 54–78.

[6] Kuner, C. (2020). Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press.

[7] Digital Personal Data Protection Act, 2023 (India).

[8] NITI Aayog. (2021). *Responsible AI for All: Operationalizing Principles for India*. New Delhi: Government of India.

[9] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).

[10] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[11] Information Technology Act, 2000 (India).

[12] United Nations Conference on Trade and Development (UNCTAD). (2022). *Data Protection and Privacy Legislation Worldwide*. Geneva: UNCTAD.

[13] *Schrems II – Data Protection Commissioner v. Facebook Ireland Ltd*, Case C-311/18, [2020] ECLI:EU:C:2020:559.

[14] *Ritesh Sinha v. State of Uttar Pradesh*, (2019) 8 SCC 1.

[15] Bhatia, G. (2017). *Offend, Shock, or Disturb: Free Speech Under the Indian Constitution*. New Delhi: Oxford University Press.

[16] Solove, D. J. (2021). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

[17] Greenleaf, G. (2019). Global Data Privacy Laws 2019: 132 National Laws and Many Bills. *Privacy Laws & Business International Report*, 157, 10–13.

[18] Narayan, R. (2023). Comparative Insights into India's Data Protection Law and the EU GDPR. *Indian Law Review*, 9(1), 22–48.