Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

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.

Confirm-Shamed and Consent Trapped: Rethinking India's Regulatory Response to Algorithmic Dark Patterns in E-Commerce

Ayush Ranjan[a]

[a]Amity University, Patna, India

Received 20 August 2026; *Accepted* 21 September 2026; *Published* 25 September 2026

India's Central Consumer Protection Authority ('CCPA') has, since 2023, moved from soft admonition to active enforcement against 'dark patterns' interface designs engineered to manipulate consumer decision-making. Penalty orders in 2025 and 2026 against Zepto, Physics Wallah and McAfee Software India mark the first sustained sanctions under the Guidelines for Prevention and Regulation of Dark Patterns, 2023. This paper asks whether India's existing architecture, the Consumer Protection Act 2019, the 2023 Guidelines, the Consumer Protection (E-Commerce) Rules 2020, and the Digital Personal Data Protection Act 2023 can address dark patterns that are algorithmically generated, personalised and adaptive, rather than static. It argues that the framework, though newly energetic in enforcement, remains reactive and calibrated to isolated instances of misleading advertisement or unfair trade practice, rather than to the data-driven architecture that produces such instances at scale. Comparing this with Article 25 of the European Union's Digital Services Act, under which the European Commission fined X Corp €120 million in December 2025 for deceptive design, and the United States Federal Trade Commission's USD 2.5 billion settlement with Amazon over Prime enrolment and cancellation design, the paper contends that India lacks an ex-ante, statute-backed design-fairness obligation and a mechanism connecting its consumer-protection, data-protection and competition regulators. It proposes elevating core dark-pattern prohibitions from guideline to statutory rule, mandating periodic algorithmic design audits for high-traffic platforms, linking penalties to platform revenue, and establishing an information-sharing protocol between the CCPA, the Data Protection Board of India and the Competition

Commission of India. The thesis is not that India has failed to act, but that it has acted at the wrong layer, addressing symptoms of manipulation one order at a time, while leaving the design systems that generate them substantially unregulated.

Keywords: *consent, competition, consumer protection.*

INTRODUCTION

Between December 2025 and August 2026, the CCPA imposed penalties totalling approximately ₹20,00,000 on platforms including Zepto, FirstCry, PharmEasy, McAfee and Physics Wallah for practices ranging from drip pricing to pre-selected donations disguised as neutral defaults. The McAfee order is instructive: the platform's subscription-renewal interface offered users a choice between 'Renew Now' and 'Accept Risk,' a framing the CCPA held to be deceptive precisely because it exploited, rather than informed, the user's decision-making.[1] These are not isolated design errors. They are outputs of interfaces that are increasingly generated, tested and iterated algorithmically through A/B testing, behavioural analytics and personalisation engines so that the specific manipulative prompt a given consumer sees may itself be the product of an optimisation process invisible to both the consumer and the regulator.

RESEARCH QUESTION

This paper asks: can India's existing consumer-protection and data-protection architecture meaningfully govern dark patterns once they are produced algorithmically and adaptively, rather than designed once and deployed uniformly?

THESIS

The paper argues that India's existing regulatory architecture is inadequate to address algorithmically generated and adaptive dark patterns in its present form. The Consumer Protection Act 2019 and the 2023 Guidelines issued under it operate primarily through ex

[1] Aakriti Bansal, 'Consumer protection authority fines PhysicsWallah and McAfee for dark patterns: what counts as consent now?' (*Medianama,* 04 June 2026) <https://www.medianama.com/2026/06/223-consumer-protection-authority-fines-physicswallah-and-mcafee-for-dark-patterns-what-counts-as-consent-now/> accessed 12 August 2026; 'Zepto, Physics Wallah Among 7 Firms Fined For Misleading Online Practices' *NDTV* (06 August 2026) <https://www.ndtv.com/india-news/zepto-physics-wallah-among-7-firms-fined-for-misleading-online-practices-11875891> accessed 12 August 2026

post intervention against identifiable instances of deceptive design. The Digital Personal Data Protection Act 2023 addresses consent but does not specifically regulate manipulative interface design, while the Competition Act 2002[2] is structurally less equipped to address individual-level manipulation in the absence of market dominance or other relevant competition concerns. Consequently, the existing framework is better suited to sanctioning a particular platform's identifiable interface after the fact than to addressing the systemic, iterative and personalised nature of algorithmic dark patterns.

THE NATURE OF THE PROBLEM: FROM STATIC DECEPTION TO ADAPTIVE MANIPULATION

Classical unfair-trade-practice law, including India's, was built to address a static misrepresentation, a false claim printed on a label or spoken in an advertisement, verifiable once and prohibited thereafter. Algorithmic dark patterns depart from this model in three respects.

First, they are personalised; the interface a consumer sees may be selected from among several variants based on that consumer's browsing history, purchase propensity or even emotional state as inferred from behavioural signals.

Second, they are iterative: platforms routinely test which framing, 'Accept Risk' or 'No Thanks, I Don't Want Protection', yields higher conversion, and deploy the version that performs best, meaning the manipulative element is optimised rather than merely present.

Third, they are cumulative; a single session may combine false urgency, a pre-ticked donation and confirm-shaming language, each individually defensible but jointly designed to overwhelm deliberation.[3] The CCPA's own Guidelines recognise thirteen categories of dark pattern, from basket sneaking to trick questions, but expressly caution that the list is illustrative rather than binding, leaving each new algorithmic variant to be litigated afresh.

[2] Competition Act 2002

[3] Guidelines for Prevention and Regulation of Dark Patterns 2023; Ansruta Debnath and Shubham Singh, 'Evaluating India's Dark Patterns Guidelines – Advocating a Comprehensive Approach' (*Law School Policy Review,* 04 March 2024) <https://lawschoolpolicyreview.com/2024/03/04/evaluating-indias-dark-patterns-guidelines-advocating-a-comprehensive-approach/> accessed 12 August 2026

Recent scholarship on Indian quick-commerce applications confirms that platforms continue to exploit design choices that are 'technically legal but functionally deceptive,' precisely because enforcement proceeds pattern-by-pattern rather than through an obligation on the design process itself.[4] The consumer-welfare harm is accordingly not confined to the transaction in question; it lies in the erosion of the very capacity for informed choice that consumer law exists to protect.

THE INDIAN LEGAL FRAMEWORK

India's response rests on four instruments:

First, the Consumer Protection Act 2019 defines 'misleading advertisement' and 'unfair trade practice' broadly enough to capture manipulative platforms that continue to exploit design loopholes that are 'technically legal but functionally deceptive' notwithstanding the 2023 Guidelines. Digital design, and empowers the CCPA under section 18 to investigate and act.[5]

Second, the Guidelines for Prevention and Regulation of Dark Patterns, 2023, notified under that section 18 power, are the first instrument in India to define 'dark pattern' as a term of art and to list specific prohibited practices.[6]

Third, the Consumer Protection (E-Commerce) Rules 2020 impose more granular obligations on marketplace and inventory e-commerce entities; Rule 4(9), invoked in the PhysicsWallah order, requires explicit and affirmative consumer action before any pre-selected charge is applied, precisely the basket-sneaking mechanism the CCPA penalised.[7]

Fourth, the Digital Personal Data Protection Act 2023 requires that consent for processing personal data be 'free, specific, informed, unconditional and unambiguous,' a standard that, if actively enforced, would independently constrain the data-driven personalisation that makes algorithmic dark patterns possible.[8]

---

[4] Tanish Taneja et al., 'Dark Patterns in Indian Quick Commerce Apps: A Student Perspective' (*arxiv,* 02 April 2026) <https://doi.org/10.48550/arXiv.2604.02257> accessed 12 August 2026
[5] Consumer Protection Act 2019, s 18
[6] Bansal (n 1)
[7] Consumer Protection (E-Commerce) Rules 2020
[8] Digital Personal Data Protection Act 2023

Taken together, these instruments give the CCPA real enforcement teeth, as the 2026 orders demonstrate: the Authority rejected McAfee's argument that an absence of individual complaints indicated an absence of harm, holding instead that dark patterns operate precisely by suppressing overt objection while steering behaviour.[9]

Yet the framework's structure remains instructive of its limits. The core prohibitions live in a Guideline issued under section 18 rather than in the Act or in rules with independent statutory force, so their content can be revised administratively, and their violation carries the penalty architecture of section 21: a maximum of ₹10,00,000 for a misleading advertisement, a sum fixed without reference to the scale of algorithmic deployment or platform revenue.[10] Nor does the DPDP Act's consent standard, though textually robust, reach interface design directly; a platform can obtain technically compliant consent to data processing while still deploying a manipulative purchase flow, because the two statutes govern different moments in the same transaction and are enforced by different bodies with no formal channel between them.[11]

COMPARATIVE PERSPECTIVE: THE EUROPEAN UNION AND THE UNITED STATES

The European Union has gone furthest in codifying an ex-ante design obligation. Article 25 of the Digital Services Act prohibits online platforms from designing, organising or operating their interfaces in a way that deceives, manipulates, or otherwise materially distorts or impairs a recipient's ability to make free and informed decisions a standalone obligation on the design system itself, not merely on individual advertisements.[12] Its force was demonstrated in December 2025, when the European Commission's first formal non-compliance decision under the DSA fined X Corp €120 million partly for the deceptive design of its 'blue checkmark' verification badge, which continued to imply identity verification after the badge became purchasable without any such check.[13] Article 25 is not without

[9] Bansal (n 1)
[10] Consumer Protection Act 2019, s 21
[11] Digital Personal Data Protection Act 2023
[12] Digital Services Act 2022, art 25
[13] Liv McMahon, 'US hits out at EU's 'suffocating regulations' after it fines Elon Musk's X' *BBC* (05 December 2025) <https://www.bbc.com/news/articles/c4g9kejzvw0o> accessed 12 August 2026; Fabrizio Esposito et al., 'Back to the Future-Proof: Four Reforms for the Better Regulation of Dark Patterns Under the Unfair Commercial Practices Directive and Article 25 of the Digital Services Act' (2026) European Journal of Risk Regulation <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/back-

weaknesses; commentators note its uncertain relationship with the older Unfair Commercial Practices Directive and a narrower subjective scope than that Directive[14], but its existence as a freestanding design obligation, independent of any single advertisement or transaction, is precisely what India's framework lacks. The United States, lacking an omnibus federal privacy or platform-design statute, has instead relied on aggressive application of existing consumer-protection tools. The Federal Trade Commission's 2023 suit against Amazon, settled in September 2025 for USD 2.5 billion, alleged that Amazon's Prime enrolment and cancellation flows violated both section 5 of the FTC Act and the Restore Online Shoppers' Confidence Act, which independently requires clear disclosure of subscription terms, express informed consent, and a cancellation mechanism as simple as enrolment.[15] The settlement's significance for comparative purposes lies less in the sum than in its structure: a dedicated negative-option statute (ROSCA) operating alongside general unfair-practices authority, together with a civil penalty scaled to the harm's magnitude 35 million affected consumers rather than to a statutory ceiling. Both jurisdictions thus supply what India presently does not: the EU through a freestanding, ex ante design obligation, and the US through a dedicated subscription-specific statute combined with penalties scaled to actual reach.

CRITICAL ANALYSIS: REGULATORY GAPS

Three gaps follow from this comparison:

The first is normative placement: India's prohibition on dark patterns exists as CCPA Guidelines rather than as a rule with independent statutory force or a provision within the Act itself, leaving its content administratively revisable and its authority contestable in a way Article 25 is not.

The second is quantum: section 21's penalty ceiling of ₹10,00,000, and the modest sums actually imposed ₹1,00,000 on McAfee, ₹5,00,000 on PhysicsWallah bear no relationship to platform revenue or to the number of consumers exposed to a given algorithmically

to-the-futureproof-four-reforms-for-the-better-regulation-of-dark-patterns-under-the-unfair-commercial-practices-directive-and-article-25-of-the-digital-services-act/B2C04326235DD360A456762AEB5BAB76> accessed 12 August 2026

[14] Digital Services Act 2022, art 25

[15] Federal Trade Commission Act 1914, s 5; Restore Online Shoppers' Confidence Act 2010

deployed pattern, in contrast to the FTC's billion-dollar redress calibrated to 35 million affected users.[16]

The third, and most significant for algorithmic manipulation specifically, is institutional fragmentation. Interface design implicates consumer protection (the CCPA), data-driven personalisation implicates data protection (the Data Protection Board of India under the DPDP Act), and platform-scale deployment of a manipulative design against a captive user base can implicate competition concerns (the Competition Commission of India), yet no statutory mechanism requires these three bodies to share findings arising from a single instance of algorithmic manipulation.[17]

A platform found to have deployed a personalised dark pattern by the CCPA faces no automatic referral to the Data Protection Board to examine whether the underlying personalisation itself breached section 6 consent standards, nor to the CCI to examine whether the practice reflects a broader pattern of exploitative conduct. Enforcement therefore proceeds in silos, each addressing a slice of what is, in the algorithmic context, a single integrated harm. A further, procedural gap compounds this: dark-pattern proceedings to date have been initiated suo motu by the CCPA rather than through consumer-led collective complaints under section 20, reflecting the reality that individual consumers rarely recognise algorithmic manipulation as such, which is, after all, the point of the design.[18]

RECOMMENDATIONS

Four reforms would address these gaps without requiring wholesale statutory reconstruction:

First, the core prohibitions presently in the 2023 Guidelines should be elevated into binding rules under the Consumer Protection Act 2019, removing the interpretive uncertainty that flows from their current status as guidance rather than a binding, exhaustive standard.[19]

[16] Bansal (n 1)
[17] Digital Personal Data Protection Act 2023; Competition Act 2002
[18] Consumer Protection Act 2019, ss 6 and 20; 'CCPA Acts Against Dark Patterns on Digital Platforms' (*PIB,* 03 June 2026) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2268302&reg=3&lang=1> accessed 12 August 2026
[19] Guidelines for Prevention and Regulation of Dark Patterns 2023

Second, high-traffic e-commerce, ed-tech and digital-service platforms above a prescribed user threshold should be subject to a periodic algorithmic design audit requirement, administered by the CCPA in coordination with the Data Protection Board, examining not individual interfaces but the A/B-testing and personalisation systems that generate them, addressing the adaptive character of algorithmic dark patterns identified in Part II.

Third, penalties under section 21 should be recalibrated, for repeat or platform-scale violations, from a fixed statutory ceiling to a formula tied to a percentage of the platform's India-derived revenue, following the logic (though not necessarily the scale) of the FTC's redress calculation and of competition-law turnover-based penalties already familiar under the Competition Act.[20]

Fourth, a formal information-sharing protocol should be established among the CCPA, the Data Protection Board of India and the Competition Commission of India, requiring automatic cross-referral whenever a dark-pattern finding by one body raises questions properly within another's jurisdiction, so that a single algorithmic harm no longer generates three independent and uncoordinated proceedings, or none at all beyond the first.[21] None of these reforms requires abandoning the CCPA's existing enforcement momentum; they instead ask that the layer at which India regulates be moved upstream, from the individual interface to the system that produces it.

CONCLUSION

India's dark-pattern enforcement since 2023, and particularly the 2025–2026 orders against Zepto, PhysicsWallah and McAfee, demonstrates real regulatory will and a CCPA increasingly comfortable rejecting platforms' procedural defences.[22] But enforcement energy directed at a legal architecture built for static, one-off misrepresentation cannot, on its own, govern manipulation that is algorithmically generated, personalised and continuously optimised. The European Union's Article 25 and the United States' combination of ROSCA and FTC Act enforcement each supply, in different ways, an obligation pitched at the level of the design system rather than the individual instance.[23] India's task is not to import either

[20] Restore Online Shoppers' Confidence Act 2010
[21] Consumer Protection Act 2019
[22] Bansal (n 1)
[23] Digital Services Act 2022

model wholesale but to translate its own instrument, the Consumer Protection Act 2019, read together with the DPDP Act 2023 and a reformed Competition Act interface, into a framework that treats algorithmic design itself, and not merely its output, as the proper object of consumer-welfare regulation.