



International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

Dark Patterns in E-Commerce: An Analysis of Consumer Protection, Legal Accountability, and Regulatory Challenges in India

Mranal Singh Chouhan

B.A. LL.B. , National Law Institute University, Bhopal

Mranalchouhan.ballb@nliu.ac.in

ABSTRACT

Digital commerce increasingly relies on interface design to guide consumers through search, selection, payment, subscriptions, and post-purchase interactions. Some design choices help consumers navigate complex services; others exploit cognitive biases or create friction that pushes users toward choices they would not otherwise make. These practices are commonly described as “dark patterns”. They raise legal questions about deception, informed consent, unfair trade practices, platform accountability, and the practical effectiveness of consumer remedies.

This paper critically examines India’s legal framework governing dark patterns in e-commerce, with particular emphasis on the Consumer Protection Act, 2019; the Consumer Protection (E-Commerce) Rules, 2020; the Guidelines for Prevention and Regulation of Dark Patterns, 2023; and the Central Consumer Protection Authority’s June 2025 advisory encouraging e-commerce platforms to conduct self-audits. It also considers the relationship between consumer protection, contract principles, data protection, and comparative approaches in the European Union and the United States. The analysis is doctrinal and desk-based: it interprets legislation, subordinate instruments, official government materials, reported decisions and selected academic commentary. It does not purport to present original empirical findings.

The paper argues that India has developed a meaningful regulatory foundation, including an enumerated list of thirteen dark patterns, but that the effectiveness of this framework depends on evidence preservation, transparent enforcement, clear allocation of responsibility across platforms and sellers, accessible redress, and regular review of emerging design practices. It recommends risk-based interface audits, standardised disclosures, cancellation symmetry, clearer consent architecture, publication of enforcement outcomes, and coordinated institutional action. The paper also distinguishes rules currently in force from the Consumer Protection (E-Commerce) (Amendment) Rules, 2026, announced in September 2026 and scheduled to commence on 1 January 2027.

Keywords: dark patterns; consumer protection; e-commerce; Consumer Protection Act 2019; CCPA; unfair trade practices; digital markets; informed consent; platform accountability.

Research Note and Scope

This manuscript is a doctrinal research draft prepared for a law student to review, personalise, and develop. It is not a guarantee of publication and should not be submitted unchanged. A publishable version requires independent verification of all primary legal materials, completion of the literature review, adherence to the target journal’s citation rules, and an originality check. The author should replace the cover placeholders and ensure that the final work reflects their own analysis.

Legal position is stated as at 12 October 2026. The 2026 E-Commerce Amendment Rules are discussed as a notified future change with a commencement date of 1 January 2027, not as rules already in force.

1. Introduction

Digital marketplaces have changed not only where consumers buy goods and services but also how commercial choices are presented. A consumer may compare products, read reviews, select delivery options, accept recurring payments, authorise data processing, and cancel a service without interacting with a human representative. The interface is therefore more than a neutral channel. It structures the available options, the information that is visible, the sequence in which decisions are made, and the effort required to accept or reject a proposal.

Choice architecture is not inherently unlawful. Clear defaults, sensible grouping, reminders, and simplified forms can reduce transaction costs and help consumers make informed decisions. The legal difficulty arises when design is used to mislead, coerce, conceal material information, or make refusal

materially harder than acceptance. A countdown timer that falsely implies scarcity, a pre-selected add-on, a price that increases only at checkout, or a cancellation path deliberately buried behind repeated screens may impair meaningful consumer choice.

The term “dark patterns” is used in policy and scholarship to describe user-interface practices that steer, deceive, manipulate, or obstruct users in ways that undermine their autonomy or interests. The literature shows that these techniques can affect purchasing decisions and data disclosure. Jamie Luguri and Lior Jacob Strahilevitz’s experimental work analyses how manipulative interfaces can alter consumer decisions, while the United States Federal Trade Commission’s 2022 staff report catalogues deceptive design practices in online commerce and privacy settings.

India’s response is significant because the Consumer Protection Act, 2019 (“CPA 2019”) expressly modernised the consumer-protection framework, created the Central Consumer Protection Authority (“CCPA”), and recognises unfair trade practices in a broad consumer marketplace. The Consumer Protection (E-Commerce) Rules, 2020 regulate specified duties of e-commerce entities. The CCPA’s Guidelines for Prevention and Regulation of Dark Patterns, 2023 identify thirteen specified practices and seek to prevent their use by platforms and sellers in the covered context. A June 2025 advisory further encouraged e-commerce platforms to undertake self-audits.

The topic has direct relevance for legal education. It connects statutory interpretation, administrative enforcement, contract formation, consumer remedies, platform governance, data protection, and comparative law. It also offers a manageable doctrinal research question: whether the present legal framework sufficiently translates the principle of consumer choice into enforceable duties for digital interface design.

2. Research Problem, Questions, Objectives and Hypothesis

2.1 Statement of the problem

Dark patterns can impose small individual losses that are difficult to challenge, while creating significant aggregate gains for a platform. A consumer who is charged for an unwanted add-on may not complain because the amount is modest; a consumer who cannot easily cancel a subscription may continue paying because the time and effort required to exit exceed the immediate perceived cost. These frictions can weaken the practical value of formal consumer rights.

The central legal problem is not simply whether a particular interface is unattractive or persuasive. It is whether the design materially undermines informed and voluntary choice, whether the conduct falls within existing statutory categories, who bears responsibility for it, what evidence is needed to prove it, and which remedy can realistically correct the harm.

2.2 Research questions

- How does Indian consumer law define and regulate dark patterns in digital commerce?
- To what extent do the CPA 2019, the E-Commerce Rules 2020, and the 2023 Guidelines address manipulative interface design?
- What legal and practical challenges arise in proving dark patterns and assigning responsibility among platforms, sellers, advertisers, and service providers?
- How do selected European Union and United States approaches illuminate possible improvements to the Indian framework?
- What reforms could improve deterrence, transparency, consumer redress, and regulatory accountability?

2.3 Objectives

- To explain the concept and principal forms of dark patterns in consumer-facing digital interfaces.
- To analyse the relevant Indian statutes, rules, guidelines, and official regulatory measures.
- To examine the interaction between consumer protection, contract principles, and personal-data protection.
- To assess enforcement and institutional challenges using reported decisions and official materials.
- To recommend legally workable reforms that preserve legitimate interface design while prohibiting manipulative practices.

2.4 Working proposition

The working proposition is that India’s framework provides a substantial legal basis for addressing dark patterns, but effective protection depends on the quality of implementation, proof, disclosure, and remedies. Enumeration of prohibited patterns is useful for certainty, yet should be complemented by a principled test capable of addressing new or functionally equivalent manipulative designs.

3. Research Methodology and Limitations

3.1 Method

This paper uses doctrinal legal research and a comparative desk-review method. Primary materials include the CPA 2019, the E-Commerce Rules 2020, the Dark Patterns Guidelines 2023, official notifications and advisories, and selected reported decisions. Secondary materials include peer-reviewed scholarship and official policy reports. Comparative materials are used for analytical contrast, not as binding law in India.

The research method is qualitative. It identifies the legal rule, explains its scope, compares related duties, and evaluates how the rule may operate in realistic interface scenarios. The paper does not claim to measure the prevalence of dark patterns across platforms, estimate consumer losses, or establish a causal relationship between design and purchasing behaviour. Those questions require empirical research, such as systematic interface audits, consumer surveys, or platform-level data.

3.2 Sources and verification

Primary legal claims should be checked against the Gazette of India, India Code, the Department of Consumer Affairs, the CCPA, and official court or commission records. A press release is useful for identifying the government's stated position and commencement dates, but the operative legal text should be consulted for the precise scope of a rule. Secondary articles may help identify arguments and cases, but should not replace the judgment or statutory instrument itself.

3.3 Limitations

First, the legal and regulatory environment is evolving. The E-Commerce Amendment Rules 2026 were announced with commencement from 1 January 2027; subsequent notifications or clarifications may affect the analysis after the cut-off date. Second, not all consumer commission decisions are reported in a uniform searchable format. Third, interface design varies by device, location, account status, and time; a doctrinal paper cannot establish platform-wide prevalence without a transparent sampling method. Fourth, this manuscript is not a formal systematic review and does not claim to exhaust every publication on the subject.

The paper therefore makes a bounded claim: it evaluates the structure and likely operation of the legal framework from identified materials, rather than asserting that every platform currently uses dark patterns or that enforcement has uniformly failed.

4. Conceptual Foundations: Choice Architecture and Dark Patterns

4.1 Choice architecture

Choice architecture concerns the way options are organised and presented. In digital commerce, it includes the order of products, default settings, button size and colour, the visibility of price information, the number of steps required to complete a task, and the timing of prompts. The same commercial offer can produce different choices depending on how it is framed. This makes interface design legally relevant where law protects informed choice, prohibits deception, or requires affirmative consent.

A distinction is needed between legitimate persuasion and manipulation. A retailer may prominently explain a genuine discount, recommend a popular product, or offer an optional membership. These practices are not dark patterns merely because they encourage a purchase. Concern arises where the interface conveys a false impression, hides a material term, creates artificial urgency, adds a charge without meaningful agreement, or deliberately obstructs refusal or cancellation.

4.2 Defining dark patterns

A workable legal definition should focus on function and context. A dark pattern is a consumer-facing interface practice that, viewed objectively and in context, materially misleads, coerces, or obstructs users in a manner that impairs their ability to make a free and informed choice, particularly where the design creates an asymmetry between accepting a commercial proposal and declining or reversing it.

This formulation does not mean that every imperfect design is unlawful. Materiality, context, the overall impression, the user's reasonable understanding, and the relevant statutory provision matter. An interface may be confusing by accident; a legal finding may require evidence of the practice, its effect, the responsible entity, and the statutory elements. Some regulatory provisions may impose obligations without requiring proof of subjective intent, while other causes of action may turn on specific elements.

4.3 Why consumer law is implicated

Consumer law traditionally addresses misleading representations, unfair trade practices, deficient services, unfair contracts, and remedies for harm. Dark patterns can fit these categories where they affect a consumer transaction. A hidden fee can undermine price transparency; a false countdown may

misrepresent scarcity; an undisclosed subscription can amount to an unauthorised charge; and a cancellation maze can frustrate the consumer's ability to end a continuing service.

The interface may also affect contract law. If a user's click is obtained through deception or without adequate notice of a material term, questions arise about whether the user objectively assented to that term and whether the resulting contract or term is enforceable. These questions must be analysed under the applicable law rather than resolved by assuming that every click constitutes informed consent.

4.4 Economic and behavioural dimensions

Dark patterns often exploit predictable limits on attention and decision-making. Consumers may rely on defaults, respond to urgency cues, avoid repeated effort, or assume that a platform's interface is neutral. Small frictions can have cumulative effects, especially for recurring subscriptions or repeated low-value charges. The aggregate commercial impact may be substantial even when an individual consumer's loss is small.

From a regulatory perspective, the challenge is to distinguish useful behavioural design from exploitation. Clear defaults, accessible explanations, and reminders may improve consumer welfare. Artificial scarcity, concealed costs, or one-sided exit processes undermine autonomy. Regulation should therefore target the deceptive or coercive mechanism, not design innovation as such.

5. Taxonomy of Dark Patterns Under Indian Guidelines

The CCPA's Guidelines for Prevention and Regulation of Dark Patterns, 2023 identify thirteen specified dark patterns. The labels are useful for compliance and enforcement, but each instance must be assessed against the definition and conditions in the Guidelines. The following table provides a plain-language overview; it is not a substitute for the legal text.

Pattern	Illustrative operation	Consumer-protection concern
False urgency	A timer or limited-stock claim creates urgency without a genuine basis.	May mislead consumers about the time available to decide.
Basket sneaking	An extra product, service, donation, or fee is inserted into a basket without a clear affirmative choice.	Can cause unwanted payment and weaken meaningful consent.
Confirm shaming	The refusal option uses guilt or insulting language to discourage declining.	Makes refusal psychologically costly or less neutral.
Forced action	A user must undertake an unnecessary action, such as signing up or sharing information, to access a desired service.	May make unrelated consent a condition of access.
Subscription trap	Joining is easy but cancellation is difficult, obscured, or unnecessarily burdensome.	Creates friction against ending recurring payments.
Interface interference	Visual hierarchy or design privileges one choice and obscures alternatives or important information.	May distort the presentation of available options.
Bait and switch	The interface suggests one outcome but delivers a materially different one after the user acts.	Can undermine the consumer's expected transaction.
Drip pricing	Mandatory or material charges are revealed late in the transaction.	Prevents meaningful comparison of total prices.
Disguised advertisement	Paid or promotional content is presented as independent content or a neutral recommendation.	Obscures the commercial nature of a message.

Pattern	Illustrative operation	Consumer-protection concern
Nagging	Repeated prompts pressure users to take an action they have declined or deferred.	Can fatigue users into accepting an unwanted choice.
Trick wording	Confusing or ambiguous wording makes the consequences of a choice difficult to understand.	Undermines informed decision-making.
SaaS billing	Subscription or software-service billing practices obscure recurring charges or make payment terms unclear.	Can create unexpected recurring obligations.
Rogue malware	Malicious or deceptive software behaviour manipulates user activity or device functionality.	Can cause financial, privacy, or security harm.

5.1 Applying the taxonomy

A label alone should not determine liability. A countdown timer can be accurate where an offer genuinely expires; it becomes problematic where scarcity is false or misleading. A default option may be lawful if the user is clearly informed and can easily change it; it is more troubling where a charge is added without a clear affirmative selection. Similarly, a prominent “subscribe” button is not inherently unlawful, but a cancellation flow that is intentionally obscure may raise a subscription-trap concern.

The legal analysis should ask: what information was presented; what choice was available; whether the user could reasonably understand the consequences; whether the design created a material asymmetry; whether consent was obtained; what records show about the user journey; and which statutory provision applies. Screenshots, screen recordings, transaction records, version history, and complaint logs may be important evidence.

The Guidelines’ enumeration promotes notice and consistency. However, digital practices evolve quickly. A purely literal approach could allow businesses to redesign a prohibited practice without changing its function. A purposive interpretation, grounded in the text and statutory authority, is therefore important, while avoiding an open-ended assumption that any commercially persuasive interface is unlawful.

6. Statutory Framework in India

6.1 Consumer Protection Act, 2019

The CPA 2019 is the principal statute for consumer protection. It defines consumer, complaint, defect, deficiency, unfair contract, unfair trade practice, and other relevant concepts; provides for consumer commissions; and establishes the CCPA. Its modern structure reflects the growth of online transactions and the need for central action against practices affecting consumers as a class.

Section 2(47) defines “unfair trade practice” through a range of practices adopted for promoting the sale, use or supply of goods or services, including specified misleading representations and other conduct. The precise statutory clauses should be checked against the current text before a legal submission. Dark patterns may fall within existing categories depending on the facts, the relevant representation or omission, and the operation of the interface. The Guidelines do not replace the Act; they operate within the legal authority conferred by it.

Section 18 empowers the CCPA to protect, promote and enforce the rights of consumers as a class and prevent violations of consumer rights, unfair trade practices, and false or misleading advertisements. The CCPA can investigate and take action within the powers specified by the Act. The availability of a central authority is important because a single manipulative interface may affect many consumers and may be difficult to address solely through individual complaints.

The Act also provides for consumer dispute redressal commissions at district, state and national levels, subject to the statutory scheme and applicable jurisdictional rules. Depending on the facts, consumers may seek remedies such as refund, removal of a deficiency, compensation, discontinuance of an unfair trade practice, or other relief authorised by law. A consumer’s individual remedy and the CCPA’s class-wide regulatory role are complementary rather than interchangeable.

6.2 Consumer Protection (E-Commerce) Rules, 2020

The E-Commerce Rules 2020 apply to goods and services bought or sold over digital or electronic networks and cover marketplace and inventory models, subject to their terms. They impose duties on e-commerce entities, including disclosure and grievance-related requirements, and address unfair trade practices in e-commerce. The Rules are particularly relevant where the interface is part of an online commercial transaction.

A marketplace model involves an intermediary platform facilitating transactions between buyers and third-party sellers, while an inventory model involves the e-commerce entity holding inventory and selling directly, as defined by the Rules. The distinction can matter when allocating responsibility. A platform cannot automatically be treated as the seller in every case, but neither does its marketplace status resolve every question about its own representations, interface design, payment flows, or role in the transaction.

The Rules should be read alongside the CPA 2019, not in isolation. If a platform's interface hides mandatory charges, misrepresents the seller, fails to disclose required information, or uses a deceptive mechanism, multiple provisions may be relevant. The legal assessment must avoid assuming that every dark pattern necessarily constitutes a breach of every e-commerce duty.

6.3 Guidelines for Prevention and Regulation of Dark Patterns, 2023

The CCPA issued the Guidelines on 30 November 2023 under the authority of section 18 of the CPA 2019. They define dark patterns and identify thirteen specified practices. The stated purpose is to prevent and regulate such practices in online platforms and digital commerce. The Guidelines provide a more tailored vocabulary for digital interface conduct than general prohibitions alone.

The legal force of the Guidelines should be described carefully. They are a regulatory instrument issued under statutory authority and should not be casually described as merely voluntary advice. At the same time, the consequences of a specific practice depend on the applicable provision, facts, the CCPA's powers, procedural fairness, and any relevant adjudication. A manuscript should cite the full official text and analyse the operative language rather than rely only on summaries.

6.4 CCPA advisory on self-audits, June 2025

On 5 June 2025, the CCPA issued an advisory encouraging e-commerce platforms to conduct self-audits to detect dark patterns and take corrective steps within three months. The advisory was intended to support compliance with the 2023 Guidelines and a fairer digital ecosystem. It is a relevant compliance development, but an advisory should not be conflated with a statutory amendment unless the text and legal basis support that characterisation.

Self-audits can help platforms identify problems across numerous screens, user journeys, and devices. Their effectiveness depends on the audit's independence, scope, testing methodology, record retention, and whether remediation is verified. A purely internal checklist may miss design choices that are harmful in practice or may focus only on enumerated labels while ignoring equivalent conduct.

6.5 E-Commerce Amendment Rules, 2026: future commencement

On 10 September 2026, the Government announced the Consumer Protection (E-Commerce) (Amendment) Rules, 2026, with commencement scheduled for 1 January 2027. As of this paper's cut-off date, they are future-effective and must not be presented as already operative. The official announcement states that the amendments address consumer grievances, search results, sponsored listings, price reductions, dark patterns, seller disclosures, consumer information, bundled fees, and imported goods.

Among the announced changes are yearly self-audits and a prominently displayed compliance certificate relating to dark-pattern compliance; clearer identification of sponsored listings; requirements concerning the display of current and prior prices where a reduction is announced; and strengthened disclosure and grievance-related duties. The exact obligations and exceptions should be checked against the notified amendment text before relying on them in practice.

The 2026 amendments indicate a move from broad principles and an advisory-based self-audit approach toward more regularised transparency and compliance mechanisms. Their practical impact will depend on implementation, regulatory monitoring, the content of the operative text, and the extent to which the CCPA and consumer commissions use the framework after commencement.

7. Contract Law, Consent and Consumer Autonomy

7.1 Contract formation in digital transactions

Online contracts commonly form through clickwrap, browsewrap, or related digital acceptance mechanisms. A click can be evidence of assent, but the legal effect depends on notice, the clarity of the term, the user's conduct, and the applicable law. A user should not be treated as having meaningfully accepted a material charge merely because a screen was technically clickable if the charge was hidden or the design materially misrepresented the choice.

The Indian Contract Act, 1872 provides the general framework for agreement, consent, free consent, fraud, misrepresentation, and voidability. Section 13 defines consent in terms of parties agreeing upon the same thing in the same sense. Section 14 addresses free consent and identifies factors including

coercion, undue influence, fraud, misrepresentation, and mistake as specified in the provision. The precise fit between a dark pattern and these doctrines is fact-sensitive; not every interface asymmetry automatically amounts to fraud or vitiates consent.

7.2 Misrepresentation and material omissions

A price or subscription term may be material to a consumer's decision. If the interface presents a low headline price while concealing mandatory charges until the final stage, the overall impression may be misleading. Likewise, a subscription may be presented as a one-time trial even though it converts automatically to a recurring paid service. Whether a representation is legally actionable depends on the evidence, the governing statute, the consumer's understanding, and the relevant legal elements.

7.3 Meaningful choice and asymmetric friction

A useful analytical concept is asymmetric friction: accepting an offer requires one simple action, while rejecting it or cancelling later requires many steps, repeated explanations, or contact with an agent. Such asymmetry is not automatically unlawful in every context, but it can be evidence that the interface is designed to impede the exercise of consumer choice. Cancellation symmetry—making exit no more burdensome than entry without a legitimate reason—is a practical compliance principle.

7.4 Evidence and burden of proof

A legal challenge may require proof of the interface as it appeared at the relevant time. Screenshots alone may not show what preceded or followed a screen, whether a default was pre-selected, or whether a user could reasonably find the refusal option. Evidence may include screen recordings, transaction receipts, versioned interface records, terms and conditions, communications, user complaints, and audit documentation.

Platforms generally control much of the technical evidence. This creates an information asymmetry between an individual consumer and a commercial entity. Procedural rules should preserve due process while allowing regulators to obtain relevant records within lawful authority. Consumer-facing complaint mechanisms should make it easy to upload evidence and identify the relevant transaction without requiring consumers to understand technical design terminology.

8. Data Protection and Privacy Dimensions

8.1 The overlap between consumer choice and data protection

Dark patterns can affect not only purchases but also consent to data collection, tracking, profiling, and targeted advertising. A platform may use repeated prompts, confusing privacy settings, or a more prominent “accept all” button to encourage data sharing. Such practices raise a dual concern: the interface may affect consumer autonomy in a commercial transaction and may also affect the validity of consent under applicable data-protection law.

The Digital Personal Data Protection Act, 2023 (“DPDP Act”) is relevant to the processing of digital personal data within its scope. Its operation must be analysed with attention to commencement notifications, applicable rules, and the legal position at the relevant date. A researcher should not assume that every provision of an enacted statute has commenced merely because the Act received assent. The current notification and implementation status should be verified before submission.

8.2 Consent must be assessed in context

A consent button may be technically affirmative while the surrounding interface undermines informed choice. The legal analysis should distinguish the existence of a click from the quality of the information and the voluntariness of the choice. Clear purpose statements, accessible refusal options, granular controls where appropriate, and the ability to withdraw consent can improve the integrity of the process.

8.3 Regulatory overlap

Consumer protection and data protection address related but distinct harms. Consumer law focuses on consumer transactions, unfair practices, and redress; data protection law regulates covered processing of personal data and the rights and obligations associated with it. The same interface may engage both regimes, but jurisdiction, statutory elements, remedies, and enforcement powers should be analysed separately.

Coordination is important to avoid inconsistent findings, duplicated burdens, or gaps in enforcement. Regulators can develop referral protocols, shared technical expertise, common terminology, and guidance on evidence preservation while respecting statutory mandates and confidentiality obligations.

9. Enforcement, Remedies and Institutional Design

9.1 Class-wide enforcement and individual redress

Dark patterns can affect large numbers of consumers through a single design decision. This makes class-wide intervention attractive: a regulator may seek to stop the practice or require correction rather than leaving every consumer to bring a separate complaint. Individual consumer commissions remain important where a consumer seeks transaction-specific relief, including refund or compensation under applicable law.

The CCPA's role should be distinguished from the role of consumer commissions. The former exercises statutory powers directed toward consumer rights and unfair trade practices as a class; the latter adjudicate consumer disputes within their jurisdiction. Effective protection requires both preventive regulation and accessible individual redress.

9.2 Compliance incentives and penalties

A credible enforcement system combines clear rules, realistic compliance expectations, detection, proportionate sanctions, and public explanation of outcomes. Penalties alone may not be enough where the commercial benefit of a manipulative interface is recurring and distributed across a large user base. Corrective orders can require interface changes, refund mechanisms, disclosure improvements, or other legally authorised measures.

Regulatory decisions should explain the factual basis for identifying a dark pattern, the applicable provision, the responsible entity, and the corrective action required. Published reasoning can help businesses comply, consumers understand their rights, and courts or commissions maintain consistency. It also reduces the risk that enforcement appears arbitrary.

9.3 The problem of small-value harms

An individual may not pursue a claim over a small unwanted charge because the cost of time and effort is greater than the amount at stake. This rational under-enforcement can allow a practice to continue even when the total harm across consumers is significant. Aggregated complaint data, platform audits, and regulator-initiated investigations can help identify patterns that individual cases do not reveal.

9.4 Technical capacity

Effective dark-pattern enforcement requires more than conventional legal expertise. Regulators may need human-computer interaction specialists, software engineers, behavioural researchers, data analysts, and consumer advocates. A technically informed investigation can assess how a design works, whether the claimed scarcity is genuine, how often a prompt is displayed, and whether the cancellation process is materially more difficult than sign-up.

9.5 Transparency and auditability

A self-audit should record the scope, devices and user journeys tested, criteria used, findings, remediation, and follow-up verification. Platforms should preserve relevant versions of the interface and maintain an internal escalation process for high-risk patterns. Where a platform claims compliance, the claim should be supported by evidence rather than a generic statement.

External audits may be appropriate for high-risk services or repeated non-compliance. The audit regime should be proportionate: small businesses should not face unnecessarily burdensome procedures for low-risk interfaces, but scale should not excuse manipulative conduct. Regulatory priorities can be guided by the number of affected consumers, financial exposure, vulnerability of the target group, duration, reversibility, and evidence of repetition.

10. Indian Case Law and Regulatory Practice

10.1 *Ashwani Chawla v Flipkart Internet Private Limited and Others*

Academic commentary in the International Journal on Consumer Law and Practice discusses the decision of the State Consumer Disputes Redressal Commission, Chandigarh in *Ashwani Chawla v Flipkart Internet Pvt Ltd and Others*. The case comment describes the dispute as involving traditional consumer-law issues, including jurisdiction, defect, deficiency, unfair contract, and unfair trade practice, and notes that the Commission explicitly referred to the 2023 Dark Patterns Guidelines. It also discusses platform responsibility in relation to third-party traders.

The case is potentially important because it indicates that dark-pattern analysis is entering consumer-dispute adjudication rather than remaining only in policy documents. However, a case comment is not a substitute for the full decision. Before citing the decision for a precise legal proposition, the researcher should obtain the order, verify the case number, date, procedural posture, facts, exact findings, and whether any appeal or later decision affects its status.

10.2 Jatin Bansal v Amazon Reseller Services Private Limited and Others

The same case comment refers to Jatin Bansal v Amazon Reseller Services Pvt Ltd and Others as part of the emerging Indian consumer-law discussion. The reference should be treated as a research lead rather than a fully verified case citation until the primary order is obtained and checked. A journal manuscript should not state a holding, quote a passage, or imply a binding precedent without verifying the judgment itself.

10.3 Regulatory action and public reporting

Official government materials have described CCPA action involving alleged or identified dark patterns such as false urgency, basket sneaking, drip pricing, confirm shaming, and charges added without meaningful consumer choice. The June 2025 advisory called on e-commerce platforms to conduct self-audits and address such practices. These materials demonstrate regulatory attention, but they should be cited precisely and not overgeneralised to claim that every allegation resulted in a final adjudication.

10.4 How to analyse a dark-pattern decision

A disciplined case analysis should identify: (i) the forum and its jurisdiction; (ii) the facts and evidence concerning the interface; (iii) the legal provisions pleaded or applied; (iv) the reasoning linking design to consumer harm; (v) the remedy or direction; (vi) whether the decision was appealed or modified; and (vii) its precedential weight. A first-instance consumer commission order may be persuasive or fact-specific rather than binding throughout India.

For publication, this section should be updated after downloading and reading the primary orders. It would be inappropriate to manufacture citations, dates, quotations, or outcomes from a secondary summary.

11. Comparative Perspectives: European Union and United States

11.1 European Union: Digital Services Act

The European Union's Digital Services Act ("DSA"), Regulation (EU) 2022/2065, includes a provision addressing online platforms' design and organisation. Article 25 prohibits online platforms from designing, organising, or operating their online interfaces in a way that deceives or manipulates recipients of the service or otherwise materially distorts or impairs their ability to make free and informed decisions. The provision contains qualifications and exceptions, including the relationship with practices covered by specified EU legal instruments.

Its precise scope should be read from the regulation itself.

The DSA is useful for India because it frames the issue at the level of interface design and decision-making, rather than relying exclusively on individual misleading statements. It also demonstrates the value of a general principle that can apply to new design practices, alongside more specific rules. It should not be described as binding on Indian businesses merely because they operate online; its territorial application depends on the EU instrument.

11.2 European Union: consumer and data protection law

The DSA operates alongside other EU regimes, including consumer-protection and data-protection law. This layered structure reflects the fact that a dark pattern may manipulate a purchase, distort advertising disclosures, or undermine consent to personal-data processing. For India, the lesson is not to copy every European rule but to clarify how overlapping legal duties interact and how enforcement bodies can coordinate.

11.3 United States: Federal Trade Commission

The United States Federal Trade Commission's 2022 staff report, *Bringing Dark Patterns to Light*, describes design tactics that can disguise advertisements, make cancellation difficult, obscure material terms, or steer users into sharing data. The report discusses how these practices may intersect with existing prohibitions on unfair or deceptive acts or practices. The FTC has also pursued enforcement involving subscriptions and deceptive online practices.

The US approach illustrates how general unfairness and deception powers can address practices that do not fit neatly within a closed list. However, the legal test, institutional structure, and remedies differ from India's system. A comparative paper should not transplant conclusions without accounting for constitutional, statutory, and procedural differences.

11.4 Comparative lessons for India

- A general principle against materially impairing free and informed choice can complement a list of named patterns.
- Interface design should be assessed in context, including the user journey and the relative friction of acceptance, refusal, and cancellation.
- Regulatory guidance and enforcement examples help businesses understand how abstract standards apply to actual design.

- Audit trails, preserved interface versions, and documented remediation improve accountability.
- Coordination among consumer, data-protection, and competition authorities can reduce gaps and duplication.

Comparative law is most useful when it identifies design principles and institutional choices. It is less useful when it treats foreign rules as directly applicable or assumes that a model that works in one regulatory system will automatically work in another.

12. Critical Analysis and Findings

12.1 A substantial but evolving framework

The first finding of this doctrinal analysis is that India is not without a legal response to dark patterns. The CPA 2019 provides the central consumer-protection structure; the E-Commerce Rules 2020 impose duties in digital transactions; the 2023 Guidelines identify thirteen specific patterns; and the 2025 advisory promotes platform self-audits. The announced 2026 amendments, once effective, are intended to add more structured obligations concerning audit, disclosure, and e-commerce transparency.

The challenge is therefore not simply to create a rule from scratch. It is to ensure that existing duties are interpreted consistently, evidence can be obtained, enforcement is transparent, and consumers can obtain practical remedies. Rules that exist only on paper may not meaningfully protect users if the regulator lacks technical resources or the consumer cannot prove what the interface displayed.

12.2 Enumeration versus general principles

An enumerated list has real advantages. It provides businesses with notice, helps compliance teams identify risk, and gives regulators a shared vocabulary. But lists can become outdated, especially where interface design changes rapidly. A practice may be renamed, moved to a different stage of the transaction, or implemented through a new technical mechanism while preserving its manipulative effect.

A sound framework should combine specific examples with a principle-based assessment. The principle should not be so vague that it captures ordinary marketing, but it should be capable of addressing functionally equivalent practices. The legal basis for any finding must remain anchored in the statute and the applicable instrument.

12.3 The challenge of intent

Some forms of dark-pattern analysis focus on whether the designer knowingly manipulated a user; other legal standards focus on the objective effect or overall impression. Intent can be difficult to prove because design decisions are distributed across product, marketing, engineering, and analytics teams. An outcome-based test may be easier to administer, but it must still respect the elements of the applicable law and procedural fairness.

Internal experiments, A/B testing records, user research, complaint data, and design documents can help establish how a feature was developed and what effects were observed. However, a commercial objective to improve conversion is not by itself proof of illegality. The key question is whether the practice crosses the legal line into deception, coercion, material obstruction, or another prohibited category.

12.4 Consumer vulnerability and proportionality

Not all consumers have equal ability to identify manipulative design. Children, older users, people with disabilities, users with limited digital literacy, and consumers facing language barriers may experience interface friction differently. A fair assessment should consider accessibility and foreseeable vulnerability without assuming that all members of a group are incapable of making choices.

Proportionality matters. Clear disclosure and symmetrical cancellation may be low-cost interventions, while extensive independent auditing can be expensive. Requirements can be calibrated by risk, scale, the type of service, and the likelihood of harm, while retaining a firm prohibition on deceptive or unauthorised charges.

12.5 Remedies and deterrence

A remedy should correct the consumer harm and reduce the likelihood of repetition. Depending on legal authority and facts, this may involve stopping a practice, changing an interface, refunding an unauthorised charge, correcting a misleading representation, or imposing an authorised penalty. Publicly reasoned decisions can provide guidance to the wider market.

Where consumers have paid recurring charges because cancellation was obstructed, merely changing the future interface may not address past harm. Conversely, a refund alone may not prevent the same design from affecting other consumers. A proportionate response can combine individual restitution, prospective correction, compliance monitoring, and deterrent measures where legally available.

12.6 Preliminary doctrinal findings

- Indian law already contains several overlapping tools that may address manipulative interface practices.
- The 2023 Guidelines improve specificity by naming thirteen patterns, but implementation and evidence remain critical.
- The legal responsibility of a platform must be assessed according to its role, conduct, statutory duties, and the facts—not assumed solely from its marketplace label.
- The interaction between consumer choice and data protection requires careful analysis of commencement, scope, consent, and remedies.
- The future-effective 2026 amendments could strengthen recurring compliance and disclosure, but their real effect can only be assessed after commencement and implementation.

These are findings from doctrinal analysis, not statistical conclusions about the frequency of dark patterns or the success rate of enforcement.

13. Recommendations and Proposed Reform

13.1 Clarify the standard for materially impaired choice

Regulatory guidance should explain how to assess whether an interface materially impairs free and informed choice. Relevant factors could include the prominence and clarity of information, the accuracy of urgency claims, the presence of pre-selected charges, the availability of a genuine refusal option, the number and complexity of steps required to cancel, and the reversibility of the consumer's action. Such factors should guide, not replace, the legal text.

13.2 Require meaningful price transparency

Total mandatory charges should be disclosed early enough for consumers to compare offers. Optional services should be clearly distinguished from mandatory fees. A price that appears low at the start but increases through unavoidable charges at checkout can distort comparison. The future-effective 2026 amendments concerning prior-price disclosures and sponsored listings should be implemented through clear guidance and monitoring.

13.3 Establish cancellation symmetry

Where sign-up is completed online, cancellation should ordinarily be available through an equally accessible channel unless a legitimate, proportionate reason justifies a different process. Repeated retention prompts, hidden cancellation controls, or unnecessary contact requirements should be treated as high-risk design features. A neutral confirmation may be appropriate, but it should not become a barrier to exit.

13.4 Improve audit standards

Platforms should use documented audits that test complete user journeys across mobile and desktop environments, logged-in and logged-out states, language variants, and relevant payment pathways. Audits should record the interface version, date, device, account status, steps taken, result, and remediation. For high-risk or repeated violations, regulators should consider independent verification within existing legal authority.

13.5 Preserve evidence

Platforms should preserve relevant interface versions and records for a reasonable period consistent with applicable law, legitimate business needs, and privacy safeguards. Evidence retention is particularly important where a complaint arises after the interface has changed.

Regulators should provide clear procedures for lawful access to relevant records.

13.6 Publish reasoned enforcement outcomes

Public decisions should explain the pattern, the factual basis, the legal provision, the remedy, and the compliance steps expected. An anonymised repository of decisions and case summaries can help consumers, legal practitioners, academics, and compliance teams understand the law.

Publication should protect personal information and legitimate confidentiality interests.

13.7 Strengthen consumer complaint pathways

Complaint interfaces should allow consumers to report a specific pattern without needing to know its legal label. A complaint form could ask what the consumer attempted to do, what the interface displayed, what charge or consequence followed, and what evidence is available. Platforms should provide a copy or reference number for the complaint and communicate the response clearly.

13.8 Coordinate regulators

Consumer, data-protection, and competition authorities should develop protocols for referral and coordination where a design practice raises overlapping issues. Coordination can reduce duplication and ensure that one regulator's findings do not unintentionally undermine another's investigation. The protocol should clarify lead authority, evidence sharing, confidentiality, and the treatment of parallel proceedings.

13.9 Encourage accessibility and plain language

Compliance should include testing for users with disabilities, different levels of digital literacy, and different language needs. Material terms should be written in plain language, important choices should be visually distinguishable, and refusal should not be hidden behind low-contrast text or confusing wording. Accessibility is not merely a design preference where it affects the consumer's ability to understand and exercise a legal right.

13.10 Support future empirical research

Researchers could conduct a transparent, time-stamped audit of a defined sample of e-commerce platforms and user journeys. The study should pre-register or clearly state the sample, coding rules, devices, dates, and limitations; avoid collecting unnecessary personal data; and distinguish observed interface features from legal conclusions. This would provide evidence about prevalence and change over time without treating isolated screenshots as proof of systemic misconduct.

14. Conclusion

Dark patterns expose a central challenge in digital consumer protection: a consumer may possess formal rights while the interface makes it difficult to exercise them. Design can determine whether a price is understood, whether an add-on is accepted, whether a subscription is continued, and whether a consumer can leave a service without undue friction. The law must therefore examine not only the words used by a trader but also the way choices are organised and presented.

India's CPA 2019, E-Commerce Rules 2020, and Dark Patterns Guidelines 2023 establish a meaningful framework for addressing deceptive or manipulative practices. The CCPA's 2025 self-audit advisory demonstrates a compliance-oriented approach. The announced E-Commerce Amendment Rules 2026, scheduled to commence on 1 January 2027, signal further attention to recurring audits, disclosure, search results, prices, and grievance handling. Their effects should be evaluated after commencement rather than presumed in advance.

The framework's success will depend on careful legal interpretation, technical capacity, evidence preservation, transparent enforcement, and remedies that address both individual loss and wider market effects. A balanced regime should not prohibit ordinary persuasion or useful choice architecture. It should target conduct that materially misleads, coerces, or obstructs consumers, while preserving due process and proportionality.

The central recommendation is a combined approach: retain the specificity of the enumerated patterns, explain a principled test for new or equivalent practices, strengthen auditability, make cancellation and refusal genuinely accessible, and improve coordination among institutions. The goal is not to remove design from commerce, but to ensure that digital design supports rather than defeats informed consumer choice.

Bibliography

A. Legislation and Regulatory Instruments

Consumer Protection Act 2019 (India), Act No 35 of 2019.

Consumer Protection (E-Commerce) Rules 2020, GSR 462(E), Gazette of India, 23 July 2020, as amended.

Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns 2023, issued 30 November 2023.

Central Consumer Protection Authority, Advisory on Self-Audit by E-Commerce Platforms for Detecting Dark Patterns, 5 June 2025.

Consumer Protection (E-Commerce) (Amendment) Rules 2026 (India), announced 10 September 2026; stated commencement 1 January 2027. Verify the Gazette notification and operative text before citation.

Indian Contract Act 1872 (India).

Digital Personal Data Protection Act 2023 (India). Verify commencement notifications and applicable rules as at the date of submission.

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.

B. Cases and Case Commentary

Ashwani Chawla v Flipkart Internet Private Limited and Others, State Consumer Disputes Redressal Commission, Chandigarh. Obtain and verify the primary order, case number, date, and subsequent procedural history before citing.

Jatin Bansal v Amazon Reseller Services Private Limited and Others. Obtain and verify the primary order and procedural history before citing.

Guha SK and Roy S, 'Ashwani Chawla v Flipkart Internet Private Ltd: Formal Recognition of Dark Pattern

Prevention and Regulation Guidelines' (2024) 12 International Journal on Consumer Law and Practice, DOI: 10.55496/BLJJ6217.

C. Secondary Literature and Reports

Luguri J and Strahilevitz LJ, 'Shining a Light on Dark Patterns' (2021) 13 Journal of Legal Analysis 43–109, <https://doi.org/10.1093/jla/laaa006>.

Federal Trade Commission, Bringing Dark Patterns to Light: Staff Report (September 2022), <https://www.ftc.gov/reports/bringing-dark-patterns-light>.

Sharma SJ and Sharma I, 'Dark Patterns in a Bright World: An Analysis of the Indian Consumer Legal Architecture' (2023) 11 International Journal on Consumer Law and Practice.

Department of Consumer Affairs, Government of India, 'Central Consumer Protection Authority issues advisory to E-Commerce Platforms for self-audit within 3 months to detect Dark Patterns and ensure its resolution' (7 June 2025), Press Information Bureau.

Department of Consumer Affairs, Government of India, 'Government amends E-Commerce Rules to strengthen consumer protection and promote transparency' (10 September 2026), Press Information Bureau.

Bureau of Indian Standards, IS 19000:2022, Online Consumer Reviews — Principles and Requirements for their Collection, Moderation and Publication. Confirm the exact title and current status from BIS before final citation.

D. Official Online Sources

India Code, 'The Consumer Protection Act, 2019', <https://www.indiacode.nic.in/indiacode/handle/123456789/16103>.

Department of Consumer Affairs, Consumer Protection Acts and Rules', <https://consumeraffairs.gov.in/pages/consumer-protection-acts>.

Central Consumer Protection Authority, 'Act and Rules', <https://ccpa.doca.gov.in/act-and-rules.php>.

Press Information Bureau, Ministry of Consumer Affairs, 'Guidelines for Prevention and Regulation of Dark Patterns, 2023' (8 December 2023), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1983994>.

Press Information Bureau, Ministry of Consumer Affairs, 'Government amends E-Commerce Rules to strengthen consumer protection and promote transparency' (10 September 2026), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2308759>.

European Union, Regulation (EU) 2022/2065, EUR-Lex, <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.

Appendix A: Suggested Verification Checklist Before Submission

- Replace all author and institution placeholders.
- Obtain the official Gazette text of every statute, rule, guideline, and amendment cited.
- Verify the commencement status of the Digital Personal Data Protection Act and related rules as at submission.
- Download and read the primary orders in Ashwani Chawla and Jatin Bansal; confirm case numbers, dates, holdings, remedies, and appeals.
- Confirm the exact Gazette notification and commencement of the 2026 E-Commerce Amendment Rules.
- Check each quotation and statutory section against the primary source; do not rely solely on a press release or case comment.
- Expand the literature review using peer-reviewed scholarship and explain how this paper differs from existing articles.
- Format footnotes and bibliography according to the chosen journal's author guidelines; OSCOLA is a working style, not a universal journal requirement.
- Run a similarity check and ensure all paraphrased ideas are properly attributed.
- Follow the target journal's policy on generative AI and disclose assistance if required.
- Do not invent empirical data, interviews, surveys, platform audits, or findings.
- Add an author declaration, conflict-of-interest statement, funding statement, and ethics statement only where accurate and required.

Appendix B: Possible Further Research

A follow-up empirical study could audit the checkout and cancellation journeys of a defined sample of Indian e-commerce platforms. The researcher should state the sampling frame, observation dates, devices, user states, inclusion criteria, coding scheme, and procedure for preserving screenshots. The

study should distinguish a descriptive observation (for example, an add-on is pre-selected) from the legal conclusion that a specific provision has been breached. Platform terms and interface features change over time; findings should be date-stamped and limited to the observed sample.

A second project could compare the Indian Guidelines with Article 25 of the EU Digital Services Act and the US FTC's unfairness and deception approach. A third could study consumer commission decisions after the 2023 Guidelines to examine how legal concepts are translated into remedies. These projects require independent source collection and should not be presented as completed within this doctrinal manuscript.

Supplementary Analysis: Applying the Law to Consumer Journeys

Search, ranking, and sponsored results

A consumer's first encounter with a product may occur through search results, recommendations, or a category page. The ordering of results can influence which products are considered and which are ignored. Ranking is not inherently deceptive: relevance, price, availability, quality, delivery speed, and user preferences may all legitimately affect ordering. The concern arises when paid placement is presented as an independent ranking, when the basis of ranking is materially misrepresented, or when design causes a consumer to mistake an advertisement for an organic result.

A legal assessment should distinguish three questions. First, is the result sponsored or commercially influenced? Secondly, is that status disclosed clearly and at the point where the consumer makes the choice? Thirdly, does the platform make any express or implied claim that the ranking is neutral, comprehensive, or based on a stated criterion? The answer may determine whether the issue is one of disclosure, misleading representation, unfair trade practice, or compliance with a specific e-commerce duty.

The announced 2026 E-Commerce Amendment Rules address manipulation of search results and clearer disclosure of sponsored listings, with commencement scheduled for 1 January 2027. Until commencement, the existing law and applicable instruments must be analysed on their own terms. After commencement, compliance reviews should compare actual ranking behaviour and labels with the precise requirements in the notified text.

Product pages and review presentation

Product pages often combine seller descriptions, customer ratings, reviews, badges, recommendations, and promotional claims. A platform may legitimately organise reviews by relevance or recency, but it should avoid creating a false impression that a rating represents all customers if material filtering or moderation has occurred. The legal issue is not that reviews are curated, but whether the presentation materially misleads users about the source, reliability, or representativeness of the information.

India's Bureau of Indian Standards has issued a voluntary standard concerning online consumer reviews and principles for their collection, moderation, and publication. The standard is relevant to integrity and transparency, but its voluntary status should not be confused with a mandatory statutory obligation. A careful paper should verify the exact standard number, title, and current status through BIS before relying on it.

A robust review system should disclose material incentives, avoid fabricating or suppressing reviews deceptively, provide a transparent moderation policy, and distinguish verified-purchase indicators from independent verification of review truth. Platforms should not imply that a review is authentic merely because it appears on their service unless the verification process supports that representation.

Checkout, add-ons, and total price

Checkout is a high-risk stage because consumers have invested time in selecting products and may be less willing to abandon the transaction. An optional warranty, membership, donation, delivery upgrade, or other add-on should be presented as optional and should not be selected without a clear affirmative choice where the applicable law requires or the context demands such consent. A consumer should be able to understand the total amount before committing to payment.

The distinction between an optional add-on and a mandatory fee matters. A mandatory charge should be included in the disclosed total price as early as practicable. An optional service may be offered separately, but the interface should make its price and effect clear and should not create an impression that it is necessary to complete the purchase when it is not. A checkbox or toggle can be technically available yet still be misleading if the surrounding wording or visual hierarchy obscures its consequence.

For evidentiary purposes, investigators should preserve the product page, cart, checkout screen, final payment screen, receipt, and relevant terms. A single screenshot of the final total may establish the charge but may not establish whether the user had a fair opportunity to reject it. The full sequence is usually more probative.

Subscription enrolment, renewal, and cancellation

Subscriptions create a continuing relationship in which the consumer's initial decision can trigger future payments. A free trial that converts into a paid plan is not necessarily unlawful, provided the conversion, amount, timing, and cancellation conditions are adequately disclosed and accepted. The risk increases where a consumer is led to believe that the trial is free without a clear explanation of automatic renewal, or where cancellation is materially more difficult than enrolment.

A fair subscription design should communicate the renewal date, recurring amount, billing frequency, method of cancellation, and any material limitations before the consumer commits. A reminder before renewal can be useful, although whether it is legally required depends on the relevant law and contract.

The cancellation control should be easy to locate, accessible on the channel used for enrolment where practicable, and followed by an unambiguous confirmation.

The subscription-trap analysis should focus on the entire user journey, not simply the presence of a cancellation link. A link may exist but be hidden in account settings, require repeated retention prompts, or lead to an unexpected telephone call. Conversely, a brief confirmation step can protect against accidental cancellation without creating an unlawful barrier. Context and proportionality are important.

A Practical Legal Test for Evaluating Interface Design

For research and compliance purposes, the following analytical sequence can help organise the facts. It is not a substitute for any statutory test and should not be presented as a binding legal standard.

- Step 1 — Identify the consumer decision. Specify what the user was trying to do: buy, compare, decline, consent, renew, cancel, or obtain a refund.
- Step 2 — Record the interface. Preserve the sequence of screens, wording, default settings, button placement, disclosures, and final transaction outcome, with dates and device context.
- Step 3 — Identify the representation or friction. Ask whether information was hidden, a claim was false or ambiguous, a charge was pre-selected, or refusal/cancellation was materially obstructed.
- Step 4 — Assess materiality and context. Consider whether the feature could reasonably affect the consumer's decision, taking account of the transaction, target users, and the prominence of information.
- Step 5 — Map to the legal rule. Identify the exact statutory section, rule, guideline, or contractual doctrine. Avoid relying on the label "dark pattern" alone.
- Step 6 — Identify the responsible actor. Determine who controlled the interface, who made the representation, who collected the payment, and which duties applied to the platform, seller, advertiser, or service provider.
- Step 7 — Evaluate evidence and explanation. Consider whether the business can demonstrate that urgency was genuine, an add-on was affirmatively selected, or the cancellation process was accessible.
- Step 8 — Select a proportionate remedy. Match the response to the harm: correction, disclosure, cancellation, refund, cessation, compliance monitoring, or other relief legally available.

This sequence promotes consistency by separating the observation of a design feature from the legal conclusion. It also reduces the risk of circular reasoning in which a feature is declared unlawful merely because it has been called a dark pattern.

Platform Responsibility and the Marketplace Model

Distinguishing seller conduct from platform conduct

E-commerce transactions may involve several actors: the manufacturer, seller, marketplace operator, payment provider, advertiser, logistics provider, and subscription service. Responsibility should be allocated according to the statutory text and the conduct of each actor. A third-party seller may be responsible for a false product claim, while the platform may separately be responsible for the way it designs checkout, labels sponsored results, presents seller information, or processes an add-on.

The marketplace label should not be treated as a universal immunity, but neither should the platform automatically be treated as the seller of every product listed on it. The legally relevant inquiry is role-specific. What did the platform promise? Which features did it control? Did it collect the payment or set the default? Did a rule impose a disclosure or grievance duty? Did the platform have knowledge of a repeated practice and fail to act where a duty required action?

Contractual allocation and consumer-facing duties

Platform agreements may allocate duties between the platform and sellers, but private allocation does not necessarily extinguish statutory duties owed to consumers. A consumer-facing representation can create a separate issue from the platform's internal contract with a seller. Likewise, an indemnity clause between commercial actors may allocate financial risk between them without determining the consumer's statutory rights.

A clear compliance programme should map each interface element to an accountable business owner. Product teams, marketing teams, payment teams, and third-party vendors should know who approves price disclosures, default settings, subscription terms, and cancellation flows. Where responsibility is fragmented internally, the platform should still maintain a process that can identify and correct problematic designs.

Due process and legal certainty

Regulatory intervention should identify the responsible entity and the legal basis for action. A finding should not rest on the broad assertion that a platform is powerful or that a design is commercially effective. The entity should have a fair opportunity to respond to the evidence, subject to applicable law and urgent interim powers where authorised. Clear findings improve the likelihood that remedies will survive review and guide future compliance.

Implementation Questions Arising from the 2026 Amendment

The September 2026 government announcement states that the E-Commerce Amendment Rules 2026 will commence on 1 January 2027. It describes strengthened duties concerning consumer complaints, search results, sponsored listings, price reductions, dark patterns, product and seller information, consumer information, bundled fees, and imported goods. The official Gazette text should be consulted before interpreting the detailed scope of each requirement.

Three implementation questions are especially important. First, what counts as a sufficiently prominent sponsored-listing disclosure in a user interface that changes across mobile screens and voice or AI-assisted search? Secondly, how will annual self-audit and display of a compliance certificate be verified, and what evidence must be retained? Thirdly, how will the requirements apply to rapidly changing prices, personalised offers, marketplace sellers, and cross-border transactions?

The prior-price requirement described in the announcement uses the lowest price during the preceding 30 days as the relevant reference for an announced reduction. This may improve comparability, but businesses will need reliable price-history records. The operative rule should be checked for the exact scope, exceptions, calculation method, and the relationship between advertised reductions and personalised pricing.

The amendment also reportedly strengthens the connection between e-commerce entities and the National Consumer Helpline. Better integration may improve complaint routing, but success will depend on whether complaints are acknowledged, tracked, assigned to a responsible entity, and resolved in a meaningful time. A helpline partnership is not itself proof that a substantive consumer grievance has been resolved.

The most important caution is temporal: as at 12 October 2026, the announced amendments are not yet in force. This paper therefore treats them as an imminent regulatory development. A manuscript submitted after 1 January 2027 should update the analysis to reflect commencement, any subsequent guidance, and early enforcement experience.

Research Agenda and Questions for Further Scholarship

The present doctrinal analysis suggests several questions that require evidence beyond statutory interpretation. Researchers could measure how often the thirteen named patterns appear in a defined sample of interfaces, whether the same platform presents different flows across devices, and whether changes follow regulatory interventions. Such research should use a transparent protocol so that results can be replicated and challenged.

A longitudinal interface audit could record a fixed sample of platforms at monthly intervals, preserving screenshots and coding each feature against a published rubric. The sample should include criteria for platform selection, user journey, device, language, account status, and the date of observation. Inter-rater reliability should be assessed if more than one researcher codes the material. Legal conclusions should be kept separate from raw observations.

A consumer survey could explore whether users notice disclosures, understand recurring charges, or can find cancellation controls. Survey design should avoid leading questions and should distinguish self-reported awareness from observed behaviour. If human participants are involved, the researcher should follow institutional ethics requirements and protect participant data.

A case-law study could collect all accessible consumer commission orders that expressly discuss dark patterns or apply related principles. Researchers should record forum, date, facts, provision, reasoning, remedy, and appellate history. This could reveal whether decision-makers apply a consistent test and whether the 2023 Guidelines are being used as a direct rule, interpretive aid, or contextual reference.

Finally, comparative work could examine whether a list-based approach, a general prohibition, or a hybrid model produces more consistent enforcement. The analysis should account for institutional capacity, available remedies, business structure, and procedural safeguards rather than comparing statutory language in isolation.