Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN:2584-184X

Research Article

Data Protection and Privacy Challenges for Indian E-Commerce Companies

Chandan Singh [1*], Dr. Prahalad [2]

[1] Research Scholar, IEC School of Law, IEC University, Himachal Pradesh, India

[2] Supervisor, Associate Professor, IEC School of Law, IEC University, Himachal Pradesh, India

Corresponding Author: * Chandan Singh

DOI: https://doi.org/10.5281/zenodo.22689289

Abstract

The rapid growth of e-commerce in India has greatly changed the relationship between the customer and the business organisations when it comes to collecting, retaining, and exploiting personal information. This paper focuses on the privacy and data protection challenges experienced by the e-commerce businesses in India in light of the Digital Personal Data Protection Act, 2023 along with the current data protection laws under the Information Technology Act, 2000 and the Consumer Protection (E-Commerce) Rules, 2020. It explores ongoing challenges like informed consent, cross-border transfer of data, data breaches, algorithmic profiling, deceptive design, and data sharing by third parties, putting all of these in the background of the constitutional recognition of privacy as a fundamental right. The paper goes ahead to conduct a comparative analysis with the GDPR in EU to identify approaches that can prove useful in regulating the issue in India. It concludes that even though India has made commendable progress in creating an extensive legal framework for data protection, there are still several challenges in terms of enforcement abilities, compliance cost for small businesses, and implementation of data subject rights in e-commerce.

Manuscript Information

- **ISSN No:** 2584-184X
- **Received:** 07-08-2026
- **Accepted:** 06-09-2026
- **Published:** 10-09-2026
- **MRR:**4(9); 2026: 76-81

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Singh C, Prahalad. Data Protection and Privacy Challenges for Indian E-Commerce Companies. Indian J Mod Res Rev. 2026;4(9):76-81.

Access this Article Online

www.mrrjournal.in

KEYWORDS: data protection, privacy, e-commerce, Digital Personal Data Protection Act 2023, consumer rights, India

I. INTRODUCTION

There has been a phenomenal transformation during the past decade in how Indian consumers procure goods and services because e-commerce has made the transition from being a luxury available only to urban consumers to become an integral part of daily economic transactions. This period has also seen a marked increase in the collection, storage, analysis, and exploitation of personal information by the e-commerce companies as part of their normal business activities.

Modern e-commerce platforms invariably have a system where the information gathered is not just limited to basic contact information or addresses but includes highly sensitive information such as financial information, purchasing habits, behavioral information, and even biometric or geolocation information collected through mobile applications. The sheer scale and nature of such information gathering raise some very important questions about the adequacy of consumer protection in laws, and the extent to which the Indian laws ensure accountability of the companies handling this information.[1]

Privacy, which had been viewed in India's legal tradition as an issue of common law and tort rather than as a constitutional right, was unequivocally recognized as being an integral part of the right to life and liberty under Article 21 of the constitution by a bench of nine judges of the Supreme Court.[2] This recognition has led to further legislative advances, resulting in the recently passed Digital Personal Data Protection Act, 2023, which marks India's first holistic and sector-agnostic data protection legislation.[3]

It is also clear that the industry of electronic commerce finds itself at a particularly vulnerable position in the midst of this developing regulatory environment since it operates on the intersection of laws protecting consumers, laws concerning contracts, competition law, and data protection law. Unlike many other information-rich industries, firms in the field of e-commerce interact with customers during the different phases of the business transaction, from looking for the products, creating an account, making payments, arranging for delivery, and post-sales services.[4]

The objective of this paper is to conduct an analysis of the key data protection and privacy concerns confronting e-commerce firms operating in India. This paper starts off with defining the theoretical aspects related to data protection and privacy within the realm of online business before describing how the laws relating to the management of personal data have evolved in India. Following that, the problems faced by the e-commerce firms in this regard are identified, analyzed, and compared with those that exist in the General Data Protection Regulation of the European Union.

II. CONCEPTUAL FOUNDATIONS OF DATA PROTECTION AND PRIVACY IN THE DIGITAL ECONOMY

Privacy and data protection are two interlinked concepts but are different from one another. Historically, privacy has been viewed as a right to be left alone, meaning that privacy entails the rights of an individual to control access to themselves, their decisions, and their surroundings. On the other hand, data protection is a narrower concept that is restricted to the laws related to the collection, processing, storage, and transferring of personal data[5].

The difference between the two terms takes on significant practical relevance in the world of e-commerce. Privacy interests of the consumer can be impacted from the very moment they use an online portal where their privacy can be compromised through cookie tracking and other monitoring tools, whereas the rights related to data protection kick in when the portal uses their personal information.

It has been traditionally recognized in academic circles that informational privacy in an interconnected economy cannot be reduced to a simple binary choice of concealment or disclosure but must be considered a question of contextual integrity, where the appropriateness of information transactions depends on the norms governing the specific context. This idea is particularly revealing with regard to e-commerce since the initial collection of data aimed at completing a transaction is often subsequently repurposed for marketing or credit assessments or sold to third-party data collectors with little consumer awareness[6].

Seven fundamental principles were highlighted by the Expert Committee headed by Justice B.N. Srikrishna as the bedrock on which the present Indian data protection laws have been built – lawfulness and fairness in processing, restriction of purpose, data minimization, accountability, data retention limitations, notice and consent, and security measures. Although these principles are generally stated in broad terms, they translate into certain duties of e-commerce organizations as far as their data collection and processing practices are concerned.

It is important to understand that the processing of e-commerce data usually does not take place in the confines of one business entity. Even the typical e-commerce transaction will involve the platform, the payment gateway, the logistics partner, the cloud service provider, and often third-party analytics and advertisement brokers, all of whom make use of the same base dataset for different purposes. This layered approach of data processing makes it difficult to assign responsibility and thus impedes the consumers from figuring out the owner and purpose of their data[7].

[1] Vakul Sharma, Information Technology: Law and Practice, 6th edn (Universal Law Publishing, 2021) 412-415.
[2] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[3] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
[4] Nandan Kamath, Law Relating to Computers Internet and E-Commerce, 5th edn (Universal Law Publishing, 2019) 221.
[5] Daniel J. Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477, 479-482.
[6] Subhajit Basu, 'Policy-Making, Technology and Privacy in India' (2010) 6 Indian Journal of Law and Technology 65, 70-74.
[7] Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press, 2013) 44-47.

III. EVOLUTION OF INDIA'S DATA PROTECTION LEGAL FRAMEWORK

India's history with data protection law started in a disorganized and largely reactive manner. The Information Technology Act, 2000, in its initial draft, did not have any major provisions with regard to protection of personal data, and this is an indication that the legislative body's primary concern at this time was electronic commerce and cybercrimes as opposed to data protection regulations.

This problem was to some extent addressed by adding Section 43A in the Information Technology (Amendment) Act, 2008, providing civil liability to companies failing to ensure reasonable security practices in handling sensitive personal data, and subsequently through the enactment of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[8] As defined by the SPDI Rules, sensitive personal data is considered to be data pertaining to finance, health information, biometric data, sexual orientation, and password. It is the responsibility of the companies to seek consent, provide a privacy policy and ensure proper security measures which include compliance with the international standard ISO/IEC 27001.

Before privacy being declared a fundamental right in Puttaswamy, the Supreme Court had already made an observation in relation to a limited right to privacy being a part of personal liberty, especially when it comes to telephonic surveillance. However, it was only in the judgment of 2017 that privacy was recognized as a fundamental right based on certain acceptable limitations in legislation[9].

After the Puttaswamy case judgment, the Central Government set up the Committee of Experts headed by Justice B.N. Srikrishna, who presented a report in 2018 which included the Draft Personal Data Protection Bill. The bill went through many amendments, including scrutiny by the Joint Parliamentary Committee before its rejection in 2022 and being replaced by the Digital Personal Data Protection Bill, which finally became an act in 2023.

In contrast to the structure that had been proposed by the Srikrishna Committee, the 2023 Act deviates from it significantly. It adopts a fairly relaxed approach that relies on consent and notice, discards the earlier proposal regarding the stricter policy of data localization, and establishes a Data Protection Board of India, which will be the principal adjudicating and enforcing entity.[10]

The Act lays down an array of obligations for e-commerce companies that are both independent and parallel to those that have already been laid down by the Consumer Protection (E-Commerce) Rules, 2020, passed by the Consumer Protection Act, 2019, and that lay down obligations of the same sort on e-commerce businesses. The overall effect of this multi-faceted regulatory system means that any e-commerce business operating in India will be required to comply with obligations that arise out of general data protection laws, sectoral consumer protection regulations, as well as payment information rules laid down by organizations like the Reserve Bank of India.

IV. E-COMMERCE IN INDIA: GROWTH AND DATA PRACTICES

From a meager beginning, the Indian e-commerce sector has transformed into one of the fastest growing digital sectors worldwide thanks to the rising use of smartphones, falling costs associated with data usage, and the existence of digital payment technologies such as the Unified Payment Interface.

The development has been accompanied by the increased sophistication of the data-driven models that these e-commerce companies employ. These platforms rely increasingly on algorithms for recommending products, dynamic pricing, and behavioral advertising all of which require constant acquisition and analysis of consumer data.[11]

It is important to note that the process of data collection within the context of e-commerce rarely remains limited to data which the consumer volunteers actively. The websites and mobile applications make use of tracking devices to collect device ID, IP address, geolocation data, and clickstream data passively without requiring any active contribution from the consumer.[12]

Such difference between the perception of the disclosure by users and the practice of data gathering by the platforms is crucial for many of the privacy problems discussed below. It explains why regulatory authorities in different countries are increasingly moving from the model of data protection based solely on consent to the one where the obligations of data controllers are based on independence, regardless of the technical consent.

V. KEY PRIVACY CHALLENGES FACED BY E-COMMERCE COMPANIES

A. Consent Fatigue and the Illusion of Informed Consent

The Digital Personal Data Protection Act, 2023 mostly relies on consent as the primary basis of processing of personal data, whereby consent must be freely given, specific, informed, unambiguous, and followed by a clear affirmative act. In actuality, the privacy policies and terms of use of e-commerce businesses tend to be extensive and standardized and hardly read or understood by consumers, a phenomenon known in the academic circle as consent fatigue.

Furthermore, the design of many e-commerce websites makes their consent structures such that the true exercise of consent is

[8] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rules 3-8.

[9] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

[10] Rishab Bailey, Smriti Parsheera, Faiza Rahman and Renuka Sane, 'Comments on the Draft Personal Data Protection Bill, 2018' (National Institute of Public Finance and Policy, Working Paper No. 253, 2018) 12-18.

[11] Lokesh Vyas, 'The Personal Data Protection Bill and E-Commerce: Mapping the Overlaps' (2021) 14 NUJS Law Review 112, 116-119.

[12] Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2014) 389-393.

not easily achievable since they present only one bundled consent for different processing activities such as marketing, profiling, and sharing of data.[13] The resultant permission, while officially legitimate, frequently lacks substantive depth, prompting significant inquiries over the efficacy of the consent-based framework in safeguarding consumer autonomy within a mass-market digital landscape.

B. Cross-Border Data Transfer and Data Localisation

There are several e-commerce organizations in India that are heavily dependent on cloud infrastructure and third-party service providers for activities such as data storage, analytics, and customer relationship management. The Digital Personal Data Protection Act of 2023 permits the transfer of personal data beyond India's territory, except those countries that have been marked out by the Central Government as exceptions to data localization.

While this approach has reduced the cost of compliance for these e-commerce organizations that are using international cloud infrastructure, there are concerns regarding the application of Indian data protection laws on an international scale after personal data leaves the territory of India, especially in cases where the foreign country has much weaker data protection laws than India.[14]

C. Data Breaches and Cybersecurity Vulnerabilities

Given that e-commerce websites store sensitive data in large quantities, they become attractive targets for cyber-attacks. There have been many major data leaks related to e-commerce websites and their associated sites in India in recent times involving personal data of customers, such as their names, contact information, and payment information, among other things.[15]

The Digital Personal Data Protection Act, 2023 provides that the data fiduciaries have to take appropriate measures for preventing the breach of personal data and report the same to the Data Protection Board of India and the respective data principals. However, while the failure of providing for a specific time frame in the Digital Personal Data Protection Act, 2023 for reporting the breach of personal data unlike seventy-two hours provided in the General Data Protection Regulation, European Union, provides great flexibility in making rules, it poses ambiguity to e-commerce businesses to formulate response plan[16].

D. Algorithmic Profiling and Behavioural Advertising

These days, e-commerce businesses have started making use of machine learning algorithms to build detailed behavioural profiles of the customer based on their web history, shopping tendencies, and time spent on particular products. This is then used for custom pricing, product recommendations, and marketing, often in conjunction with third-party advertising networks.[17]

These forms of profiling create specific fears that extend beyond the scope of traditional notions of data protection, including the possibility of discriminatory pricing, maintaining old biases through automation, and reducing consumer autonomy by the use of persuasive design tactics customized to individual psychological profiles. The Digital Personal Data Protection Act, 2023, unlike the General Data Protection Regulation, does not have a clause on exclusive automated decision-making, thereby depriving Indian consumers of any legal means to combat this form of algorithmic profiling.[18]

E. Third-Party Data Sharing and the Role of Aggregators

E-commerce involves heavy data exchanges between e-commerce platform providers and third parties, including payment service providers, logistics companies, marketing partners, and vendors in marketplace environments, who need consumer data for order fulfilment. Each time data is transferred to a third party, a new way of leakage or abuse opens up, and users do not usually have the ability to trace the entire downstream flow of their data once it is out of the jurisdiction of the platform.

The aim of the Consumer Protection (E-Commerce) Rules, 2020 is to deal with the problem by ensuring that e-commerce entities are not allowed to obtain consent for data collection as a requirement for using their services, and also ensure that any transfer of user data to third parties should be done only after obtaining explicit consent. However, this rule has not been followed strictly, and consumers get to know about how much third-party data has been shared only when they start receiving marketing messages from unrelated organizations.

F. Dark Patterns and Manipulative Design Practices

The problem associated specifically with the e-commerce field is that of dark patterns. These are special interfaces that are created for the purpose of forcing consumers to perform actions that they normally would not, for example, accepting data collection that is unrelated to the transaction at hand. Examples include pre-ticked consent checkboxes, shaming language that makes one think twice about rejecting marketing messages, and designs that make giving up consent far harder than giving it out.

The Central Consumer Protection Authority has issued guidelines identifying thirteen types of dark patterns as deceptive business practices according to the Consumer Protection Act, 2019, which include false urgency, basket sneaking, subscription traps, and forced action, among others

[13] Apar Gupta, Commentary on Information Technology Act, 3rd edn (LexisNexis, 2022) 267-270.
[14] Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press, 2013) 112-116.
[15] Vakul Sharma, Information Technology: Law and Practice, 6th edn (Universal Law Publishing, 2021) 445-449.
[16] Digital Personal Data Protection Act, 2023, Section 8(6).
[17] Paul M. Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 New York University Law Review 771, 780-785.
[18] Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins India, 2018) 101-105.

that impact data consent directly on e-commerce platforms.[19] While these regulations can be seen as an effort in the right direction, there is still uncertainty regarding whether the penalties will be enough to prevent such behaviour by well-funded e-commerce websites.

VI. REGULATORY AND COMPLIANCE CHALLENGES

In addition to the privacy risks discussed above, there are also particular compliance challenges faced by e-commerce enterprises due to the complexity of some overlapping components of India's legislation framework. Under the Digital Personal Data Protection Act, 2023, there is the concept of the Significant Data Fiduciary which can be designated by the Central Government depending on the amount and type of data processed, harm to data subjects, and other characteristics, including electoral democracy, national security, and sovereignty. With regard to their huge scale of operation, it can be expected that many large e-commerce companies belong to the category of Significant Data Fiduciaries, which brings additional obligations for such enterprises, such as designation of Data Protection Officer in India and conducting regular Data Protection Impact Assessment.

With regard to small e-commerce enterprises, especially those micro, small and medium-size companies which have moved online, the total cost of meeting these requirements poses a serious challenge for them.[20] Small sellers using marketplaces lack the capacity to independently verify the data handling practices of the platforms on which they operate compared to large platforms with dedicated legal and compliance departments, creating a problem of diffusion of responsibility that the existing system fails to address adequately.

The creation of the Data Protection Board of India as an exclusively digital judicial body, empowered to impose fines worth two hundred and fifty crore rupees on companies with insufficient protection measures against cybersecurity threats, represents a clear enforcement measure. Nevertheless, in light of the scale of online business activity in India, doubts remain as to the efficiency of the Board to resolve disputes quickly enough and protect itself from executive influence.

Another potential compliance challenge arises due to interaction between the Digital Personal Data Protection Act, 2023, and industry-specific regulation such as the one imposed by the Reserve Bank of India, stipulating that transaction data related to payments made in India should only be stored in India. Online companies that use integrated payment systems face stricter restrictions regarding storing data on payments than the cross-border transfer limitations outlined in the 2023 Act[21].

VII. COMPARATIVE PERSPECTIVE: LESSONS FROM THE GENERAL DATA PROTECTION REGULATION

The most important data protection law in the world is believed to be the General Data Protection Regulation of the European Union, and a comparative review of its provisions would shed light on possible improvements of the Indian system.

Unlike the Digital Personal Data Protection Act, 2023, the General Data Protection Regulation recognizes a number of legitimate bases for the data processing besides the consent, such as legitimate interest, performance of contract, and compliance with legal obligations, which allows decreasing reliance of data controllers on consent-based frameworks that are procedural rather than material. The Regulation gives data subjects the right to object to processing based on the purpose of direct marketing, including profiling for such marketing purposes, which right cannot be found in the Indian law.

The General Data Protection Regulation stipulates that any personal data breach, the likelihood of which poses a risk to the rights and freedoms of individuals, should be reported to the corresponding supervisory authority within seventy-two hours from the moment when data controllers get aware about it. Furthermore, the penalties for violations range from warnings to the highest penalties that make up to four percent of a company's annual revenue worldwide. Contrary to this, the fixed financial sanctions prescribed by the Indian Act, although quite high in their absolute amount, do not depend on the revenue of the entity, which prompts to question their proportionality as deterrent measures in respect of the largest e-commerce sites in India.

Therefore, it is important to avoid automatic use of the European model in India. While the regulatory burdens of the General Data Protection Regulation have been heavily criticized even by small European companies, the relatively liberal approach taken by India may represent a certain strategy.[22]

VIII. RECOMMENDATIONS AND THE WAY FORWARD

Firstly, the sub-regulations prescribed by the Digital Personal Data Protection Act, 2023 should stipulate a definite timeline for breach notifications, similar to the seventy-two-hour threshold set by the General Data Protection Regulation, in order to provide clarity to e-commerce businesses about their responsibilities and ensure timely notification to affected individuals.

Secondly, the authorities may consider prescribing a scale of penalties based on the turnover of large data holders within the e-commerce sector, thus ensuring that the punitive value of regulatory measures is in proportion to the size and influence of the particular platform, rather than imposing a uniform standard of penalties for all platforms irrespective of their sizes.

[19] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, Notification dated 30 November 2023.

[20] Anirudh Burman, 'Understanding India's New Data Protection Law' (Carnegie Endowment for International Peace, Carnegie India, October 2023) 14-17.

[21] Reserve Bank of India, Storage of Payment System Data, Notification No. RBI/2017-18/153, 6 April 2018.

[22] Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2014) 402-406.

Thirdly, the guidelines prescribed by the Central Consumer Protection Authority for dark patterns should be further integrated into the consent mechanism prescribed by the Digital Personal Data Protection Act, 2023 in a manner that consent obtained by using deceptive interface designs is treated as invalid consent under data protection laws, and not only as an unfair trade practice under consumer protection law.[23]

Finally, due to the accountability diffused nature of marketplace-driven e-commerce models, it is important to take into account the application of joint and several liability on platform operators and third parties with regard to any data protection violations resulting from the data distributed using the platform, thus ensuring that major platforms do not escape their liability with regard to the activities of sellers who gain access to customer data through their platform.

First, it is important to increase the capacity of the Data Protection Board of India with regard to the e-commerce and digital platforms governance issues, in order to be able to cope with the number and complexity of the cases coming out of such data-intensive industry as e-commerce.

In general, e-commerce companies should abandon a tick-box approach to compliance and adopt a privacy by design approach as a basic tenet, making data minimization and purpose limitation part of their platform.

IX. CONCLUSION

The enactment of the Digital Personal Data Protection Act, 2023 represents an important step forward in India's endeavor to adopt an all-encompassing data protection regime and is a considerable improvement from the earlier fragmented, sectoral laws regulating the handling of personal data by e-commerce companies.

The purpose of this study is to prove that several significant challenges still exist in translating legislative provisions into adequate protection of consumer rights in the e-commerce realm. Issues surrounding permission fatigue, algorithmic profiling, sharing of personal data with third parties, deception design, and disparity in compliance capacity between leading platforms and smaller vendors continue to pose serious threats to Indian consumers insufficiently protected by the current legislation.

An effective data protection regime in the Indian e-commerce industry requires not only the adoption of legal standards but also the ability to enforce those standards, the political will to bring the wealthy platforms to account, and a shift towards privacy by design rather than mere compliance. With the rapid development of India's digital economy, the solutions found to these challenges in the next few years will determine the level of consumer trust in electronic commerce and consequently its sustainable development.

REFERENCES

1. Burman A. Understanding India's new data protection law. Washington, DC: Carnegie Endowment for International Peace, Carnegie India; 2023 Oct.
2. Gupta A. Commentary on Information Technology Act. 3rd ed. New Delhi: LexisNexis; 2022.
3. Kuner C. Transborder data flows and data privacy law. Oxford: Oxford University Press; 2013.
4. Solove DJ. A taxonomy of privacy. Univ Pa Law Rev. 2006; 154:477.
5. Greenleaf G. Asian data privacy laws: trade and human rights perspectives. Oxford: Oxford University Press; 2014.
6. Justice A.P. Shah Committee. Report of the Group of Experts on Privacy. New Delhi: Planning Commission of India; 2012.
7. Justice B.N. Srikrishna Committee. A free and fair digital economy: protecting privacy, empowering Indians: report of the Committee of Experts on Data Protection Framework for India. New Delhi: Ministry of Electronics and Information Technology; 2018.
8. Vyas L. The Personal Data Protection Bill and e-commerce: mapping the overlaps. NUJS Law Rev. 2021; 14:112.
9. Kamath N. Law relating to computers, internet and e-commerce. 5th ed. New Delhi: Universal Law Publishing; 2019.
10. Schwartz PM. Global data privacy: the EU way. NYU Law Rev. 2019; 94:771.
11. Matthan R. Privacy 3.0: unlocking our data-driven future. New Delhi: HarperCollins India; 2018.
12. Bailey R, Parsheera S, Rahman F, Sane R. Comments on the Draft Personal Data Protection Bill, 2018. Working Paper No. 253. New Delhi: National Institute of Public Finance and Policy; 2018.
13. Basu S. Policy-making, technology and privacy in India. Indian J Law Technol. 2010; 6:65.
14. Sharma V. Information technology: law and practice. 6th ed. New Delhi: Universal Law Publishing; 2021.
15. Ministry of Commerce and Industry, Government of India. National e-commerce policy (draft). New Delhi: Department for Promotion of Industry and Internal Trade; 2019.

[23] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, Notification dated 30 November 2023.