International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(20s) 2026 pp. 1570-1579
https://doi.org/10.70917/ijcisim-2026-6017
Article

CONSUMER PROTECTION IN THE ERA OF DIGITAL COMMERCE: EMERGING CHALLENGES, REGULATORY GAPS, AND FUTURE REFORMS UNDER INDIAN LAW

Anagha Kadam[1*], Pragati Dehliwal[2], Vallabh Ganesh Waghole[3]

[1]Late Tukaram Dhondiba Kunjir Law College, Pune, Maharashtra 411046, India
[1997]anaghakadam@gmail.com,
[2]PES Modern Law College, Pune, Maharashtra 411016, India
pragatidehliwal2@gmail.com
[3]Pune Cambridge Institute of Management & Computer Application, Pune, Maharashtra 411046, India
vallabhwaghole2@gmail.com
*Corresponding Author: 1997anaghakadam@gmail.com (Anagha Kadam)

Abstract: The digital marketplace in India has expanded so rapidly that the current consumer-protection regime has been unable to maintain pace with the developments. Consequently, consumers find themselves confronted with numerous legal issues that were never considered by the current regulatory framework. This paper analyzes the Consumer Protection Act, 2019 ("CPA 2019") along with the overall legal regime of digital commerce which including the Indian Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, and the rules made thereunder. It examines the effectiveness of these provisions in light of the modern day realities of online shopping. Through the use of doctrinal and comparative analysis, this study highlights the major shortcomings in the area of algorithmic manipulation, dark patterns, transboundary disputes, platform liability, manipulated reviews, fake products and the burgeoning trend of social commerce. Furthermore, the new issues like Non-Fungible Tokens, subscription traps and misleading marketing through AI have been considered as well. In light of lessons learnt from the Digital Services Act of European Union (2022), Online Safety Act of United Kingdom (2023) and enforcement by the United States Federal Trade Commission, this study suggests reforms for India. It is argued that India requires a novel E-Commerce Consumer Protection Framework, which encompasses data protection, algorithm accountability, regulator-platform cooperation and a simple dispute resolution mechanism. Such an E-commerce regime will be more appropriate to meet the challenge posed by the 450+ million people who do their shopping online. The conclusions reached in this study will be of relevance to academia, policymakers, judiciary, and the platform companies equally.

Keywords: Consumer Protection Act 2019; digital commerce; e-commerce regulation; algorithmic accountability; dark patterns; platform liability; data privacy; cross-border disputes; Indian law; digital markets

1. INTRODUCTION

1.1 The Scale of Digital Commerce

India is at an important stage in the development of consumer-rights law. More than 950 million Indians were online by 2024, and the domestic digital commerce sector is projected to surpass USD 350 billion by 2030, marking an extraordinary surge in online transacting (IAMAI, 2024; IBEF, 2024). The COVID-19 pandemic compressed years of anticipated digital uptake into a few months, cementing e-commerce as a routine feature of daily life for consumers in both cities and villages (Chawla & Sharma, 2021).

Copyright: © 2026 by the authors

1.2 Limits of the Legal Response

Legal measures, however, have been evolving at a somewhat slower pace. The Consumer Protection Act, 2019, although being an important development at the time of its introduction due to the recognition of the notion of e-commerce and creation of the Central Consumer Protection Authority (CCPA), was formulated long before some of the currently existing harmful digital practices even arose (Singh, 2020). The problems with the statute have become obvious over time, namely, the wording of the legislation is too broad; the enforcing bodies are understaffed and undersupplied; the secondary regulations are not sufficiently detailed and enforceable (Mehta & Gupta, 2022).

1.3 Research Gap

While the academic interest in the area of digital consumer protection has grown, the research is still fragmented between the separate areas of law. Much of the literature either focuses on the CPA 2019 (Jain, 2021; Sharma, 2022) or discusses the data protection issue without mentioning how it impacts consumer rights (Raghavan, 2023). Few works analyze Indian legislation with regards to international issues of digital marketplace fairness, platform dominance, and algorithmic harm (Kapoor & Mehta, 2023). The goal of this paper is to fill this research niche.

1.4 Objectives of the Paper

The paper aims to achieve four objectives. First, to review the current state of the statutory and regulatory framework in India regarding digital consumer protection. Second, to identify and analyze the key regulatory gaps arising due to new business practices. Third, to learn lessons from foreign jurisdictions with more advanced regulation. Fourth, to suggest practical and evidence-based recommendations for the Indian legislative system.

1.5 Organisation of the Paper

The paper is organized as follows.

Section 2 surveys the existing legal framework.

Section 3 considers the principal emerging threats to digital consumers.

Section 4 undertakes a comparative study of other jurisdictions.

Section 5 draws together the identified regulatory gaps.

Section 6 sets out reform proposals

Section 7 concludes with suggestions for future research.

2. THE EXISTING LEGAL FRAMEWORK GOVERNING DIGITAL COMMERCE IN INDIA

2.1 The Consumer Protection Act, 2019

There are many reasons why India currently finds itself at a crucial point in developing the legal regime concerning consumers' rights. Firstly, as of 2024, over 950 million Indians were online, and the value of the domestic digital commerce industry is forecast to exceed $350 billion by 2030, which signifies an unprecedented growth of e-transacting (IAMAI, 2024; IBEF, 2024). Secondly, the COVID-19 pandemic accelerated all expected digital adoption in a matter of months, thus making e-commerce a routine component of consumers' lives in cities and villages (Chawla & Sharma, 2021).
Nevertheless, the legal regime is developing much slower than required. For instance, the Consumer Protection Act, 2019 at the time of its passing was indeed an innovation because it acknowledged e-commerce transactions and established the Central Consumer Protection Authority (CCPA); however, the act was formulated before a lot of destructive digital practices emerged (Singh, 2020). In recent years, a number of flaws of this legislation became apparent, namely, its overly broad and general character, insufficiently staffed and resourced enforcement agencies,

and lack of sufficient detail in the subordinate regulations, in particular, the E-Commerce Rules of 2020 (Mehta & Gupta, 2022).

Research on the digital consumer protection issue gained momentum recently. However, this topic receives academic coverage fragmented into several fields of law. Existing literature mainly explores the act or its amendments (Jain, 2021; Sharma, 2022) or data protection issues without paying equal attention to their impact on consumer rights (Raghavan, 2023). Fewer articles discuss Indian legislation in the context of international discourse about fairness in the digital market, platform influence, and algorithms harm (Kapoor & Mehta, 2023). This paper intends to bridge this gap.

In this paper, there are four goals to pursue: to explore the current statutory and regulatory landscape of the digital consumer protection in India, to identify and analyze the regulatory gaps caused by new commercial practices, to derive useful information from more developed jurisdictions and their experiences, and to provide evidence-based recommendations for the reforms in the Indian legal system.

2.2 Consumer Protection (E-Commerce) Rules, 2020

Under the provisions of Section 101 of CPA 2019, the Consumer Protection (E-Commerce) Rules, 2020, revised in 2021, represent the most focused Indian legal initiative aimed at regulating the online marketplace itself. The Rules mandate disclosures to be made by e-commerce entities, prohibit the manipulation of search ranking for commercial advantage, mandate the provision of a grievance redressal system with the involvement of designated officials, and mandate labelling for products being listed. As revised in 2021, the Rules include the "fall-back liability" requirement for marketplace entities and forbid flash sales intended to deceive customers (Kapoor & Mehta, 2023).

Nonetheless, the Rules have attracted criticism for several reasons. Firstly, the line between the "inventory model" and the "marketplace model" is vague enough to leave potential loopholes that could be taken advantage of by the operators (Raghavan, 2023). Secondly, the enforcement is still quite ineffective as penalties are rather small, the monitoring is reactive in nature, and the CCPA does not have the capacity to monitor platforms in a proactive manner. Thirdly, the Rules do not address several modern-day phenomena such as social commerce, live commerce, and dark patterns (CUTS International, 2022).

2.3 Intermediary Guidelines and the Information Technology Act, 2000

The Information Technology Act, 2000 ("ITA 2000") is a more general law that provides the underlying legal framework for electronic commerce in India. In particular, Section 79 exempts intermediaries from liability for any third-party content as long as the intermediary has not "initiated", "selected", or "modified" it, and meets some due diligence standards. However, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules 2021") greatly increased the range of due diligence responsibilities, since the said Rules require the appointment of a grievance officer, implementation of content moderation, and communication traceability (Gupta, 2022).

It is not clear how the interplay of intermediary liability under the ITA and platform liability under the CPA 2019 works from the legal perspective

. If a platform deletes a fake listing in response to complaints but fails to take action against a repeated attempt to list the item by the same seller, it is not quite clear whether this is a failure of due diligence under the ITA, an unfair trade practice under the CPA, or both at the same time.

2.4 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ("DPDPA") grants a number of data-principal rights, which are applicable to digital consumers, and includes the rights of access, correction, and erasure of personal data; a right to revoke consent; and child-specific rights as per Section 9. Companies offering services involving behavioral advertising, profiling, or recommendation targeting have to abide not only by DPDPA but also by the CPA obligations (Raghavan, 2023).

However, the DPDPA and the CPA 2019 can be considered two separate regulatory silos. The Data Protection Board set up by the DPDPA and the CCPA set up under the CPA do not have any formal mechanism for coordination between each other. Such fragmentation is likely to lead to inconsistencies in enforcement and also makes regulatory arbitrage possible for platform companies (Bhandari, 2024).

3. EMERGING CHALLENGES IN DIGITAL CONSUMER PROTECTION

3.1 Algorithmic Manipulation and Dynamic Pricing

Perhaps the most common risk and one of the least regulated is algorithmic manipulation. In the contemporary age of e-commerce, machine-learning systems are employed by online marketplaces to customize the ranking of products, the recommendations made to customers, as well as pricing of products depending on the characteristics of an individual such as the profile, browsing history, the device used and geographical location (Ezrachi & Stucke, 2016). The system makes it possible for platforms to practice "price discrimination" and "steering".

While Indian legislation has not prohibited price discrimination targeted at consumers explicitly, section 2(47) of the CPA 2019 defines "unfair trade practices" as acts detrimental to consumers. Whether the aforementioned act is included in the definition and thus prohibited is debatable. Proving that the platform uses algorithmic discrimination is a challenge, as it requires access to proprietary code and training data which a platform has no legal obligation to provide (Kapoor & Mehta, 2023). Thus, the existing prohibition is unlikely to deter from practices harming consumers via the mechanism of algorithms.

3.2 Dark Patterns

Dark patterns are interfaces designed to steer a consumer in favor of the platform instead of serving the needs of the latter. They include subscription sign-ups that are disguised as free trials, disguised ads, urgency prompts and "roach motels" – interfaces that are designed to make the process of cancelation difficult and inconvenient (Mathur et al., 2019). In a survey conducted in 2023, 40 major e-commerce platforms in India were found to use at least one dark pattern in the purchasing process (CUTS International, 2022).

3.3 Platform Liability for Counterfeit and Unsafe Goods

The problem of counterfeits is a real issue when it comes to safety of consumers using Indian e-commerce platforms. The Confederation of Indian Industry estimated in 2022 that about INR 1.05 lakh crore worth of counterfeit goods including pharmaceuticals, electronics, cosmetic and food products are sold online in India annually (CII, 2022). In cases where counterfeit goods pose a threat to consumer safety, the issue of platform's liability becomes pertinent.

According to CPA 2019, product liability is established in Chapter VI of the legislation. It concerns "product service providers" as well as "product sellers". Whether a marketplace platform that only facilitates purchases and not performs them directly is considered to be a "product seller" for the purpose of imposing liability is open to debate. The E-Commerce Rules were amended in 2021 and now provide for "fall-back liability" of a marketplace entity in cases where it fails to settle grievances related to the seller properly, but the provision is hardly used as its triggering criteria is unclear (Singh & Rao, 2023).

3.4 Fake Reviews and Misleading Ratings

Product ratings and peer reviews have disproportionate influence over purchase decisions made through e-commerce websites. An increase of just one star rating in the average rating can lead to an improvement in conversion rate of 5–9% (Luca, 2016). This economic incentive has resulted in creation of a full-fledged industry that specializes in generating fraudulent product reviews. Even AI-created reviews that are almost indistinguishable from authentic ones are created.

No specialized legislation exists in India for dealing with fake reviews. Clause 2(47)(viii) of CPA 2019 prohibits "any false or misleading representation in respect of the goods." It might be considered as prohibiting fraudulent

reviews as well. IS 19000:2022 is the first national standard for consumer reviews generated online in India developed by Bureau of Indian Standards. It describes principles of collecting, moderating, and publishing of consumer reviews. Nevertheless, the standard is voluntary and self-certified (Mehta & Gupta, 2022).

3.5 Cross-Border E-Commerce and Jurisdictional Challenges

Given that digital trade is international by nature, Indian consumers constantly engage in transactions with foreign-based traders or platforms. In case of a dispute, the resulting asymmetry leads to an access-to-justice issue of major magnitude. While Section 34 of the CPA 2019 provides consumer forums jurisdictional reach based on the consumer's place of residence, the territorial limitation fails to bind the traders who lack a legitimate presence in India, do not have Indian bank accounts and work via foreign companies (Chawla & Sharma, 2021). There is particularly little recourse to enforcement regarding Chinese and Southeast Asian online platforms, which ship directly to Indian consumers. These entities ignore the directives of CCPA, BIS certification standards, and import labeling procedures. The customs regulations concerning concessional duty imports and the Legal Metrology (Packaged Commodities) Rules were not formulated to handle high-volume/low-value shipments that directly come from China to Indian consumers (Raghavan, 2023).

3.6 Social Commerce and Influencer Marketing Deception

In the field of social commerce, where the whole process of product discovery, recommendation, and purchase is completed inside social media platforms, rapid growth has been seen in India with Meesho, Shop101, and Instagram Shopping aggregating more than 100 million users (KPMG, 2023). Social commerce creates a confusion between true endorsement and paid promotion, giving rise to unique opportunities for consumer misrepresentation. According to the ASCI Guidelines for Influencer Advertising (2021) and CCPA Guidelines on Endorsements (2022), influencers should disclose all significant commercial connections with brands. Nevertheless, enforcement is lax, fines are low, and platforms do not share any liability when influencers using their platform fail to make these disclosures. Moreover, there is a new development of "live commerce," where product demonstrations along with links to purchase products instantly are provided, adding another layer of difficulty to enforcement since live streaming involves dynamic content (Kapoor & Mehta, 2023).

3.7 AI-Generated Misinformation and Synthetic Product Claims

Generative AI usage in product marketing presents a frontier issue for the law of consumer protection. This technology is capable of producing images of the products that distort their physical characteristics, forging testimonials that cannot be distinguished from real ones, and designing advertisements that take advantage of personal psychological weaknesses.

Unscrupulous vendors on Indian e-commerce platforms are already deploying these capabilities (Singh & Rao, 2023).

No Indian legislation currently addresses AI-generated commercial misinformation directly. The IT Rules 2021 obligate intermediaries to remove "false or misleading" content once notified, but this after-the-fact mechanism cannot keep pace with synthetic content that can be regenerated faster than it can be identified and taken down. The forthcoming Digital India Act, expected to replace the ITA 2000, will need dedicated provisions on AI-generated commercial content (Gupta, 2022).

4. COMPARATIVE LEGAL ANALYSIS: LESSONS FROM ADVANCED JURISDICTIONS

4.1 European Union: Digital Services Act and Consumer Omnibus Directive

The European Union has built the most comprehensive digital consumer-protection regime in the world. The Digital Services Act, 2022 ("DSA") imposes tiered obligations depending on a platform's size, with "very large online

platforms" subject to the strictest requirements — algorithmic risk assessments, independent audits, researcher access to data, and bans on advertising targeted at minors or based on sensitive personal characteristics (European Commission, 2022). The DSA's systemic risk-assessment mechanism, under which platforms must evaluate and address risks to consumer welfare, fundamental rights, and public discourse, has no counterpart in Indian law.

The Omnibus Directive (2019/2161/EU), transposed by member states by May 2022, targeted e-commerce deception specifically. It requires platforms to state whether a seller is a trader or a private individual — since different protections attach to each — mandates transparency around price history for discount claims, and requires that personalised pricing be disclosed to the consumer. These provisions speak directly to the algorithmic price-discrimination gap identified above in Indian law (Strycharz et al., 2021).

4.2 United Kingdom: Online Safety Act and Consumer Duty

The UK's Online Safety Act, 2023 places a "safety by design" obligation on platforms, requiring proactive risk assessment and mitigation against various online harms, including fraudulent advertising and user-generated content that harms consumers. In parallel, the Financial Conduct Authority's Consumer Duty (2023) requires financial-services firms to deliver good outcomes for consumers, building a positive duty of care into the regulatory structure rather than simply banning specific harmful practices. This outcomes-focused style of regulation, which looks at results rather than process compliance, may offer a more adaptable model for India's fast-moving digital market (CMA, 2021).

4.3 United States: FTC Enforcement and State Legislation

The US Federal Trade Commission has grown increasingly active in tackling digital consumer harm through its Section 5 authority over unfair and deceptive acts and practices. Notable actions include proceedings against Amazon for enrolling consumers in Prime subscriptions without adequate consent (FTC v. Amazon, 2023), against platforms using dark patterns (FTC Report on Dark Patterns, 2022), and against companies deploying AI-generated fake reviews (FTC Endorsement Guides, 2023). The California Consumer Privacy Act and the California Privacy Rights Act further show that sub-national regulators can lead effectively on consumer data protection (Bhandari, 2024).

4.4 China: E-Commerce Law and Platform Governance

China's E-Commerce Law, 2019 offers a useful, if context-specific, point of comparison. It makes platform operators jointly and severally liable for consumer harm wherever they "knew or should have known" that a seller on their platform was violating consumer rights and failed to act. This is a stricter liability standard than anything currently found in India, and it has driven substantial investment by Chinese e-commerce companies in consumer-protection infrastructure (Dong, 2020). China's experience also cautions against over-regulation, which can stifle innovation and concentrate market power among a handful of dominant domestic platforms.

5. SYNTHESIS OF REGULATORY GAPS

5.1 Principal Regulatory Gaps

The analysis above points to eight principal regulatory gaps in India's digital consumer-protection landscape, summarised below.

Table 1: Summary of Principal Regulatory Gaps in Indian Digital Consumer Protection Law

Sr. No.	Regulatory Gap	Current Legal Position
1	Algorithmic Price Discrimination	No direct statutory bar; CPA 2019 s.2(47) is theoretically available but effectively unenforced.

2	Dark Patterns	CCPA's 2023 guidelines exist but are advisory, carrying no binding authority.
3	Platform Liability (Counterfeit Goods)	Fall-back liability is left undefined, and the marketplace-versus-inventory distinction remains ambiguous.
4	Fake Reviews	IS 19000:2022 is a voluntary standard with no enforcement teeth.
5	Cross-Border Disputes	Jurisdictional reach is limited and no treaty-based cooperation framework exists.
6	Social Commerce / Influencers	The CCPA's 2022 guidelines are weakly enforced and impose no platform co-liability.
7	Subscription Traps	CPA 2019 s.2(46) on unfair contracts is applied only case-by-case, with no dedicated rule.
8	AI-Generated Misinformation	No dedicated provision exists; the IT Rules 2021 offer only a reactive takedown mechanism.

6. REFORM PROPOSALS: A MULTI-LAYERED FRAMEWORK

6.1 Enactment of a Dedicated Digital Consumer Protection Act

The most important reform would be a Digital Consumer Protection Act ("DCPA") as a lex specialis that works parallel to CPA 2019. It should be technology-neutral in terms of legislation but substance-specific in the matter of consumer rights to algorithmic transparency, personalization disclosure, and explainable AI recommendations. After the example of EU's DSA, DCPA should have a tiered structure, imposing stricter duties on platforms over user counts ("significant digital platforms") and giving easier ways of compliance to smaller digital firms. In particular, the DCPA should give: (i) the right to an explanation if algorithmic decision-making has an effect on the consumer choice; (ii) the right not to suffer from discriminatory pricing if there is no personalization based on consent and transparency; (iii) the right to accessible and free dispute resolution for transactions below INR 1 lakh; and (iv) the right to data portability between competing platforms to eliminate consumer lock-in (Kapoor & Mehta, 2023).

6.2 Strengthening the CCPA: Institutional Capacity and Proactive Enforcement

The CCPA suffers from inadequate resources vis-à-vis the size of the market that needs to be regulated. The restructured CCPA would borrow from the investigatory power of the UK Competition and Markets Authority and the rule-making power of the US FTC. The revamped CCPA must be allowed to conduct independent investigations, demand access to data from platforms in real time during investigations, impose binding interim orders while waiting for final rulings, and impose fines as a percentage of the platform's annual revenues in India (2 percent of annual Indian turnover).

A dedicated Digital Markets Division within the CCPA, staffed by data scientists, AI ethicists, and e-commerce specialists alongside lawyers, should also be created (CMA, 2021; Mehta & Gupta, 2022).

6.3 Mandatory Algorithmic Audits and Transparency Registers

Drawing on the EU AI Act's treatment of "high-risk AI systems", Indian law should require significant digital platforms to submit their consumer-facing recommendation, ranking, and pricing algorithms to periodic independent audits, with reports filed with the CCPA and key findings made public. Platforms should also be required to maintain a public "transparency register" that discloses, in plain language: (i) the main factors driving product rankings; (ii) whether personalised pricing is used and on what basis; and (iii) how sponsored results are distinguished from organic ones. This would address the evidentiary problem that currently makes algorithmic-discrimination cases so hard to bring (Ezrachi & Stucke, 2016; Strycharz et al., 2021).

6.4 Statutory Dark Patterns Prohibition and UI Audit Framework

The CCPA's 2023 dark-patterns guidelines should be given statutory force through an amendment to Schedule I of the CPA 2019, which lists unfair trade practices. A statutory prohibition should be paired with a mandatory annual UI/UX compliance audit conducted by CCPA-accredited third-party auditors for significant digital platforms; a consumer complaints portal for dark-pattern grievances with a mandated 30-day response window; and penalties calculated per consumer exposed, rather than per incident, to create a meaningful deterrent at scale. Platforms should also be required to make cancellation, refund, and opt-out routes as visible and accessible as sign-up and purchase flows (Mathur et al., 2019; Bhandari, 2024).

6.5 Cross-Border Dispute Resolution: Bilateral Treaties and Escrow Obligations

India should negotiate bilateral digital-trade agreements with the leading source countries of direct-to-consumer imports — notably China, the UAE, Singapore, and the United States — that include cooperation on consumer-protection enforcement. In the meanwhile, non-Indian e-commerce platforms that cross a certain transaction-value benchmark should have to register a legal entity or designate a legal representative in India, set up an escrow account with an Indian scheduled bank based on their sales in India, and accept the jurisdiction of Indian consumer forums as a precondition for accessing India’s payment system. Such a framework would build upon Australia’s approach towards regulation of non-resident digital platforms and EU’s geo-blocking and consumer redress mechanisms (Raghavan, 2023).

6.6 Integrated Data-Consumer Rights Framework

However, the difference between the regulation in DPDPA and CCPA must be bridged through formal mechanisms. A Joint Digital Consumer Rights Oversight Committee must be established whose members will be selected from CCPA, the Data Protection Board, Competition Commission of India, TRAI, and SEBI (for fintech and digital lending). These members will devise unified protocols for dealing with such cases where there is a possibility of overlapping jurisdictions related to consent manipulation, behavioural advertising, and price discrimination based on data. Further, the consent regime under the DPDPA should be harmonized with the CPA 2019's regime of unfair trade practices such that platforms cannot hide behind their long and ambiguous terms of service for unfair practices (Bhandari, 2024; Gupta, 2022).

6.7 AI Content Governance in the Forthcoming Digital India Act

The forthcoming Digital India Act, which is intended to replace the ITA 2000, presents an ideal platform to tackle the issue of consumer harm caused by artificial intelligence. The new legislation should mandate labeling of any artificial intelligence content used for commercial purposes such as pictures of products, customer testimonials, videos, and chatbots' advice.

Platform operators should face strict liability for unlabelled AI content that causes consumer harm, with a safe harbour available only where the platform has implemented CCPA-specified detection and removal protocols for AI content. The Act should further empower the CCPA to issue AI consumer-protection standards, allowing regulation to keep pace with AI development without requiring constant legislative amendment (Singh & Rao, 2023; Gupta, 2022).

7. CONCLUSION

7.1 Limits of the Present Regime

In conclusion, this paper has focused on consumer protection law in light of the dynamic nature of the digital commerce industry in India. It has been established that while the Consumer Protection Act, 2019 and other rules that have been enacted with it are a marked improvement over the older system, they fall significantly short in terms of dealing with the intricacies of contemporary e-commerce issues.

7.2 The Regulatory Gaps

There have been eight important regulatory gaps that include algorithmic price discrimination, dark patterns, liability of platforms for counterfeit products, fake reviews, cross-border dispute resolution, social-commerce deception, subscription traps and AI generated misinformation. These issues demonstrate the problem of a disparity of resources available to the operators of digital platforms and consumers who lack the means of combating commercial harm caused by technology.

7.3 Lessons from Other Jurisdictions

A comparative analysis demonstrates that there is no need for India to reinvent the wheel since there already exists a rich legal toolkit for consumer protection which was developed by the European Union (in the case of the DSA), the UK (Consumer Duty) and the FTC (enforcement doctrine). At the same time, China's approach to platform liability should be considered. India must act quickly before the power of the platforms will make it difficult to implement regulatory framework.

7.4 The Reform Agenda

The recommendations put forward here - Digital Consumer Protection Act, CCPA 2.0, algorithmic auditing, ban on dark patterns, cooperation on cross-border enforcement, harmonization of data and consumer protection law, AI content labelling - form a feasible and coherent policy agenda. Implementation of it will only solidify India's position as the leader in the sphere of digital consumer protection, which corresponds to India's demographic significance and rapid development of its digital economy.

7.5 Directions for Future Research

In terms of future research on this topic, it is possible to consider researching how courts interpret the provisions of the CPA 2019 in case of e-commerce disputes, whether the dark pattern rules of the CCPA decreased the use of these tactics, and how does the result differ in case of application of other liability regime on the platform.

REFERENCES

1. Bhandari, M. (2024). Intersection of data protection and consumer rights in the digital economy: An Indian perspective. *Journal of Indian Law and Society, 15*(2), 45–78.
2. Chawla, R., & Sharma, P. (2021). E-commerce and consumer protection during COVID-19: Emerging legal issues in India. *Indian Journal of Law and Technology, 17*(1), 88–112.
3. Competition and Markets Authority. (2021). *Digital markets taskforce: A new pro-competition regime for digital markets*.
4. Confederation of Indian Industry. (2022). *Combating counterfeits in digital markets: Policy recommendations for India*.
5. Consumer Protection Act, 1986, No. 68 of 1986 (India) (repealed).
6. Consumer Protection Act, 2019, No. 35 of 2019 (India).
7. Consumer Protection (E-Commerce) (Amendment) Rules, 2021 (India).
8. Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 255(E) (India).
9. CUTS International. (2022). *Dark patterns in Indian e-commerce: A study of consumer manipulation tactics*.
10. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
11. Digital Services Act, Regulation (EU) 2022/2065. (2022). *Official Journal of the European Union, L 277*.
12. Dong, Y. (2020). Platform governance and consumer protection under China's E-Commerce Law 2019: A comparative analysis. *Asian Journal of Law and Society, 7*(3), 523–548.
13. E-Commerce Law of the People's Republic of China (2019).
14. European Commission. (2022). *The Digital Services Act package: Explanatory memorandum*.
15. Ezrachi, A., & Stucke, M. E. (2016). *Virtual competition: The promise and perils of the algorithm-driven economy*. Harvard University Press.
16. Federal Trade Commission. (2022). *Bringing dark patterns to light: An FTC report*.
17. Federal Trade Commission. (2023). Guides concerning the use of endorsements and testimonials in advertising (16 C.F.R. Part 255).
18. Gupta, A. (2022). Reforming intermediary liability in India: The IT Rules 2021 and the road to the Digital India Act. *NUJS Law Review, 15*(3), 1–34.
19. India Brand Equity Foundation. (2024). *E-commerce industry in India*.

20. Information Technology Act, 2000, No. 21 of 2000 (India).
21. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
22. Internet and Mobile Association of India. (2024). *India internet report 2024*.
23. Jain, R. (2021). Consumer protection in the age of e-commerce: An analysis of the Consumer Protection Act, 2019. *Journal of Consumer Policy, 44*(2), 183–210.
24. Kapoor, S., & Mehta, D. (2023). Algorithmic accountability and consumer harm: Bridging the regulatory gap in Indian e-commerce law. *Indian Journal of International Law, 62*(1–2), 45–82.
25. KPMG. (2023). *The future of social commerce in India*.
26. Luca, M. (2016). *Reviews, reputation, and revenue: The case of Yelp.com* (Harvard Business School Working Paper No. 12-016).
27. Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM Human-Computer Interaction, 3*(CSCW), 81:1–81:32.
28. Mehta, V., & Gupta, S. (2022). Regulatory architecture for e-commerce consumer protection in India: Gaps and way forward. *National Law School of India Review, 34*(1), 67–99.
29. National Consumer Disputes Redressal Commission. (2023). *Annual report 2022–2023*. Ministry of Consumer Affairs.
30. Omnibus Directive, Directive (EU) 2019/2161. (2019). *Official Journal of the European Union, L 328*.
31. Online Safety Act 2023, c. 50 (United Kingdom).
32. Raghavan, S. (2023). Data sovereignty and consumer rights in the age of the Digital Personal Data Protection Act. *Economic and Political Weekly, 58*(18), 29–37.
33. Sharma, K. (2022). Jurisdictional challenges in e-commerce consumer disputes: A study of the Consumer Protection Act, 2019. *Symbiosis Law Review, 3*(1), 112–138.
34. Singh, A. (2020). The Consumer Protection Act 2019: A paradigm shift in the Indian consumer rights regime. *Journal of Business Law, 4*, 301–322.
35. Singh, R., & Rao, M. (2023). Product liability in e-commerce: Platform accountability for counterfeit and defective goods under Indian law. *NLU Delhi Law Review, 11*(2), 55–90.
36. Strycharz, J., van Noort, G., Helberger, N., & Smit, E. (2021). Contrasting perspectives: Practitioners' understanding of personalised communication. *European Journal of Marketing, 53*(4), 635–660.