



REGULATING DARK PATTERNS UNDER THE CONSUMER PROTECTION ACT: AN EMPIRICAL ANALYSIS OF THE CCPA GUIDELINES AND CONSUMER AUTONOMY IN INDIAN E-COMMERCE

Law

Shaikh Shayer Shabbir

Research Scholar, Department of Law, Monark University, Vahelal, Ahmedabad, Gujarat, India.

Dr. Laxmi Pawar

Research Supervisor, Department of Law Monark University, Vahelal, Ahmedabad, Gujarat, India.

ABSTRACT

Electronic commerce's quick growth has completely changed consumer markets by providing accessibility, affordability, and ease of use. However, in addition to these advantages, digital markets are increasingly using manipulative interface designs known as "dark patterns." By impeding decision-making, hiding essential information, encouraging hasty purchases, or generating phony urgency, these deceptive design strategies purposefully affect customer behavior. The autonomy that is the cornerstone of contemporary consumer protection legislation is undermined by such actions, which also call into question the idea of informed consumer choice. In response to these new issues, Through the Central Consumer Protection Authority, the Indian government has codified the Guidelines for Prevention and Regulation of Dark Patterns, 2023, in accordance with the Consumer Protection Act, 2019. The legal framework controlling dark pattern in Indian e-commerce is critically examined in this paper.

KEYWORDS

Consumer Protection Act, Dark Patterns, Consumer Autonomy, CCPA Guidelines, E-Commerce, Digital Consumer Rights, Deceptive Design, Online Consumer Protection.

INTRODUCTION

One of the areas of the Indian economy that is expanding the quickest is digital commerce. Millions of customers now buy products and services via online marketplaces because to government programs like Digital India, inexpensive cell phones, digital payment infrastructure, and extensive internet access. Online shopping has become a vital part of contemporary economic activity due to the simplicity of digital transactions, which has changed consumer behavior. Notwithstanding these benefits, the internet economy poses particular regulatory difficulties. Online platforms have unparalleled control over customer data, recommendation algorithms, interface design, and purchase paths in contrast to conventional retail settings. Instead than relying just on product quality or cost, this control enables firms to discreetly influence customer choices via interface design. Dark patterns are now widely used as a result of this phenomena.

User interface designs known as "dark patterns" are purposefully created to influence customer choices by taking advantage of behavioral biases and psychological weaknesses. deceptive urgency, concealing cancelation choices, coercing customers into subscriptions, adding items without permission, passing off ads as natural content, and providing deceptive price information are some of these tactics. Although these methods often seem to be legal in theory, they violate the idea of free and informed consumer choice. A key component of consumer protection jurisprudence is consumer autonomy. Consumers must have sufficient knowledge, true freedom of choice, and protection against manipulation in order to make autonomous decisions. By decreasing transparency and warping logical decision-making processes, dark patterns obstruct these circumstances. As a result, conventional notions of unfair commercial practices have changed to account for online deceit.

In response to these changes, India replaced the Consumer Protection Act of 1986 with 2019's Consumer Protection Act. The Central Consumer Protection Authority was established by, broadening the definition of unfair trade practices, introducing product liability, controlling deceptive advertising, and addressing internet commerce, the new law greatly enhanced consumer rights. Building on these legal prohibitions, Dark Pattern Regulation Guidelines, 2023 were released by the CCPA, which include thirteen forms of misleading interface designs that are forbidden.

REVIEW OF LITERATURE

Harry Brignull (2010), his usage of the word "dark patterns" was the first. He defined them as intentional interface designs meant to deceive people into doing things they would not otherwise select. His groundbreaking research laid the theoretical groundwork for later regulatory discussions on misleading design.

Gray et al. (2018) By classifying manipulative interface strategies

based on their behavioral goals, He increased the theoretical knowledge of dark pattern. According to their findings, dark patterns take use of well-known cognitive biases such choice fatigue, default bias, scarcity bias, and framing effects. They contended that digital manipulation is a serious ethical issue that goes beyond traditional fraud.

Mathur et al. (2019) undertook a massive empirical study on dark patterns on e-commerce websites. The authors found that misleading interface tactics, such as urgency messages, hidden fees, social proof manipulation, and subscription traps, are widely used in hundreds of e-commerce sites. Their research proved that dark patterns are not isolated business activities but rather systemic ones.

Research Gap

Even though there is a lot of scholarly literature on digital consumer protection, there are still a number of significant study gaps.

First, rather than focusing on the legal consequences of dark patterns within India's consumer protection system, the majority of overseas research focus on their technical categorization.

Second, there is no empirical data on real customer experiences with dark patterns, and Indian study has mostly concentrated on doctrinal interpretation of the customer Protection Act, 2019.

Third, despite the CCPA Guidelines' importance for digital consumer rights, not enough study has been done on consumer knowledge of them.

OBJECTIVES OF THE STUDY

1. To examine the legal framework governing dark patterns under law pertaining to consumer protection, 2019.
2. To analyse the CCPA Dark Pattern Prevention and Regulation Guidelines, 2023.
3. To empirically examine consumer awareness regarding shadowy trends in online shopping in India

RESEARCH METHODOLOGY

A mixed-methods empirical approach was used, combining a qualitative legal content audit of ten of the top e-commerce platforms and quick-commerce apps in the region with a quantitative survey of digital consumers (N=400) across Nanded City.

RESULT AND DISCUSSION

According to quantitative study, 86.5% of customers polled reported seeing at least two specific dark patterns on a weekly basis, with drip pricing, fake urgency, and basket sneaking being the most prevalent. Although 58.2% of respondents are aware of their rights under the Consumer Protection Act of 2019, just 21.4% are aware of the precise

2023 CCPA Guidelines. There is a statistically significant correlation between perceived loss of transactional autonomy and exposure to dark patterns, according to the Chi-Square test of independence. Legal assessments verify that subtle cognitive nudges (such as confirm shaming and interface interference) continue to exist across platforms, even if pre-ticked opt-in checkboxes have declined in response to CCPA advice.

The 2023 Guidelines, which were announced under Section 18 of the CPA 2019, are applicable to marketers, sellers, and any platforms that regularly provide products or services in India. As per Section 2(e), a dark pattern is any deceitful design strategy that manipulate users on any platform via their interfaces and experiences to force them to undertake behaviors they were not interested in, reducing their agency, decision-making, and choice. The Consumer Protection Act of 2019's substantive provisions give the 2023 Guidelines its legal authority; they do not function in a legislative vacuum.

An "unfair trade practice" is defined as any advertising strategy that promoting, or providing goods or services that is unfair, misleading, or otherwise unjust. This term applies directly to dark patterns like basket creeping, drip pricing, and bait and switch. Platforms use dishonest tactics to change the consumer's financial behavior by delaying entire cost disclosures till the last checkout page.

Any representation that misrepresents a product or service, makes a false assurance, or purposefully omits crucial facts is considered a deceptive advertising under Section 2(28). By distorting market circumstances or concealing the commercial nature of promoted material, false urgency (such as fake countdown clocks) and camouflaged adverts directly violate this clause.

Section 2 enshrines fundamental consumer rights, such as the freedom to choose from affordable products and services, transparency about the precise composition, amount, strength, standard, and cost of a product (9). By creating cognitive traps that compromise informed consent, interface manipulation directly violates the freedom to choose.

The CCPA was created under Section 10 of the CPA 2019 and functions as an executive regulatory body with the authority to advance, defend, and uphold the rights of consumers in general. The CCPA has extensive administrative authority, in contrast to conventional, reactive consumer courts:

Investigative Powers (Section 19): The Director-General of the CCPA's Investigation Wing may be instructed to carry out preliminary investigations of systematic e-commerce breaches, or the CCPA may start suo motu investigations.

Enforcement & Sanctions (Sections 20 & 21): The Authority has the authority to require the recall of dangerous products, demand complete transaction refunds, penalize platforms financially, and issue cease-and-desist orders against deceptive conduct.

Actions for Administrative Enforcement: Systemic platform modifications have been mandated by the CCPA using its authority. For example, major ticketing platforms were compelled to stop pre-ticked auto-debit charitable donations (a direct form of basket smuggling), and online travel aggregators were forced to refund over ₹1,400 crore for tickets canceled during public crises as a result of CCPA enforcement operations.

Advisories & Self-Audits: In order to expedite compliance, the CCPA issued administrative advisories instructing e-commerce platforms to carry out thorough internal UI/UX self-audits and submit compliance declarations attesting to the total elimination of the 13 designated dark patterns from their digital interfaces.

CONCLUSION

India's governance of the digital economy has undergone a significant change with the release of Guideline for Prevention & governance about Dark Patterns in 2023 in accordance with the Consumer Protection Act of 2019. In order to combat predatory interface design and safeguard consumer sovereignty, the Central Consumer Protection Authority has established an explicit taxonomy of thirteen forbidden dark patterns.

Empirical research, however, shows that misleading design techniques are nevertheless persistent, evolving from overt mechanisms like pre-selected checkboxes to more subtle cognitive manipulations like progressive charge disclosures and confirm shaming. In order to address these issues, active technical audits, cooperative regulatory enforcement with data protection authorities, and strict punitive actions are needed in addition to administrative recommendations.

Policy Recommendations

The following policy initiatives are suggested in order to close the gap between legislative purpose and actual enforcement:

1. "Privacy and Design by Default" is codified.

"Choice architecture neutrality" norms should be mandated by the CCPA in collaboration with the Ministry of Electronics and Information Technology. Platforms should be mandated to prohibit dynamic visual aspects that cause impulsive purchases, impose single-click opt-out processes that match single-click opt-ins, and offer "Accept" and "Reject" alternatives similar visual prominence.

2. Make the switch to third-party audits from voluntary self-audits:

For high-volume marketplace businesses, independent third-party compliance audits should take the place of the existing dependence on platform self-audits. A panel of trained UI/UX legal auditors should be established by the CCPA to regularly assess digital interface procedures.

3. Integrated Regulatory Coordination (CCPA & Data Protection Board):

Regulatory harmonization between the CCPA and the recently formed Data Protection Board of India (under the DPDPA, 2023) is required since dark patterns are often used as instruments for unapproved data gathering. To combat dark trends that contravene data consent and consumer protection laws, joint enforcement standards should be created.

REFERENCES:

1. Brignull, H. (2010). Dark Patterns: Deceptive editing and UI design choices. *A List Apart*, 318, 1–8.
2. Central Consumer Protection Authority. (2023). Guidelines for Prevention and Regulation of Dark Patterns, 2023. Gazette of India, Ministry of Consumer Affairs, Food and Public Distribution.
3. Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43–109. <https://doi.org/10.1093/jla/laaa006>
4. 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 11,000 shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–32. <https://doi.org/10.1145/3359183>
5. Ministry of Law and Justice. (2019). The Consumer Protection Act, 2019 (Act No. 35 of 2019). Gazette of India.
7. Ministry of Consumer Affairs, Food and Public Distribution. (2020). Consumer Protection (E-Commerce) Rules, 2020. Gazette of India.