

International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham



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.

Digital Consumer Protection in India: The Case for Structural Redesign in the Age of Dark Patterns

Ravi Raj^a

^aUniversity School of Law and Legal Studies, GGSIPU, New Delhi, India

Received 13 March 2026; Accepted 13 April 2026; Published 17 April 2026

The rapid expansion of digital commerce has transformed the architecture of consumer decision-making, shifting influence from overt representations to embedded interface design. In this environment, so-called “dark patterns”¹ exploit behavioural biases² and asymmetries of information to distort consumer autonomy without necessarily engaging in traditional misrepresentation. India’s existing consumer protection framework, primarily structured around unfair trade practices and misleading advertisements, remains inadequately equipped to address such design-based manipulation. Recent regulatory efforts, while significant, operate within a legal architecture not originally designed for algorithmic governance. This article argues that the proliferation of dark patterns reveals a structural deficiency in India’s digital consumer protection regime. Incremental reform or guideline-based interventions are insufficient. Instead, a comprehensive structural redesign is necessary—one that explicitly recognises interface manipulation, recalibrates evidentiary burdens, establishes specialised institutional oversight, and integrates transparency with proportional enforcement. To substantiate this claim, the article advances a model legislative framework aimed at restoring meaningful consumer autonomy while safeguarding innovation and economic freedom. The proposed approach seeks to reorient digital consumer governance from reactive redressal toward proactive architectural accountability.

¹ ‘What are deceptive patterns?’ (Deceptive Patterns) <<https://www.deceptive.design/>> accessed 13 February 2026

² *Dark Commercial Patterns* (OECD Publishing 2022)

Keywords: *dark patterns, digital consumer protection, digital market regulation, structural reforms.*

INTRODUCTION

The rapid expansion of digital commerce has transformed the way consumers make decisions. Transactions that once took place in physical marketplaces are now mediated through algorithmic interfaces, personalised recommendations, and carefully designed digital environments. In this setting, influence is no longer exercised only through price or advertisement; it is embedded within design itself. Default settings, subscription flows, countdown timers, and ranking mechanisms shape consumer choices in ways that are often subtle and difficult to detect.

This transformation has led to the rise of what are commonly known as ‘dark patterns’ that exploit behavioural biases and information asymmetries to steer consumers toward decisions they might not otherwise make. Unlike traditional deception, dark patterns rarely depend on false statements. Instead, they operate by structuring the conditions under which consent is formed. The concern, therefore, is not merely unfairness in outcomes but distortion of consumer autonomy at the stage of decision-making.

India’s existing consumer protection framework, particularly under the Consumer Protection Act, 2019, was primarily designed to address misleading advertisements, defective goods, and unfair trade practices. These categories focus on misrepresentation or contractual imbalance. However, design-based manipulation embedded within digital interfaces does not fit easily within these traditional doctrines. When harm arises from the architecture of choice rather than explicit falsehoods, existing legal tools reveal their limitations.

Although recent regulatory efforts have acknowledged dark patterns, these measures remain incremental and operate within a framework not originally structured to address algorithmic influence or behavioural engineering. As digital markets become increasingly complex, reactive enforcement and fragmented oversight are insufficient to address systemic distortions of consumer choice.

This article argues that the proliferation of dark patterns exposes a structural deficiency in India's digital consumer protection regime. Incremental reform is inadequate. What is required is a structural redesign—one that expressly recognises interface manipulation, recalibrates evidentiary burdens in light of informational asymmetry, establishes specialised institutional oversight, and balances transparency with innovation. To illustrate this approach, the article proposes a model legislative framework aimed at restoring meaningful consumer autonomy while preserving economic freedom in the digital marketplace.

WHAT ARE DARK PATTERNS? CONCEPTUAL AMBIGUITY AND COMPARATIVE REGULATION

Any argument for structural reform must begin with conceptual precision. Yet defining 'dark patterns' is itself a regulatory challenge. The term, first popularised in design scholarship,³ broadly refers to digital interface practices that manipulate user behaviour by exploiting cognitive biases, asymmetries of information, or behavioural vulnerabilities. Unlike traditional deception, dark patterns typically do not involve false representations. Instead, they operate through the architecture of choice – shaping how options are presented, sequenced, and prioritised.

Examples include subscription traps that complicate cancellation, asymmetrical consent interfaces that make acceptance more prominent than rejection, false urgency cues, hidden costs revealed late in the transaction process, and default settings that favour data disclosure. In each instance, the consumer formally retains the ability to choose. However, the conditions under which that choice is exercised are strategically engineered to produce predictable behavioural outcomes. Dark patterns, by contrast, influence pre-contractual cognition. They distort the decision-making environment itself. The harm is not merely transactional but structural.

The European Union: Rights-Based Recognition and Its Limits: The European Union has been the most explicit in recognising the autonomy dimension of digital manipulation. Under the General Data Protection Regulation (GDPR),⁴ consent must be freely given, specific, informed and unambiguous. Regulatory guidance from European Data Protection Authorities

³ Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press 2008)

⁴ General Data Protection Regulation 2016

has clarified that consent obtained through manipulative interface design, such as visually deceptive consent banners or disproportionate friction in opt-out mechanisms, may be considered invalid.⁵ The emphasis is not solely on disclosure but on the quality of voluntariness.

Further, the Digital Services Act (DSA) explicitly prohibits online platforms from designing or organising interfaces in ways that deceive or materially distort user decision-making. This marks a doctrinal shift: the law recognises choice architecture itself as a site of regulatory concern.⁶ However, despite this conceptual strength, the EU approach faces structural challenges. Enforcement authority is distributed across multiple regulators, including data protection authorities and consumer protection bodies, creating institutional fragmentation.

The United States: Enforcement-Driven Flexibility and Reactive Governance: In contrast, the United States relies primarily on broad unfairness and deception standards under the authority of the Federal Trade Commission (FTC).⁷ Rather than defining dark patterns legislatively, regulators pursue specific practices – such as subscription traps or misleading cancellation mechanisms through case-by-case enforcement.⁸ Certain state-level laws, including the California Consumer Privacy Act (CCPA),⁹ address manipulative consent mechanisms in data processing contexts, but without establishing a comprehensive architectural prohibition.

The American model offers flexibility and avoids heavy ex ante regulation. However, it remains largely reactive. Enforcement depends on regulatory discretion and political priorities. Absent explicit statutory recognition of design-based manipulation, businesses may operate within grey zones until challenged. This creates uncertainty and uneven deterrence.

The United Kingdom: Fairness Doctrine Without Structural Redesign: The United Kingdom, through investigations by the Competition and Markets Authority (CMA),¹⁰ has scrutinised online choice architecture practices under general consumer protection law. While

⁵ *Guidelines 05/2020 on Consent under Regulation 2016/679* (European Data Protection Board 2020)

⁶ Digital Services Act 2022

⁷ Federal Trade Commission Act 1914

⁸ *Bringing Dark Patterns to Light* (Federal Trade Commission 2022)

⁹ California Consumer Privacy Act 2018

¹⁰ *Online Choice Architecture: How digital design can harm competition and consumers 2022* (Competition and Market Authority 2022)

reports have acknowledged the manipulative potential of interface design, regulation remains grounded in traditional fairness and misrepresentation standards.

This approach shares the United States' incremental character. It adapts existing doctrines rather than reconstructing institutional architecture. While such flexibility may reduce regulatory overreach, it does not directly confront the systemic embedding of behavioural manipulation within digital platforms.

The Definitional Tension: Persuasion, Manipulation, and Autonomy: Comparative experience reveals a persistent definitional tension. If dark patterns are defined too broadly, ordinary persuasive design may fall within regulatory prohibition, potentially stifling innovation and commercial expression. If defined too narrowly, consumer autonomy remains unregulated.

The difficulty lies in distinguishing between permissible 'nudging' and impermissible manipulation. Behavioural economics recognises that all choice architecture influences decisions to some degree. The normative threshold, therefore, must turn on material impairment of autonomy rather than mere influence. The European model gestures toward this distinction by grounding regulation in the quality of consent, whereas the U.S. and UK approaches rely more heavily on demonstrable consumer harm.

Yet none of these jurisdictions fully resolves the structural problem. Dark patterns are often embedded at scale, personalised through algorithmic profiling, and continuously modified through experimentation. Proving individual harm or deception may be insufficient to address systemic distortions occurring in real time. Moreover, fragmented regulatory competence may weaken oversight.

Structural Implications: The comparative analysis demonstrates that dark patterns are not merely instances of unfair practice but manifestations of a broader governance challenge in digital markets. They reveal the limits of regulatory models built around post-facto harm, disclosure-based compliance, or isolated enforcement actions. The central issue is architectural: how to regulate the conditions under which consent is formed without undermining innovation or legitimate persuasion.

Recognising dark patterns as distortions of meaningful autonomy exposes the inadequacy of purely incremental reform. While international models offer valuable lessons, they also illustrate

the need for institutional coherence, proportional safeguards, and explicit statutory articulation tailored to domestic conditions. For India, where digital commerce is expanding rapidly across diverse economic actors, the question is not whether to regulate dark patterns, but how to design a framework capable of addressing them structurally rather than episodically.

WHY EXISTING INDIAN LAW REMAINS STRUCTURALLY INADEQUATE?

India has taken important steps toward strengthening consumer protection, yet its existing framework remains structurally ill-suited to regulate design-based manipulation in digital markets. The limitation lies less in regulatory intent and more in the architecture of the law itself.

The Consumer Protection Act, 2019 (CPA 2019)¹¹ is primarily designed to address misleading advertisements, unfair trade practices, and defective goods or services. Its doctrinal foundations assume that harm arises from misrepresentation, false claims, or contractual imbalance.¹² Dark patterns, however, often involve no explicit falsity. A pre-selected consent box, a subscription flow that complicates cancellation, or an interface that visually emphasises acceptance over rejection may not amount to deception in the traditional sense. Yet such practices can materially impair decision-making. The Act does not expressly recognise distortion of autonomy through interface architecture as an independent ground of liability.

The institutional structure reinforces this limitation. The Central Consumer Protection Authority (CCPA) possesses investigative and enforcement powers, but its model remains largely reactive. Intervention typically follows complaints or identifiable violations. In digital markets where manipulation is embedded in design and continuously refined through algorithmic experimentation, post-facto enforcement struggles to address systemic harms.

The Guidelines for Prevention and Regulation of Dark Patterns 2023¹³ acknowledge manipulative practices and represent a significant regulatory development. However, they operate within the broader CPA framework and do not restructure institutional oversight or evidentiary standards. Their executive character may also limit long-term doctrinal stability compared to statutory reform.

¹¹ Consumer Protection Act 2019

¹² Consumer Protection Act 2019, ss 10–27

¹³ Guidelines for Prevention and Regulation of Dark Patterns 2023

Similarly, the Digital Personal Data Protection Act, 2023 (DPDP Act)¹⁴ addresses consent in the context of data processing, but it does not comprehensively regulate commercial interface manipulation unrelated to personal data.

More fundamentally, existing law is outcome-oriented. It focuses on compensating identifiable harm after a transaction has occurred. Dark patterns, by contrast, distort the conditions under which consent is formed. The injury is often diffuse, cumulative, and embedded within behavioural architecture rather than easily quantifiable loss. Coupled with acute informational asymmetry between platforms and consumers, the current evidentiary model places a disproportionate burden on individuals. Taken together, these features reveal a structural misalignment. India's consumer protection regime was crafted for markets shaped by informational asymmetry in representation, not behavioural engineering in interface design. Incremental adaptation may capture isolated practices, but it does not provide a coherent framework for supervising digital choice architecture. The inadequacy is therefore architectural rather than incidental, necessitating reconsideration of institutional design rather than mere doctrinal extension.

A STRUCTURAL REDESIGN OF DIGITAL CONSUMER GOVERNANCE: A MODEL FRAMEWORK

If dark patterns represent distortions embedded within digital choice architecture, the regulatory response must be architectural in character. Incremental expansion of existing doctrines cannot adequately address systemic design-based manipulation. What is required is a coherent framework that recognises interface influence, recalibrates enforcement mechanisms, and harmonises consumer autonomy with innovation. To illustrate how such a structural redesign may be operationalised, this section outlines a model legislative framework organised around four interrelated pillars: substantive recognition, institutional oversight, procedural recalibration, and proportional compliance.

Substantive Recognition of Design-Based Manipulation: The first pillar of structural reform is explicit statutory recognition of dark patterns as a distinct category of harm. Rather than subsuming interface manipulation within general unfair trade practices, the law must

¹⁴ Digital Personal Data Protection Act 2023

acknowledge that design itself can impair meaningful autonomy. Such recognition should be anchored in a clear definition that focuses on material distortion of consumer choice, rather than mere influence. The regulatory threshold must distinguish between legitimate persuasion and manipulative architecture that exploits cognitive vulnerabilities. This approach shifts attention from transactional outcomes to the conditions under which consent is formed.

In addition, special protection for vulnerable consumers such as minors, digitally illiterate users, or economically dependent individuals ensures that regulation accounts for differential susceptibility to behavioural manipulation. This moves consumer protection beyond a formal equality model toward substantive fairness.

Institutional Oversight Tailored to Digital Markets: The second pillar concerns institutional design. Digital markets are technologically complex and rapidly evolving. Traditional consumer forums, designed for individual grievances concerning defective goods or misleading advertisements, may lack the technical expertise required to supervise algorithmic design practices.

A specialised authority with supervisory, adjudicatory, and facilitative functions would enable coherent oversight of digital commerce practices. Importantly, such an authority must operate within clear constitutional safeguards, adhering to proportionality, natural justice, and non-interference with content regulation or price control. The objective is not expansive state surveillance but calibrated supervision of design-based harm. Decentralised redressal mechanisms, supported by technical expertise, would ensure accessibility while preventing concentration of regulatory power. Structural redesign, therefore, involves not only substantive prohibition but institutional competence aligned with contemporary market realities.

Procedural Recalibration and Evidentiary Balance: The third pillar addresses informational asymmetry. In cases involving digital interface manipulation, platforms possess exclusive control over behavioural data, interface experimentation, and internal decision-making processes. Requiring consumers to prove deception or harm without access to such information risks rendering enforcement ineffective.

A recalibrated evidentiary framework, where the burden shifts to the platform once a prima facie impairment of choice is demonstrated, which reflects the structural imbalance inherent in digital

markets. This approach does not impose strict liability but aligns procedural standards with technological realities. Further, time-bound digital redressal mechanisms are essential. Harm in digital environments occurs rapidly and often at scale. Delayed adjudication weakens deterrence and undermines consumer trust. Structural reform, therefore, includes procedural efficiency as a core component of autonomy protection.

Transparency and Proportionate Compliance: The fourth pillar integrates transparency with economic inclusion. Rather than imposing intrusive disclosure of proprietary algorithms, a calibrated transparency regime may require platforms to disclose material factors influencing ranking, recommendation, or subscription practices. This enhances informed decision-making without mandating exposure of trade secrets.

Equally important is proportional compliance. Micro and small enterprises form a substantial segment of India's digital economy. Structural redesign must avoid imposing disproportionate regulatory burdens that create entry barriers or chill innovation. Risk-based audits, graded penalties, and voluntary trust certifications can promote cooperative compliance rather than adversarial enforcement. By combining substantive clarity, institutional competence, procedural balance, and proportional oversight, the proposed framework reorients digital consumer protection from reactive compensation toward proactive architectural accountability.

From Incremental Reform to Architectural Governance: The central insight of structural redesign is that digital markets cannot be effectively regulated through doctrines conceived for physical marketplaces. When harm is embedded within interface design and algorithmic optimisation, governance must address the architecture of influence itself.

The proposed framework does not seek to duplicate existing consumer protection mechanisms but to complement and recalibrate them for the digital age. It recognises that meaningful autonomy in online markets depends not only on truthful disclosure but on the integrity of the decision-making environment. In this sense, structural redesign represents not regulatory expansion but regulatory alignment, bringing institutional architecture into coherence with technological transformation.

CONSTITUTIONAL FOUNDATIONS AND NORMATIVE JUSTIFICATION

Structural redesign of digital consumer governance is not merely a policy preference; it finds support within constitutional doctrine. As digital markets increasingly shape economic participation and personal decision-making, the protection of consumer autonomy assumes constitutional significance.

The Supreme Court's recognition of informational privacy and decisional autonomy in Justice K.S. Puttaswamy v Union of India¹⁵ established that autonomy is central to constitutional dignity. While the judgment arose in the context of data protection, its reasoning extends beyond informational control. When digital interfaces manipulate behavioural vulnerabilities or impair meaningful choice, the concern is not confined to commercial fairness but implicates autonomy itself. Regulation aimed at preserving authentic consent is therefore consistent with constitutional values.

At the same time, structural redesign must respect economic freedom under Article 19(1)(g).¹⁶ Commercial innovation and digital entrepreneurship are protected interests. However, as affirmed in *Modern Dental College v State of Madhya Pradesh*,¹⁷ restrictions on economic activity are constitutionally valid when proportionate to legitimate regulatory objectives. Preventing material distortion of consumer autonomy qualifies as such an objective. A framework grounded in proportionality – eschewing content control, price regulation, or intrusive surveillance – remains aligned with constitutional limits.

The principle of non-arbitrariness under Article 14¹⁸ further reinforces the need for coherent institutional design. Fragmented oversight and reactive enforcement risk inconsistent application. Structural redesign, by clarifying standards and aligning institutional competence with technological realities, promotes predictability and fairness in governance.

Finally, consumer protection has long been treated as social welfare legislation, warranting purposive interpretation, as observed in *Lucknow Development Authority v M.K. Gupta*.¹⁹ In the

¹⁵ *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1

¹⁶ Constitution of India 1950, arts 14 and 19(1)(g)

¹⁷ *Modern Dental College and Research Centre and Ors v State of Madhya Pradesh and Ors* (2016) 7 SCC 353

¹⁸ *Ibid*

¹⁹ *Lucknow Development Authority v MK Gupta* (1994) 1 SCC 243

digital context, purposive interpretation requires recognition that harm may arise not only from defective goods or misrepresentation but from systemic distortion of decision-making environments. Thus, structural redesign does not represent regulatory overreach. Rather, it reflects constitutional calibration – balancing autonomy, proportionality, economic freedom, and fairness. By addressing design-based manipulation through measured institutional reform, digital consumer governance can remain both innovation-friendly and autonomy-protective.

CONCLUSION

The regulation of dark patterns presents more than a narrow consumer protection issue; it raises foundational questions about autonomy, fairness, and the architecture of digital markets. As commercial influence increasingly operates through interface design rather than explicit representation, traditional legal categories reveal their structural limits. Deception is no longer confined to false statements – it may be embedded within the very environment in which consent is formed.

Comparative experience demonstrates that jurisdictions across the world are grappling with this challenge, yet most responses remain either fragmented or reactive. India's existing framework, while robust in addressing misleading practices and defective transactions, was not designed to supervise algorithmic choice architecture. Incremental adaptation risks perpetuating doctrinal strain and institutional fragmentation.

This article has argued that the proliferation of dark patterns exposes a structural deficiency in digital consumer governance. The appropriate response is not merely expanded enforcement but architectural recalibration. By explicitly recognising design-based manipulation, recalibrating evidentiary burdens, establishing specialised yet proportionate institutional oversight, and integrating transparency with economic inclusion, regulatory design can align with technological transformation.

Structural redesign does not entail regulatory excess. Properly calibrated, it advances constitutional values of autonomy and fairness while preserving innovation and ease of doing business. In doing so, it reorients digital consumer protection from reactive compensation toward proactive safeguarding of meaningful choice.

In an economy increasingly mediated by algorithms, the integrity of consent cannot be left to interface design alone. Governance must evolve alongside technology. The challenge, therefore, is not whether digital markets should remain free but whether that freedom can be meaningful without structural accountability.