The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Consumer Law: Deconstructing "Dark Patterns" and the Protection of Digital Consumers in India

Vanshika Choudhary

Abstract

The rise of algorithmic commerce creates new types of threats for customers. Digital architecture is manipulated to obfuscate customers' control to make choices. The intersection of behavioural psychology and digital capitalism design deceptive systems for customers to unknowingly give up control of choice. This study analyses India's legislative and regulatory response to dark patterns. It focuses on India's Section 2(47) of the Consumer Protection Act, 2019 CPA (2019), the CCPA Dark Patterns Guidelines, 2023, and India's Digital Personal Data Protection Act, 2023 ("DPDP Act"). India's regulatory response is a positive first step, but suffers from a lack of enforcement, under-inclusive definitions, and the failure to truly establish "Fairness by Design." A comparison to the U.S. FTC and the EU's DSA illustrates the need for more comprehensive systems of dark patterns.

Keywords: Dark Patterns, Consumer Protection Act 2019, Vitiated Consent, DPDP Act, Unfair Trade Practices, Information Asymmetry

Introduction: From Bazaar to Algorithm

Consumer protection laws remain remedial laws that cannot catch up to sophisticated commerce. The Consumer Protection Act, 1986 focuses on tangible defects of products and false advertising. It is an ex-post legislative response to disappointment after consumption in traditional post systems.[1]

[1] Consumer Protection Act, 1986, No. 68, Acts of Parliament, 1986 (India).

The digital economy has shifted the paradigm. The greatest consumer harm now resides in the digital interface and not the physical product. In the marketplace of algorithms, the greatest harm is not physical but mental and manipulative. The consumer's ability to make autonomous and informed choices has been undermined and intentionally corrupted.

The 1986 Act could never have imagined asymmetrical information architecture. Platforms have developed real-time data for consumer psychology. They use this data against consumers through competitor-designed interfaces.

This change in architecture led to the creation of more "dark patterns". UX designer Harry Brignull describes these patterns as user interfaces constructed in a specific way to trick users into purchasing more expensive insurance or using other contracts that lead to payment obligations after the fact. India has responded to Brignull's black patterns through the CPA 2019 and the CCPA Dark Patterns Guidelines 2023[2]. Although these responses are the most detailed at the domestic level, this article shows that they have structural deficiencies that will enable a committed platform operator to exploit them.

II. Taxonomical Framework: A Behavioural-Legal Anatomy

2.1 The Cognitive Architecture of Manipulation

Dark patterns are effective in targeting the systematic abuse of documented and defensively known cognitive biases. Several of these are now described.

- **Loss Aversion:** This term comes from Kahneman and Tversky's Prospect Theory[3], which holds that losses are weighted about twice as heavily as a gain of the same amount. False urgency practices, such as countdown clocks or low-stock-and-least-notice alerts, create a sense of duress to make a user make a decision, which indirectly relates to the doctrine of vitiated consent.
- **Default Bias:** People disproportionately stick to the predetermined default-thus ignoring their own preferences.[4] The traps are extension and consent boxes which are also ticked beforehand. This is consent that is manufactured structurally and thus is not authentic.

[2] Harry Brignull, Dark Patterns: Deception vs. Honesty in UI Design, A List Apart (2011).
[3] Daniel Kahneman & Amos Tversky, Prospect Theory: An Analysis of Decision Under Risk, 47 Econometrica 263, 279 (1979).
[4] Eric J. Johnson & Daniel Goldstein, Do Defaults Save Lives?, 302 Science 1338 (2003).

- **Drip Pricing and Present Bias:** Consumers overvalue immediate rewards as compared to future costs. This is seen in the exhaustion of a consumer's price sensitivity through the present costs coupled with the completion of the transaction[5].

2.2 Principal Dark Pattern Species

The CCPA Guidelines include thirteen dark patterns and the following analysis dismantles the three most influential patterns.

False Urgency: Platforms that display countdown clocks that say "Only 1 seat left!" when inventory data do not support these statements are false representations of a material fact and are actionable under Section 2(47) of the CPA 2019.

Basket Sneaking: When a consumer adds priority support, donations, or insurance to a consumer's cart without express affirmative action, there is a clear lack of meeting of the minds. The consumer's consent, which is given by the completion of the transaction, does not extend to the additional term to which the consumer was not informed.

Confirm Shaming: The phrasing of the opt-out "No thanks, I don't want to save money" is social shame. While a false statement of fact is not provided, this is psychological coercion and is below the threshold of legally recognizable duress. However, it does achieve the same goal of an obstruction to the consumer's autonomous decision-making.

Subscription Traps (Roach Motel): Subscription systems that are easy to sign up for but difficult to cancel are a clear violation of consumer rights[6].

Privacy Zuckering: Fragmented privacy settings to confuse consumers into giving more of their personal data is a clear violation of consumer rights.

III. Legislative Analysis: The Statutory Architecture

3.1 Section 2(47), CPA 2019: The Definitional Foundation

The central statutory provision is Section 2(47) of the CPA 2019, which lists "unfair trade practice," as including, among other things, "any unfair method or unfair or deceptive practice" and includes a residual category of "any other deceptive practice."[7] The result of the vague

[5] David Laibson, Golden Eggs and Hyperbolic Discounting, 112 Q.J. Econ. 443 (1997).
[6] See Competition and Markets Authority (UK), Online Choice Architecture: How Digital Design Can Harm Competition and Consumers (2022).
[7] Consumer Protection Act, 2019, § 2(47), No. 35, Acts of Parliament, 2019 (India).

presence of that formulation is that the CCPA has the authority under that provision to categorize dark patterns as ‘unfair trade practices’ without the requirement of mentioning the dark patterns. The most dangerous and exploitable deficiency of that formulation is the definitional uncertainty. It is a formulation that encompasses misleading advertising, unfair trade practices, and violation of consumers’ rights. It places dark patterns regulation within existing statutes and constructs the standard of ‘consumers’ rights.’ It provides the Indian regulatory system a meritorious practice.

3.2 The CCPA Dark Patterns Guidelines, 2023

Issued on November 30, 2023, the Guidelines define dark patterns as:

"any practices or deceptive design patterns using UI/UX interactions on any platform that is designed to mislead or trick users into doing something they didn't intend to or didn't want to do; by subverting or impairing the consumer autonomy, decision making or choice; amounting to misleading advertisement, unfair trade practice or violation of consumer rights."[8]

Although these guidelines are a positive step forward, three aspects must be criticized. First, the closed taxonomy of thirteen practices introduced risks quick obsolescence due to rapid changes. Second, no obligations of transparency in the design of the algorithms are described. No obligations to the disclosure of A/B testing or of the parameters or the scales of the dark patterns are described. Third, The CCPA is granted sole-enforcement authority, which results in a ‘single funnel’ approach with no private enforcement rights. The penalty for repeat offenses of Rs. 50 lakhs are, for multinational companies that operate in India and make billions in profit annually, simply the cost of doing business.

IV. The DPDP Act: Consent Validity and the Intersection Problem

4.1 Consent Architecture Under the DPDP Act, 2023

Section 6 of the DPDP Act requires the personal data processing consent to be unambiguous, specific, informed, free, unconditional, and demonstrated through a clear affirmative action[9]. This taxonomy corresponds with precision to the dark pattern pathologies. In a cookie consent wall, placing “Accept All” in a position of dominance while “Reject Non-Essential” is buried in a footnote demonstrates that consent is not “free” in any legal sense; it is consent generated

[8] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, F. No. J-25/55/2022-CCPA (Nov. 30, 2023) (India).

[9] Digital Personal Data Protection Act, 2023, § 6, No. 22, Acts of Parliament, 2023 (India).

via the methodical manipulation of salience. The idea of vitiated consent is the foundation of contract law and the data protection law.

4.2 Vitiation of Consent: A Doctrinal Analysis

According to Section 16 of the Indian Contract Act, 1872, so-called “undue influence” exists when one party has the ability to “dominate the will of the other” and uses that capability to gain an “unfair advantage”[10]. A broader interpretation is warranted in dark pattern circumstances. A platform’s technical and informational dominance - including a granular possession of user data, control of the data and interface architecture, and the ability to perform real-time psychological profiling of the user - is an example of the kind of dominance that Section 16 was meant to address.

Significant consequences of invalid consent under the DPDP Act arise from Section 6(7), which states that data processing based on non-compliant consent is unlawful, and the data fiduciary is subject to a penalty imposed by the Data Protection Board of India (“DPBI”)[11]. A single deployment of a dark pattern engages both the jurisdiction of the CCPA (as an unfair trade practice) and the jurisdiction of the DPBI (as a consent validity case) due to a regulation fragmentation that the current laws have not addressed through any formal coordination.

V. Enforcement Challenges and Comparative Perspectives

5.1 Systemic Enforcement Hurdles

Even with the existing digital redressal infrastructure-the e-DAAKHIL portal, the National Consumer Helpline, and the CCPA's investigative powers-certain structural barriers still hamper the implementation of redressal mechanisms.

The digital divide brings a differential distribution of protective regulation. The consumers hit the hardest are those with low digital literacy, therefore consumers are unable to document and/or file complaints. The result is a widespread under-enforcement of regulation for those consumers that require the most protection.

The lack of evidence further complicates the situation. Dark patterns are used in interfaces that are frequently modified by A/B testing, and thus the manipulative stimuli presented to the

[10] 10 Indian Contract Act, 1872, § 16(1), No. 9, Acts of Parliament, 1872 (India).
[11] Digital Personal Data Protection Act, 2023, § 6(7), No. 22, Acts of Parliament, 2023 (India).

consumer may not be present to the investigators. Transforming the Psychological injury of the violation of consumer autonomy and choice is yet another challenge for the courts.

5.2 Comparative Perspectives

The absence of bilateral enforcement cooperation agreements has allowed massive digital behemoths based in offshore territories to globalize their regulatory offerings to the Indian market. The EU has regulations in place that can provide a reference. For example, the GDPR (Recital 32) and the DSA (Article 25) provide a substantial regulatory framework to ensure that pre-ticked boxes and deceptive/ manipulative interfaces are prosecutable violations and can result in a fine based on a platform's global turnover[12]. The Guidelines 3/2022 on Dark Patterns[13] issued by the EDPB provide a detailed and sophisticated multibillion euro enforcement action regulatory framework.

The U.S. FTC's implementation of Section 5 of the FTC Act in the Matter of Amazon.com, Inc. (2023)[14], and the 2022 report Bringing Dark Patterns to Light[15], uses Section 5 of the FTC Act to flex the agency's enforcement power. The U.S. FTC's Section 5 of the FTC Act implementation has more enforcement flexibility compared to the EU. India's penalty cap of ₹50 lakhs is more inadequate at a global level.

VI. Policy Recommendations and Conclusion

6.1 Prescriptive Recommendations

Legislative reforms that directly reference deceptive digital interface design should amend Section 2(47) of the CPA 2019, so that the prohibition is elevated from the guidelines to primary legislation. The penalty cap should be increased to the India-revenue split (minimum 2% of annual Indian revenue for repeated violations), with a floor of ₹ 2 crore for platform-level violations.

“Fairness by Design” mandates should be established through the CCPA's binding technical standards. These standards should include visual parity of commercially similar options, and the asymmetry of the steps in the flow of enrolment and the flow of cancellation should be minimized.

---

[12] 12 Council Regulation 2016/679, General Data Protection Regulation, Recital 32, 2016 O.J. (L 119) 1 (EU).
[13] Regulation (EU) 2022/2065, Digital Services Act, art. 25(1), 2022 O.J. (L 277) 1.
[14] In the Matter of Amazon.com, Inc., FTC File No. 2123130 (2023) (consent order).
[15] Fed. Trade Comm'n, Bringing Dark Patterns to Light (Sept. 2022).

Coordination of the CCPA and the DPBI requires a formal Memorandum of Understanding that delineates jurisdiction and sets protocols for combined investigations of dark patterns that impact consumer and data protection, addressing the current regulatory inconsistency.

The individual enforcement burden should be reduced, and the platform-level manipulation systematically opposed by allowing legitimate consumer complaints to be brought by Consumer and Civil Society organizations against the CCPA.

6.2 Conclusion

At its core, dark pattern regulation aims to protect the necessary environments for real autonomous agency within digital commerce. India's efforts (the CPA 2019, the CCPA Guidelines, and the DPDP Act) are commendable first-generation efforts, though they fall short of capturing the full extent of the challenges presented by the threats. The absence of tiered penalties and a resilient, adequately staffed response to the needs of the system are just a few of the many issues present in the system.

A paradigm shift is what the present situation warrants. Enforcement needs to be proactive and design-focused, and responses should be based on principles of fairness and the willingness to cooperate internationally, as opposed to leading primarily on a national basis. Given the context of an algorithmically driven market, the importance of the law in the initial phases to protect the dignity of the contracting party cannot be overstated.