INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

DARK PATTERNS IN CONSUMER PROTECTION ACT, 2019

AUTHORED BY - AARTI S. JAIN,
GD Goenka University

ABSTRACT

Dark patterns are deceptive design methods on e-commerce websites that target consumer interests for the benefit of online platforms rather than the consumer's ability to make informed choices. According to the Consumer Protection Act, 2019, and the issued Guidelines for Prevention and Regulation of Dark Patterns, the way in which dark patterns are used on e-commerce platforms will be considered an unfair trade practice that a consumer will have protections under the law in India. The analysis will examine the taxonomy of dark patterns while covering empirical and regulatory developments (including the Consumer Protection (E-Commerce) Rules, 2020 and recent steps undertaken by the Central Consumer Protection Authority), compare the Indian situation with the international regime (focusing on the U.S. Federal Trade Commission and the EU's ongoing attempts with the Digital Services and Digital Markets regulation), highlight statute and enforcement gaps, and outline doctrinal and solution-level changes to better protect online consumers. This study examines the responsiveness of India's consumer protection framework to digital deception, having used an examination of statutory provisions, and studies from around the world for comparative analysis. It proposes recommendations for increased regulatory oversight and enforcement efforts.[1] It will be demonstrated why, despite CPA 2019 and E-commerce Rules having established a solid framework by treating dark patterns as unfair trade practices and requiring transparency, there is an urgent need for stricter rule-making, greater ex-ante obligations on larger platforms, uniform UI/UX audits, and a more calibrate approach to consumer remedies arising from digital harms.

[1] Dark patterns continue on eCommerce marketplaces in India: Survey

ISSN: 2582-6433

1. INTRODUCTION

Dark patterns are becoming more prevalent in online shopping, creating serious threats to consumer rights and trust. These misleading design tactics manipulate psychological biases and hide crucial information, often resulting in users making unintentional purchases, disclosing personal information, or missing out on refunds. Authorities around the globe have acknowledged the seriousness of these practices, with India making significant progress in addressing them through the Consumer Protection Act of 2019.[2]

Rationale and Research Problem

The rapid growth of e-commerce in India has changed the way people shop and a larger marketplace framework. With digital convenience at the forefront of today's consumption, online platforms have gained tremendous power over consumption decisions. However, the power is not always used in a fair or transparent manner. More frequently, online platforms incorporate design components and elements of the interface that covertly influence user decisions, directing them toward actions that are advantageous to the seller but disadvantageous to the buyer. These manipulative interface designs, referred to as dark patterns, are among the most serious ethical and legal issues in e-commerce today.

This study's justification is rooted in the pressing need to understand how these deceptive design techniques operate, how they impact consumers psychologically and how effective India's current legal and regulatory systems are at preventing them. Whereas more traditional forms of unfair trading practices (such as misinformation in advertising or misrepresentations) are well-defined in consumer protection law, the more covert forms of technologically-mediated deception inherent in dark patterns are detectable but harder to prove. As the dark patterns are embedded within the interface architecture, they are typically undetectable to a traditional legal framework and difficult for consumers to articulate as a grievance.

In addition, as the Indian consumer base becomes digital, the possibility for damages only exponentially grows. E-commerce platforms today transact millions of transactions every single day: each via algorithms and design frameworks that could either help or further exploit hapless consumers. The 2019 Consumer Protection Act (CPA 2019) proves to be fairly strong legislative backing against unfair trade practices, and the scope of laws on interface

[2] Press Release:Press Information Bureau

ISSN: 2582-6433

manipulation is still developing or evolving. This study, therefore, aims to explore the interface between user experience design (UX), behavioural economics, and consumer protection law to see whether the existent provisions will suffice or whether a more tailored regulatory approach is needed.

Objectives of the Study

The main aim of the research is to conduct a critical study into the subject of dark patterns in e-commerce and assess how they are regulated under the provisions of the Consumer Protection Act, 2019 and other subordinate legislation such as the Consumer Protection (E-Commerce) Rules, 2020. The purpose of the study is also to:

1. Determine and classify the primary categories of dark patterns that are common among Indian e- commerce sites.
2. Explore the psychological and behavioural factors that make dark patterns successful in coercing consumers.
3. Review the statutory framework of CPA 2019 and related rules and identify whether dark patterns could be considered an unfair trade practice or misleading advertisement.
4. Assess recent regulatory developments, such as directives from the Central Consumer Protection Authority (CCPA) and other enforcement against dark patterns.
5. Contrast India's evolving regulatory landscape against international approaches, especially the United States Federal Trade Commission (FTC) and European Union (EU) Digital Services Act (DSA).
6. Identify legal, policy, and design-level reforms to enhance consumer protection in the face of misleading digital design strategies.

Through these objectives, the project is intended to develop legal protections that work in step with technological realities facing consumers in the digital marketplace.

Research Questions

To shape the research inquiry, the project will respond to the following central research questions:

1. What are dark patterns, and how are they used by e-commerce platforms to manipulate consumer behaviour?
2. What extent are dark patterns considered in the category of unfair trade practices and misrepresentation/false advertising under the Consumer Protection Act, 2019?
3. How well does the Indian regulatory framework, such as the E-Commerce Rules and

ISSN: 2582-6433

CCPA Guidelines function to regulate the issues surrounding dark patterns?

4. What lessons can be learned from comparative international approaches to regulation of manipulative design in digital environments?
5. What legal and policy reforms are warranted to develop a coherent framework to abolish and sanction the use of dark patterns in India?

Collectively, these questions will be at the heart of the analysis, guiding doctrinal analysis and policy evaluation.

Scope and Limitations

The scope of this research is confined to examining the dark patterns in the context of e-commerce that is commercial transactions in digital platforms where consumers purchase goods or services; the Indian legal and regulatory environment has been put in greater focus. References are made to other jurisdictions only for comparative purposes to the extent that such comparisons have any useful insight for domestic reform.

The analysis remains focused on manipulative design practices that are exercised towards influencing consumer decision-making and does not traverse into broader territories of data protection, algorithmic bias, and online content moderation, unless engaged with consumer deception. Besides, based on mobile regulatory developments up to the year 2025 on the variant forms of existence of dark patterns, legislative changes or technological changes that arise thereafter will probably call for fresh studies.

The empirical dimension is another limitation. While global literature has quantitatively mapped the prevalence of dark patterns across several sectors, there is currently no thorough dataset produced in India on this subject. Thus, the research relies more on doctrinal, descriptive, and comparative methods, rather than large-scale empirical measurements.

Research Methodology

The study employs a methodological framework that is doctrinal and analytical, supplemented by comparative and descriptive approaches.

1. Doctrinal Methodology

   The study analytically surveys the statutory provisions of the Consumer Protection Act, 2019, the Consumer Protection (E-Commerce) Rules, 2020, as well as applicable

ISSN: 2582-6433

notifications, advisories, and case law of the CCPA regarding the interpretation of their applicability in such instances of dark patterns.

2. Comparative Legal Approach

   To learn from internationally best practices, the study analyses the legal framework of the U.S. Federal Trade Commission (FTC), and the European Union (EU) through, among other things, its Digital Services Act and directives on fairness towards consumers, with a view to identify best practices as well as gaps in the Indian framework and present reasonable recommendations for reform.

3. Descriptive and Analytical Approach:

   The project employs a systematic approach to describe the types, characteristics, and psychological mechanisms of dark patterns based solely on secondary sources, such as scholarly literature, regulatory publications, and policy briefs.

4. Qualitative Content Analysis:

   The qualitative analysis of government-led reports, journalistic articles, or advisories shared by the Department of Consumer Affairs and the CCPA enables assessment of trends in enforcement and provides a framework for understanding regulatory intent.

5. Information Sources:

   This research is based primarily on secondary information – legislation, government notifications, court decisions, policy documents, and academic commentary.

The methodology accordingly combines legal analysis with interdisciplinary perspectives from behavioural economics and design studies - representing an attempt to explore more fully the normative and empirical dimensions of dark patterns.

Significance of the Study

This study holds significance for several reasons. To begin with, it enhances the academic understanding of how digital manipulation relates to established concepts of consumer protection. The Consumer Protection Act of 2019 highlights India's dedication to defending consumer rights in a rapidly evolving marketplace; however, the interpretation of this Act in digital scenarios is still lacking. This research addresses this issue by situating dark patterns

ISSN: 2582-6433

within the current legal framework and suggesting targeted regulatory approaches.

Furthermore, this analysis tackles an emerging area of policy that has tangible real-world effects. As India moves towards a predominately digital economy, many consumers engage with online platforms daily without realizing their choices are being subtly steered by persuasive design elements. Such practices diminish consumer independence, skew market fairness, and erode trust within e-commerce environments.

Third, by examining how India's regulatory strategy compares to international standards, this study offers policy recommendations based on evidence that could guide future changes or guidelines from the CCPA or the Ministry of Consumer Affairs.

Lastly, this research acts as a valuable source for legal scholars, practitioners, and policymakers who wish to grasp the relationship between law, technology, and behavioural design. It provides a conceptual basis for creating ethical digital design frameworks that align with consumer rights.

2. CONCEPTUAL FRAMEWORK OF DARK PATTERNS

Understanding Dark Patterns

In today’s digital world, the interaction between a consumer and an online platform acts like a modern shopping environment. Every action—from clicking to scrolling to dealing with pop-ups—is thoughtfully crafted to navigate users through their buying experience. Yet, what seems like a straightforward and user-friendly design often hides strategic psychological manipulation. These sneaky design tactics are referred to as dark patterns.

The phrase “dark pattern,” introduced by Harry Brignull in 2010, describes interface elements that are deliberately designed to mislead or pressure users into making choices they didn’t plan on or that aren't in their best interest. Rather than relying on clear deceit, these manipulations utilize subtle nudges, visual hierarchy, word choices, and cognitive biases that affect decision-making at an unconscious level.

Dark patterns differ from conventional deceptions in that they function at the technical level of a product, integrated into the framework of applications, websites, and online platforms. They are especially cunning because they take advantage of users’ divided attention during their

ISSN: 2582-6433

instinctive and rushed actions. Meanwhile, companies assemble teams of behavioural scientists, UX designers, and data analysts to tailor every digital experience for maximum profit.

Evolution of Dark Patterns in Digital Commerce

The concept of dark patterns stems from foundational theories in behavioural economics and choice architecture, primarily those proposed by Richard Thaler and Cass Sunstein in their book "Nudge: Improving Decisions About Health, Wealth, and Happiness" (2008). Their research illustrated how minor tweaks in design could greatly affect behaviour without changing the underlying incentives. Marketers later exploited this principle within digital environments.

In the early 2000s, as e-commerce started to flourish, businesses began incorporating persuasive design features like countdown timers, pre-checked boxes, and intrusive alerts to boost user engagement and enhance conversion rates. What initially was termed “growth hacking” gradually morphed into deliberate manipulation tactics. With the rise of mobile applications, gamified rewards systems, and algorithm-driven targeting strategies, dark patterns became standard practice across the industry rather than a rare occurrence.

This transformation was further expedited by the COVID-19 pandemic. With tens of millions of Indian consumers purchasing essential goods online due to COVID-19, competition intensified. In a bid to keep users on their platforms and make more sales, many platforms implemented design strategies that made it difficult to distinguish between convenience and coercion from hidden "cancel order" buttons to misrepresenting stock availability.

These examples illustrate a key point of change: while physical marketplaces are atheoretical reliant on visible products and choice, the architecture of digital marketplaces can obscure user perception through invisible design choices.

Typology of Dark Patterns

Academic research and regulatory studies (particularly the U.S. FTC, OECD, and European Commission) have recognized multiple commonly occurring dark patterns. The following taxonomy presents the most common uses of dark patterns within an e-commerce context:

ISSN: 2582-6433

a) Bait and Switch

A platform offers a product or service at a deep discount; however, when the user goes to purchase it, they are redirected to another offer in the same product category with a higher price, or which carries some additional obligation. In this case, a user's expectations are manipulated in accordance with their original offer, and the more time and commitment that user puts into an action, the more likely they are to complete the purchase, even if the terms have changed.

b) False Urgency and Scarcity

False Urgency and Scarcity is type of dark pattern that involves displaying countdown timer messages (like "Only 2 rooms left" at a hotel) on websites, which display that item to be low in stock, when in reality, the stock may be more than enough. When the user is confronted with the countdown timer or a message like "Only 2 rooms left" on the existing item, it gives an added reason for users to be fearful of missing out.

c) Drip Pricing and Hidden Fees

This dark pattern is one that specifically displays the total cost of a product after a purchase has been initiated, usually once a user is close to confirming the purchase at checkout on the website. Users will generally view a lower price, before having to view a service fee or delivery charge presented to them prior to confirming their purchase upon checkout.

d) Basket Sneaking and Default Opt-ins

Several services employ default strategies like automatically adding extra items, insurance, donations, or extended warranties to carts, or pre-selecting optional services. This exploits the status quo bias, wherein users rarely change the defaults.

e) Shame Confirmation

This is when there's the use of guilt-inducing or emotionally charged language in an attempt to make users move in a certain direction. For example, in canceling a promotional subscription, users may be given statements like, "No, I don't care about saving money." The idea is to instil psychological discomfort for making a rational choice.

ISSN: 2582-6433

f) Obstruction and Forced Continuity

Also known as the "roach motel," this happens when it's easy to sign up, but hard to unsubscribe. Platforms can bury cancellation options deep in settings or require superfluous verification steps. Subscription traps rank among the most frequent dark patterns scrutinised by regulators worldwide.

g) Disguised Advertising

Here, the sponsored content is woven in a manner that makes it look organic-recommendations or user-generated reviews. The practice is a brazen violation of transparency norms, often convincing users that paid endorsements constitute disinterested opinions.

h) Privacy Zuckering

Named humorously after Facebook's founder, this involves the coercion of users to disclose more personal data than is actually required often through ambiguous privacy settings or misleading consent banners. Users are nudged toward "Accept All" options while privacy-friendly choices are hidden or time-consuming.

i) Nagging and Interference

Repeated pop-ups, reminders, or manipulative notifications infringe on user autonomy. For example, apps that constantly ask users to activate notifications or upgrade to premium versions create fatigue that leads to compliance.

Each of these types represents a calculated exploitation of psychological principles such as anchoring, social proof, loss aversion, and decision fatigue. While some may seem minor, the cumulative impact across millions of transactions is significant.

Behavioural Science Behind Dark Patterns

The effectiveness of dark patterns emanates from the application of very universal cognitive biases: systematic errors in judgment arising from mental shortcuts that humans use to make quick decisions. Some key biases relied on in this regard include:

1. Scarcity Heuristic – The perception that limited availability signals higher value or urgency.
2. Default Bias: The tendency to stick with pre-selected options.

ISSN: 2582-6433

3. Anchoring Effect - The use of an initial piece of information as one's reference point.
4. Loss Aversion - The preference for avoiding losses over gaining something; many consumers will more readily accept unfavourable terms to avoid the loss of a "deal."
5. Social Proof - The influence of others' behaviour, often exploited through fake "Recently bought" or "Trending now" messages.
6. Cognitive Overload: When users are overloaded with information, they rely on heuristics and hence become susceptible to manipulation.

Dark patterns exploit these biases, transferring control from the user to the designer by converting consent into a product and decision-making into monetized behaviour.

Impact on Consumers and the Marketplace

The proliferation of dark patterns has profound implications for both consumer welfare and market integrity.

(a) Erosion of Autonomy and Informed Consent

But the most fundamental harm is to consumer autonomy. Users think they're making free choices, yet their decisions are influenced by manipulations invisible to them. Consent through dark design is not informed consent or voluntary consent.

(b) Financial Harm and Hidden Costs

Drip pricing, pre checked boxes, and auto-renewals cause unintentional spending. Repeated small charges add up and trickle to real losses for the consumer.

(c) Privacy Intrusion and Data Exploitation

Dark patterns contribute to large-scale privacy violations by tricking users into oversharing data. Data collected through the deception of consent mechanisms can be monetized in advertising and profiling, thereby further eroding consumer trust.

(d) Market Distortion and Unfair Competition

Ethical platforms that maintain transparent practices are at a disadvantage in competition with those using dark patterns to drive conversions. This creates a "race to the bottom" in which manipulation becomes the industry norm, distorting fair competition.

ISSN: 2582-6433

(e.) Psychological Fatigue and Consumer Distrust

Long-term exposure to these manipulative interfaces will result in decision fatigue and cynicism; consumers will become distrustful of all digital transactions. Over time, this will undermine e- commerce as a whole.

Empirical Insights and Indian Context

While globally a plethora of research on dark patterns is available, Indian scholarship and data are scant. However, several anecdotal and governmental observations show the growing prevalence of these.

In 2024, the CCPA, under the Ministry of Consumer Affairs, issued an advisory on dark patterns - directing every e-commerce entity to review and eliminate manipulative design practices. The advisory explicitly listed several of the prohibited behaviours: false urgency, drip pricing, basket sneaking, and obstruction of cancellation.

Consequently, notices were sent to several leading platforms, such as online retailers, food delivery apps, and travel booking websites, for indulging in unfair digital practices. The advisory also encouraged self-regulation, which mandated UX audits with certification.

These actions marked a turning point in Indian consumer protection enforcement, signaling that digital design could no longer be treated as a mere technical domain but was now a matter of legal accountability.

Meanwhile, self-regulating bodies like the Advertising Standards Council of India have started scrutinizing misleading online ad formats, for instance, disguised influencer promotions, which conceptually overlap with dark patterns.

However, enforcement remains a challenge. This is due to a lack of standardized definitions, an absence of a dedicated technical audit framework, and the rapid evolution of user interfaces, which make consistent detection difficult. In addition, most consumers remain unaware that what they perceive as "annoying" design choices may actually be legally actionable unfair trade practices.

ISSN: 2582-6433

Relationship Between Dark Patterns and Unfair Trade Practices

Section 2(47) of the Consumer Protection Act, 2019, defines unfair trade practice as any deceptive method or unfair means adopted to promote the sale, use, or supply of goods or services. The dark patterns that induce consumers to make unintended purchases or hide material information squarely fall within this ambit.

For example, pre-ticked boxes for paid add-ons breach the principle of free and informed consent and can be seen as a misrepresentation under the Act; similarly, false urgency messages amount to dissemination of misleading information.

Also, Section 21 of the Act enables the CCPA to halt misleading advertisements. If a platform employs false scarcity or disguises sponsored products as genuine recommendations, such acts are liable to invite CCPA action.

Therefore, dark patterns can also be treated both as unfair trade practices and as misleading advertisements. Such a dual classification widens the reach of regulation but also creates certain interpretative challenges, which are addressed later in the paper.

The Technological Challenge of Detection

Unlike traditional unfair trade practices, dark patterns cannot be found simply through textual review or documentary evidence. Dark patterns are dynamic, interactive, and often change with user behaviour, location, or device. This means that a given website will only present false scarcity to first-time visitors or manipulate price displays in a certain way for returning users.

Detection of such patterns requires behavioural audits observing how users interact with a digital interface under controlled conditions. It also requires collaboration between technologists, behavioural scientists, and legal experts. Unfortunately, Indian regulatory institutions still lack this interdisciplinary capacity.

While advisories are a good initiative on the part of CCPA, the scant presence of forensic UX investigation frameworks curtails its enforcement powers. A digital monitoring division within CCPA, consisting of data scientists and design experts, can turn the tables on detection and deterrence.

ISSN: 2582-6433

The Ethical Dimension

Beyond legality, the utilization of dark patterns brings about highly profound questions of morality regarding the responsibilities of enterprises in this digital age. The imbalance between corporations and consumers turns what might seem like persuasive marketing into manipulation. From a Kantian's ethical viewpoint, dark patterns treat consumers purely as a means to a profit rather than as an autonomous end, that is, capable of rational choice. The utilitarian analysis may well suggest that short-term gains for the companies are not sufficient to outweigh long-term harm to trust, welfare, and efficiency of the market.

Corporate ethics therefore require platforms not only to comply with the letter of the law but also the spirit of fairness. Ethical design principles, transparency, choice symmetry, and consent clarity could ensure consumer well-being without compromising business success.

Psychological Mechanisms

Dark patterns use biases like scarcity, anchoring, and FOMO to promote impulsive buying behaviors in consumers. Countdown timers prey on urgency, while misleading language manipulates perceptions and expectations.[3]

- ***Prevalence in India Survey Findings***

Recent studies and audits, such as LocalCircles in 2025, report that up to 97% of major Indian e- commerce platforms use dark patterns. Drip pricing affects 75% of users, while false urgency and privacy zuckering affected over 40%. Other very prevalent techniques are forced actions and basket sneaking.[4]

Platform Compliance

These include platforms like Amazon, Flipkart, Tata Neu, Jiomart, and Myntra, which have been found non-compliant, using multiple dark patterns consistently. Interestingly, Meesho was found to be dark-pattern-free after exhaustive audits.[5]

- ***Regulatory Framework Consumer Protection Act, 2019***

According to Section 2(47), the unfair trade practices under the Consumer Protection Act,

[3] Dark Patterns in Indian E-Commerce, ETBrandEquity
[4] 97% E-commerce Platforms Use Dark Patterns, Says LocalCircles
[5] Dark patterns continue on eCommerce marketplaces in India: Survey

ISSN: 2582-6433

2019, include what is commonly referred to as 'dark patterns'. The CCPA has powers to investigate complaints, order withdrawal of deceptive services, recall goods, and impose penalties.[6]

Guidelines for Prevention and Regulation of Dark Patterns, 2023

In November 2023, India issued formal guidelines listing 13 recognized dark patterns in e- commerce. These guidelines[7]:

- Apply to all platforms, sellers, and advertisers offering goods or services online.
- Explicitly prohibiting listed dark patterns in Annexure 1 of the guidelines.
- Allow CCPA to issue penalties against offenders, including fines and imprisonment in serious or repeated cases[8].

Enforcement and Case Law

CCPA has acted against platforms such as BookMyShow for basket sneaking and IndiGo, ordering withdrawal of the services and making corrections. In case of repeat offenders, the penalties are increased up to 5 years imprisonment and fines up to ₹50 lakh.[9]

- ***Impact on Consumers and E-Commerce Consumer Harm***

Dark patterns erode consumer trust, cause financial loss, and undermine autonomy. Some of the common complaints involve hidden fees, misleading prompts, and pre-selected add-ons.[10]

Market Response

While compliance remains inconsistent, the pressure from regulatory scrutiny and consumer advocacy is pushing e-commerce players toward auditing and reforming interface design.[11]

[6] Microsoft Word - Dark Patterns.docx
[7] induslaw-shedding-light-on-dark-pattern-regulations-in-india-final-version.pdf
[8] The Legal Perils of Dark Patterns in India: Intersection between Data Privacy and Consumer Protection | SCC Times
[9] The Legal Perils of Dark Patterns in India: Intersection between Data Privacy and Consumer Protection | SCC Times
[10] Dark patterns continue on eCommerce marketplaces in India: Survey
[11] Dark Pattern Rules in India: Lessons from Flipkart's Self-Audit

ISSN: 2582-6433

3. DARK PATTERNS IN INDIAN E-COMMERCE: EMPIRICAL EVIDENCE

Prevalence and Common Practices

Research and investigations by consumer protection organizations have documented the widespread use of dark patterns across Indian e-commerce platforms.

Major Online Marketplaces:

Some of the dark patterns found in major Indian e-commerce include pre-selected add-ons like warranties or insurance that consumers pay for without realizing. There's false scarcity and countdown timers that create fake urgency. Drip pricing is when the charges of delivery or service at the time of making the payment are hidden. Search result manipulation by showing sponsored products on top without transparency affects consumer decisions negatively.

Travel and Hospitality Booking Platforms:

These platforms very often deploy false scarcity messages, such as "Only 1 room left," in an effort to hurry people's decisions. There is often drip pricing, whereby taxes, resort fees, and service charges are only shown at the final step. Users are also put through default add-ons like insurance, and there are pressure tactics such as notifications of recent bookings to cause rushed purchases.

Food Delivery Applications:

Dark patterns include showing platform fees only at checkout, making real price comparisons impossible for consumers earlier in the process. Restaurant rankings are influenced by commercial partnerships rather than genuine customer ratings. Other manipulative practices that keep consumers spending include hidden surge pricing and auto-renewing subscriptions without due notice.

Subscription Services:

It often happens that consumers get automatically transferred to paid subscriptions from a free trial, with no clear warning in advance. The design of the cancellation pathways on platforms is done in a confusing way to increase involuntary retention. In many cases, consumers don't understand the true cost of long-term subscription commitments since pricing structures and renewal terms are obscured.

ISSN: 2582-6433

Consumer Impact

The impact of dark patterns on Indian consumers manifests in several ways:

Financial Impact:

Dark patterns mislead customers into making unintended purchases, subscriptions, or incurring additional charges that were not clearly disclosed. Hidden fees and drip pricing will raise total transaction costs hugely. Such manipulative practices also bring about financial loss in terms of extra services or products acquired that were provided without full consent.

Time Costs:

It makes consumers waste significant amounts of time in navigating cumbersome interfaces that are deliberately designed to make cancellations, refunds, and opt-outs difficult. The time spent resolving unwanted transactions contributes to frustration and fatigue. Such time burdens, ultimately, reduce satisfaction and confidence in digital platforms by consumers.

Psychological Impact:

Dark patterns erode consumers' confidence through feelings of being tricked or cheated. Decision fatigue arises in creating repeated pressure prompts or misleading design elements, which over time undermine autonomy, causing stress and diminishing the consumer's sense of control and dignity.

Informational Harm:

Manipulative consent flows compromise privacy by inducing or forcing users to divulge more data than they plan to. When disclosures are hidden or misleading, consumers misplace their control over personal information. Long-term consequences of such situations are those related to data misuse, profiling, and erosion of privacy.

Business Perspectives

From the business perspective, dark patterns are often justified through:

Conversion Optimization: Dark patterns are viewed as legitimate optimization techniques to reduce friction and increase conversions.

Competitive Pressure: Competitive markets are a prime example of where aggressive tactics

ISSN: 2582-6433

and strategies are necessary to hold one's market share.

Business Imperatives: Revenue growth and shareholder value are given the utmost importance. However, these rationales are contradictory to:

- Long-term brand value and consumer trust
- Ethical business practices
- Legal compliance obligations
- Sustainable business models

4. WHY DARK PATTERNS MATTER: HARMS AND CONSUMER VULNERABILITY

Dark patterns produce manifold harms:

- Financial harm: Hidden charges, subscription traps, and unintended purchases incur direct monetary loss.
- Informational harm: It is impossible to make informed choices when important terms, prices, or opt-outs are suppressed or mis-portrayed.
- Autonomy Erosion: The design manipulates meaningful consent by exploiting cognitive shortcuts.
- Disproportionate impact: This is a disproportionate impact on the most vulnerable: elderly, less digitally literate, those under stress.
- Data harms: Dark patterns often force users to over-share personal data, increasing privacy risks. Because of these harms, regulators treat dark patterns not as benign design variants but as actionable unfair trade practices.

5. LEGAL FRAMEWORK IN INDIA: CPA 2019, E-COMMERCE RULES, AND RECENT REGULATORY ACTION

Consumer Protection Act, 2019: scope and relevant provisions

The Consumer Protection Act, 2019 modernized Indian consumer law. It defines "unfair trade practice" and provides for statutory authorities, including the CCPA, to prohibit unfair practices, order recalls/refunds, impose penalties, and direct corrective measures. Sectional specifics and definitions in the Act furnish the legal basis for treating deceptive interface designs as unfair trade practices or misleading advertisements actionable under consumer law.

ISSN: 2582-6433

(Text of Act and definitions are codified in official CPA 2019 materials.)[12]

Consumer Protection (E-Commerce) Rules, 2020

The Central Government, therefore, enacted the Consumer Protection (E-Commerce) Rules, 2020 under CPA 2019 to address digital marketplace specificities. The Rules impose duties on e- commerce entities-including identity and registration obligations, disclosure of important information (like return, refund, cancellation policies), obligations for grievance redressal portals, and liability matrices for marketplace vs inventory models. Rule language emphasizes transparency and prohibits unfair trade practices via digital platforms. These rules are key in framing dark patterns as regulatory non-compliance where platforms fail to display material terms or make cancellations/refunds unduly difficult.[13]

CCPA advisories and enforcement (2024–2025)

From 2024–2025 onwards, the CCPA and Department of Consumer Affairs started treating dark patterns as a serious regulatory issue publicly. The CCPA asked e-commerce platforms to selfaudit and remove dark patterns. Notices were issued to various firms, including those offering app-based services, on practises such as false urgency, basket sneaking, and impeding cancellations. This proactive regulatory stance demonstrates an acknowledgment that UI/UX design may amount to an unfair trade practice within the meaning of CPA 2019. Advisory and notices to firms, requesting corrective measures, were reported by government press releases and mainstream reporting.[14]

6. COMPARATIVE PERSPECTIVES: U.S. AND EU APPROACHES

United States — FTC's enforcement and guidance

The U.S. Federal Trade Commission has made dark patterns a priority. In Bringing Dark Patterns to Light (2022), the Commission documented manipulative practices, explained the enforcement theory behind them/deception and unfairness, and showed enforcement actions in which interface design formed part of the unfair practice. The FTC uses statutes already on the books to challenge designers and platforms and pursue disgorgement and injunctive relief when subscription traps, misleading disclosures, or hidden fees have occurred. The FTC's approach

[12] https://ncdrc.nic.in/bare_acts/CPA2019.pdf
[13] Consumer Protection (E-Commerce) Rules, 2020.pdf
[14] Govt issues notices to 11 firms including Zepto, Uber for using dark patterns to sway consumers, warns action - The Times of India

ISSN: 2582-6433

to dark patterns is to enforce laws alongside public education and research.[1515]

European Union - DSA and digital fairness agenda

The DSA and ancillary instruments under the EU treat manipulative design as against consumer fairness and digital safety. Article 25 of the DSA and other consumer protection fitness checks name dark patterns as prohibited practices; the EU has also been active in investigating major platforms with regard to design choices frustrating user rights, for instance, complaints processes. In this respect, the DSA gives regulators powers to issue guidance and impose obligations on Very Large Online Platforms (VLOPs) that are analogous to India's concerns but framed within a wider set of content moderation and transparency obligations.[16]

Lessons for India

Comparing regimes reveals two complementary approaches: (1) leveraging existing unfair-practice/deception laws in pursuit of enforcement and remedies, and (2) ex-ante rule-making that involves transparency, audited design processes, and specific prohibitions. India's CPA/e-commerce Rules embody both, but stand to benefit from further prescriptive guidance-say, standardized UI audits-and more robust mechanisms for platform accountability where systemic abuse is evident.[17]

7. DOCTRINAL ANALYSIS: HOW DARK PATTERNS FIT WITHIN CPA 2019

Unfair trade practices and misleading advertisements

CPA 2019 defines unfair trade practices in ways that naturally encompass deceptive interface tactics. Practices like hiding fees until the final stage, misrepresenting offers, making opt-outs difficult, or disguising ads as neutral content can be framed as misrepresentations or unfair trade practices. Where the UI choices materially mislead a reasonable consumer, legal claims under the unfair practice provisions of the CPA and the transparency obligations under the E-commerce Rules are plausible.

[15] https://www.ftc.gov/reports/bringing-dark-patterns-light?utm

[16] https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA%282025%29767191_EN.pdf?utm

[17] https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA%282025%29767191_EN.pdf

ISSN: 2582-6433

Liability of intermediaries and marketplace platforms

The E-Commerce Rules distinguish between inventory e-commerce entities-that sell directly- and marketplace entities-that host third-party sellers. Rule 5 and related provisions establish duties and liability matrices, among these being to disclose seller information, make contract terms available, and address consumer complaints. Where the marketplace owner introduces dark patterns, such as by defaulting add-ons across listings by third-party sellers, they could be directly liable. Where a third-party seller uses manipulative interfaces through the facilities provided by the platform, questions of mediation, platform facilitation, and 'reasonable steps' under the Rules will determine liability.

Remedies and powers of enforcement

The CCPA has powers to investigate, order recalls/refunds, impose penalties, and issue corrective communications. Under the CPA framework, consumers can also pursue complaints before consumer commissions for redressal. In this regard, particularly relevant are the market-level enforcement powers of the CCPA for systematic design issues affecting broad user groups.

(Statutory text and administrative rules grant such powers, and the public advisories issued by the CCPA also show their active use recently.)[18]

8. EMPIRICAL EVIDENCE AND GOVERNMENT FINDINGS

A number of empirical studies and regulatory reviews have documented the prevalence of dark patterns across apps and websites. International reports (OECD, FTC) and domestic analyses (ASCI studies, government reviews) indicate that dark patterns are pervasive across booking, travel, food delivery, mobility, and subscription services. Indian government press releases and news coverage in 2024–2025 reported notices to major firms and a CCPA advisory, directing e- commerce entities to self-audit and eliminate dark patterns-an indication of systemic issues requiring remediation.[19]

[18] https://ncdrc.nic.in/bare_acts/CPA2019.pdf
[19] https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf

ISSN: 2582-6433

9. GAPS AND CHALLENGES IN INDIA'S APPROACH

While there are clear legal foundations, the practical enforcement of dark-pattern harms under CPA 2019 can be problematic for a number of reasons:

1. Technical complexity and evidence gathering: Proving intent-that is, that a design was deliberately manipulative-and isolating UI elements as the proximate cause of consumer harm requires technical UI/UX forensic analysis and reproducible evidence.
2. Standards and definitions: Although the issue of unfair practices falls within the ambit of the CPA/Rules, there is no authoritative and detailed taxonomy or binding guidelines indicating what design techniques are prohibited and threshold limits beyond which a label may be considered misleading. The various advisories issued by regulators, though useful, are non- binding.
3. Scale and remedies: Consumer commissions are designed around individual or class complaints; systemic, platform-level violations require enterprise-scale enforcement, including audits, design remediation and large-scale consumer redress.
4. Overlap with data protection: Dark patterns often intersect with concerns of privacy and data protection-for example, manipulative consent. The data protection regime in India is developing, and the absence of a settled data-protection law-or even wide gaps in its implementation-complicates cross-regulatory action.
5. Intermediary defenses and platform design control: Platforms may argue that the content is controlled by third parties, or that design choices are neutral; regulators must have the ability to establish platform responsibility when design tools, defaults, or ranking promote manipulative outcomes.

10. RECOMMENDATIONS- LEGAL, REGULATORY AND DESIGN INTERVENTIONS

To enhance consumer protection from dark patterns, the paper proposes a multi-faceted approach:

Clarify and codify forbidden practices

- Issue binding Dark Patterns Guidelines under the Consumer Protection Act or E-Commerce Rules that define specific prohibited practices - such as forced continuity, pre-checked purchases, deliberate hindering of cancellations, or fake urgency. They should be drafted with consumer- behaviour experts, HCI researchers, and industry

ISSN: 2582-6433

input. The lines of the EU and FTC offer useful models.[20]

Compulsory UX/UI impact assessments and audits

- Require e-commerce entities above a certain threshold in terms of users/transactions to conduct periodic UX impact assessments and third-party audits certifying absence of dark patterns, whose results should be filed with the CCPA and summary findings published for transparency.

Standardised disclosure format and UI rules

- Mandate standardized, machine-readable disclosures of pricing, refund/cancellation policies, and subscription terms. Require a standard 'final-price' display prominently before checkout and a single-click cancellation mechanism for recurring payments.

Stronger ex-ante obligations for large platforms (VLOPs)

- Stricter obligations for platforms with significant market share, similar to the EU's VLOP rules: design transparency reports, data for independent researchers, and stricter penalties for systemic misuse.

Regulatory collaboration and technical capacity building

- Build specialized tech teams within the CCPA to perform interface audits, partner with academic HCI labs, and issue periodic public reports.

Remedies and collective redress mechanisms

- Enable representative or class remedies and facilitate mass redress in order to ensure that diffuse harms are efficiently remediatised - for example, fast track refunds for the affected cohorts.

Cross-regulatory coordination with data protection authorities and advertising regulators

- Coordinate with data protection authorities because manipulation generally involves data collection and consent, and Advertising Standards Council of India (ASCI) on disguised advertising and influencer transparency.

20 https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA%282025%29767191_EN.pdf

ISSN: 2582-6433

Industry standards and design ethics codes

- Encourage industry adoption of design ethics codes-e.g., opt-in defaults, frictionless exit options-linked to certification labels for 'consumer-friendly' platforms.

11. ILLUSTRATIVE APPLICATION: A HYPOTHETICAL COMPLAINT AND ENFORCEMENT PATHWAY

Suppose a consumer finds out that an online food delivery app auto-adds an expensive insurance add-on at checkout, pre-checked, with minimal disclosure and an onerous multi-step cancellation. The consumer loses ₹1,200. Which of the following applies in this situation?

- Unfair trade practice under CPA 2019: Misrepresentation/Omission of material term.
- E-Commerce Rules non-compliance due to failure to show clear refund/cancellation policy and for fraudulent pricing.
- Possible redress: Ordering refunds to concerned consumers, administrative penalty against the platform, mandatory UI remediation, and a market notice. Consumer commission could provide individual redress if the consumer files a complaint. For mass incidents, representative complaints and CCPA-led class redress would be efficient. Recent advisories by CCPA encourage this exact remediation model.[21]

12. COUNTERARGUMENTS AND INDUSTRY CONCERNS

The common industry arguments are that: a) personalized interface design increases user experience and conversion; b) heavy regulation would stifle innovation and hurt small sellers; c) design choices are a matter of product strategy, not consumer law. Responses:

- Distinguish ethical personalization vs. manipulation: Personalization that helps users make choices with clear defaults is legal and benefits consumers, while intentional obfuscation is not.
- Proportionate rules: Rule thresholds and scaled obligations ensure small sellers are protected while still targeting platforms that are systemically risky.
- Innovation with constraints: Ethical design can preserve innovation while protecting consumer autonomy regulation steers design incentives rather than banning experimentation.

[21] https://thc.nic.in/Central%20Governmental%20Rules/Consumer%20Protection%20%28E-Commerce%29%20Rules%2C%202020.pdf

ISSN: 2582-6433

13. FUTURE DIRECTIONS AND RESEARCH AGENDA

Key areas for future research and policy development include:

1. Empirical prevalence studies in India: Rigorous mapping of dark patterns across sectors like travel, food delivery, fintech, and quantification of aggregate consumer loss.
2. Behavioral experiments: controlled studies that measure the causal effect of specific UI elements on consumer decisions in Indian contexts.
3. Interaction with emerging technology: AI-driven personalization and generative interfaces could weaponize dark patterns; research needs to anticipate algorithmic manipulation and propose guardrails.
4. Standardization of audit protocols: Creating reproducible forensic methods for UI audits that are applicable in litigation and regulatory enforcement.
5. Cross-jurisdiction learning to compare enforcement outcomes (FTC, EU DSA, India CCPA) for determining best practices for remedying systemic platform abuses.

14. CONCLUSION

Dark patterns are a modern manifestation of long-standing consumer protection concerns. The Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 give Indian regulators statutory backing to treat manipulative interface design as an unfair trade practice. The recent advisories and notices issued by the CCPA indicate regulatory intent. However, law and enforcement must keep pace with rapid technological sophistication. Clearly binding guidance, mandatory UX audits, stronger obligations for large platforms, and cross-regulatory coordination will be required for translating statutory principles into meaningful protection for digitally transacting consumers. Thoughtfully implemented, these steps will preserve the benefits of digital commerce while protecting consumer autonomy, privacy, and financial interests.