International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838
Received: 07-02-2026, Accepted: 08-03-2026, Published: 24-03-2026
Volume 8, Issue 1, 2026, Page No. 243-245

Consumer rights in the digital realm: Comprehending India's Cyber law framework

Dr. Ankit Sourav Sahoo
Assistant Professor, Lajpat Rai Law College, Sambalpur, Odisha, India

Abstract
The rapid expansion of digital commerce has transformed traditional consumer markets into complex online ecosystems where transactions occur through mobile applications, digital payments, and virtual platforms. This article examines the legal framework governing consumer protection in India's digital marketplace and analyses how cyber laws safeguard consumer rights in the era of e-commerce and fintech. The study highlights the transition from the traditional doctrine of *caveat emptor* ("let the buyer beware") to *caveat venditor* ("let the seller beware"), reflecting the growing responsibility of businesses to ensure transparency, fairness, and accountability in online transactions. A central focus of the article is the Consumer Protection Act, 2019, which modernised India's consumer law by recognising online consumers and establishing the Central Consumer Protection Authority (CCPA) to investigate unfair trade practices and misleading advertisements. The Consumer Protection (E-Commerce) Rules, 2020 further regulate digital marketplaces by mandating grievance redressal mechanisms, disclosure of product information, and accountability of online platforms. The article also explores emerging challenges such as dark patterns in digital interfaces, misuse of consumer data, and the rise of cyber fraud in digital payment systems. It explains how multiple laws including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and Reserve Bank of India guidelines on electronic banking fraud collectively create a multilayered protection mechanism for digital consumers. The study concludes that while India has developed a robust legal framework for consumer protection in cyberspace, effective enforcement and consumer awareness remain essential to ensure that digital marketplaces remain fair, transparent, and secure for users.

Keywords: Consumer Protection, E-Commerce, Consumer Rights, Data Protection, Online Marketplace

Introduction

The Development of the Online Marketplace gives us a Reflection on the shopping habits of our parents or grandparents. They visited a physical market, examined the fabric of a shirt, verified the expiry date on a milk carton, and made a cash payment. If an issue arose, they were aware of the specific establishment to return to for confrontation. This period adhered to the notion of "Caveat Emptor," a Latin expression signifying "Let the Buyer Beware [1]." The responsibility of the customer was to inspect the items before to payment. Advance to the year 2026. You are probably purchasing a pizza on Zomato, acquiring sneakers on Ajio, or reserving a cab on Uber. The "shop" is now an application on your mobile device. The commodity is intangible, the vendor may be located 2,000 kilometres away, and your payment is a digital transaction. Due to the buyer's current disadvantage, the legislation has transitioned to "Caveat Venditor" meaning "Let the Seller Beware." In the digital era, the law mandates that companies maintain honesty, transparency, and fairness." As the internet expands, so are the tactics employed to exploit customers. This article explores the intricate framework of rules established to safeguard individuals in the digital realm.

The Significance of Consumer Protection in Cyberspace

The way customers buy goods and services has changed dramatically as a result of India's digital economy's explosive expansion. Cyberspace is a new environment created by the replacement of traditional physical markets by online marketplaces, mobile applications, digital payment methods, and social media platforms. Consumer rights are vital in this changing digital marketplace because they shield people against fraud, unfair business practices, and the exploitation of personal information. Strong legislative protections and consumer awareness are crucial as the number of digital transactions rises. The knowledge imbalance between customers and sellers is one of the main reasons consumer rights are crucial in cyberspace. Online shoppers are unable to personally inspect products before making a purchase, in contrast to traditional markets. Customers find it challenging to confirm the authenticity or quality of products since they are sometimes supplied by sellers that are spread across several nations or regions. Consequently, legislative safeguards guarantee that vendors uphold transparency, offer precise product details, and fulfill their commitments to supply goods and services. The Consumer Protection Act of 2019 updated India's consumer protection laws to take internet commerce into account. In addition to establishing safeguards against deceptive advertising, faulty goods, and unfair business practices, the legislation acknowledges internet shoppers as consumers. By enabling the government to look into and take action against businesses that engage in widespread consumer exploitation, the creation of the Central Consumer Protection Authority significantly enhances enforcement.

Online platforms are also subject to the Consumer Protection (E-Commerce) Rules, 2020, which mandate that they designate grievance officers, reveal product details including the place of origin, and promptly address customer concerns. These regulations give consumers easily accessible grievance redressal methods and aid in ensuring responsibility among e-commerce enterprises. The misuse of customer data is another significant issue in internet. Numerous internet services gather personal data, including financial, location, and contact facts. Businesses risk financial loss and privacy concerns if they don't protect this

data. The Data Protection Board of India oversees compliance and looks into data breaches, while the Digital Personal Data Protection Act, 2023 regulates how businesses gather, handle, and keep personal data.
In order to address new issues like dark patterns deceptive digital interface designs that trick users into making unwanted purchases or disclosing personal information consumer rights are also crucial. The government has strengthened consumer protection in the digital economy by outlawing a number of these behaviors and classifying them as unfair trade practices. given conclusion, given India's quickly growing digital economy, consumer rights in cyberspace are critical to preserving justice, trust, and openness. People can safely engage in online transactions while being shielded from exploitation and digital fraud thanks to robust regulatory frameworks, efficient enforcement methods, and raised consumer awareness.

Modernising the Legislation for the 21st Century with Reforms

For more than thirty years, India depended on the Consumer Protection Act of 1986. Although it was an exemplary regulation, it was written prior to the internet being ubiquitous in households. It lacked the term "e-commerce" entirely. In 2019, the government substituted it with the Consumer Protection Act (CPA), 2019 [2]. This was not merely a modest upgrade; it constituted a complete overhaul. There have been some significant modifications for digital consumers in the new act which are to be discussed. The law now specifically encompasses anyone who purchases products or services via online transactions, electronic methods, teleshopping, or multi-level marketing to be a consumer. Also, there comes a Central Consumer Protection Authority. Consider this entity as the "Super-Cop" for consumer protection. In contrast to the previous system requiring individuals to initiate cases independently, the CCPA can independently commence investigations upon identifying a "class" of customers being deceived, such as in instances of widespread deceptive advertising. Also, If an online purchase explodes or inflicts harm, you may initiate legal action against the manufacturer, the seller, and occasionally the service provider.
Moreover, The E-Commerce Regulations, 2020 envisages as a "Guide" for Online Retailers. In accordance with the CPA 2019, the government promulgated the Consumer Protection (E-Commerce) Rules, 2020 [3]. These regulations delineate the "dos and don'ts" for platforms such as Amazon, Flipkart, and smaller Instagram boutiques.
The law differentiates internet stores according to their operational mechanisms.

1. Inventory Model: This refers to a scenario in which the website possesses the merchandise and sells it directly to consumers (e.g., a brand's proprietary website such as Nike.com). They bear complete responsibility for the product.

2. Marketplace Model: This refers to a website that serves solely as a "platform" for various vendors to list their products (e.g., Amazon or eBay).
According to Section 79 of the IT Act, 2000 [4], platforms such as Amazon are afforded "Safe Harbour" protection. This indicates that companies are typically not held accountable if a third-party vendor delivers a counterfeit item EXCEPT when the marketplace fails to exercise "due diligence" or disregards your grievance.
The new legislation also provides for a robust grievance redressal mechanism. There have been instances where consumers attempted to contact a company and found themselves engaged with an automated system for hours. The 2020 Regulations rendered this unlawful. Every e-commerce firm is required to designate a Grievance Officer. They are required to acknowledge your complaint within 48 hours. They are required to rectify the issue within one month. Products must prominently display the "Country of Origin" to facilitate informed decision-making.
The legislation also puts a restriction on "Dark Patterns" or “Dark Designs”. These are the designs, patterns, schemes or advertisements or messages which are intentionally created by vendors to influence the decisions of the customer. For example, If a customer visits a website of a travel agency, it may show a flashing red message stating, "Only 1 room left!"? Fifty individuals are currently observing this. Also, sometimes when a customer attempts to terminate a subscription, he may encounter the application prompting him to navigate through five distinct "Are you sure?" pages including perplexing "Double Negative" buttons. These are referred to as Dark Patterns. They are misleading UI/UX (User Interface/User Experience) designs intended to manipulate customers into actions they did not plan, such as purchasing insurance alongside a flight or disclosing their contacts [5].
There are certain CCPA Regulations Regarding Dark Patterns (2023) [6] whereby the Indian government has formally prohibited many dark designs, including:

a. **Spurious Urgency:** Deceptive timing or inventory counts.
b. **Basket Sneaking:** Incorporating additional products (such as a contribution or service fee) into your cart without prior consent.
c. **Confirm Shaming:** Employing guilt to maintain your subscription (e.g., a button labelled "No, I prefer being unprotected" instead than just "Unsubscribe").
d. **Subscription Traps:** Facilitating effortless enrolment but rendering cancellation exceedingly difficult.

The legal implication is that employing these patterns is now classified as a "Unfair Trade Practice." The CCPA can impose substantial penalties and compel companies to modify their app design if violations occur.
In a conventional retail establishment, "Consideration" (the payment rendered) is currency. However, numerous services in cyberspace are provided at no cost. You do not incur expenses for Google or Facebook. You compensate with your data [7]. Legal experts in India contend that a data breach involving a corporation such as Zomato or Uber constitutes a "Deficiency in Service" under the Consumer Protection Act. You compensated the firm with your personal information in return for their service. If they neglect to safeguard that information, they have violated their contractual obligations.

The Role of Data Protection Laws

The Digital Personal Data Protection (DPDP) Act, 2023 addresses penalties for data breaches, whereas the Consumer Protection Act permits consumers to seek compensation for distress or damage incurred. The Data Protection Board of India (DPBI) is the regulatory authority

established under Section 18 of the Digital Personal Data Protection Act, 2023 to enforce provisions related to the protection of personal data. Its primary function is to ensure that organisations handling personal data comply with the law and respect the privacy rights of individuals. The DPBI acts as an adjudicatory and enforcement body that deals with complaints related to data breaches, misuse of personal data, and violations of obligations by data fiduciaries (entities that collect and process personal data). It has the power to conduct inquiries, investigate complaints, and impose penalties on organisations that fail to protect personal data or violate the provisions of the Act. One of the key responsibilities of the Board is to ensure accountability in digital data processing. When a data breach occurs, affected individuals can file complaints before the Board. After examining the case, the DPBI may issue directions to organisations, require remedial measures, and impose significant financial penalties depending on the severity of the violation. The establishment of the Data Protection Board represents an important step toward strengthening data privacy governance in India. By providing a formal mechanism for addressing data protection violations, the DPBI plays a crucial role in safeguarding citizens' personal data in the rapidly expanding digital economy [8].

Fintech and Consumer Fraud:

The proliferation of UPI (PhonePe, Google Pay) has led to a significant increase in cyber-fraud. An somebody contacts you as a bank representative, you click a link, and subsequently your funds are depleted. The Reserve Bank of India (RBI) has released a significant circular about "Customer Liability in Unauthorised Electronic Banking Transactions [9]." If fraud occurs due to an error by the bank or a third-party breach of the system, and you disclose it within three business days, you are granted Zero Liability. The bank is obligated to refund your money. A delay in reporting (4 to 7 days) may result in a loss of a little sum, typically restricted to ₹5,000 to ₹25,000 based on your account classification. The bank is not liable for fraud unless you report it after sharing your OTP or PIN. Upon reporting it, any subsequent loss becomes the bank's responsibility.

To be an astute digital consumer, it is essential to comprehend that three distinct regulations collaboratively safeguard your interests. Consider them like three strata of a shield. Firstly the Consumer Protection Act of 2019 which safeguards against substandard quality, fraudulent advertisements, and excessive charges. Secondly, the IT Act of 2000 which establishes the technical regulations for digital signatures and imposes penalties on hackers. Thirdly, the DPDP Act, 2023, which prohibits companies from misusing or selling personal data without consent.

Conclusion

India is presently the globe's most rapidly expanding digital economy. However, a "Digital India" cannot thrive if individuals are apprehensive of clicking "Buy." The legislative evolution from the 1986 Act to the contemporary 2023 standards illustrates the law's attempt to keep pace with technological advancements. We currently possess a "Super-Cop" (CCPA), a "Data Guardian" (DPBI), and explicit regulations regarding UPI and e-commerce. Nonetheless, the most effective safeguard is not merely legislation it is awareness. Understanding your entitlement to a refund, recognising the illegality of "Dark Patterns," and being aware that you can report bank fraud within three days defines you as a "Sovereign Consumer." In the digital realm, your "click" constitutes your vote. Utilise it judiciously, and recognise that the law is firmly supporting you.

References

1. Avtar Singh, Law of Sale of Goods (Eastern Book Company, 2021)
2. Consumer Protection Act, 2019 (Act No. 35 of 2019), Government of India
3. Consumer Protection (E-Commerce) Rules, 2020, Ministry of Consumer Affairs, India
4. Information Technology Act, 2000, Section 79 (Intermediary Liability)
5. Harry Brignull, Dark Patterns: Inside the Interfaces Designed to Trick You (UX Research, 2013)
6. Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023
7. Digital Personal Data Protection Act, 2023, Government of India
8. Israel R, Barat DD, Gupte RV, Anand P. 2025, November 24). India's digital personal data protection regime takes effect. S&R Associates. https://www.lexology.com/library/detail.aspx?g=2073ac40-628f-4112-81f3-fffdfd4b8858
9. Reserve Bank of India. (2025). Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, Notification dated 06/07/2017
10. https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336