INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

 ISSN: 3049-043X

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

 ISSN: 3049-043X

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

WWW.ijlar.com
Volume 3 Issue 7 | Aug 2026 *ISSN: 3049-043X*

A CRITICAL ANALYSIS OF CONSUMER PROTECTION IN E-COMMERCE UNDER THE CONSUMER PROTECTION ACT, 2019

AUTHORED BY - DR. ASHOK KUMAR[1] & SHIFA SIDDIQUI[2]

Abstract

The explosive growth of e-commerce in India has fundamentally altered the manner in which goods and services are marketed, sold and consumed, exposing consumers to novel forms of harm that the Consumer Protection Act, 1986 was structurally incapable of addressing. The Consumer Protection Act, 2019, together with the Consumer Protection (E-Commerce) Rules, 2020, represents Parliament's attempt to modernise India's consumer law regime by introducing product liability, a dedicated regulator in the form of the Central Consumer Protection Authority, e-filing of complaints, mediation, and specific obligations on marketplace and inventory-based e-commerce entities. This paper undertakes a critical, doctrinal examination of the statutory and regulatory architecture governing e-commerce consumer protection in India. It traces the legislative evolution from 1986 to 2019, analyses the definitional and enforcement scheme of the 2019 Act and the E-Commerce Rules, evaluates the recent Guidelines for Prevention and Regulation of Dark Patterns, 2023 and CCPA enforcement practice, and identifies persistent gaps relating to jurisdiction over offshore entities, the interface with intermediary liability under the Information Technology Act, 2000, inadequate remedies for design-based manipulation, and institutional under-capacity in consumer commissions. The paper concludes with recommendations for strengthening the framework, drawing comparative insight from the European Union and the United States.

Keywords: *Consumer Protection Act 2019; e-commerce; Central Consumer Protection Authority; product liability; dark patterns; unfair trade practice.*

[1] Assistant Professor, CMP Degree College, University of Allahabad
[2] Research Scholar, CMP Degree College, University of Allahabad

I. Introduction

India's legal institutions have been unable to keep up with the rapid expansion of the country's digital retail business. Due to growing internet penetration, reasonably priced smartphones, and an increasing number of digitally native customers, the nation is expected to grow into one of the world's top e-commerce markets.[3] However, this shift has resulted in a unique set of consumer harms that were not present in the brick-and-mortar marketplace: product misrepresentation via carefully chosen photos and reviews; algorithmic price discrimination; deceptive design interfaces ("dark patterns") that influence purchasing decisions; delayed or non-existent grievance redressal; counterfeit goods sold based on unreliable third-party sellers; and cross-border transactions that put foreign sellers outside the practical reach of Indian consumer forums.

The Consumer Protection Act, 1986 was mute on electronic commerce, digital advertising, and platform-based intermediation during a time when the paradigm of consumer transactions was predominantly physical.[4] The 1986 Act was progressively expanded by judicial interpretation to allow for online transactions, ruling that an individual making an online purchase qualified as a "consumer",[5] but the absence of a statutory basis for regulating intermediaries left significant regulatory gaps. The Consumer Protection Act, 2019 was enacted to remedy this deficiency. The Act, which was published in the official gazette on August 9, 2019, went into effect in two stages: the majority of its provisions went into effect on July 20, 2020, and the remaining provisions, including those pertaining to the Central Consumer Protection Authority, went into effect on July 24, 2020.[6] The Consumer Protection (E-Commerce) Rules, 2020 were notified shortly thereafter, on 23 July 2020, under the rule-making power of the Central Government.[7]

[3]Ministry of Commerce and Industry, Government of India, "National Policy Framework Note" (2019); see also Department for Promotion of Industry and Internal Trade, Draft National E-Commerce Policy (2019).
[4]The Consumer Protection Act, 1986 (Act 68 of 1986). The 1986 Act did not define "e-commerce", "electronic service provider" or "unfair trade practice" in terms adequate to online transactions.
[5]See Rakesh Kumar Gupta v. Airport Retail Pvt. Ltd., Consumer Complaint No. 447 of 2012 (NCDRC), where online purchases were held amenable to the jurisdiction of consumer fora.
[6]Ministry of Consumer Affairs, Food and Public Distribution, Notification No. S.O. 2351(E), dated 15 July 2020; Notification No. S.O. 2421(E), dated 23 July 2020.
[7]The Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 462(E), notified under s. 101(1) of the Consumer Protection Act, 2019.

This study critically investigates whether the CPA 2019 and the subordinate legislation issued thereunder provide a sufficient and enforceable framework for the protection of consumers transacting in the e-commerce arena. The development of Indian consumer law is examined in Part II. The Act's substantive provisions and the E-Commerce Rules as they relate to online transactions are examined in Part III. The CCPA's regulatory changes, especially the Guidelines for Prevention and Regulation of Dark Patterns, 2023, are examined in Part IV. Enforcement practices are surveyed in Part V. Before the paper's conclusion in Part VIII, Part VI conducts a critical analysis of the framework's remaining deficiencies and Part VII makes recommendations.

II. Evolution of Consumer Protection Law in India: From 1986 to 2019

The 1986 Act, which was based on the caveat emptor theory tempered by statutory consumer rights, was a product of its era and was organized around a three-tier adjudicatory hierarchy of District, State, and National Commissions.[8] Although it worked well for its time, it was hampered by procedural delays, financial jurisdiction that did not keep up with inflation, and—most importantly for the present—the incapacity to control multi-party digital transactions where the seller, the platform, and the payment intermediary might be separate legal entities situated in different jurisdictions.[9]

Following the dissolution of the Sixteenth Lok Sabha, the Consumer Protection Bill, 2018 expired. On July 8, 2019, a new bill was proposed in Lok Sabha and approved by Rajya Sabha on 6 August, and it soon received presidential assent on 9 August 2019.[10]. The Bill's Statement of Objects and Reasons clearly acknowledged that "the modes of running businesses and doing trade and commerce have undergone tremendous changes" and that modern problems like teleshopping and e-commerce needed to be addressed.[11] A concept of "unfair contracts" was introduced, the definition of "unfair trade practice" was expanded to include data-related privacy breaches, a dedicated executive regulator (the CCPA) independent of the adjudicatory commissions was established, a chapter on product liability was introduced for the first time in Indian legislative

[8]J.N. Barowalia, Commentary on the Consumer Protection Act 3 (Universal Law Publishing, 5th edn., 2018).
[9]Avtar Singh, Law of Consumer Protection: Principles and Practice 42 (Eastern Book Company, 6th edn., 2019).
[10]Lok Sabha Secretariat, Statement of Objects and Reasons, The Consumer Protection Bill, 2019, Bill No. 89-C of 2019.
[11]Id.

history, and—most importantly for the current inquiry—it specifically included "electronic service providers" and e-commerce transactions within its definitional net.[12]

III. E-Commerce Under the CPA 2019: Statutory and Regulatory Framework

A. Definitional Architecture

Section 2(16) of the Act defines "e-commerce" broadly as "buying or selling of goods or services including digital products over digital or electronic network".[13] This definition is purposefully broad, including subscription services, marketplace models, inventory-based models and the selling of only digital goods such as software or e-books. According to Section 2(17),"any online marketplace or online auction site" is specifically included in the definition of "electronic service provider" as someone who offers technologies or procedures that allow a product seller to advertise or sell goods or services to a consumer,[14] Thus, even if they don't sell any goods directly, platforms like Amazon, Flipkart, and other like middlemen are drawn inside the regulatory boundaries. The definitions of "e-tailer" and "seller" in Section 2(20) and Section 2(41) are sufficiently broad to encompass both platforms and third-party merchants using them.[15]

Equally important is the broadened definition of "unfair trade practice" under Section 2(47), which, in contrast to its predecessor under the Monopolies and Restrictive Trade Practices Act, 1969, now expressly includes the practice of a trader or service provider disclosing personal information provided in confidence by a customer unless such disclosure is made in accordance with law and the practice of failing to issue a bill or receipt.[16] This clause has particular relevance to e-commerce, where large volumes of personal and behavioural data are collected and monetised, often without meaningful consumer consent.

B. The Consumer Protection (E-Commerce) Rules, 2020

The E-Commerce Rules cover all items and services purchased or sold via digital or electronic networks, including digital goods, all e-commerce models, and—most importantly—e-commerce

[12]The Consumer Protection Act, 2019 (Act 35 of 2019), ss. 2(46), 2(47), Chapter VI, ss. 10-27.
[13]The Consumer Protection Act, 2019, s. 2(16).
[14]Id., s. 2(17).
[15]Id., ss. 2(20), 2(41).
[16]Id., s. 2(47)(vii); Sudhanshu Ranjan, Consumer Protection Law in India 118 (LexisNexis, 2021).

businesses that are not based in India but provide goods or services to Indian customers.[17] In order to assure compliance, Rule 4 mandates that all e-commerce entities be either international companies with a place of business in India or companies incorporated under Indian company law. They must also designate a resident nodal person of contact or another senior designated functionary.[18] Notably, the Rules were allegedly issued in the exercise of authority granted by "sub-clause (zg) of sub-section (1) of section 101" of the Act—a subclause that, according to a plain reading of the Act, does not exist, with section 101(2) (zg) being the relevant provision. Despite being primarily academic, this drafting error shows how quickly the subordinate law was drafted.[19]

In essence, the Rules impose general obligations on all e-commerce entities, including: displaying accurate and sufficient information about goods and services, including country of origin, to enable consumers to make informed purchasing decisions; ensuring that advertisements for goods or services conform to the actual characteristics; establishing an adequate grievance redressal mechanism with a grievance officer to acknowledge complaints within 48 hours and resolve them within a month; refraining from engaging in unfair trade practices; and refusing to manipulate prices of goods or services in order to make unreasonable profit.[20] Marketplace e-commerce entities are subject to specific obligations under Rule 5, including obtaining an undertaking from sellers regarding the accuracy of product descriptions, not using consumer information for the unfair advantage of its related parties, keeping a record of information provided by sellers, and applying terms of service equally to sellers in similar situations.[21] Accordingly, Rule 6 requires vendors in these marketplaces to give correct information, have a working grievance redressal system, and not refuse to accept returns or refunds in cases when the delivered goods are faulty, inadequate, fraudulent, or not as advertised.[22] The Rules' ban against e-commerce companies automatically recording customer agreement for a transaction, including thru pre-ticked

[17]The Consumer Protection (E-Commerce) Rules, 2020, r. 2.
[18]Id., r. 3(1)-(2).
[19]See India's New Consumer Protection (E-Commerce) Rules, 2020: Novelty and Nuances, Lexology (2 Oct. 2020); the error has not, to date, been formally corrected by amendment.
[20]The Consumer Protection (E-Commerce) Rules, 2020, r. 4.
[21]Id., r. 5.
[22]Id., r. 6.

checkboxes, is a recurring and genuinely innovative feature. This is an early legislative anticipation of what would later be properly described as a "dark pattern".[23]

C. The Central Consumer Protection Authority

The establishment of the Central Consumer Protection Authority ("CCPA") under Section 10, which went into effect on July 24, 2020, to regulate matters pertaining to violations of consumer rights, unfair trade practices, and false or misleading advertisements detrimental to the interests of the public and consumers as a class, is perhaps the most structurally significant innovation of the CPA 2019.[24] The CCPA has inquisitorial and injunctive powers, in contrast to the adjudicatory consumer commissions, which deal with individual complaints. It can start a class inquiry suo motu, order the recall of goods, order reimbursement of the price paid, order the cessation of unfair trade practices, and impose penalties for misleading advertisements that can include up to two years in prison and a fine of up to ten lakh rupees for a first infraction, up to five years in prison and a fine of up to fifty lakh rupees for subsequent infractions. [25]Because of this, the CCPA has a regulatory nature more akin to a sectoral regulator like the Securities and Exchange Board of India than to a traditional adjudicatory tribunal. In actuality, this body has taken on the role of primary enforcer against e-commerce malpractice thru advisories, guidelines, and penalty orders, which are covered in Part V below.

D. Product Liability under Chapter VI

For the first time in Indian statute law, a comprehensive product liability regime is introduced in Chapter VI (Sections 82 to 87). According to Section 2(34), "product liability" refers to a manufacturer's or seller's obligation to make up for any harm that a defective product or a lack of related services causes to a customer.[26] Importantly, Section 2(37) defines "product seller" broadly enough to include e-commerce platforms even in cases where the platform does not manufacture the goods itself, as long as it is involved in placing the product for commercial

[23]Id., r. 5(3); see also Novelty and Nuances, supra note 12.
[24]The Consumer Protection Act, 2019, s. 10; Ministry of Consumer Affairs, Notification No. S.O. 2421(E), 23 July 2020.
[25]The Consumer Protection Act, 2019, ss. 18, 20, 21, 88, 89.
[26]The Consumer Protection Act, 2019, s. 2(34).

purposes.[27]Additionally, Section 86 states that an e-commerce platform, as a "electronic service provider," is shielded from product liability lawsuits in cases where it only gives users access to information rather than acting as the seller, as long as it takes reasonable precautions to verify the information, does not have actual knowledge or reasonable cause to believe the product is defective, and has not made any explicit warranties regarding its performance.[28] This clause is crucial to the discussion of platform liability covered in Part VI and is model after the intermediate safe-harbour of Section 79 of the Information Technology Act, 2000.[29]

IV. Regulatory Innovations: The CCPA's Guidelines Regime

In the years since the Act's implementation, the CCPA has addressed types of consumer injury that neither the Act nor the E-Commerce Rules specifically addressed by using its authority to create guidelines under Section18. The Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 addressed bait advertisements, established due-diligence requirements for endorsers, including social media influencers, and specified requirements for advertisements to be considered non-misleading.[30] The Guidelines for Prevention and Regulation of Dark Patterns, 2023, which were announced on November 30, 2023, have greater implications for e-commerce. They define "dark patterns" as any practice or deceptive design pattern using user interface or user experience interactions on any platform intended to mislead or trick users into doing something they did not originally intend to do by subverting or impairing consumer autonomy or choice.[31] The Guidelines identify thirteen specific practices, including "false urgency" (fabricated countdown timers or stock warnings), "basket sneaking" (adding items to a cart without consent), "confirm-shaming" (using guilt-inducing language to dissuade a user from declining an offer), "forced action", "subscription trap" and "drip pricing" (revealing additional charges only at the final stage of checkout).[32] For the purposes of the parent

[27]Id., s. 2(37); see also Product Liability Under Consumer Protection Act, 2019, Live Law (23 Dec. 2019).
[28]The Consumer Protection Act, 2019, s. 84.
[29]Information Technology Act, 2000, s. 79; see also At a Glance: The Sources of Product Liability Law in India, Lexology (2023).
[30]Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022, issued by the CCPA under s. 18, Consumer Protection Act, 2019.
[31]Guidelines for Prevention and Regulation of Dark Patterns, 2023, cl. 3, issued under s. 18, Consumer Protection Act, 2019.
[32]Id., Annexure I.

Act, any platform, supplier, or advertiser that exhibits a dark pattern is considered to be participating in unfair trade practices or creating deceptive advertisements.[33]

The CCPA has penalized Physics Wallah Limited (₹5 lakh, for false urgency and pre-selected donation options directed at a student user base that includes minors) and McAfee Software India Private Limited (₹1 lakh, for a subscription-renewal interface that framed non-renewal as a risk rather than a neutral choice). The enforcement of the Dark Patterns Guidelines has been evident, albeit on a small scale.[34] In accordance with Section 18(1) of the Act, the CCPA published an advice on June 5, 2025, directing all e-commerce platforms to perform a self-audit within three months in order to find and fix dark patterns on their platforms.[35] Although the guidelines represent a significant conceptual advancement, they have a major structural flaw in that they do not provide an independent penalty of their own. As a result, a violation must still be reported thru the underlying provisions on unfair trade practices or misleading advertisements, along with the associated procedural and evidentiary burdens.[36]

V. Enforcement in Practice

District and State Consumer Disputes Redressal Commissions have, since the Act's commencement have started to hold marketplace platforms partially responsible for third-party listings by applying the due-diligence standard under Rule 5(4) of the E-Commerce Rules. In one example ruling, the Commission found that the marketplace was partially liable for not exercising the due diligence required by the Rules, and as a result, a consumer who received a non-functional and counterfeit goods represented as new and tested was awarded compensation of ₹50,000 .[37] Additionally, District Commissions have started to provide compensation for e-commerce platform data security breaches, viewing a failure to protect credit card information as a service

[33] Id., cl. 4.
[34] PIB, Ministry of Consumer Affairs, "CCPA Acts Against Dark Patterns on Digital Platforms" (2026); the authority also examined First Cry, Pharm Easy, Zepto and others for drip pricing and basket sneaking, with cumulative penalties reported at approximately ₹20 lakh.
[35] CCPA Advisory dated 5 June 2025, issued under s. 18(1), Consumer Protection Act, 2019; see Dark Patterns and Weak Remedies: Why the CCPA Advisory Falls Short, Internet Freedom Foundation (2025).
[36] Guidelines for Prevention and Regulation of Dark Patterns, 2023 — Lexology (4 Dec. 2023).
[37] See discussion in E-Commerce and Consumer Rights under the Consumer Protection Act, 2019, Legal Service India (2025) (summarising representative State Commission practice on marketplace due diligence).

fault subject to liability under the Act. Even tho each of these rulings is small in scope, they are important from a jurisprudential standpoint because they demonstrate that the E-Commerce Rules' "due diligence" and grievance-redressal requirements are being incorporated into consumer commissions' adjudicatory standards rather than being merely hortatory.

Although it is still in its early stages of development, the CCPA's enforcement record shows that it is a regulator prepared to take action against large and well-resourced platforms. This is a significant change from the 1986 Act's individual-complaint model, which seldom gave systemic practices that affected a large number of consumers the attention they deserved. Additionally, the CCPA has issued advisories directing e-commerce platforms to delist products that pose a risk to consumer safety, such as seatbelt-alarm-stopper clips and unapproved wireless jammers.[38]

VI. Critical Analysis: Gaps and Challenges

A. Jurisdiction over Offshore Entities and Cross-Border Enforcement

The E-Commerce Rules claims to apply to foreign e-commerce companies that sell goods or services to Indian consumers, and mandates that these companies designate a resident nodal officer,[39] but there are still insufficient practical means of enforcing compliance from a company that has no assets or establishment in India. It is challenging to carry out CCPA or consumer commission orders against a foreign seller who does not have an Indian presence, and India's mutual legal aid agreements are not designed to handle the volume and value of individual consumer disputes that usually result from cross-border e-commerce. The Act does not provide a private international law framework that addresses the choice of venue or choice of law for such transactions; instead, normal civil procedural concepts are used to fill this gap in an unsatisfactory manner.[40]

[38]PIB, Ministry of Consumer Affairs, Press Release (2023).
[39]The Consumer Protection (E-Commerce) Rules, 2020, r.2(1)(V), r. 4(1)(b).
[40]Compare the position under the European Union's Regulation (EU) No 1215/2012 (Brussels I Recast), which specifically addresses jurisdiction in consumer contracts, including where the trader directs commercial activity to the consumer's member state.

B. The Intermediary Liability Interface with the Information Technology Act, 2000

Similar to the safe-harbour afforded to "intermediaries" under Section 79 of the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Section 86 of the CPA 2019 provides e-commerce platforms with a conditional exemption from product liability when they serve as passive conduits. However the coexistence of these two overlapping safe-harbour regimes—one under the CPA 2019 based on due diligence in a consumer-facing marketplace and one under the IT Act based on the platform's role as a neutral technological intermediary—creates interpretive uncertainty as to which standard applies in a particular fact situation. This is especially true when a marketplace exercises algorithmic curation, ranking, or promotional control over listings that may go beyond passive intermediation.[41] The absence of harmonising guidance, whether legislative or judicial, leaves platforms able to plausibly invoke whichever regime offers the more favourable standard of care, undermining the deterrent purpose of Chapter VI.

C. Weak and Non-Specific Penalties for Design-Based Manipulation

As noted in Part IV, the Dark Patterns Guidelines, 2023 create no independent cause of action or penalty; a complainant or the CCPA must still establish that the impugned design amounts to a "unfair trade practice" or "misleading advertisement" under the parent Act. This indirection dilutes deterrence: penalties actually imposed to date have been modest relative to the scale of the platforms involved and the revenue plausibly generated by the impugned practices, a mismatch that critics have characterised as rendering enforcement more symbolic than substantive.[42]The CCPA acts primarily in a reactive, complaint- or media-report-driven capacity, further shifting the burden of compliance monitoring onto the regulated entities themselves through the use of advisory self-audits rather than required pre-clearance or a permanent technical audit mechanism.

D. Data Protection and Privacy: An Incomplete Interface

While Section 2(47)(vii) of the Act treats unauthorised disclosure of a consumer's confidential personal information as an unfair trade practice, the Act was not designed as, and does not function

---

[41]Information Technology Act, 2000, s. 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

[42]Dark Patterns and Weak Remedies: Why the CCPA Advisory Falls Short, Internet Freedom Foundation (2025).

as, a comprehensive data protection statute. Its enactment preceded the Digital Personal Data Protection Act, 2023, and the two statutes now operate in parallel without express provision for their interaction — for instance, as to whether a data breach on an e-commerce platform is more appropriately proceeded against under the data protection statute's dedicated enforcement mechanism or as an unfair trade practice before a consumer forum, or both.[43] This absence of regulatory coordination is a significant gap in consumer protection, especially for vulnerable populations like minors, given the importance of data collecting, profiling, and targeted advertising to the e-commerce business model.

E. Institutional Capacity of Consumer Commissions

The effectiveness of any substantive right established by the CPA 2019 depends on the District, State, and National Commissions' institutional ability to decide claims in a timely manner. Despite the Act's ambitious substantive reforms, the practical experience of an individual e-commerce consumer seeking redress for a defective product or a denied refund frequently remains one of significant delay due to persistent vacancies in the appointment of Presidents and Members of these Commissions, inadequate staffing, and the accumulation of cases carried over from the 1986 Act.[44] Although the Act's provision of e-filing and mediation as an alternative dispute resolution method under Chapter V is a positive procedural innovation, the adjudicatory tier's capacity bottlenecks continue to limit its impact.[45]

F. A Note in Comparative Perspective

When compared to analogous regimes in developed digital markets, India's framework is nonetheless less extensive, although being progressive in comparison to its predecessor. The Digital Services Act of the European Union imposes graded due-diligence standards that are scaled to platform size. These obligations include a specified regime for "very large online platforms" and specific transparency requirements for online marketplaces, along with the potential for

[43]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023); see also Guidelines for Prevention and Regulation of Dark Patterns, 2023, Tri legal Update (Dec. 2023) (noting the overlapping compliance burden).

[44]See generally Department-Related Parliamentary Standing Committee on Food, Consumer Affairs and Public Distribution, Report on the Functioning of Consumer Fora (Lok Sabha Secretariat, various years), noting chronic vacancies across State Commissions.

[45]The Consumer Protection Act, 2019, ss. 74-81 (mediation); s. 17 read with the Consumer Protection (Consumer Disputes Redressal Commissions) Rules, 2020 (e-filing).

turnover-linked fines.[46] The Federal Trade Commission's broad authority under Section 5 of the Federal Trade Commission Act to take action against "unfair or deceptive acts or practices" is supplemented by state-level unfair-and-deceptive-practices statutes. In recent years, the Federal Trade Commission has specifically used this authority against dark-pattern practices in online subscription cancelation flows, despite the lack of an omnibus consumer protection code similar to the CPA 2019. There is a gap between the goal of the Dark Patterns Guidelines and their actual deterrent effect because India's CCPA-led model currently operates mainly through advisories and case-by-case guideline enforcement rather than either a scaled statutory due-diligence regime or turnover-linked penalties.[47]

VII. Suggestions for Reform

First, rather than requiring recourse to the general unfair trade practice provisions, the CPA 2019 or the E-Commerce Rules should be amended to prescribe a specific, quantified penalty regime for violations of the Dark Patterns Guidelines. Additionally, turnover-linked penalties for recurrent or widespread violations by major platforms should be taken into consideration.

Second, Parliament should make clear how the safe-harbour under Section 84 of the CPA 2019 and Section 79 of the Information Technology Act, 2000 relate to each other. Ideally, this would mean that a platform that uses algorithmic curation, promotion, or ranking of listings cannot claim passive-intermediary status for the purposes of either statute.

Third, there must be explicit statutory coordination between the Act and the Digital Personal Data Protection Act, 2023, especially with regard to the handling of data.

Fourth, required escrow or bond requirements for foreign businesses without an Indian establishment, as well as bilateral or multilateral cooperation agreements with significant source jurisdictions for cross-border e-commerce, should boost cross-border enforcement power.

[46]Regulation (EU) 2022/2065 (Digital Services Act), arts. 30-32; see also E-Commerce and Consumer Protection: Legal Framework under the Consumer Protection Act, 2019, Law Curb (2025) (comparative note).
[47]Federal Trade Commission Act, 15 U.S.C. § 45; Federal Trade Commission, Bringing Dark Patterns to Light: An FTC Staff Report (2022).

Lastly, and perhaps most importantly, for any of the Act's substantive changes to result in a significantly better consumer experience, there must be ongoing budgetary and administrative investment in the District and State Commissions.

VIII. Conclusion

The expanded definitions of "e-commerce" and "electronic service provider," the establishment of the CCPA, the introduction of statutory product liability, and the due-diligence and grievance-redressal obligations of the E-Commerce Rules all demonstrate a thoughtful legislative response to the realities of digital commerce. The Consumer Protection Act, 2019 is a true and essential modernization of Indian consumer law. The Guidelines for Prevention and Regulation of Dark Patterns, 2023 that followed the CCPA further show an institutional ability to address new harms that the original legislation was unable to foresee in 2019.

However, a critical analysis shows that the framework's efficacy is limited by structural flaws, including an inadequate jurisdictional framework for offshore sellers, unresolved conflict between overlapping intermediary safe-harbours, indirect and relatively light penalties for design-based manipulation, an unfinished interface with data protection law, and ongoing capacity issues within the adjudicatory commissions that ultimately support the entire structure. In the end, the success of the Act in the e-commerce space will be determined more by the coherence, consistency, and resources of its implementation than by the aspirations of its wording.