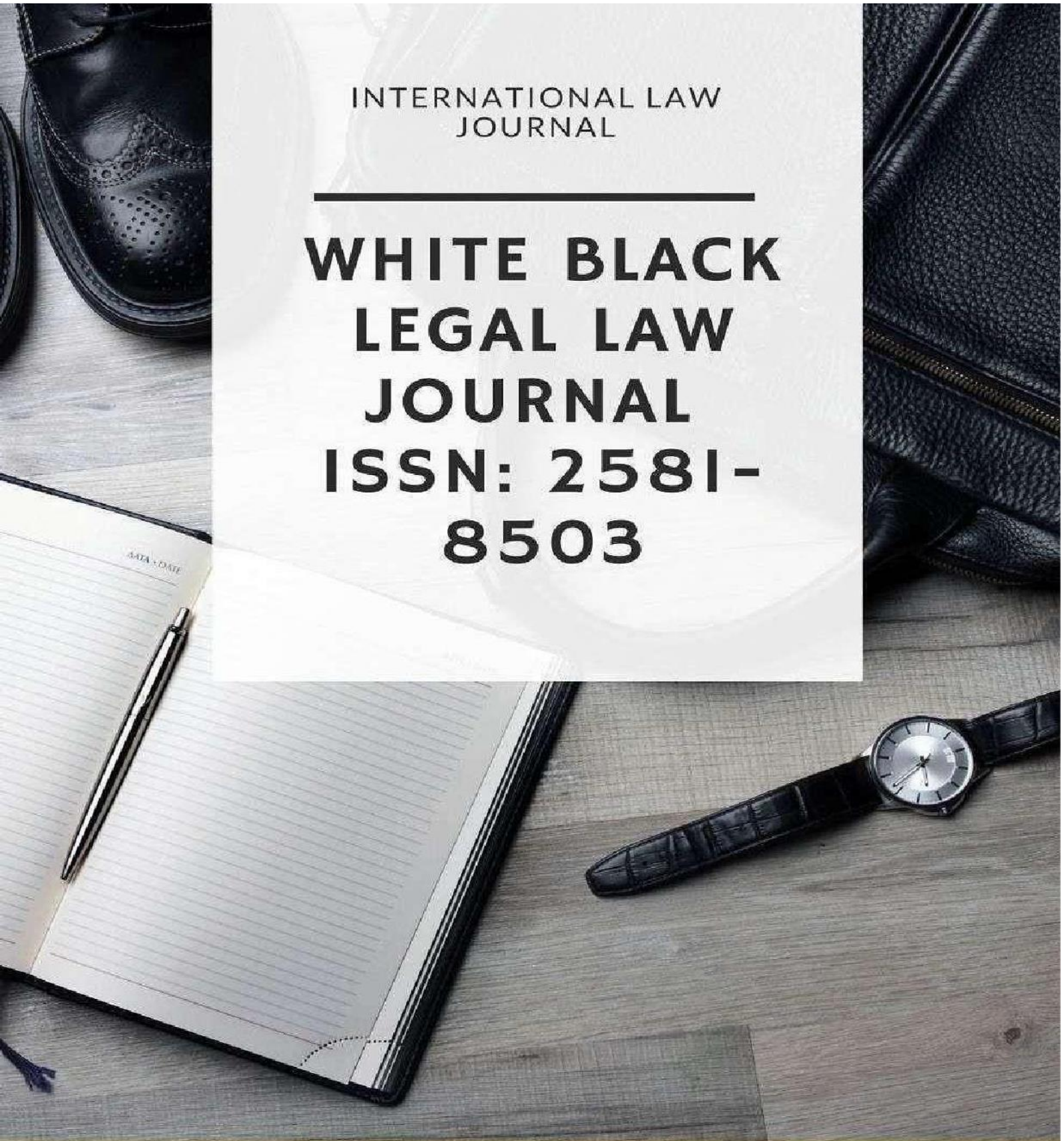




INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

MISLEADING AND UNFAIR TRADE PRACTICES **IN PLATFORM-BASED SERVICES**

Study of Consumer Autonomy, Digital Choice Architecture and Platform Accountability

AUTHORED BY - AVDHESH MISHRA:

Research Scholar: S.N. College of Law – Nirwan University-Jaipur

CO-AUTHOR - PROF. (DR.) RAKESH DAIYA

Principal & Dean: S.N. College of Law – Nirwan University-Jaipur

Abstract

Platform-based services have transformed consumer transactions from relatively linear exchanges into data-intensive, multi-actor environments in which search ranking, interface design, targeted advertising, recommender systems, reviews, automated pricing and standard-form digital contracts shape the consumer's decision before the legal act of purchase is completed. This article examines whether conventional doctrines of MISLEADING and unfair trade practice can adequately respond to this transformation, with India as the principal jurisdiction and the European Union, United Kingdom and United States used for comparison. The study adopts a doctrinal-comparative method supported by peer-reviewed literature on dark patterns, deceptive reviews, algorithmic pricing and platform governance. It argues that digital deception should not be confined to provably false words. A legally relevant MISLEADING may arise from an overall transactional architecture where design, omission, ranking or personalization materially distorts the consumer's understanding or choice. The Indian Consumer Protection Act, 2019, Consumer Protection (E-Commerce) Rules, 2020, CCPA advertising guidelines and the Guidelines for Prevention and Regulation of Dark Patterns, 2023 provide an increasingly coherent consumer-law response, while the Information Technology Act, 2000 continues to govern conditional intermediary safe harbour. The Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 add an important but phased data-governance layer. Comparative analysis shows that the EU Digital Services Act moves most clearly toward interface-level accountability, while the United States retains a broad deception model under Section 5 of the Federal Trade Commission Act. The article proposes a control-and-contribution test for platform accountability, auditable design

duties for high-impact interfaces, verifiable review systems, transparent total-price rules and coordinated consumer-data enforcement. The central claim is that platform law should protect not only informational accuracy but the integrity of the consumer decision-making environment.

Keywords: Misleading; unfair trade practices; platform economy; e-commerce; dark patterns; consumer autonomy; fake reviews; algorithmic pricing; intermediary liability; digital consumer protection.

1. Introduction

Digital commerce is no longer adequately described as the electronic equivalent of a physical sale. A contemporary platform does more than host an offer. It determines which products are visible, how alternatives are ranked, when urgency is displayed, whether a review appears credible, what information is highlighted, how difficult cancellation will be and, increasingly, what price or promotional message a particular consumer sees. The legal character of the transaction therefore depends not only on statements made by a seller but also on the architecture through which the platform structures attention and choice. This shift is especially important for the law of MISLEADING and unfair trade practices because both fields are concerned with the quality of the information and influence that precede consent.

Traditional MISLEADING doctrine is built around identifiable representations, inducement and consent. In India, Sections 17 and 18 of the Indian Contract Act, 1872 distinguish fraud from MISLEADING, while Section 19 addresses voidability where consent has been caused by coercion, fraud or MISLEADING. These principles remain important, yet platform transactions create a harder attribution problem. The consumer may be influenced by a scarcity banner generated by the platform, a seller-supplied product description, an algorithmically ordered review list, a sponsored recommendation that resembles neutral content, and a preselected add-on presented in the same transaction. A legal framework that asks only whether one sentence was false risks overlooking the cumulative effect of the digital choice environment.

Consumer law has begun to respond to this gap. The Consumer Protection Act, 2019 recognizes unfair trade practices and misleading advertisements and establishes the Central Consumer Protection Authority (CCPA). The Consumer Protection (E-Commerce) Rules, 2020 impose duties on e-commerce entities, marketplace entities and sellers. The CCPA's 2022 Guidelines

on misleading advertisements and its 2023 Guidelines on dark patterns move regulation closer to the interface itself. The 2023 Guidelines identify specified patterns such as false urgency, basket sneaking, confirm shaming, forced action, subscription traps, interface interference, bait and switch, drip pricing and disguised advertisement. Their significance is doctrinal as well as regulatory: they accept that deception may be embedded in design rather than expressed through a conventional verbal representation.

The empirical literature supports this regulatory concern. Mathur et al. (2019), in a large-scale crawl of approximately 11,000 shopping websites, identified 1,818 instances of dark patterns across multiple categories and found third-party entities offering such techniques as services. Luguri and Strahilevitz (2021) experimentally demonstrated that several dark-pattern techniques can materially alter consumer decisions. Brenncke (2024) places the problem within a theory of behavioural exploitation and consumer autonomy, arguing that digital choice architecture can interfere with reflective decision-making even when formal freedom of choice remains. Recent work on algorithmic pricing also shows that dynamic pricing can reduce trust and extend consumer search (Vomberg, Homburg & Sarantopoulos, 2025), while research on deceptive reviews demonstrates that review integrity directly affects brand evaluation, search visibility and purchasing behaviour.

These developments create a central research problem. Platform-based services combine characteristics of intermediaries, marketplaces, advertisers, data processors, payment facilitators and, in some models, sellers. The platform may disclaim responsibility for third-party content while simultaneously shaping the commercial meaning of that content through ranking, badges, fulfilment labels, review moderation and personalized display. Safe-harbour doctrine was never designed to become a general immunity from independent consumer-law obligations. A legally defensible framework must therefore distinguish liability for merely hosting third-party information from liability arising from the platform's own representation, design choice, commercial intervention or failure to perform a statutory duty.

This article makes three contributions. First, it develops an integrated account of digital MISLEADING that links contract doctrine with unfair-trade-practice regulation and behavioural evidence. Second, it proposes a functional approach to platform responsibility based on control, contribution and consumer reliance rather than the formal label attached to the platform. Third, it places the Indian framework in comparative perspective with the EU Digital Services Act (DSA), the EU Artificial Intelligence Act, UK consumer law and the US Federal Trade Commission's deception standard. The resulting argument is not that every persuasive interface is unlawful. Commercial persuasion is ordinary market conduct. The legal

threshold should instead focus on whether a representation, omission or design practice materially distorts the consumer's capacity to make a free and informed transactional decision or creates a misleading overall impression that the responsible actor could reasonably prevent or correct.

The timing of the inquiry is also significant. India has moved beyond a purely sectoral approach to digital consumer problems. At the same time, the Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 are being brought into force on a phased schedule. As of September 2026, the commencement notification of November 2025 has activated specified institutional and miscellaneous provisions, while major substantive processing obligations are scheduled for later phases. Any analysis that treats the entire DPDP regime as fully operative today would therefore be legally imprecise. This article uses the data-protection framework as part of the emerging regulatory architecture while distinguishing enacted norms from provisions whose commencement is deferred.

2. Research Questions, Objectives and Methodology

The article addresses four research questions: (i) how should MISLEADING be conceptualized when deception is produced by interface design, ranking, personalization or omission rather than a single false statement; (ii) to what extent do Indian contract and consumer-protection laws regulate such practices; (iii) when should a platform bear responsibility for seller-originated or algorithmically amplified deception; and (iv) which comparative regulatory techniques can strengthen Indian law without converting intermediaries into insurers of every third-party act? The objectives are correspondingly doctrinal, evaluative and reform-oriented. The research uses a doctrinal-comparative method. Primary Indian materials include the Indian Contract Act, 1872; Consumer Protection Act, 2019; Consumer Protection (E-Commerce) Rules, 2020; Information Technology Act, 2000; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; the 2022 misleading-advertising guidelines; the 2023 dark-pattern guidelines; and the DPDP Act and Rules. Judicial materials are used selectively to explain intermediary safe harbour, platform participation and the relationship between statutory duties and online facilitation. Comparative primary materials include Regulation (EU) 2022/2065 (Digital Services Act), Directive 2005/29/EC on unfair commercial practices, Regulation (EU) 2024/1689 (Artificial Intelligence Act), UK consumer law and the US Federal Trade Commission Act.

The literature component is designed in a Scopus-oriented manner: priority is given to recent

peer-reviewed work from established journals and conference proceedings addressing online choice architecture, consumer autonomy, fake reviews, algorithmic pricing and platform governance. The purpose is not a statistical meta-analysis and no claim is made that the search reproduces the proprietary Scopus database exhaustively. Instead, the reviewed studies are used to identify empirically documented forms of consumer influence and to test whether legal doctrine is capable of recognizing those forms. This distinction matters because a doctrinal article should not convert behavioural evidence into legal conclusions without identifying the normative step that connects the two.

The analytical method applies five criteria to each practice: source of the representation or influence; degree of platform control; materiality to the consumer decision; transparency and verifiability; and availability of an effective remedy. These criteria permit comparison across seemingly different practices such as false scarcity, fake reviews and dynamic pricing. They also support a more disciplined approach to platform liability than a binary distinction between 'publisher' and 'neutral intermediary'.

3. Literature Review: From False Statements to Manipulative Choice

Architecture

The first strand of relevant literature concerns dark patterns and online choice architecture. Mathur et al. (2019) demonstrated that manipulative interface practices are not isolated design accidents but observable patterns at scale. Their taxonomy and large empirical dataset helped shift scholarly attention from individual instances of poor design to systematic techniques capable of steering consumers. Luguri and Strahilevitz (2021) then provided experimental evidence that certain dark patterns materially affect consumer behaviour. Their findings are legally significant because materiality and inducement are central concepts in both deception law and MISLEADING doctrine. Where a design intervention reliably changes a transactional decision, a regulator has a stronger basis for treating the practice as more than mere aesthetic persuasion.

Brenncke (2024) adds a normative dimension. Rather than reducing consumer harm to economic welfare alone, the analysis treats behavioural exploitation as an interference with autonomy. This is especially useful for platform law because many dark patterns do not remove formal choice. The consumer can technically refuse a preselected option, find the cancellation route or ignore a repeated prompt. The concern is that the interface deliberately increases friction for one option and decreases it for another in order to exploit predictable biases. The

legal question then becomes whether formal click-based consent should carry the same weight when the platform has engineered the pathway to secure it.

Koh and Seah (2023) provide additional experimental support from e-commerce settings, finding that multiple dark-pattern techniques can influence product selection and that limited-time messaging can be particularly effective. Their study also indicates that vulnerability may not be evenly distributed across consumers. For legal analysis, this reinforces two propositions: first, interface interventions can have measurable transactional effects; second, the reasonable-consumer inquiry should remain sensitive to contexts in which particular groups are predictably more susceptible to pressure or confusion.

A second strand concerns online reviews and reputation systems. Harrison-Walker and Jiang (2023) show that suspicion of fake reviews affects attitudes toward reviewers, brands and websites. Yin, Bond and Zhang (2025) examine consumers' truth bias in judging review authenticity, demonstrating that consumers may systematically over-credit apparently genuine reviews. Jin, Yang and Hosanagar (2022) study 'brushing', where merchants create fake orders to improve ranking, showing how manipulation of platform metrics can affect search visibility even before a consumer reads a review. These findings broaden the legal conception of deception. The unfair advantage may arise not merely because a fake review contains a false opinion, but because fabricated transaction signals alter the ranking system that determines what consumers encounter.

Technical research on fake-review detection similarly confirms that review integrity is a platform-governance problem. Deshai and Bhaskara Rao (2023) and other computational studies develop detection techniques based on content, behaviour and relational features. The existence of such tools does not imply that every undetected fake review proves negligence. It does, however, weaken claims that platforms are technologically incapable of taking proportionate preventive measures. A reasonable-duty inquiry can therefore consider the availability, cost and reliability of detection mechanisms alongside the scale and risk profile of the platform.

A third strand addresses algorithmic pricing. Dynamic pricing is economically legitimate in many settings: prices may reflect demand, inventory, time, capacity or competitor activity. Legal concern arises when consumers are misled about the nature of the price, when additional mandatory charges are hidden until a late stage, when false urgency is coupled with personalized pricing, or when sensitive data are used contrary to applicable law. Vomberg et al. (2025) find that algorithmic dynamic pricing can reduce consumer trust and increase search duration, even though adaptation may occur over time. Spann et al. (2026) situate algorithmic

pricing within both marketing strategy and regulation, highlighting the need to distinguish efficiency-enhancing pricing from manipulative or collusive applications.

A fourth strand concerns platform liability and the changing boundary between intermediary and market organizer. Aade (2025), examining social-media commerce under the DSA, observes that social platforms increasingly function as commercial marketplaces. The conceptual difficulty is familiar in India: a service may claim intermediary status while offering integrated payments, advertising, shopping tags, seller verification, recommendation tools and transaction support. The more a platform designs the commercial encounter, the less persuasive a purely passive characterization becomes for duties that arise from its own conduct.

Taken together, the literature reveals a gap in legal analysis. Computer science and behavioural research can identify manipulative design; marketing research can measure trust and search effects; information-systems research can study ranking manipulation; and consumer-law scholarship can theorize autonomy. Yet MISLEADING doctrine often remains organized around a relatively discrete statement made by an identifiable contracting party. The platform economy requires a bridge between these literatures. That bridge should not abandon established legal elements. It should reinterpret representation, inducement, materiality and responsibility in light of how digital transactions are actually structured.

Table 1. Selected Peer-Reviewed Literature and Its Legal Relevance

Study	Field / Source	Principal contribution	Legal relevance
Mathur et al. (2019)	HCI/ Proceedings of the ACM on Human-Computer Interaction	Large-scale identification and taxonomy of dark patterns on shopping sites	Supports prevalence, foreseeability and design-based deception analysis
Luguri & Strahilevitz (2021)	Journal of Legal Analysis	Experimental evidence on effectiveness of dark patterns	Links design interventions to material consumer decisions and consent
Brenncke (2024)	Journal of Consumer Policy	Autonomy-based theory of behavioural	Provides normative threshold for regulating

		exploitation	manipulative choice architecture
Harrison-Walker & Jiang (2023)	Journal of Business Research	Consumer cues and consequences of suspected fake reviews	Shows reputational and purchasing consequences of review deception
Yin, Bond & Zhang (2025)	Information Systems Research	Truth bias and authenticity judgments in online reviews	Supports stronger review-integrity and provenance duties
Vomberg et al. (2025)	International Journal of Research in Marketing	Trust and search effects of algorithmic dynamic pricing	Distinguishes legitimate dynamic pricing from transparency/fairness risks
Aade (2025)	Computer Law & Security Review	Consumer protection in social-media commerce under DSA	Shows convergence of social networks and marketplaces and need for functional platform duties

4. Reconstructing MISLEADING for Platform-Based Services

MISLEADING in platform transactions should begin with the conventional requirement of a representation or legally relevant misleading conduct. Section 18 of the Indian Contract Act addresses positive assertions not warranted by information, breach of duty that gains an advantage by misleading another, and innocent causation of mistake as to the substance of the subject matter. Section 17 separately defines fraud, including active concealment and promises made without intention of performing them. The distinction between fraudulent and non-fraudulent MISLEADING remains important because intention, proof and remedies differ. Digitalization does not erase these elements; it changes the form in which the misleading impression may be produced.

A representation should therefore be understood functionally. A prominent 'Only one room left' banner communicates a factual proposition even if generated automatically. A crossed-out

reference price communicates a comparison. A platform badge labelled 'verified' communicates something about authentication. A default add-on positioned as necessary may communicate an implication even where the text is technically qualified. The legal system has long recognized that half-truths, context and conduct can matter. Platform design simply increases the range of non-verbal and composite signals from which a reasonable consumer forms an understanding.

Materiality offers the necessary limiting principle. Not every visual asymmetry should trigger legal liability. A practice becomes legally serious when it is capable of affecting a transactional decision concerning whether, with whom, on what terms or at what price a consumer contracts. This criterion aligns the Indian consumer-law concept of misleading commercial conduct with the US FTC's long-standing focus on representations, omissions or practices likely to mislead consumers acting reasonably where the matter is material. It also resembles the EU emphasis on practices that materially distort or impair free and informed decisions.

Inducement must also be adapted carefully. In a conventional bilateral transaction, the claimant may identify a statement and testify that it induced the contract. In a high-volume platform, a particular representation may be one element of a sequence: ranking creates visibility, a review creates trust, a scarcity signal creates urgency and a preselected option affects price. Courts and regulators should permit proof of inducement through the transaction as a whole, supported where appropriate by interface records, A/B testing evidence, internal metrics and behavioural data. This does not reverse the burden of proof automatically; it recognizes that platforms themselves often possess the best evidence of how interface interventions are designed and measured.

The concept of consumer autonomy adds a second limiting principle. The objective is not to forbid persuasion. A well-designed interface may legitimately reduce complexity and help consumers decide. The legal concern is asymmetric manipulation: the platform intentionally or foreseeably makes the commercially preferred option easier to select while making refusal, cancellation or price comprehension materially harder. Where design interferes with the consumer's ability to translate genuine preferences into action, formal assent becomes less persuasive as evidence of meaningful consent.

5. Indian Legal Framework Governing Digital MISLEADING and Unfair Trade Practices

5.1 Consumer Protection Act, 2019 and the E-Commerce Rules

The Consumer Protection Act, 2019 is the principal statutory anchor for unfair digital trade practices. Section 2(47) defines 'unfair trade practice' broadly and includes false representations concerning quality, standard, sponsorship, approval, price and other characteristics, as well as misleading conduct associated with the promotion or supply of goods and services. The Act also defines misleading advertisements and gives the CCPA market-wide powers that go beyond the resolution of a single bilateral dispute. This architecture is particularly suitable for platform harms because a single interface practice may affect thousands or millions of consumers even where the monetary injury to each individual is small.

The Consumer Protection (E-Commerce) Rules, 2020 recognize the institutional role of e-commerce entities. They apply duties concerning grievance redress, transparency and information, while separate provisions address marketplace entities, sellers and inventory models. The legal importance of the Rules lies in their functional differentiation. A marketplace may not be the seller of every product, but that fact does not eliminate duties imposed on it in its capacity as an e-commerce entity. Conversely, the presence of platform duties does not automatically make the marketplace liable for every defect or MISLEADING created solely by a seller. Liability must be tied to the specific statutory obligation or the platform's own conduct.

The Rules also challenge the notion that platform disclaimers can settle liability in advance. Consumer law is mandatory in important respects. A contractual term describing the platform as a mere facilitator cannot negate a statutory obligation to provide specified information, maintain grievance mechanisms or avoid unfair conduct. Where a platform independently makes a representation—such as a verification claim, fulfilment guarantee, ranking label or sponsored endorsement—that representation should be assessed as the platform's own, even if the underlying product is supplied by a third party.

5.2 Misleading Advertisements and Endorsements

The CCPA's Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 strengthen the regulatory treatment of digital promotion. They require advertising claims to satisfy conditions of truthfulness and substantiation and address bait advertisements, free-claim advertisements and endorsements. This is important for

platform services because the distinction between editorial content, influencer communication and paid promotion is often visually blurred. A sponsored result that resembles an organic recommendation can mislead not because the product claim is false but because the commercial relationship is concealed or insufficiently prominent.

Digital advertising also raises attribution issues. Advertisers, endorsers, agencies and platforms may each contribute to the final message. Consumer law should therefore distinguish the originator of the substantive claim from the actor that controls its presentation. A platform that simply transmits an advertisement under a transparent advertising system occupies a different position from a platform that rewrites claims, assigns credibility badges, suppresses sponsorship disclosures or targets vulnerable groups through data-driven optimization. The appropriate legal response is actor-specific rather than collective liability without fault.

5.3 Dark Patterns Guidelines, 2023

The 2023 Dark Patterns Guidelines are among the most important Indian developments for this field. Issued under the CCPA's statutory authority, the Guidelines identify thirteen specified dark patterns and treat manipulative design as a consumer-protection issue. The list includes false urgency, basket sneaking, confirm shaming, forced action, subscription traps, interface interference, bait and switch, drip pricing, disguised advertisement and other practices. The significance of the Guidelines is not merely the taxonomy. They articulate a principle that the design and choice architecture of a digital interface can amount to an unfair trade practice where it subverts or impairs consumer autonomy, decision-making or choice.

False urgency illustrates the convergence between MISLEADING and design. If a platform displays a fabricated countdown timer or scarcity message, the practice contains a factual MISLEADING and a behavioural nudge. Drip pricing illustrates a different mechanism: the initial price may be literally true but incomplete in a way that prevents meaningful comparison until the consumer has invested time in the transaction. Subscription traps and difficult cancellation show that unfairness can arise after contract formation, where exit friction is deliberately made disproportionate to entry. A coherent legal framework should therefore regulate the lifecycle of the digital transaction, not merely the pre-contract advertisement.

The Guidelines also help resolve a common objection that 'nudges' are too subjective to regulate. The law need not determine whether every interface is psychologically manipulative in the abstract. It can identify objective design features: default selections, hidden mandatory charges, asymmetrical cancellation steps, repeated prompts after a decision, false stock indicators and disguised advertising. Evidence of consumer impact and internal design intent

can then inform enforcement priority and penalty, but basic illegality may be established from the practice itself where the guideline is sufficiently specific.

5.4 Information Technology Act, 2000 and Intermediary Safe Harbour

Section 79 of the Information Technology Act, 2000 provides conditional safe harbour for intermediaries in relation to third-party information, subject to statutory requirements. The provision is essential to the functioning of online services because automatic liability for every third-party statement would produce excessive monitoring and removal. Yet safe harbour should be kept conceptually separate from independent duties. If liability is alleged because a marketplace itself displayed a misleading verification badge, designed an unlawful dark pattern or failed to satisfy a consumer-rule obligation, the claim is not necessarily one 'for third-party information' merely because a third-party seller participated in the transaction.

Shreya Singhal v. Union of India, (2015) 5 SCC 1, remains central to the interpretation of 'actual knowledge' in Section 79(3)(b), which the Supreme Court read down in the context of unlawful content to knowledge through a court order or notification by the appropriate government or agency. The judgment protects intermediaries from being required to adjudicate the legality of all user content on private notice alone. Consumer-platform disputes, however, may involve different questions: statutory disclosure duties, contractual representations, product listing systems and platform-created transaction architecture. *Shreya Singhal* should therefore not be transformed into a general proposition that intermediaries owe no consumer-facing duties until a court order arrives.

Christian Louboutin SAS v. Nakul Bajaj, 2018 SCC OnLine Del 12215, is frequently discussed because the Delhi High Court examined the extent of an e-commerce platform's participation in the sale process when considering intermediary protection. The case arose in an intellectual-property setting and should not be mechanically transplanted into consumer law, but its functional inquiry is useful: the more a platform contributes to the commercial transaction and representation, the more carefully courts should identify which conduct is genuinely third-party content and which is the platform's own activity. *Google India Pvt. Ltd. v. Visakha Industries*, (2020) 4 SCC 162, similarly confirms that Section 79 is a statutory safe-harbour regime whose conditions and temporal application matter; it is not a freestanding immunity detached from the text of the Act.

5.5 Digital Personal Data Protection: Relevance and Current Commencement

Data processing is increasingly inseparable from digital MISLEADING because

personalization determines what a consumer sees, in what sequence and sometimes at what price. The Digital Personal Data Protection Act, 2023 creates a statutory framework for digital personal data, and the Digital Personal Data Protection Rules, 2025 provide implementation details. The 2025 commencement notification, however, staggers the entry into force of the Act. As of September 2026, specified provisions concerning definitions, the Data Protection Board and miscellaneous matters have commenced, while substantial processing obligations are scheduled for later dates under the notification. The same phased structure appears in the Rules, with only specified rules immediately effective and others commencing after one year or eighteen months.

This phased status matters for legal scholarship. It is tempting to state that a personalized dark pattern already violates every consent and data-fiduciary obligation in the DPDP Act, but such a claim may be premature before the relevant section commences. A more accurate position is that data-protection legislation establishes the direction of Indian digital governance and will increasingly interact with consumer law as substantive provisions come into force. Until then, consumer law, contract law, existing information-technology duties and sectoral rules remain central to deceptive platform design.

Table 2. Indian Legal Framework and Platform Conduct

Instrument	Relevant subject	Platform implication
Indian Contract Act, 1872, ss. 17-19	Fraud, MISLEADING and voidability	Applies to consent induced by materially misleading representations or conduct
Consumer Protection Act, 2019	Unfair trade practices, misleading advertisements, CCPA powers	Supports individual and market-wide remedies against deceptive digital conduct
Consumer Protection (E-Commerce) Rules, 2020	Duties of e-commerce entities, marketplaces and sellers	Creates platform-specific disclosure and grievance obligations
CCPA Misleading Advertisement Guidelines, 2022	Truthfulness, substantiation and endorsements	Relevant to sponsored results, influencer promotion and platform advertising
CCPA Dark Patterns	Manipulative interface	Directly addresses choice

Guidelines, 2023	design	architecture such as false urgency, drip pricing and subscription traps
Information Technology Act, 2000, s.79	Conditional intermediary safe harbour	Protects qualifying third-party hosting but does not erase independent platform duties
DPDP Act, 2023 & Rules, 2025	Digital personal data; phased commencement	Emerging relevance to profiling, personalization and data-driven consumer influence

6. Principal Forms of MISLEADING and Unfair Trade Practice on Platforms

6.1 False Urgency, Scarcity and Reference Pricing

Scarcity and urgency claims illustrate the clearest overlap between conventional MISLEADING and behavioural design. Statements such as 'two seats left', 'twenty people are viewing this room' or 'offer ends in five minutes' can affect purchasing speed and reduce comparison. Where the statement is fabricated or materially misleading, the issue is not merely that the consumer was nudged; a factual proposition has been communicated. Automated generation does not remove responsibility. The legally relevant inquiry is who designed or supplied the rule, whether the data supporting the claim existed, whether the representation was reasonably verifiable and whether it was material to the transaction.

Reference pricing raises a related problem. A crossed-out 'original price' may imply that the product was genuinely offered at that higher price or that the reduction is meaningful. If the reference price is artificial, stale or selectively constructed, the consumer receives a misleading comparative signal. Platforms can reduce this risk by requiring sellers to substantiate reference prices and by retaining price-history data for enforcement. Such measures are technically feasible in a digital environment and may be less burdensome than post-hoc litigation over millions of transactions.

6.2 Drip Pricing and Hidden Mandatory Charges

Drip pricing occurs when a consumer is attracted by an incomplete headline price and

mandatory or practically unavoidable charges are disclosed progressively. The harm is not simply surprise at checkout. Late disclosure distorts comparison because the consumer may have already invested time, disclosed data or become psychologically committed to the transaction. The 2023 Dark Patterns Guidelines expressly identify drip pricing as a dark pattern in specified circumstances. A strong legal rule should require the total unavoidable price to be displayed sufficiently early for meaningful comparison, while variable charges should be explained through objective criteria rather than hidden until the final screen.

6.3 Fake Reviews, Review Suppression and Ranking Manipulation

Reviews have become a substitute for physical inspection and personal recommendation. Their informational value depends on authenticity, independence and reasonably neutral presentation. Fake positive reviews, coordinated negative attacks, undisclosed incentivized reviews and suppression of legitimate criticism can each create a misleading impression. The legal wrong is compounded when platform ranking systems convert manipulated reviews into increased visibility, making deception self-amplifying.

A proportionate platform duty should focus on systems rather than perfect outcomes. Large marketplaces should maintain reasonable verification, anomaly detection, conflict-of-interest rules and disclosure mechanisms for incentivized reviews. Consumers should be told whether a reviewer completed a verified transaction and whether any material benefit was provided for the review. Platforms should not claim that reviews are 'verified' unless the verification standard is clear and meaningful. Where an algorithm determines which reviews appear first, the platform should also avoid designs that systematically suppress representative negative information while presenting the resulting score as neutral.

The problem of fake orders or 'brushing' demonstrates why consumer deception can occur upstream of the visible review. Fabricated transactions may improve product ranking and generate a veneer of popularity. A narrow content-based approach that removes only obviously false text will miss this structural manipulation. Platform governance therefore requires integrity controls for transaction signals as well as for written reviews.

Recent platform research strengthens this point. Schneider and Teubner (2024) examine fake reviews in closed reputation systems and show that transaction-linked review systems can still face credibility problems, especially during early reputation formation. Gu, Cao and Fang (2026) find that manipulated reviews can affect product market performance even when platforms later filter them. The regulatory implication is that ex post deletion alone may be insufficient where ranking and visibility effects occur before detection; platforms need

preventive controls, rapid correction and mechanisms capable of addressing downstream ranking consequences.

6.4 Sponsored Rankings, Native Advertising and Influencer Commerce

A search result can mislead by omission when paid placement is presented in a form substantially similar to an organic result. The consumer may reasonably assume that higher placement reflects relevance, quality or popularity rather than payment. Clear, proximate and visually meaningful sponsorship disclosure is therefore necessary. The same principle applies to influencer and creator commerce. A disclosure hidden among hashtags or placed after an expanded caption may be legally inadequate if the overall presentation suggests independent opinion. The 2022 CCPA Guidelines provide a statutory basis for evaluating endorsements, while the platform's own advertising architecture may create additional responsibility where it controls labels and placement.

6.5 Algorithmic Dynamic Pricing and Personalization

Algorithmic pricing should not be treated as inherently deceptive. Airlines, hotels, ride services and retailers have long adjusted prices based on capacity, timing and demand. The legal risk emerges where personalization is opaque in a way that creates a false impression of a universal or time-limited price, where a consumer is shown fictitious discounts, or where the system uses data in a legally impermissible manner. The empirical finding that algorithmic pricing can reduce trust does not itself establish unlawfulness; distrust is a market response, while deception requires a misleading representation, omission or practice or another applicable statutory violation.

A workable regulatory approach should therefore distinguish dynamic pricing from deceptive price architecture. Platforms should disclose the total price and material mandatory components, avoid false scarcity, explain material personalization where legally required or necessary to prevent a misleading impression, and retain audit records for high-impact pricing systems. Competition law may address collusive or parallel-pricing concerns, while consumer law should focus on transparency, fairness of presentation and misleading individualized claims.

6.6 Subscription Traps, Confirm Shaming and Asymmetric Friction

Subscription traps reveal why post-contract design matters. A consumer may sign up through one click but face multiple menus, retention prompts, hidden links or mandatory telephone calls

to cancel. The DSA expressly identifies making termination more difficult than subscription as a paradigmatic dark-pattern concern, and India's 2023 Guidelines similarly address subscription traps and interface interference. The legal principle should be symmetry of material transactional friction: businesses may confirm a cancellation or explain consequences, but they should not deliberately convert exit into an obstacle course designed to defeat the consumer's previously expressed decision.

7. A Functional Test for Platform Accountability

The central liability question is not whether platforms are always publishers or always neutral conduits. Both propositions are too crude. Platform responsibility should be assessed through a functional test based on control, contribution and reliance. 'Control' asks whether the platform could determine the design, ranking, label, disclosure or transaction process at issue. 'Contribution' asks whether the platform created, materially modified, amplified or commercially integrated the misleading element. 'Reliance' asks whether the platform presented itself to consumers as performing a verification, guarantee, curation or trust function that reasonably influenced the transaction.

This test preserves safe harbour for genuinely third-party information while recognizing independent platform conduct. If a seller uploads a false product description and the platform merely stores it subject to statutory due diligence, the seller is the primary source of the representation. If the platform adds a 'verified authentic' badge without a reasonable verification process, the badge is the platform's own representation. If the platform designs a ranking system that knowingly rewards fake orders or offers sellers paid tools that manufacture false scarcity, contribution and control increase. Liability can therefore be calibrated rather than assumed.

A second principle is proportionality. A small classified-ad service cannot be expected to deploy the same detection infrastructure as a dominant marketplace processing millions of transactions. Duties should reflect scale, risk, technical capacity and the platform's role. However, scale can also increase responsibility because large platforms benefit from extensive behavioural data, centralized interface control and sophisticated experimentation. A firm that can optimize a checkout flow at massive scale can often implement compliance interventions at the same scale.

A third principle is evidentiary accountability. Digital platforms routinely conduct A/B tests, maintain event logs and measure conversion. These records can be highly relevant where the

legality of a design practice depends on whether it was intended or known to distort choice. Regulators should be empowered, subject to confidentiality safeguards, to require production of relevant design and experimentation records in serious investigations. Courts may also draw appropriate evidentiary consequences where a platform fails to preserve records that it was legally required to maintain.

A fourth principle is remedy matching. Deceptive interface cases often involve small individual losses but large aggregate gains. Individual damages alone may under-deter. Effective remedies may include cessation orders, corrective disclosures, refund programmes, interface redesign, administrative penalties, publication of enforcement outcomes and, where legally available, compensation. Online dispute resolution can complement these tools for transaction-specific disputes, while the CCPA is better positioned to address recurring market-wide practices.

8. Comparative Regulatory Perspective

8.1 European Union

The European Union offers the clearest statutory movement toward interface-level regulation. Article 25 of the Digital Services Act prohibits providers of online platforms from designing, organizing or operating interfaces in a manner that deceives or manipulates recipients or otherwise materially distorts or impairs their ability to make free and informed decisions. Recital 67 specifically discusses practices such as giving choices unequal prominence, repeatedly requesting a decision already made and making cancellation significantly more cumbersome than sign-up. The provision is important because it treats interface organization itself as a regulated activity rather than requiring every case to be forced into a conventional false-statement model.

The DSA operates alongside the Unfair Commercial Practices Directive (UCPD), which already prohibits misleading and aggressive commercial practices in business-to-consumer relations. Article 25(2) DSA limits overlap by excluding practices covered by the UCPD or GDPR from the DSA prohibition. This layered structure has advantages and complexity. It allows specialized regimes to apply, but it also requires regulators and businesses to identify the correct legal basis. India's more centralized CCPA guidance avoids some of this fragmentation, though India lacks the same breadth of platform-systemic obligations found in the DSA.

The EU Artificial Intelligence Act, Regulation (EU) 2024/1689, adds another layer relevant to platform manipulation. The Act is risk-based and does not convert all recommendation or

pricing algorithms into high-risk systems. It nevertheless demonstrates a broader regulatory willingness to impose transparency, governance and prohibited-practice rules where AI creates specified harms. For Indian reform, the lesson is not to copy the EU classification wholesale but to recognize that algorithmic consumer influence may require auditable governance when its scale and impact become significant.

8.2 United States

The United States relies heavily on Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices. The FTC's Policy Statement on Deception identifies three familiar elements: a representation, omission or practice likely to mislead; assessment from the perspective of consumers acting reasonably in the circumstances; and materiality. This formulation is notably broad enough to address conduct rather than words alone. US enforcement against negative-option practices, deceptively formatted advertising and manipulative online design demonstrates the adaptability of a general deception standard, although the precise scope of federal rulemaking and remedial authority is institutionally different from India.

8.3 United Kingdom

UK consumer law combines statutory rights, unfair-commercial-practice rules and increasingly assertive competition-and-consumer enforcement. The Consumer Rights Act 2015 remains central to contractual fairness and digital content, while the Competition and Markets Authority has developed substantial work on online choice architecture, subscriptions and consumer-facing digital practices. The UK experience supports a practical point: guidance, enforcement and market studies can evolve faster than primary legislation and can identify design practices before they are fully litigated. India can use CCPA guidance similarly, provided that important coercive duties remain anchored in statutory authority and due process.

Table 3. Comparative Approaches to Digital Consumer Deception

Jurisdiction	Primary legal technique	Strength	Potential limitation
India	CPA 2019 + E-Commerce Rules + CCPA guidelines	Specific dark-pattern taxonomy and centralized	Fragmentation with IT/data regimes; developing platform

	contract law	consumer authority	case law
European Union	UCPD + DSA + GDPR + AI Act	Express interface and systemic platform duties	Complex overlap among legal instruments
United States	FTC Act Section 5 + sectoral rules/enforcement	Flexible deception and unfairness standards	Remedial/rulemaking questions vary with statutory authority
United Kingdom	Consumer statutes + CMA enforcement/guidance	Strong practical enforcement and market studies	Post-Brexit regulatory evolution can produce transitional complexity

9. Findings and Discussion

The first finding is that digital MISLEADING is best understood as an 'overall-impression' problem. The consumer's decision may be shaped by text, colour, ordering, defaults, review signals, price presentation and timing. A legal rule limited to explicit false propositions will under-capture deception, while a rule that treats every persuasive design as unlawful will over-capture ordinary commerce. Material distortion of a transactional decision provides a defensible middle threshold.

The second finding is that Indian law already contains more tools than is sometimes acknowledged. The Consumer Protection Act, e-commerce rules, advertising guidelines and dark-pattern guidelines collectively reach many platform practices. The principal deficiency is not total statutory silence but coordination, evidentiary access and uncertainty regarding how platform-specific consumer duties interact with intermediary safe harbour. Legislative reform should therefore clarify interfaces between regimes rather than simply add another broad prohibition.

The third finding is that platform liability should be functional. The legal position should change as the platform's role changes. A service that hosts a seller's statement is not situated identically to a service that verifies the seller, controls fulfilment, authors a badge, ranks the product using paid criteria and designs the checkout. Control, contribution and consumer reliance provide administrable factors for assigning responsibility without abolishing safe harbour.

The fourth finding is that review and ranking integrity should be treated as consumer-

information infrastructure. Fake reviews are not only false speech; they can corrupt the metrics that structure visibility. A platform's duty should therefore extend to reasonable anti-manipulation systems and accurate statements about verification. The goal is not perfect authenticity, which is unattainable, but a defensible governance process proportional to scale and risk.

The fifth finding concerns algorithmic systems. The law should resist treating 'algorithmic' as a synonym for unlawful. Dynamic pricing, personalization and recommendation can improve matching and reduce search costs. Legal intervention becomes justified when the system creates a misleading impression, exploits hidden mandatory charges, uses fabricated scarcity, unlawfully processes data, discriminates contrary to applicable law or makes significant consumer decisions without adequate transparency and accountability. Regulation should target the harmful mechanism rather than the mere use of automation.

The sixth finding is temporal. Data-protection law is becoming more relevant to consumer manipulation, but India's current phased DPDP commencement requires precise legal writing. Consumer-law enforcement should not be postponed while data provisions await commencement. At the same time, regulators should prepare for convergence because future personalization disputes may simultaneously implicate consent, purpose limitation, consumer deception and algorithmic governance.

The comparative analysis indicates that the EU has moved furthest toward direct regulation of interface design, while the US model demonstrates the continuing value of a broad deception standard. India's distinctive advantage is the CCPA's ability to issue specific consumer guidelines within a general statutory framework. The challenge is to combine specificity with procedural clarity and to avoid guidance becoming a substitute for legislation where substantial new liabilities are created.

10. Legislative and Policy Recommendations

First, India should codify a general digital-choice principle within consumer legislation or rules: an e-commerce entity should not design, organize or operate a transactional interface in a manner that materially deceives, manipulates or impairs a consumer's ability to make a free and informed decision. The existing 2023 Guidelines provide a strong foundation, but a statutory or rule-based articulation would improve durability, enforcement clarity and judicial application.

Second, platform accountability should be expressly separated into two categories: liability for

third-party information and liability for the platform's independent conduct. Section 79 safe harbour should continue to protect qualifying intermediary activity, while consumer rules should clarify that safe harbour does not exempt a platform from its own statutory disclosures, guarantees, verification claims, advertising practices, dark patterns or transaction design. This would reduce unnecessary doctrinal conflict.

Third, large marketplaces should maintain review-integrity programmes proportionate to scale. Minimum expectations should include detection of anomalous review and transaction patterns, clear disclosure of incentivized reviews, meaningful verified-purchase labels, documented procedures for contesting review manipulation and periodic transparency reporting. Regulators should avoid prescribing a single detection algorithm because technical methods evolve rapidly.

Fourth, total-price transparency should be strengthened. Mandatory charges that are unavoidable for completion of a transaction should ordinarily be incorporated into the price displayed at the stage at which consumers compare offers. Where the charge genuinely depends on information not yet available, the platform should explain the calculation basis prominently. False reference pricing and fabricated discount claims should be supported by auditable price history.

Fifth, cancellation and refusal should satisfy a symmetry principle. A consumer should not face materially greater procedural friction to reject an optional add-on, withdraw from a recurring service or exercise a cancellation right than was required to accept it, subject to legitimate security and identity checks. This principle translates the dark-pattern taxonomy into an administrable design standard.

Sixth, sponsored ranking and native advertising require standardized disclosure. The label should be immediate, proximate and understandable, and the consumer should be able to distinguish paid placement from organic relevance without opening secondary menus. Platforms should also disclose the principal commercial parameters that materially determine sponsored ranking where such disclosure is necessary to avoid a misleading impression.

Seventh, regulators should develop secure access to platform design evidence. In serious investigations, the CCPA should be able to seek relevant A/B testing records, interface change logs, complaint patterns and conversion metrics within statutory powers and subject to confidentiality safeguards. Such evidence can show whether a challenged design was accidental, experimental, known to affect consumer decisions or deliberately retained because of increased conversion despite consumer harm.

Eighth, online dispute resolution should be integrated more closely with platform grievance

systems and consumer commissions. Standardized digital complaint data would allow authorities to identify recurring practices rather than treating each consumer's problem as isolated. Refunds, corrective disclosures and interface changes can often provide more effective relief than conventional litigation alone.

Ninth, the CCPA, MeitY, competition authorities and sectoral regulators should establish a formal coordination protocol for cases involving overlapping consumer, data, competition and cybersecurity issues. Coordinated enforcement reduces duplicative demands on firms while preventing regulatory gaps. As substantive DPDP obligations commence, this coordination will become increasingly important for personalized advertising, recommendation and profiling disputes.

Tenth, India should adopt risk-based audit expectations for high-impact automated consumer systems rather than a generic requirement to disclose source code. Audits can examine input governance, testing for deceptive outputs, pricing logic, complaint outcomes, human oversight and change management. Source-code disclosure is often neither necessary nor proportionate; what regulators need is evidence capable of testing legal compliance and causal responsibility. Eleventh, consumer literacy should be treated as a complement to regulation, not a substitute for it. Public campaigns can explain fake reviews, paid rankings, subscription traps and data-driven personalization, but firms should not be permitted to defend manipulative architecture on the ground that a sufficiently sophisticated user could have discovered the truth. The legal benchmark must remain reasonable consumer decision-making in the relevant context, with sensitivity to vulnerable groups.

Finally, enforcement should be outcome-sensitive. Repeated, scalable dark patterns that generate substantial aggregate revenue deserve higher priority than isolated technical defects. Penalties, corrective orders and refund programmes should account for the number of affected consumers, duration of the practice, knowledge, benefit obtained, remedial cooperation and risk of recurrence. This approach would align deterrence with the economic scale of platform-based harm.

11. Limitations and Scope for Future Research

This article is doctrinal and comparative rather than empirical. It does not measure the prevalence of particular dark patterns in Indian platforms, nor does it estimate consumer loss. Future research should conduct systematic interface audits across Indian e-commerce, travel, food-delivery, fintech and subscription services and should test how Indian consumers respond

to scarcity, defaults and cancellation friction. Empirical work would also help determine whether particular groups are disproportionately affected by deceptive design.

A second research agenda concerns AI-generated commercial communication. Generative systems can produce personalized product descriptions, virtual influencers, synthetic endorsements and automated customer-service representations at scale. Future legal research should examine attribution, evidentiary provenance and the standard of reasonable testing before such systems are deployed. A third agenda concerns the interaction between consumer law and the phased DPDP framework as substantive provisions commence. Longitudinal analysis will be necessary to determine whether the two regimes converge effectively or create overlapping and inconsistent compliance duties.

12. Conclusion

Platform-based services have changed the mechanics of consumer deception. The legally relevant representation may now be a sentence, a badge, a ranking position, a countdown timer, a hidden fee, a review score, a default setting or a sequence of design choices that collectively create a misleading impression. Contract law remains relevant because consent and inducement still matter, but consumer law is better equipped to address scalable practices that affect entire markets.

India's present framework is not empty. The Consumer Protection Act, 2019, E-Commerce Rules, advertising guidelines and Dark Patterns Guidelines create a substantial foundation. Section 79 of the Information Technology Act appropriately protects qualifying intermediary functions but should not be interpreted as immunity from a platform's independent consumer-facing duties. The DPDP regime will add another layer as its substantive provisions enter into force on the notified schedule.

The most workable legal principle is functional accountability. Responsibility should follow control over the relevant interface or information, contribution to the misleading practice and the reliance reasonably invited from consumers. Combined with materiality, proportionality and effective remedies, this framework can distinguish legitimate persuasion and innovation from deception without requiring courts to treat every algorithm or marketplace feature as inherently suspect.

The deeper policy objective is the integrity of the consumer decision-making environment. Digital markets cannot depend solely on the fiction that every click represents a fully autonomous and informed choice when platforms can experimentally optimize the path to that

click. A trustworthy platform economy requires accurate information, intelligible prices, authentic reputation signals, fair exit mechanisms and accountability for design practices that materially distort choice. Protecting those conditions is not hostile to innovation; it is part of the legal infrastructure that makes digital commerce sustainable.

References

1. Aade, L. (2025). The regulation of social media commerce under the DSA: A consumer protection perspective. *Computer Law & Security Review*, 59, 106181. <https://doi.org/10.1016/j.clsr.2025.106181>
2. Brennecke, M. (2024). A theory of exploitation for consumer law: Online choice architectures, dark patterns, and autonomy violations. *Journal of Consumer Policy*, 47, 127-164. <https://doi.org/10.1007/s10603-023-09554-7>
3. Deshai, N., & Bhaskara Rao, B. (2023). Unmasking deception: A CNN and adaptive PSO approach to detecting fake online reviews. *Soft Computing*, 27, 11357-11378. <https://doi.org/10.1007/s00500-023-08507-z>
4. Harrison-Walker, L. J., & Jiang, Y. (2023). Suspicion of online product reviews as fake: Cues and consequences. *Journal of Business Research*, 158, 113780. <https://doi.org/10.1016/j.jbusres.2023.113780>
5. Jin, C., Yang, L., & Hosanagar, K. (2022). To brush or not to brush: Product rankings, consumer search, and fake orders. *Information Systems Research*. <https://doi.org/10.1287/isre.2022.1128>
6. Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43-109. <https://doi.org/10.1093/jla/laaa006>
7. Koh, W. C., & Seah, Y. Z. (2023). Unintended consumption: The effects of four e-commerce dark patterns. *Cleaner and Responsible Consumption*, 11, 100145. <https://doi.org/10.1016/j.clrc.2023.100145>
8. Schneider, F., & Teubner, T. (2024). Fake it till you make it—A statistical assessment of the proportion of fake reviews in closed reputation systems. *International Journal of Electronic Commerce*, 28(4), 450-480. <https://doi.org/10.1080/10864415.2024.2401949>
9. Gu, X., Cao, J., & Fang, Y. (2026). Review manipulation and filtering on digital platforms. *Information Systems Research*, 37(2), 927-947. <https://doi.org/10.1287/isre.2022.0694>

10. Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), Article 81, 1-32. <https://doi.org/10.1145/3359183>
11. Spann, M., Bertini, M., Koenigsberg, O., Zeithammer, R., Aparicio, D., Chen, Y., Fantini, F., Jin, G. Z., Morwitz, V. G., Popkowski Leszczyc, P., Vitorino, M. A., Williams, G. Y., & Yoo, H. (2026). Algorithmic pricing: Implications for marketing strategy and regulation. *International Journal of Research in Marketing*, 43(2), 560-579. <https://doi.org/10.1016/j.ijresmar.2025.05.001>
12. Vomberg, A., Homburg, C., & Sarantopoulos, P. (2025). Algorithmic pricing: Effects on consumer trust and price search. *International Journal of Research in Marketing*, 42(4), 1166-1186. <https://doi.org/10.1016/j.ijresmar.2024.10.006>
13. Yin, D., Bond, S. D., & Zhang, H. (2025). The illusion of authenticity in online reviews: Truth bias and the role of valence. *Information Systems Research*, 37(1), 103-116. <https://doi.org/10.1287/isre.2023.0339>
14. Zhang, W., Wang, Q., Li, J., Ma, Z., Bhandari, G., et al. (2023). What makes deceptive online reviews? A linguistic analysis perspective. *Humanities and Social Sciences Communications*, 10, 769. <https://doi.org/10.1057/s41599-023-02295-5>
15. Government of India. (1872). Indian Contract Act, 1872.
16. Government of India. (2000). Information Technology Act, 2000.
17. Government of India. (2019). Consumer Protection Act, 2019.
18. Government of India, Department of Consumer Affairs. (2020). Consumer Protection (E-Commerce) Rules, 2020.
19. Central Consumer Protection Authority. (2022). Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022.
20. Central Consumer Protection Authority. (2023). Guidelines for Prevention and Regulation of Dark Patterns, 2023.
21. Government of India. (2023). Digital Personal Data Protection Act, 2023.
22. Government of India, Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025 and commencement notification G.S.R. 843(E).
23. European Parliament and Council. (2005). Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market.

24. European Parliament and Council. (2022). Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act).
25. European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
26. Federal Trade Commission. (1983). FTC Policy Statement on Deception.
27. United Kingdom. (2015). Consumer Rights Act 2015.
28. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
29. Christian Louboutin SAS v. Nakul Bajaj, 2018 SCC OnLine Del 12215.
30. Google India Pvt. Ltd. v. Visakha Industries, (2020) 4 SCC 162.

