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

DESIGNED TO DECEIVE: REGULATING DARK PATTERNS IN INDIA'S DIGITAL MARKETPLACE

~ RITU MUKHI

INTRODUCTION

The remarkable expansion of India's digital economy is projected to reach $1 trillion by 2030; this has fundamentally reshaped consumer behaviour and e commerce business models. However, this massive digital growth has also been accompanied by a pervasive and insidious practice known as "dark patterns". These are deceptive user interface and user experience (UI/UX) designs engineered to exploit cognitive biases, nudging consumers into making purchases or sharing personal data that they did not intend to make or disclose.

From a business perspective, dark patterns are often defended as aggressive optimization strategies intended to increase conversion rates and maximize short term revenue. From a legal standpoint, however, they undermine consumer autonomy and informed consent. This article examines India's evolving regulatory framework governing dark patterns, examining the critical interaction between consumer protection and data privacy laws, recent enforcement actions, and strategic compliance measures for digital platforms.

CONCEPTUAL TAXONOMY AND THE BEHAVIOURAL ECONOMICS OF DIGITAL DECEPTION

Dark patterns mark a paradigm shift from traditional form of misrepresentation to subtle, design-based manipulation, a phenomenon frequently termed as "coercive choice architecture" [1] While choice architecture can be used to nudge users positively, its malicious application in the digital sphere was identified by UX designer **Harry Bringull** in 2010[2], who coined the term "dark patterns" which refers to interface designs that **subvert deliberative** *system 2*

[1] Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press.

[2] Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A List Apart (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/

decision- making by triggering **reflexive** *system 1* **heuristic- driven behaviours**. Empirical research indicates that up to 82% of major Indian e commerce platforms utilize some form of manipulative design, resulting in an estimated annual financial drain of ₹25,000 to ₹28,000 crore on consumers. [3]

Recognising this threat, the central consumer protection Authority (CCPA) issued specific guidelines in 2023, identifying and defining thirteen core dark patterns. Prominent examples include:

- **Drip pricing:** The practice of concealing incremental fees, such as convenience fees or handling costs, until the final stage of checkout, thereby locking consumers into a transaction after they have invested time in the transaction.
- **Basket Sneaking:** Automatically adding supplementary products, warranties or charitable contributions to a user's shopping cart without obtaining explicit and affirmative consent.
- **Confirm shaming:** Using guilt- inducing or emotionally manipulative language (e.g., "No thanks, I will leave my family's device unsecured") to pressure users into making purchases or data sharing.
- **Subscription Traps ("Roach Motel"):** Designing a user flow that makes signing up for a service seamless and effortless, while making the cancellation process intentionally obscure or functionally impossible.

THE STATUTORY FRAMEWORK: CPA 2019 AND CCPA GUIDELINES

India's primary consumer protection law, The Consumer Protection Act, 2019 (CPA,2019) does not explicitly mention "dark patterns". However, it contains provisions that prohibit trade practice harmful to consumers such as deceptive practices that take away or restrict their choice. Specifically, **section 2(47)** of CPA, 2019 **and Section 2(28) of CPA 2019** addresses deceptive trade practices and misleading advertisements respectively. [4]

In addition, **section 18** provides for the enforcement mechanisms giving powers to the Central Consumer Protection Authority (CCPA) to inquire and prove complaints relating to unfair trade

[3] Datum Intelligence. (June 2026). *Dark Patterns in India's Online Marketplaces*. Indian online buyers losing up to ₹28,000 crore annually to dark patterns, hidden charges: Report - The Hindu ***Also see,*** Local Circles. (2026). *Survey on Deceptive Design Practices and Interface Interference in Indian Digital Platforms*.

[4] The Consumer Protection Act, 2019, § 2(28), 2(47), 18, 89, No. 35, Acts of Parliament, 2019 (India).

practices and issues directions for the regulation of such practices and for the promotion and protection of consumer rights.

The authority directed the Consumer Protection Act 2019 (CPA), 2019 and issued the dark pattern guidelines on consumer protection and prevention of misleading advertisements on November30, 2023, under the provision of **18(2)(1) of the CPA, 2019.**[5]

In *National Restaurant Association of India (NRAI) V. Union of India* (2025), the Delhi High Court held that CCPA guidelines issued under this provision possess binding statutory force under **Article 13 of the constitution**.[6] Furthermore, **Rule 4(9) of the consumer protection** (E commerce) Rules 2020 strengthens this framework by expressly prohibiting the use of pre-ticked checkboxes to obtain consumer consent. [7]

DUAL REGULATION: THE INTERSECTION OF CONSUMER PROTECTION AND DATA PRIVACY

A major legal liability for modern digital platforms is the dual regulatory framework created by the overlap between consumer protection law and the Digital Personal Data Protection Act, 2023 (DPDP Act).

Under **Section 6 of the DPDP Act**, the processing of personal data strictly requires consent that is free, specified, informed, unconditional and communicated through clear affirmative action.

When platforms employ dark patterns such as Forced Action (requiring users to provide unrelated personal data to access a primary service) or *Privacy Zuckering* (making privacy opt-out options difficult to locate or use), they incur liability under both statutes. Such practices constitute unfair trade practices under the CPA 2019 and also violate the DPDP Act because the resulting consent is legally invalid.

The financial stakes of this dual liability are severe. The CPA 2019 permits penalties of up to ₹50 lakh, along with potential imprisonment **under Section 89**, while the DPDP Act authorises the Data Protection Board of India (DPBI) to impose penalties of up to under ₹250 crore section 33 for systemic consent failures. [8]

---

[5] Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns*, 2023, F. No. J-24/34/2023-CPU (Reg.) (Notified Nov. 30, 2023).
[6] *National Restaurant Association of India v. Union of India*, (2025) Delhi High Court (India).
[7] The Consumer Protection (E-Commerce) Rules, 2020, Rule 4(9), G.S.R. 462(E) (Issued July 23, 2020).
[8] The Digital Personal Data Protection Act, 2023, § 4, 6, 8(4), 33, No. 22, Acts of Parliament, 2023 (India).

REGULATORY ENFORCEMENT TRENDS AND PRECEDENTS.

India's regulatory landscape has rapidly transitioned from issuing guidance and advisories undertaking direct punitive actions. Following a CCPA advisory directing e-commerce platform to conduct mandatory self-audits[9], major digital platforms (including Flipkart, Swiggy and MakeMyTrip) were required to submit declarations confirming that their interfaces were free from dark patterns by late 2025. [10]

The emphasis on voluntary compliance has now been reinforced through active regulatory enforcement. Recent cases illustrate this increasingly stringent approach. The CCPA imposed **a ₹5 lakh penalty on PhysicsWallah** for engaging in Basket Sneaking by automatically selecting donations during course purchases and for using Forced Action mechanisms. [11]

Similarly, McAfee Software India was fined ₹1 lakh for employing confirm shaming and Interface Interference, particularly through a coercive subscription renewal prompt that presented users with the options "Renew Now" or "Accept Risk" without providing a neutral and easily accessible opt- out alternative. [12]

CONCLUSION AND WAY FORWARD

Regulating dark patterns requires a paradigm shift in understanding of UI/UX design as both a marketing tool and a legal compliance issue, While the use of manipulative interfaces elements may provide short- term gains in conversion rates, they ultimately undermine consumer trust, damaging the bottom line and inviting regulatory scrutiny from both the CPA, 2019 and the DPDP Act. The issue can be tackled from four pillar strategy:

1. By developing fairness design standards, such as requiring visual consistency between 'accept' and 'decline' buttons and one click unsubscribe options for marketing communications.
2. By introducing mandatory UI/UX audits to detect manipulative design elements and algorithmic upselling;

[9] Central Consumer Protection Authority, *Advisory on Self-Audit by E-Commerce Platforms for Detecting Dark Patterns* (Issued June 5, 2025).
[10] Press Information Bureau, *26 Leading E-Commerce Platforms Declare Compliance with Self-Audit to Eliminate Dark Patterns*, Ministry of Consumer Affairs (Nov. 20, 2025).
[11] *Central Consumer Protection Authority v. PhysicsWallah Ltd.*, CCPA Order (June 1, 2026) (India).
[12] *Central Consumer Protection Authority v. McAfee Software India Pvt. Ltd.*, CCPA Order (May 20, 2026) (India).

3. By establishing a jurisdictional coordination mechanism between the CCPA and the DPBI in cases of jurisdictional overlap;
4. By amending the CPA 2019 and Section 2(47) to explicitly prohibit dark patterns in digital commerce and imposing large- scale turnover penalties on firm found guilty of deploying them.