INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ROLE OF CENTRAL CONSUMER PROTECTION AUTHORITY IN PROTECTING E-COMMERCE CONSUMERS UNDER THE CONSUMER PROTECTION ACT, 2019

AUTHORED BY - BALJINDER KAUR

Student, Master of Law, University Institute of Law, Sant Baba Bhag Singh University

CO-AUTHOR - POOJA BALI

Dean, University Institute of Law, Sant Baba Bhag Singh University

ABSTRACT

The digital economy has witnessed exponential growth in India, with e-commerce platforms becoming integral to consumer transactions. However, this rapid expansion has also given rise to unprecedented challenges in consumer protection, including unfair trade practices, false advertising, and deceptive design patterns. The Consumer Protection Act, 2019, marks a paradigm shift in India's consumer protection framework by establishing the Central Consumer Protection Authority (CCPA) as a specialized regulator dedicated to safeguarding consumer rights in the digital marketplace. This article examines the multifaceted role of the CCPA in protecting e-commerce consumers, analyzing its constitutional authority, powers, functions, and recent enforcement actions. Through a comprehensive review of the regulatory framework, this paper demonstrates how the CCPA has evolved as a crucial institutional mechanism for ensuring fair, transparent, and ethical e-commerce practices in India.[1]

1. INTRODUCTION

1.1 Background and Context

The Consumer Protection Act, 2019, represents a comprehensive overhaul of consumer protection legislation in India, replacing the outdated Consumer Protection Act, 1986. This new legislation reflects India's commitment to modernizing its legal framework in alignment with contemporary market dynamics, particularly the explosive growth of e-commerce. The Act explicitly recognizes e-commerce as a distinct commercial activity and defines it as "the buying or selling of goods or services including digital products over digital or electronic network"[2].

[1]The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
[2]Press Information Bureau, *Consumer Protection (E-Commerce) Rules, 2020*, Ministry of Consumer Affs., Food

ISSN: 2582-6433

The proliferation of e-commerce platforms has created a complex ecosystem involving multiple stakeholders: e-commerce entities, marketplace operators, sellers, service providers, advertisers, and consumers. This multifaceted structure necessitates a robust regulatory authority capable of monitoring compliance, investigating violations, and enforcing consumer rights across diverse digital platforms.

1.2 Significance of the CCPA

Prior to 2020, India lacked a centralized authority specifically empowered to regulate consumer protection matters at the national level. Consumer grievances were primarily addressed through the multi-tiered redressal mechanism comprising District Consumer Disputes Redressal Commissions, State Commissions, and the National Commission. While these institutions played a vital role, they operated reactively, addressing individual complaints rather than proactively preventing systemic violations and unfair practices.[3]

The establishment of the Central Consumer Protection Authority, which came into force on July 24, 2020, filled this critical gap. The CCPA represents a proactive regulatory approach, empowering the government to intervene in matters affecting consumer rights as a class and the public at large, rather than addressing isolated disputes.

1.3 Scope and Objectives

This article examines the CCPA's role in protecting e-commerce consumers through five primary lenses: (1) Constitutional authority and regulatory framework; (2) Powers and functions; (3) E-commerce-specific regulatory interventions; (4) Enforcement mechanisms and recent actions; and (5) Challenges and future directions. The analysis incorporates recent advisory notices, guidelines, and enforcement actions issued by the CCPA through 2025.

2. CONSTITUTIONAL AUTHORITY AND REGULATORY FRAMEWORK

2.1 Establishment and Authority

The Central Consumer Protection Authority is established under Section 60 of the Consumer Protection Act, 2019[4]. The CCPA is vested with authority to regulate matters relating to

& Pub. Distrib. (July 23, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945167.
[3]*Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).
[4]The Consumer Protection Act, 2019, S 60–65, No. 35, Acts of Parliament, 2019 (India).

ISSN: 2582-6433

violation of consumer rights, unfair trade practices, and misleading or false advertisements that are prejudicial to consumers as a class and the public at large.

Unlike the National Commission and District Consumer Commissions, which primarily adjudicate individual consumer disputes, the CCPA operates as a regulatory authority with quasi-legislative and quasi-executive functions.[5] This distinction is crucial: the CCPA can take suo motu action, issue advisories, impose penalties, and direct discontinuation of unfair practices without requiring individual complaints to initiate enforcement proceedings.

2.2 Governance Structure

The CCPA is headed by a Central Government-appointed Chief Commissioner and comprises Central Information Commissioners. The Authority operates under the administrative oversight of the Ministry of Consumer Affairs, Food and Public Distribution.[6] This organizational structure ensures both independence and accountability in regulatory decision-making.

2.3 Scope of CCPA Authority in E-Commerce

Section 2(t) of the Consumer Protection Act, 2019, defines "e-commerce" comprehensively to include all forms of buying and selling of goods and services, including digital products, over electronic networks.[7] This expansive definition ensures that the CCPA's authority extends to:

- **Marketplace e-commerce entities** (platforms like Amazon, Flipkart, Myntra)
- **Inventory-based e-commerce entities** (companies that own and sell inventory directly)
- **Online service providers** (food delivery, logistics, financial services)
- **Digital product sellers** (software, e-books, online courses)
- **Advertisers and promoters** engaging in digital advertising
- **Online aggregators** (ride-sharing, accommodation sharing platforms)

This broad jurisdictional scope reflects the legislature's recognition that consumer protection must adapt to the realities of digital commerce.

[5]Sankar Ghosh, *Evolution of E-commerce and Consumer Protection Act 2019 Legal Framework*, LinkedIn (May 17, 2024), https://www.linkedin.com/pulse/evolution-e-commerce-consumer-protection-india-analyzing-sankar-ghosh-nx09c(last visited Jan. 26, 2026).

[6]*Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).

[7]Press Information Bureau, *Consumer Protection (E-Commerce) Rules, 2020*, Ministry of Consumer Affs., Food & Pub. Distrib. (July 23, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945167. (last visited Jan. 26, 2026).

ISSN: 2582-6433

3. POWERS AND FUNCTIONS OF THE CCPA

3.1 Investigative Powers

The CCPA possesses extensive investigative authority under Section 61 of the Act. It can[8]:

- Call for information and documents from any e-commerce entity, seller, or service provider
- Conduct inspections and raids on business premises
- Summon and examine witnesses
- Direct recall of unsafe or defective goods
- Order cessation of unfair trade practices
- Seek expert opinions on technical and scientific matters.

These investigative powers enable the CCPA to proactively identify violations rather than rely solely on consumer complaints. For instance, the CCPA's investigation into dark patterns across multiple e-commerce platforms revealed systematic violations that might have otherwise gone undetected through individual grievances.

3.2 Regulatory Authority

The CCPA can issue rules, guidelines, and regulations governing e-commerce transactions. Notably, the Consumer Protection (E-commerce) Rules, 2020, were notified specifically to address the unique challenges posed by digital commerce.[9] These rules establish comprehensive obligations for e-commerce entities, including:

- Seller information disclosure requirements
- Grievance redressal mechanisms
- Return and refund policies
- Quality and authenticity standards
- Transparency in pricing and terms

3.3 Enforcement and Penalty Powers

The CCPA can impose significant penalties on entities violating consumer protection provisions. Section 62 of the Act empowers the CCPA to[10]:

[8]The Consumer Protection Act, 2019, S 60–65, No. 35, Acts of Parliament, 2019 (India).
[9]Press Information Bureau, *Consumer Protection (E-Commerce) Rules, 2020*, Ministry of Consumer Affs., Food & Pub. Distrib. (July 23, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945167. (last visited Jan. 26, 2026).
[10]The Consumer Protection Act, 2019, S 60–65, No. 35, Acts of Parliament, 2019 (India).

ISSN: 2582-6433

- Direct removal or correction of misleading advertisements
- Impose penalties of up to ₹10 lakhs for first violation and ₹50 lakhs for subsequent violations
- Direct payment of compensation to affected consumers
- Recommend prosecution under criminal provisions
- Suspend operations of non-compliant sellers on e-commerce platforms.

The graduated penalty structure reflects the principle of proportionality while ensuring sufficient deterrence against violations.

3.4 Advisory and Guidance Functions

Beyond enforcement, the CCPA issues advisory notices and guidelines providing authoritative guidance on consumer protection requirements. Recent advisories on dark patterns, subscription traps, and false urgency notifications have become industry standards, shaping compliance across the e-commerce sector.[11]

4. CONSUMER PROTECTION (E-COMMERCE) RULES, 2020

4.1 Framework and Objectives

The Consumer Protection (E-commerce) Rules, 2020, represent a specialized regulatory framework addressing the unique vulnerabilities of online consumers.[12] These rules establish a comprehensive set of obligations for e-commerce entities, reflecting the principle that digital commerce must provide protections equivalent to, or exceeding, those available in traditional retail.

4.2 Obligations of E-Commerce Entities

4.2.1 Seller Information and Verification

E-commerce platforms must collect, verify, and display accurate information about sellers, including:

- Legal business name and address
- Contact details
- Country of origin

[11] *Regulatory Crackdown on Dark Patterns: CCPA's Enforcement Actions and Emerging Compliance Landscape in Indian E-Commerce*, AZB & Partners (Oct. 5, 2025), https://www.azbpartners.com/bank/regulatory-crackdown-on-dark-patterns-ccpas-enforcement-actions-and-emerging-compliance-landsca

[12] Press Information Bureau, *Consumer Protection (E-Commerce) Rules, 2020*, Ministry of Consumer Affs., Food & Pub. Distrib. (July 23, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945167.

ISSN: 2582-6433

- Return and refund policy specifics

This transparency requirement addresses the significant information asymmetry between e-commerce platforms and consumers, enabling informed purchasing decisions.

4.2.2 Grievance Redressal Mechanism

E-commerce entities must establish effective grievance redressal systems with:

- Single-point contact for consumer grievances
- Acknowledgment within 24 hours
- Resolution within 30 days of complaint receipt
- Escalation procedures to the Chief Commissioner or dedicated nodal officer.

These mechanisms ensure that consumers have recourse within the e-commerce ecosystem before escalating disputes to formal redressal commissions.

4.2.3 Explicit Consent and Anti-Dark Pattern Requirements

A particularly important provision requires that e-commerce entities shall "record the consent of a consumer for the purchase of any good or service offered on its platform where such consent is expressed through an explicit and affirmative action, and no such entity shall record such consent automatically, including in the form of pre-ticked checkboxes.[13]

This requirement directly addresses manipulative design practices that exploit cognitive biases and default settings to extract consumer consent without genuine volition.

4.2.4 Quality and Authenticity Standards

Rules impose liability on e-commerce platforms for ensuring that goods sold through their platforms meet quality and authenticity standards. This addresses the widespread problem of counterfeit products on online marketplaces.[14]

4.3 Liability Framework

The rules establish differentiated liability regimes:

Marketplace E-Commerce Entities: Platforms acting as intermediaries bear secondary

[13]*Regulatory Crackdown on Dark Patterns: CCPA's Enforcement Actions and Emerging Compliance Landscape in Indian E-Commerce*, AZB & Partners (Oct. 5, 2025), https://www.azbpartners.com/bank/regulatory-crackdown-on-dark-patterns-ccpas-enforcement-actions-and-emerging-compliance-landsca(last visited Jan. 26, 2026).

[14]Press Information Bureau, *Consumer Protection (E-Commerce) Rules, 2020*, Ministry of Consumer Affs., Food & Pub. Distrib. (July 23, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945167.

ISSN: 2582-6433

liability for sellers' failures to deliver goods or services, ensuring consumers have recourse against the platform rather than being left to pursue individual sellers.

Inventory-Based E-Commerce Entities: Companies that directly own and control inventory bear full liability as both seller and platform operator.

This liability structure incentivizes platforms to rigorously monitor seller compliance and maintain quality standards.

5. PROTECTION AGAINST UNFAIR TRADE PRACTICES IN E-COMMERCE

5.1 Definition and Scope

Section 2(47) of the Consumer Protection Act, 2019, defines unfair trade practices broadly to encompass any practice that causes injury to consumers through deception or manipulation[15].

The CCPA has interpreted this definition to cover numerous practices prevalent in e-commerce, including[16]:

- Misleading claims about product features or benefits
- False information about availability or scarcity
- Deceptive pricing practices
- Manipulation of search results and recommendations
- Subscription traps and hidden charges
- Dark patterns and deceptive user interface design

5.2 Dark Patterns: A Critical Emerging Issue

Dark patterns represent one of the CCPA's most significant recent regulatory focuses. These are deceptive design practices that manipulate user interfaces to nudge consumers toward unintended actions.

Common Dark Patterns Identified:

- **False Urgency**: Creating artificial scarcity through language like "Only 2 items left" or countdown timers, even when inventory is abundant.

[15]The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).

[16]*Regulatory Crackdown on Dark Patterns: CCPA's Enforcement Actions and Emerging Compliance Landscape in Indian E-Commerce*, AZB & Partners (Oct. 5, 2025), https://www.azbpartners.com/bank/regulatory-crackdown-on-dark-patterns-ccpas-enforcement-actions-and-emerging-compliance-landsca

ISSN: 2582-6433

- **Drip Pricing**: Revealing additional charges only at the final checkout stage, making it difficult for consumers to abandon purchases.
- **Subscription Traps**: Automatically charging consumers for subscriptions after free trials, often with difficult-to-find cancellation options.
- **Nagging**: Persistent notifications or pop-ups encouraging specific actions.
- **Pre-Ticked Checkboxes**: Automatically enrolling consumers in add-on services unless explicitly deselected.

5.3 CCPA's Regulatory Response

On June 5, 2025, the CCPA issued a landmark advisory mandating all e-commerce platforms to conduct self-audits within three months to identify and eliminate dark patterns. This advisory followed high-level stakeholder consultations and signaled the CCPA's determination to eliminate deceptive design from the digital ecosystem.

The advisory emphasized four core principles:

1. **Transparency**: Clear disclosure of terms, conditions, and charges.
2. **Explicit Consent**: Affirmative, unambiguous user action before transaction completion.
3. **Non-Manipulative Design**: User interfaces designed to serve consumer interests, not platform interests.
4. **Easy Exit**: Simple mechanisms to cancel subscriptions, modify preferences, or withdraw consent.

5.4 Enforcement Against Dark Patterns

The CCPA has demonstrated its enforcement resolve by issuing show-cause notices to eleven companies, including quick commerce platforms and online transport aggregation services. These notices required companies to explain dark pattern deployments and propose remedial measures. Non-compliance risks significant penalties, suspension of operations, and reputational damage.

Notable enforcement cases have included actions against IndiGo and BookMyShow, establishing precedent that even major corporations cannot ignore dark pattern prohibitions.

ISSN: 2582-6433

6. PRODUCT LIABILITY AND CONSUMER SAFETY

6.1 Introduction of Product Liability

The Consumer Protection Act, 2019, introduces a comprehensive product liability regime, representing a significant expansion of consumer protections[17]. This provision holds manufacturers, sellers, service providers, and e-commerce platforms accountable for harm caused by defective products or deficient services.

6.2 Liability Chain in E-Commerce

In the e-commerce context, the product liability framework creates a clear chain of responsibility:

For Marketplace Platforms: Liability extends to monitoring seller compliance, withdrawing non-compliant sellers, and ensuring adequate safety standards across their ecosystems.

For Direct Sellers and Manufacturers: Full liability attaches for any defects in products or services provided through e-commerce channels.

For Service Providers: Liability encompasses both direct services (like food delivery) and facilitated services (like transportation through aggregator platforms)

This layered approach ensures no gap in liability while recognizing different roles within the e-commerce ecosystem.

6.3 CCPA's Role in Product Safety

The CCPA monitors product safety issues across e-commerce platforms, particularly regarding[18]:

- Counterfeit goods
- Substandard products
- Unsafe or defective items causing injury
- Pharmaceutical and food products of questionable provenance
- Electronic goods lacking necessary safety certifications

The Authority can direct recalls, suspension of sellers, and investigation of systematic quality failures.

[17]The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
[18]*Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).

ISSN: 2582-6433

7. FALSE AND MISLEADING ADVERTISEMENTS IN E-COMMERCE

7.1 Regulatory Framework

Section 30 of the Consumer Protection Act, 2019, grants the CCPA specific authority over false or misleading advertisements that prejudice consumers or contravene public interest. In e-commerce, misleading advertisements take diverse forms:

- Product descriptions inconsistent with actual specifications
- Before-and-after claims for health or cosmetic products lacking substantiation
- Celebrity endorsements presenting opinions as scientific fact
- Comparison claims presenting competitor products unfavorably through selective data
- Price comparisons claiming false discounts (showing inflated "original" prices)
- Testimonial claims presented as universal results rather than isolated experiences.

7.2 Burden of Substantiation

The Act places burden of substantiation on advertisers and e-commerce platforms displaying advertisements. The CCPA can demand scientific evidence, testing reports, and expert opinions supporting advertising claims. Failure to substantiate results in orders for advertisement removal or correction and potential penalty imposition.

7.3 Influencer and Affiliate Marketing

The rapid growth of influencer marketing on e-commerce platforms presents novel regulatory challenges. The CCPA expects[19]:

- Clear disclosure of sponsored content and affiliate relationships
- Substantiation of claims made by influencers
- Platform responsibility for monitoring influencer compliance
- Verification that influencers actually use and recommend products.

Recent CCPA communications emphasize that influencers and platforms share liability for misleading endorsements.

8. CONSUMER REDRESSAL AND DISPUTE RESOLUTION

8.1Tiered Redressal Mechanism

The Consumer Protection Act, 2019, establishes a three-tier redressal system:

[19]*Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).

ISSN: 2582-6433

District Level: District Consumer Disputes Redressal Commissions handle complaints with value up to ₹1 crore

State Level: State Commissions address appeals and cases exceeding district jurisdiction limits

National Level: National Consumer Disputes Redressal Commission handles appeals from state commissions[20]

8.2 E-Commerce Platform Grievance Mechanisms

The Consumer Protection (E-Commerce) Rules, 2020, mandate that platforms establish in-house grievance redressal mechanisms as a prerequisite to legal compliance.[21] These mechanisms serve as the first line of dispute resolution, with formal commission proceedings available if e-commerce platform grievance procedures prove inadequate.

8.3 Mediation and Alternative Dispute Resolution

The Consumer Protection Act, 2019, incorporates provisions for mediation and alternative dispute resolution, recognizing that many e-commerce disputes can be resolved efficiently through negotiation. The National Commission and other redressal bodies are empowered to recommend mediation, reducing litigation burdens and accelerating consumer relief.

8.4 Online Dispute Resolution Mechanisms

The CCPA has encouraged development of online dispute resolution (ODR) systems for e-commerce disputes, recognizing that digital disputes warrant digital resolution mechanisms. ODR platforms can efficiently handle large volumes of small-value disputes while providing adequate consumer protection[22].

9. RECENT CCPA ENFORCEMENT ACTIONS AND COMPLIANCE DEVELOPMENTS

9.1 Dark Pattern Enforcement (2024-2025)

The period from 2024-2025 witnessed intensified CCPA focus on dark patterns. Key actions included:

[20]The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
[21]Press Information Bureau, *Consumer Protection (E-Commerce) Rules, 2020*, Ministry of Consumer Affs., Food & Pub. Distrib. (July 23, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945167. (last visited Jan. 26, 2026).
[22]*Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).

ISSN: 2582-6433

- **June 5, 2025 Advisory**: Universal mandate for e-commerce platforms to conduct self-audits on dark pattern elimination[23]
- **Show-Cause Notices**: Issuance of notices to eleven companies across quick commerce, online transport, and other sectors
- **November 19, 2025 Compliance Declaration**: 26 major e-commerce platforms voluntarily submitted self-audit compliance declarations, demonstrating substantial industry responsiveness.[24]

This enforcement sequence exemplifies the CCPA's graduated approach: guidance → advisory → enforcement → penalty, allowing platforms opportunity to self-correct while maintaining credible enforcement threat.

9.2 Sector-Specific Scrutiny

The CCPA has directed particular attention to vulnerable consumer segments and emerging business models:

Quick Commerce: Focus on false urgency claims, subscription traps, and delivery time guarantees that exceed realistic capacity

Online Travel and Booking: Scrutiny of drip pricing in ticket and hotel bookings, where final prices materially exceed displayed base prices

Food Delivery: Monitoring of food quality standards, safety protocols, and surge pricing practices

Financial Services: Verification of product claims by fintech platforms, particularly regarding returns and risk levels[25].

9.3 Compliance Declarations and Industry Response

The substantial industry response to the June 2025 advisory, with 26 leading platforms submitting compliance declarations within the stipulated timeframe, suggests successful regulatory signaling. Platforms recognized that dark pattern compliance represents a competitive necessity and regulatory imperative.

---

[23] *Regulatory Crackdown on Dark Patterns: CCPA's Enforcement Actions and Emerging Compliance Landscape in Indian E-Commerce*, AZB & Partners (Oct. 5, 2025), https://www.azbpartners.com/bank/regulatory-crackdown-on-dark-patterns-ccpas-enforcement-actions-and-emerging-compliance-landsca

[24] Press Information Bureau, *26 Leading E-Commerce Platforms Declare Compliance with CCPA Dark Patterns Advisory*, Ministry of Consumer Affs., Food & Pub. Distrib. (Nov. 19, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2191948

[25] *Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).

ISSN: 2582-6433

10. CHALLENGES AND LIMITATIONS

10.1 Technological Capacity Challenges

As e-commerce platforms grow increasingly sophisticated in deploying algorithmic systems, artificial intelligence, and machine learning, the CCPA faces technological capability constraints. Identifying subtle manipulations embedded in algorithmic recommendations requires technical expertise exceeding traditional consumer protection backgrounds[26].

10.2 Cross-Border and Jurisdiction Issues

Global e-commerce platforms operating in India but headquartered abroad present jurisdictional complexities. The CCPA's authority is limited to India, complicating enforcement against foreign entities. International cooperation mechanisms remain underdeveloped, requiring enhanced bilateral and multilateral coordination.

10.3 Resource and Staffing Constraints

Despite expanded authority, the CCPA operates with resource constraints relative to the scope of e-commerce activity in India. The vast number of e-commerce entities, sellers, and transactions exceeds CCPA investigative and enforcement capacity, necessitating reliance on platforms' self-regulation and consumer complaint information.

10.4 Balancing Innovation and Protection

A critical challenge involves balancing consumer protection with encouragement of innovation and competition. Overly aggressive regulation risks stifling the e-commerce sector's growth and competitiveness. The CCPA must calibrate enforcement to achieve protection objectives without imposing disproportionate compliance burdens.[27]

10.5 Consumer Awareness and Information Asymmetry

Despite regulatory advances, many e-commerce consumers lack awareness of their rights and redressal mechanisms. Information asymmetry persists, with sellers and platforms possessing superior information about products, terms, and practices. The CCPA has undertaken awareness campaigns but faces resource constraints in reaching diverse consumer populations.

---

[26] *Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).

[27] Sankar Ghosh, *Evolution of E-commerce and Consumer Protection Act 2019 Legal Framework*, LinkedIn (May 17, 2024), https://www.linkedin.com/pulse/evolution-e-commerce-consumer-protection-india-analyzing-sankar-ghosh-nx09c

ISSN: 2582-6433

11. INTERNATIONAL COMPARISONS AND BEST PRACTICES

11.1 European Union Framework

The European Union's approach to e-commerce consumer protection, particularly through the Unfair Commercial Practices Directive and emerging Digital Services Act, provides instructive comparisons. The EU emphasizes:

- Explicit consent requirements for data processing and marketing
- Algorithmic transparency and explainability
- Platform accountability for third-party seller compliance
- Substantial penalties for violations (up to 4% of annual revenue)

The CCPA has incorporated several EU principles, particularly regarding consent and transparency, while adapting them to India's specific context.

11.2 Comparative Regulatory Approaches

While the U.S. primarily relies on Federal Trade Commission authority under Section 5 of the FTC Act and relies heavily on market competition, the Indian approach through CCPA represents a more proactive, regulations-based model. This difference reflects India's assessment that market forces alone are insufficient to protect consumers in the e-commerce context.

11.3 Lessons for CCPA Enhancement

International experience suggests several areas for CCPA enhancement:

- Increased technical expertise in algorithms and AI systems
- Formalized international cooperation mechanisms
- Enhanced penalty structures incorporating revenue-based calculations
- Greater transparency requirements for algorithmic decision-making.

12. FUTURE DIRECTIONS AND RECOMMENDED ENHANCEMENTS

12.1 Algorithmic Accountability

As e-commerce increasingly relies on algorithmic systems for recommendations, pricing, and consumer interaction, the CCPA should develop frameworks requiring[28]:

[28]Sankar Ghosh, *Evolution of E-commerce and Consumer Protection Act 2019 Legal Framework*, LinkedIn (May 17, 2024), https://www.linkedin.com/pulse/evolution-e-commerce-consumer-protection-india-analyzing-sankar-ghosh-nx09c

ISSN: 2582-6433

- Algorithmic transparency documentation
- Impact assessments for recommendation systems
- Regular audits of algorithmic bias and discriminatory outcomes
- Consumer rights to algorithmic explanation

12.2 Enhanced Data Protection Integration

Consumer protection increasingly overlaps with data protection concerns. The CCPA should strengthen coordination with data protection authorities to address privacy-linked consumer vulnerabilities, including[29]:

- Consent mechanisms protecting both commercial and data privacy interests
- Enhanced breach notification requirements
- Consumer rights regarding data deletion and portability.

12.3 Strengthened International Cooperation

The CCPA should establish formal cooperation mechanisms with international consumer protection authorities, including memoranda of understanding, joint investigations, and coordinated enforcement actions against multinational platforms.

12.4 Capacity Building and Resource Enhancement

Addressing resource constraints requires:

- Increased budget allocations reflecting CCPA's expanded responsibilities
- Specialized recruitment of data scientists, engineers, and technology experts
- Training programs for investigators in emerging e-commerce practices
- Regional offices enhancing field investigation capacity

12.5 Consumer Awareness and Financial Literacy

The CCPA should expand consumer awareness initiatives through:

- Multi-language outreach across diverse media platforms
- School curricula incorporating e-commerce consumer rights education
- Partnerships with consumer advocacy organizations and civil society

[29] *Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).

ISSN: 2582-6433

13. IMPACT ON E-COMMERCE BUSINESS MODELS AND OPERATIONS

13.1 Compliance Investments by Platforms

The CCPA's regulatory expansion has necessitated substantial platform investments in compliance infrastructure[30]:

- Redesign of user interface elements to eliminate dark patterns
- Enhanced seller verification and monitoring systems
- Upgraded grievance redressal technology and staffing
- Compliance training programs for internal staff and affiliated sellers.

13.2 Seller Ecosystem Effects

Small and medium-sized sellers on marketplace platforms have experienced mixed effects:

Positive: Enhanced consumer trust in marketplace ecosystems may increase overall purchasing volume and seller opportunities

Negative: Compliance requirements increase operational costs, potentially disadvantaging sellers with limited resources[31]

13.3 Market Competition Dynamics

CCPA enforcement may influence market structure by[32]:

- Creating compliance advantages for larger platforms with greater resources
- Disadvantaging platforms specializing in gray-market or counterfeit goods
- Increasing barriers to entry for new market entrants lacking established compliance infrastructure

14. CONSUMER RIGHTS AND EMPOWERMENT

14.1 Substantive Consumer Rights

The Consumer Protection Act, 2019, and CCPA enforcement expand consumer substantive

[30]*Regulatory Crackdown on Dark Patterns: CCPA's Enforcement Actions and Emerging Compliance Landscape in Indian E-Commerce*, AZB & Partners (Oct. 5, 2025), https://www.azbpartners.com/bank/regulatory-crackdown-on-dark-patterns-ccpas-enforcement-actions-and-emerging-compliance-landsca

[31]Press Information Bureau, *Consumer Protection (E-Commerce) Rules, 2020*, Ministry of Consumer Affs., Food & Pub. Distrib. (July 23, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945167.

[32]Sankar Ghosh, *Evolution of E-commerce and Consumer Protection Act 2019 Legal Framework*, LinkedIn (May 17, 2024), https://www.linkedin.com/pulse/evolution-e-commerce-consumer-protection-india-analyzing-sankar-ghosh-nx09c

ISSN: 2582-6433

rights, including:

Right to Accurate Information: Access to truthful product descriptions, seller details, and pricing information

Right to Explicit Consent: Prohibition of automatic consent or pre-selected options advancing seller interests

Right to Refund and Return: Clear policies governing return periods, refund mechanisms, and restoration conditions

Right to Safety: Protection against defective, unsafe, or counterfeit products

Right to Redressal: Access to effective complaint mechanisms and dispute resolution[33]

14.2 Procedural Protections

Procedural reforms enhance consumer ability to assert rights:

- Simplified complaint filing procedures (including online mechanisms)
- Presumption of product liability on sellers absent contrary proof
- Recovery of litigation costs from unsuccessful defendants
- Class action provisions enabling collective grievance addressing[34]

14.3 Consumer Awareness and Education

Despite regulatory expansion, consumer awareness remains limited. Many consumers[35]:

- Lack knowledge of available redressal mechanisms
- Fail to recognize unfair trade practices or dark patterns
- Underestimate their substantive rights
- Hesitate pursuing disputes through formal channels

The CCPA and state authorities have undertaken awareness campaigns, but these require substantial expansion to reach diverse, multilingual consumer populations across India's varied markets.

[33]Press Information Bureau, *Consumer Protection (E-Commerce) Rules, 2020*, Ministry of Consumer Affs., Food & Pub. Distrib. (July 23, 2020), https://www.pib.gov.in/PressReleasePage.aspx?PRID=1945167. (last visited Jan. 26, 2026).
[34]The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India).
[35]*Central Consumer Protection Authority Establishment and Functions*, Dep't of Consumer Affs., https://doca.gov.in/ccpa/ (last visited Jan. 26, 2026).

ISSN: 2582-6433

15. CONCLUSION

The Central Consumer Protection Authority represents a transformative development in India's consumer protection architecture, establishing a proactive, specialized regulatory authority capable of addressing systemic consumer vulnerabilities in the e-commerce context. Through investigation, enforcement, and guidance functions, the CCPA has effectively shifted consumer protection from purely reactive dispute resolution toward preventive regulation addressing industry-wide practices.

The CCPA's evolving role demonstrates several key developments:

Institutional Innovation: The CCPA exemplifies effective institutional design for digital era consumer protection, combining investigative authority, enforcement powers, and guidance functions within a unified structure.

Substantive Expansion: The Consumer Protection Act, 2019, and related rules substantially expand consumer rights in e-commerce transactions, addressing previously unregulated areas including dark patterns, product liability, and algorithmic decision-making.[36]

Enforcement Commitment: Recent CCPA actions—particularly the dark pattern advisory and compliance tracking—demonstrate serious regulatory commitment backed by credible enforcement threats.[37]

Adaptive Regulation: The CCPA has demonstrated capacity to adapt regulatory frameworks to emerging challenges, responding rapidly to novel deceptive practices through advisory notices and enforcement action.

However, significant challenges remain. Technological capacity constraints, resource limitations, international coordination gaps, and persistent consumer awareness deficits require sustained attention. The CCPA must continue evolving its regulatory approaches to address algorithmic manipulation, data protection intersections, and emerging business models while maintaining appropriate space for innovation and competition.

Looking forward, the CCPA's success in fostering fair, transparent, and ethical e-commerce will depend on[38]:

[36]The Consumer Protection Act, 2019, S 60–65, No. 35, Acts of Parliament, 2019 (India).
[37]*Regulatory Crackdown on Dark Patterns: CCPA's Enforcement Actions and Emerging Compliance Landscape in Indian E-Commerce*, AZB & Partners (Oct. 5, 2025), https://www.azbpartners.com/bank/regulatory-crackdown-on-dark-patterns-ccpas-enforcement-actions-and-emerging-compliance-landsca(last visited Jan. 26, 2026).
[38]Sankar Ghosh, *Evolution of E-commerce and Consumer Protection Act 2019 Legal Framework*, LinkedIn (May 17, 2024), https://www.linkedin.com/pulse/evolution-e-commerce-consumer-protection-india-analyzing-sankar-ghosh-nx09c(last visited Jan. 26, 2026).

ISSN: 2582-6433

1. Continued resource investment and technological capacity building
2. Strengthened international cooperation mechanisms
3. Enhanced consumer awareness and financial literacy initiatives
4. Balanced regulatory approaches protecting consumers without stifling beneficial innovation
5. Integration with complementary regulatory regimes, particularly data protection authorities.

The CCPA's trajectory suggests that India is committed to establishing e-commerce consumer protection standards comparable to leading jurisdictions while adapting these approaches to India's unique market conditions, consumer diversity, and developmental priorities. As the CCPA matures and expands its institutional capacity, it will play an increasingly central role in shaping the digital economy's evolution toward greater fairness, transparency, and consumer-centricity.

IJLRA