

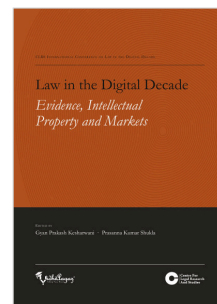
CHAPTER 13

Consumer Protection Against Dark Patterns in E-Commerce: Regulating Manipulative Online Choice

Prachi Sharma

in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 141–147

DOI <https://doi.org/10.63108/VAB.LDD.2.13>



CITATIONS

BLUEBOOK (21ST ED.)

Prachi Sharma, *Consumer Protection Against Dark Patterns in E-Commerce: Regulating Manipulative Online Choice*, in *LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS* 141 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Prachi Sharma, 'Consumer Protection Against Dark Patterns in E-Commerce: Regulating Manipulative Online Choice' in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 141.

CHICAGO (17TH ED.)

Sharma, Prachi. "Consumer Protection Against Dark Patterns in E-Commerce: Regulating Manipulative Online Choice." In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 141–147. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.2.13>.

APA (7TH ED.)

Sharma, P. (2026). Consumer protection against dark patterns in e-commerce: Regulating manipulative online choice. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 141–147). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.2.13>

SOURCE

<https://doi.org/10.63108/VAB.LDD.2.13>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 13

Consumer Protection Against Dark Patterns in E-Commerce: Regulating Manipulative Online Choice

PRACHI SHARMA*

The rapid expansion of electronic commerce has transformed how consumers search, compare, and purchase goods and services. Alongside convenience, however, online platforms increasingly use “dark patterns” – deceptive or manipulative interface designs that influence consumers toward choices they may not otherwise make. Examples include hidden costs, pre-selected options, disguised advertisements, difficult cancellation processes, and misleading countdown timers. These practices raise an important consumer-protection question: whether existing legal frameworks are sufficiently equipped to protect genuine consumer choice in digital marketplaces. Rather than examining consumer protection in e-commerce broadly, this study focuses specifically on the effectiveness of consumer-protection law in addressing dark patterns during online transactions. The topic is significant because traditional consumer-protection principles generally assume that consumers make decisions based on clear and accessible information. Digital interfaces can challenge this assumption by deliberately shaping the way information and choices are presented. Understanding this problem is therefore essential for determining whether legal protection should extend beyond false information to manipulation of the consumer decision-making process itself. The research will adopt a doctrinal and comparative legal approach. It will examine relevant consumer-protection legislation, regulatory guidelines, judicial decisions, and enforcement actions concerning deceptive online interface practices. Particular attention will be given to the Indian legal framework, especially the Consumer Protection Act, 2019 and regulatory measures addressing dark patterns. Selected approaches from other jurisdictions, particularly the European Union, will be comparatively analysed to identify effective regulatory mechanisms. The study will assess whether existing rules provide adequate remedies, transparency requirements, and deterrence against manipulative design practices. The research argues that effective e-commerce consumer protection requires regulation not only of misleading content but also of misleading choice architecture. Strengthening legal standards concerning dark patterns could promote more transparent digital markets while preserving legitimate innovation in online commerce.

Keywords: Dark Patterns; E-Commerce; Consumer Protection; Digital Markets; Online Manipulation

1 INTRODUCTION

With the advent of technology, India has moved since 1991 from Phase 0 (offline consumers) towards the subjective goods purchase phase, with about 150 million Indians ready to begin e-commerce shopping, depending on the income, education and occupation of their households.¹ This rapid change reflected the pattern of consumers and purchasing behaviour of society. India soon became the second largest digital market at the global level with over 62 billion UPI transactions in 2022 and 172 billion UPI transactions in 2024, growing 46% year on year.²

A majority of Indian consumers are influenced more by the time they spend on digital media than by traditional channels. This also contributes to the sudden rise in e-commerce tendencies. Therefore, to

* Assistant Professor at Vivekananda Institute of Professional Studies, Technical Campus, New Delhi, India.

¹ Manoj Singhal, “E-Commerce in India: A Review” *International Journal of Computer Applications (IJCA)*, 2012.

² Shivani Anand, “Decade-wise Transformation of E-Commerce in India: A Comprehensive Analysis” 13 *JETIR* 105 (2025).

boost consumption, businesses rely on a range of digital tactics aimed at expanding their customer base while pulling in more data and revenue.³ One well-known example is growth hacking, a technique that traces back to Hotmail's early tagline "Get your free email at Hotmail" appended to outgoing messages.⁴ Not every such tactic is harmless, however. A particularly troubling category has come to be known as "dark patterns" – interface designs that steer users toward certain decisions by manipulating the information presented to them. These designs work by tapping into cognitive biases, such as the fear of scarcity or the pull of the bandwagon effect, to drive up revenue and push consumers toward greater consumption.⁵

As businesses have leaned more heavily on data-driven marketing and outcome-based metrics, the use of dark patterns in online retail has grown correspondingly. Firms keep close track of figures like click-through rates, cart completions, and subscription renewals and this focus tends to push them toward tactics that chase immediate gains, sometimes at the cost of keeping customers satisfied over time. The fallout is that shoppers frequently find themselves pushed into purchases they never intended to make, locked into subscriptions they didn't mean to sign up for, or misled about what exactly they're buying. Such deception chips away at the trust that underpins the relationship between consumers and brands, making it a serious concern both ethically and from a legal standpoint.

Dark patterns take many forms in practice – drip pricing, disguised advertising, bait-and-switch tactics, artificially manufactured urgency, and several others. Under Indian law, these practices are captured within the broad definition of "unfair trade practice" found in Section 2(47) of the Consumer Protection Act, 2019.⁶

Acting under its powers under Section 18 of the Act, the Central Consumer Protection Authority (CCPA) took a concrete step on 30th November 2023, releasing the "Guidelines for Prevention and Regulation of Dark Patterns, 2023." These guidelines went further than the general statutory language by naming thirteen distinct dark patterns specifically observed in the e-commerce space: false urgency, basket sneaking, confirm shaming, forced action, subscription traps, interface interference, bait and switch, drip pricing, disguised advertisements, nagging, trick wording, SaaS billing tricks, and rogue malware.⁷

Building on this regulatory groundwork, the Department of Consumer Affairs organised a stakeholder meeting on 28th May 2025, chaired by the Union Minister for Consumer Affairs, Food & Public Distribution and New and Renewable Energy.⁸ The meeting brought together representatives from major e-commerce companies, industry bodies, voluntary consumer organisations, and National Law Universities to discuss ways of curbing deceptive online practices.

This dialogue led directly to a follow-up measure: on 5th June 2025, the CCPA issued an advisory under the Consumer Protection Act, 2019, calling on e-commerce platforms to carry out self-audits aimed

³ Arunesh Mathur *et al.*, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 Proceedings of the ACM on Human-Computer Interaction (CSCW) 1, 1–32 (2019).

⁴ Harry Brignull, *Dark Patterns: Inside the Interfaces Designed to Trick You*, HTG Reports (2018) (originating the term "dark patterns").

⁵ Arvind Narayanan *et al.*, *Dark Patterns: Past, Present, and Future*, 18(2) ACM Queue 67, 67–92 (2020).

⁶ The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019, §2(47) (India).

⁷ Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, F. No. J-24/9/2022-CPU, Gazette of India, Nov. 30, 2023 (India), issued under §18 of the Consumer Protection Act, 2019 (Annexure 1 lists the thirteen specified dark patterns).

⁸ Ministry of Consumer Affairs, Food and Public Distribution, Government of India, Press Release: Stakeholder Meeting on Eliminating Deceptive Online Practices, May 28, 2025 (India), <https://pib.gov.in>.

at detecting dark patterns on their own sites, with the broader goal of fostering a fair, ethical, and consumer-oriented digital marketplace.⁹

Through this advisory, e-commerce platforms were directed to take active measures against engaging in dark-pattern-style deceptive practices. They were also given a three-month window from the date of the advisory to complete self-audits identifying any such patterns and to remedy them. Once these audits were done, platforms were expected to issue self-declarations confirming they were free of dark patterns, a step intended to reinforce trust between businesses and consumers while supporting a more transparent digital ecosystem.¹⁰

Alongside this, a Joint Working Group was formally set up through an Office Memorandum dated 5th June 2025.¹¹ Comprising representatives from various ministries, National Law Universities, and voluntary consumer organisations, the group's mandate is to identify dark patterns collaboratively and bring stakeholders together to build a transparent, ethical, and user-focused online environment.

Are existing consumer-protection laws in India effective enough to deal with dark patterns in e-commerce, or do digital manipulative practices require stronger, different legal regulation? This research dives into analysis of existing Indian laws and thereafter, selected approaches from other jurisdictions, particularly the European Union, will be comparatively analysed to identify effective regulatory mechanisms.

2 ANALYSING THE EFFECTIVENESS OF EXISTING CONSUMER PROTECTION LAWS IN INDIA

One study drew on a labelled dataset of over 50,000 text samples pulled from e-commerce websites, achieving 93.2% accuracy in flagging manipulative language patterns. Commonly identified deceptive phrases included false scarcity cues such as “Only a few left in stock!”, confirm-shame prompts like “Are you sure you want to miss this deal?”, and misdirection tactics such as “By continuing, you agree to our terms.” A parallel visual analysis, trained on more than 10,000 images of checkout flows, pop-ups, and other UI elements from e-commerce platforms, achieved an 89.5% detection rate for deceptive visual features including greyed-out cancel buttons, fake countdown timers, and pre-ticked opt-in checkboxes.¹²

These high accuracy rates suggest that AI-driven detection tools offer a viable route for monitoring dark patterns at scale. Beyond their immediate effect on purchasing behaviour, dark patterns were found to erode consumer trust over time. In the short term, users tend to be pressured into transactions without realising they are being manipulated; in the long term, however, this manipulation breeds distrust, driving customers away and generating negative reviews. The study reported that 74% of surveyed users expressed concern about manipulative design tactics, while 49% said they would avoid returning to a website if they felt deceived by it and platforms that relied heavily on dark patterns tended to show weaker customer retention overall.¹³ Taken together, these findings suggest that although dark patterns may yield

⁹ Central Consumer Protection Authority, Advisory in terms of Consumer Protection Act, 2019 on Self-Audit by E-Commerce Platforms for Detecting the Dark Patterns on their Platforms to Create a Fair, Ethical and Consumer Centric Digital Ecosystem, June 5, 2025 (India), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2134765>.

¹⁰ Id.

¹¹ Ministry of Consumer Affairs, Food and Public Distribution, Government of India, Office Memorandum Constituting a Joint Working Group on Dark Patterns, June 5, 2025 (India).

¹² S.V.J. Manikanta Gupta et al., Identifying and Mitigating Dark Patterns in E-Commerce Websites, SSRN, at 3 (Nov. 30, 2025), <https://ssrn.com/abstract=5832222>.

¹³ Ibid.

short-term sales gains, they ultimately come at the cost of brand reputation and long-term customer loyalty.

The working of the CCPA is best illustrated through its enforcement record rather than through the guidelines alone. Beyond issuing advisories and guidance documents, the Authority has begun translating these standards into concrete penalties against platforms found violating them.¹⁴ In one instance, an online coaching platform was penalised to the tune of Rs 3,00,000 for displaying a countdown timer that gave the false impression of a time-bound offer, a tactic meant to rush buyers into decisions they might not otherwise make so quickly. In another case, a baby-products retailer was fined Rs 2,00,000 for a pricing practice known as drip pricing – the platform had displayed prices as inclusive of tax, only to add GST separately at the point of checkout, leaving buyers to discover the actual cost later than they should have. A third instance involved an online pharmacy platform, penalised Rs 1,00,000 for quietly adding a paid membership to users' shopping carts without seeking their explicit approval beforehand.¹⁵

The clearest instance of enforcement to date remains the CCPA's Rs 7 lakh penalty imposed on Zepto Marketplace, issued through an order dated 4th December 2025 for two identified violations: drip pricing, where handling charges were disclosed only at the final stage of checkout rather than upfront, and basket sneaking, involving the automatic or pre-selected addition of a paid membership to the customer's cart. Following the order, the platform discontinued both practices.¹⁶ Zepto has since challenged the penalty before the National Consumer Disputes Redressal Commission (NCDRC), securing an interim stay on 20th January 2026, and the matter remains pending before the tribunal. Government statements made to Parliament in August 2026 listed this penalty among those collected and confirmed that the flagged features had been removed by the company. A separate notice issued by the CCPA on 4th June 2025, concerning alleged overcharging beyond the Maximum Retail Price (MRP) and alleged disguised advertisement, is also reported to remain pending.¹⁷

Complaints surrounding differential pricing have received similar public attention. Consumer testing and independent reviews have pointed to instances where identical products were priced higher for iOS users than for Android users, a pattern also observed on comparable platforms. Regulatory authorities have sought clarifications on this practice, though no conclusive, platform-specific finding of violation has yet been recorded.¹⁸

If substantiated, complaints of this kind on a high-frequency delivery platform would point to recurring consumer harm of the sort that the law on unfair trade practices is designed to address.

These examples reflect a broader pattern in how the CCPA operates: it does not merely lay down definitions and categories of dark patterns on paper but follows through with monetary penalties once

¹⁴ Himanshi Hans, *CCPA Fines Zepto, Physics Wallah, BookMyShow For Using 'Dark Patterns' To Mislead Consumers*, LawBeat (Aug. 7, 2026), <https://lawbeat.in/news-updates/ccpa-fines-zepto-physics-wallah-bookmyshow-for-using-dark-patterns-to-mislead-consumers-1620072> (reporting on written reply by B.L. Verma, Minister of State for Consumer Affairs, Food and Public Distribution, in the Rajya Sabha).

¹⁵ Rajya Sabha, Unstarred Question, Ministry of Consumer Affairs, Food and Public Distribution, Reply by B.L. Verma, Minister of State for Consumer Affairs, Food and Public Distribution, on CCPA Enforcement Action Against Dark Patterns (Rajya Sabha, Aug. 6, 2026) (India).

¹⁶ *Rajya Sabha reply*, *supra* note 15.

¹⁷ *Zepto, BookMyShow, IndiGo Among Nine Fined Nearly Rs 20 Lakh by CCPA Over Dark Patterns*, BestMediaInfo (2026), <https://bestmediainfo.com/mediainfo/mediainfo-marketing/zepto-bookmyshow-indigo-among-nine-fined-nearly-rs-20-lakh-by-ccpa-over-dark-patterns-12236513>.

¹⁸ *Inside India's Dark Pattern Crackdown: Why Zepto, BookMyShow and Others Are Under CCPA Scanner*, Outlook Business (2026), <https://www.outlookbusiness.com/news/inside-indias-dark-pattern-crackdown-why-zepto-bookmyshow-and-others-are-under-ccpa-scanner>.

violations are identified, signalling that compliance is being actively monitored rather than left to voluntary adherence alone.

3 COMPARATIVE APPROACH WITH THE EUROPEAN UNION

The first source under review is a guidance document on deceptive interface design, released in March 2022 by the European Data Protection Board (EDPB) for member states within the European Union. Its focus lies in offering developers practical direction on designing social media interfaces in a manner that avoids manipulative practices. Within this document, dark patterns are organised into six broad categories, further broken down into fifteen sub-categories, each illustrated with concrete examples. This classification framework is anchored in core data-protection principles – lawfulness, fairness, transparency, purpose limitation, and data minimisation – as they apply to interface design choices. Enforcement against violations identified under this framework operates alongside, and draws its authority from, the General Data Protection Regulation (GDPR), 2016.¹⁹

TABLE 1. *Regulation of dark patterns: CCPA (India) and EDPB (EU) compared*

Aspects	CCPA (India)	EDPB (EU)
Issuing Authority	Central Consumer Protection Authority, under the Consumer Protection Act, 2019	European Data Protection Board, under the GDPR, 2016
Year of Issuance	2023 (Guidelines); 2025 (Advisory)	2022 (v1.0); finalised 2023 (v2.0)
Legal Basis	Consumer Protection Act, 2019 (Section 18)	General Data Protection Regulation (GDPR), 2016
Primary Focus	Consumer protection and fair trade practices in e-commerce	Data protection and privacy in social media interfaces
Scope of Application	All e-commerce platforms	Primarily social media platforms (though broader relevance acknowledged)
Classification	13 specified dark patterns	6 categories, 15 sub-categories
Underlying Principles	Prevention of unfair trade practices, transparency, consumer trust	Lawfulness, fairness, transparency, purpose limitation, data minimisation
Compliance Mechanism	Self-audit by platforms + self-declaration	Recommendatory guidance for interface design
Enforcement Mechanism	Enforcement under Consumer Protection Act, 2019	Enforcement linked to GDPR provisions
Nature of Document	Regulatory guidelines + advisory	Guidelines (non-binding recommendations)

The table above sets out a comparative overview of the regulatory approaches adopted by India and the European Union in addressing dark patterns, highlighting the divergences and overlaps between the two frameworks. In India, the Central Consumer Protection Authority (CCPA), acting under the powers conferred by Section 18 of the Consumer Protection Act, 2019, has issued a dedicated set of guidelines identifying thirteen specific dark patterns prevalent in the e-commerce sector, later reinforced through a compliance-driven advisory mandating self-audits by platforms. This approach is rooted primarily in

¹⁹ European Data Protection Board, *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them* (Mar. 14, 2022) (version 1.0, for public consultation), <https://www.edpb.europa.eu>.

consumer-protection law, with an emphasis on preventing unfair trade practices and preserving consumer trust in digital transactions.²⁰

By contrast, the European framework, represented through the European Data Protection Board's (EDPB) guidelines, approaches the issue predominantly through the lens of data protection rather than consumer protection, situating dark patterns within the broader architecture of the General Data Protection Regulation (GDPR).²¹ Here, the concern is less about unfair commercial practices in the transactional sense and more about how deceptive interface design undermines core data-protection principles such as lawfulness, fairness, transparency, purpose limitation, and data minimisation. The EDPB's classification is also comparatively more granular, spanning six overarching categories and fifteen sub-categories, and its scope is centred on social media platforms rather than e-commerce broadly, even though its principles carry wider applicability.²²

Taken together, the comparison illustrates two distinct regulatory philosophies: the Indian model treats dark patterns chiefly as a consumer-protection concern enforced through sector-specific guidelines and compliance obligations, whereas the EU model treats them as a data-protection concern enforced through the overarching machinery of the GDPR.²³ This distinction is significant for the present study, as it demonstrates that the effectiveness of legal protection against dark patterns may depend considerably on which regulatory lens – consumer protection or data protection – a jurisdiction chooses to adopt.

4 CONCLUSION AND SUGGESTIONS

Concern over regulating manipulative digital design has grown steadily, as governments and regulators grapple with new and evolving forms of online manipulation aimed at swaying user behaviour. India took a meaningful step in this direction through the Consumer Protection Act, 2019, followed by the Dark Pattern Guidelines, 2023, both of which mark a significant move toward reinforcing consumer safeguards within the digital economy. Through these measures, the government has sought to curb deceptive practices online while fostering greater transparency in how digital transactions unfold.

That said, legislation alone cannot fully root out such practices. For the law to serve its intended purpose, it must be paired with robust enforcement, heightened public awareness, and an ongoing capacity to keep pace with technological change. As digital platforms lean more heavily on artificial intelligence and increasingly personalised interfaces, regulators will need to stay alert to fresh and evolving forms of manipulation that may emerge. This piece has sought to demonstrate that while the existing legal framework represents meaningful progress, its real effectiveness hinges on stronger enforcement mechanisms, more precise compliance benchmarks, and regular review of the law to keep it responsive

²⁰ Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns*, 2023, Gazette of India, Nov. 30, 2023 (India); Central Consumer Protection Authority, *Advisory in terms of Consumer Protection Act, 2019 on Self-Audit by E-Commerce Platforms for Detecting the Dark Patterns on their Platforms to Create a Fair, Ethical and Consumer Centric Digital Ecosystem*, June 5, 2025 (India).

²¹ European Data Protection Board, *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them* (Feb. 14, 2023) (version 2.0).

²² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

²³ European Data Protection Board, *supra* note 22.

to change. Striking the right balance – one that safeguards consumers without stifling innovation – is what will ultimately shape a digital marketplace that is fairer, more transparent, and more trustworthy.

* * *