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

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DARK PATTERNS IN E-COMMERCE: IS CONSUMER CONSENT BECOMING AN ILLUSION?

— Irine Elsa Cherian

It starts innocently enough. A flight booking, a food order, a pair of shoes added to a cart at eleven at night. Somewhere between browsing and paying, a box appears already ticked for travel insurance you never asked for. A timer counts down from ten minutes, warning that the fare will vanish if you hesitate. When you try to leave without buying, a pop-up asks, in a faintly accusing tone, whether you really want to "miss out on savings." None of this feels like fraud. It feels like ordinary shopping.

These small nudges have a name: dark patterns. They are not glitches or aggressive sales tactics in the traditional sense; they are deliberately engineered features of an interface, built by people who understand behavioural psychology better than most consumers understand their own decision-making. And because Indian consumers now transact almost entirely through screens, the law has had to catch up with a market where persuasion has been automated.

What Exactly Is a Dark Pattern?

A dark pattern is any design choice on a website or app that steers a user toward an outcome they did not intend, by exploiting habit, urgency, or inattention rather than by informing them. Some versions are almost comic in retrospect: a "cancel subscription" button buried three menus deep, or a discount that appears only once the checkout page detects the cursor moving toward the browser's close button. Others are subtler, such as a countdown timer that resets the moment the page reloads, or a default setting that quietly opts a user into marketing communications unless they scroll down to find the opt-out.

Common categories now recognised by regulators include hidden charges revealed only at the final payment stage, subscriptions that are simple to start but deliberately difficult to end,

confirm-shaming language that guilts a user into a purchase, fabricated urgency and scarcity cues, pre-selected consent boxes, and advertisements disguised as neutral content or genuine user reviews.

What unites all of them is not deception in the classic sense of a false statement, but the manipulation of the environment in which a choice is made. Consumer law has traditionally asked whether information given to a buyer was accurate. Dark patterns raise a different question: was the buyer given a fair chance to think at all?

The Legal Position in India

India's response has been built in layers. The Consumer Protection Act, 2019 replaced the older 1986 statute with a considerably wider definition of unfair trade practice, one broad enough to capture deceptive digital conduct that no one had imagined when the earlier law was drafted.[1] The Consumer Protection (E-Commerce) Rules, 2020 followed, placing specific disclosure duties on marketplaces and sellers, including obligations around pricing transparency and the identification of sponsored listings.[2]

The most direct intervention came in November 2023, when the Central Consumer Protection Authority notified the Guidelines for Prevention and Regulation of Dark Patterns, exercising powers granted to it under Section 18 of the 2019 Act.[3] These Guidelines take an unusually concrete approach for Indian consumer law: rather than relying on an open-textured standard, they list thirteen specified dark patterns in an annexure, ranging from false urgency to disguised advertising, while leaving the CCPA free to expand the list as new techniques surface.[4] The Guidelines also apply to any platform offering goods or services to Indian consumers regardless of where it is based, an extraterritorial reach that acknowledges how little geography matters to an app store.

The CCPA's authority here is not merely advisory. Section 18 gives it the power to inquire into unfair trade practices, order the discontinuation of a practice, and impose penalties, which is

[1] Consumer Protection Act, No. 35 of 2019, § 2(47), India Code (2019) (defining "unfair trade practice").

[2] Consumer Protection (E-Commerce) Rules, 2020, G.S.R. 456(E) (India).

[3] Ministry of Consumer Affairs, Guidelines for Prevention and Regulation of Dark Patterns, 2023, F. No. J-24/9/2023-CCPA (Nov. 30, 2023) (India).

[4] Id. Annexure I (listing thirteen specified dark patterns, subject to periodic revision by the Central Consumer Protection Authority).

why the 2023 Guidelines carry more weight than a code of conduct.[5] In practice, enforcement has so far leaned on advisories and self-audits rather than large-scale prosecutions, which tells its own story about how difficult these provisions are to police at speed.

Why 'I Agree' No Longer Means Much

Contract law has always assumed a consenting party who reads, understands, and then decides. Behavioural economics has spent two decades quietly dismantling that assumption, showing how choice architecture, the sequencing, framing, and defaults built into any decision environment, can predict outcomes far better than a consumer's stated preferences can.[6] A pre-ticked box does not need to lie to be effective; it merely needs to exploit inertia, the well-documented tendency of people to leave things as they find them.

This is what makes the current moment legally uncomfortable. The click on "I Agree" still satisfies the formal requirements of a contract, yet it may reflect nothing more than the sequencing of a screen. The asymmetry is structural: platforms run thousands of interface experiments to learn what converts a hesitant browser into a paying customer, while the consumer sees only a single, seemingly natural version of that screen. Consent obtained this way is real in form but increasingly hollow in substance.

How Other Jurisdictions Are Responding

India is not alone in wrestling with this. The European Union's Unfair Commercial Practices Directive already prohibited misleading and aggressive commercial practices,[7] and the newer Digital Services Act goes further by expressly banning interface designs that impair a user's ability to make free and informed decisions.[8]

The United States has no single federal dark-patterns statute, but the Federal Trade Commission has used its general power under Section 5 of the FTC Act to act against manipulative design, and its 2022 staff report catalogued the same techniques Indian regulators would recognise from local shopping apps.[9] The United Kingdom, meanwhile, has moved

[5]Consumer Protection Act, No. 35 of 2019, § 18 (India) (empowering the Central Consumer Protection Authority to issue guidelines for the prevention of unfair trade practices).

[6]OECD, Dark Commercial Patterns 21-24 (OECD Digital Economy Papers No. 336, 2022).

[7]Directive 2005/29/EC, of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices, 2005 O.J. (L 149) 22.

[8]Regulation (EU) 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), art. 25, 2022 O.J. (L 277) 1.

[9]Fed. Trade Comm'n, Bringing Dark Patterns to Light: An FTC Staff Report 7-9 (2022).

toward a more codified model through its 2024 competition and consumer reforms, giving its regulator direct powers to penalise unfair commercial practices without needing to go to court first.[10] Set against these frameworks, India's 2023 Guidelines look reasonably ambitious in scope, if still light on enforcement muscle.

What Makes This Hard to Regulate

Several problems will outlast any single set of guidelines. Interface design changes faster than rule-making; a platform can retire one dark pattern and deploy a new variant within a product update cycle, long before a regulator has finished investigating the first version. Cross-border platforms complicate jurisdiction, since a server in one country and a user in another leave enforcement authorities negotiating cooperation rather than issuing orders. And the newest complication is personalisation: interfaces increasingly adapt to an individual's browsing history and psychological profile, which means two users can see entirely different manipulative prompts, making it harder to build the kind of uniform evidentiary record regulators are used to relying on.

None of this is solved by better statutes alone. A regulator with limited technical staff cannot audit every checkout flow in the country, and a consumer who does not recognise manipulation cannot complain about it. Awareness, in this sense, is doing as much regulatory work as the Guidelines themselves.

Has Consent Become an Illusion?

Not entirely, but the direction of travel is unmistakable. India's legal framework has, in a relatively short span, moved from silence to a fairly detailed set of prohibitions, and the CCPA's willingness to name specific practices is more than symbolic. What the law has not yet solved is the gap between prohibiting a practice on paper and detecting it inside a codebase that changes overnight.

Perhaps the more useful question for the next decade is not whether a click counts as consent, but whether consent, as a legal concept built for face-to-face bargaining, can be meaningfully translated onto a screen at all. Until interface design is treated with the same regulatory

[10] Digital Markets, Competition and Consumers Act 2024, c. 13 (UK).

seriousness as the contract terms it delivers, every “I Agree” button will carry a small, unresolved question mark.