IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

Dark Patterns in AI-Driven UX: How Algorithms Manipulate Consumer Behaviour in E-Commerce

Shivani Sonkar[1], Rizwana Momin[2], Soni Pandey[3], Gitanjali Thakur[4], Himani Mokal[5]
Assistant Professor, Computer Science, RTCCS Kharghar, India[1,2,3,4]
Student, Computer Science, RTCCS Kharghar, India[5]

Abstract: *Have you ever added something to your online cart that you never meant to buy? Have you ever paid more at checkout than what was shown at the start? Have you ever clicked "No thanks, I hate saving money" just to close a popup? If yes — you have been a victim of dark patterns. Dark patterns are deceptive design tricks built into apps and websites that push users into doing things they never intended to do. They are not bugs or accidents. They are deliberate. And now, with the power of Artificial Intelligence (AI), these manipulation techniques have become smarter, faster, more personalised, and far more difficult to spot. This paper investigates how AI-powered algorithms in e-commerce platforms use dark patterns to manipulate consumer behaviour — exploiting psychological biases, personal data, and real-time behavioural signals to drive purchases, subscriptions, and data sharing. Using real-world examples from Indian and global platforms — including Zomato, Swiggy, Flipkart, BookMyShow, IndiGo, Amazon, and Epic Games — the study maps the most common AI-driven dark patterns and their impact on consumer trust and decision-making autonomy. The research also examines India's regulatory response: the Central Consumer Protection Authority (CCPA) notified the Guidelines for Prevention and Regulation of Dark Patterns in November 2023, banning 13 specific manipulative practices, and in June 2025 issued a mandatory self-audit directive to all e-commerce platforms. Drawing on these findings, this paper proposes an Ethical UX Compliance Framework (EUXCF) — a practical tool for businesses to evaluate and redesign their AI-driven interfaces from a consumer-first ethical perspective. The paper argues that in the age of AI, protecting consumer autonomy is not just a legal obligation — it is a business strategy that builds lasting trust.*

Keywords: Dark Patterns, AI-Driven UX, Consumer Manipulation, E-Commerce Ethics, CCPA Guidelines, Deceptive Design, Behavioural Targeting, User Autonomy, Digital Consumer Rights

I. INTRODUCTION

Picture this: You are on Zomato, ordering your favourite biryani. The app shows the price as ₹199. You add it to your cart. By the time you reach checkout, the bill reads ₹347 — after a platform fee, delivery charges, packaging charges, GST, and a pre-selected tip that you never chose. You pay it anyway because you are hungry and the process of removing each charge feels more exhausting than just accepting it. You have just experienced drip pricing — one of the oldest and most effective dark patterns in e-commerce.

Now imagine that same manipulation engine powered by Artificial Intelligence. The AI knows your order history, the exact time you usually order, your price sensitivity, and even whether you are in a hurry. It dynamically adjusts what you see — the urgency messages, the suggested tips, the checkout flow — to maximise its outcome, not yours. This is AI-driven dark pattern design, and it is the subject of this paper.

Dark patterns are user interface design choices that trick users into actions they did not intend — buying something they did not want, sharing data they did not mean to, or subscribing to services they cannot easily cancel. The term was coined by British UX designer Harry Brignull in 2010. Back then, dark patterns were mostly static — a misleading

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

button here, a hidden opt-out there. Today, AI has turned dark patterns into a dynamic, personalised, and real-time manipulation system.

India's digital economy makes this issue urgently relevant. With over 900 million internet users, a booming quick-commerce sector, and millions of first-generation online shoppers who may be unfamiliar with deceptive design tactics, India is particularly vulnerable to AI-powered consumer manipulation. Recognising this, India's CCPA introduced the Guidelines for Prevention and Regulation of Dark Patterns in November 2023 — a landmark regulatory step that has since pressured major platforms including Flipkart, Swiggy, Zomato, and BookMyShow to audit and reform their interfaces.

This paper examines how AI supercharges dark patterns, what the real-world consequences are for Indian consumers, how regulators are responding, and what a genuinely ethical AI-driven UX looks like in practice.

II. LITERATURE REVIEW

A. What Are Dark Patterns? The Origins

Harry Brignull (2010) first systematically catalogued dark patterns as deliberately crafted UX features designed to serve business interests at the direct expense of the user. His taxonomy included tricks like "roach motel" (easy to get into, hard to get out), "confirm shaming" (guilt-tripping users who decline), and "misdirection" (drawing attention away from important information). Early academic interest in dark patterns focused on identification and classification (Gray et al., 2018; Mathur et al., 2019).

Princeton University's 2019 study of over 11,000 e-commerce websites found dark patterns in more than 10% of sites — with urgency messaging, social proof manipulation, and hidden subscriptions being the most common (Mathur et al., 2019). A University of Zurich study of 240 popular Google Play apps found dark patterns in 95% of applications, with over half containing seven or more separate manipulative design features (Digelidis et al., 2020). By 2022, the European Commission reported that 97% of popular apps used by EU consumers showed at least one dark UX pattern (European Commission, 2022).

B. How AI Amplifies Dark Patterns

Traditional dark patterns were static — the same misleading design shown to every user. AI has fundamentally changed this. Modern recommendation algorithms, behavioural prediction models, and natural language generation systems allow platforms to personalise dark patterns in real time, targeting each individual user at their most psychologically vulnerable moment (Aicritique.org, 2025).

For example, AI systems can detect from browsing behaviour when a user is in a "high intent" state (likely to buy) and simultaneously trigger a false scarcity message ("Only 1 left!") and a countdown timer — even when the product is abundantly available. Research has confirmed that AI-driven dynamic pricing and urgency messaging significantly increase conversion rates compared to static versions (ScienceDirect, 2025). The manipulation is no longer guesswork — it is precision-targeted.

Generative AI adds another layer of sophistication. AI-generated chatbots now impersonate helpful customer service agents while quietly steering users toward upsells and away from cancellations. AI-written product descriptions can use emotionally charged language tuned to individual user psychographic profiles. As AI Critique (2025) observes, without safeguards, an AI system optimising for short-term conversion metrics will inevitably "discover" that deceptive interfaces produce better numbers — and iteratively refine those manipulations.

C. Psychological Mechanisms Behind Dark Patterns

Dark patterns work because they exploit well-documented cognitive biases. Scarcity bias makes us value things more when we believe they are rare — exploited by false "Only 2 left!" warnings. Loss aversion makes us fear losing more than we enjoy gaining — exploited by countdown timers. Commitment bias makes us reluctant to abandon processes we have already started — exploited by multi-step checkout flows that reveal hidden charges only at the final stage.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

Social proof exploits our tendency to trust the crowd — exploited by fake "1,200 people viewed this today" notifications. AI systems are now trained specifically to identify which bias is most effective for each individual user profile and deploy the corresponding dark pattern at the optimal moment (Cialdini, 2009; Eleken, 2025).

D. The Indian Regulatory Response

India has taken a globally notable regulatory step with the CCPA's Guidelines for Prevention and Regulation of Dark Patterns, notified on 30 November 2023. The guidelines explicitly ban 13 dark pattern categories: False Urgency, Basket Sneaking, Confirm Shaming, Forced Action, Subscription Trap, Interface Interference, Bait and Switch, Drip Pricing, Disguised Advertisements, Nagging, Trick Wording, SaaS Billing, and Rogue Malwares. In June 2025, the CCPA escalated enforcement by issuing a mandatory self-audit directive to all e-commerce platforms, with a three-month deadline for compliance declarations (Tribune India, 2025).

III. RESEARCH METHODOLOGY

This paper uses a qualitative and descriptive research methodology. Data was collected through secondary sources including peer-reviewed academic journals, official government regulatory documents (CCPA guidelines and notices), investigative news reporting, consumer complaint records, and published industry analyses. Real-world case examples from Indian and international platforms were selected to illustrate each category of AI-driven dark pattern discussed.

The research follows a three-phase structure. Phase 1 catalogues the main types of AI-driven dark patterns observed in Indian e-commerce with real platform examples. Phase 2 analyses the consumer impact and the regulatory actions taken. Phase 3 proposes the Ethical UX Compliance Framework (EUXCF) as a practical tool for businesses.

IV. RESULTS AND DISCUSSION

A. AI-Driven Dark Patterns in Indian E-Commerce: Real Examples

The following are the most prevalent AI-powered dark patterns documented on Indian digital platforms, with specific real-world examples:

TABLE I: Common AI-Driven Dark Patterns and Real Indian Platform Examples (2023-2025)

Dark Pattern Type	How AI Makes It Worse	Real Indian Example	Consumer Impact
Drip Pricing	AI adds charges progressively based on user's likelihood to abandon cart	Zomato/Swiggy: ₹199 meal becomes ₹347 at checkout after platform fee, delivery, GST, packaging, and pre-selected tip	40% of consumers experienced unplanned financial loss (Dovetail, 2023)
False Urgency	AI detects high-intent browsing and triggers timers/scarcity messages in real time	MakeMyTrip: "Only 1 room left at this price!" shown when more rooms were available (CCPA flagged)	Users rush decisions, bypass price comparison
Basket Sneaking	AI pre-selects add-ons based on user purchase history to maximise order value	BookMyShow: Auto-added ₹1 charity donation per ticket via pre-ticked checkbox (CCPA notice, Feb 2025)	Unintended charges accumulated across millions of transactions
Confirm Shaming	AI generates psychologically tuned	IndiGo Airlines: "No, I will take risk" shown to users	Users coerced into purchases through manufactured shame

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

	guilt-language personalised to user profile	opting out of add-ons (CCPA notice, June 2024)	
Roach Motel / Subscription Trap	AI makes sign-up frictionless; cancellation requires navigating AI-generated barriers	Amazon Prime globally: Easy 1-click subscription, cancellation requires 6+ steps (FTC action, 2023)	Users pay for unwanted subscriptions for months
Personalised False Scarcity	AI cross-references inventory with user urgency signals to show targeted scarcity messages	Quick commerce apps (Blinkit, Zepto, Swiggy Instamart): Items shown as "almost out" to trigger impulse orders	Impulse purchases driven by manufactured scarcity

Source: CCPA India (2023-2025), Tribune India (2025), Varun Sharma Analysis (2025), FTC USA (2023), Bricx Labs (2025).

B. Case Study 1 — BookMyShow and Basket Sneaking

BookMyShow is India's largest online ticketing platform, processing millions of transactions monthly for movies, concerts, and sporting events. In early 2025, the CCPA issued a formal notice after discovering that BookMyShow was automatically adding a ₹1 donation per ticket to the BookASmile charity initiative through a pre-ticked checkbox — without explicit user consent.

While ₹1 may seem trivial, consider the scale: if BookMyShow processes even 1 million tickets per month, this represents ₹1 crore collected monthly from users who never consciously agreed to donate. This is textbook basket sneaking — a practice explicitly banned under Clause 2 of the CCPA's 2023 Dark Pattern Guidelines. Following the CCPA notice on February 11, 2025, BookMyShow modified its interface to give users a clear, voluntary opt-in choice for the donation (CCPA, 2025). This case perfectly illustrates how a seemingly minor design choice, scaled by AI across millions of transactions, constitutes significant consumer harm.

C. Case Study 2 — Zomato and Swiggy: The Checkout Shock

Most Indian consumers who use food delivery apps have experienced what researchers now call "checkout shock" — the jarring difference between the price shown when browsing and the final bill at checkout. On Zomato and Swiggy, a ₹200 meal routinely becomes ₹300-₹350 after the platform adds a platform fee, a delivery fee, packaging charges, GST, and — critically — a pre-selected tip that users must actively remove.

What makes this AI-driven is the dynamic nature of these charges. AI algorithms adjust delivery fees in real time based on demand, weather, and distance — sometimes using surge pricing language such as "Raining nearby! Order now before surge pricing kicks in" — a message designed to create urgency and bypass rational price evaluation. Both platforms faced CCPA scrutiny for these practices and were among the 26 platforms that submitted compliance declarations in November 2025 (Tribune India, 2025). However, critics note that self-declaration audits are not the same as independent verification.

D. Case Study 3 — Epic Games and the Global Precedent

Though not an Indian company, the Epic Games case is the most significant legal precedent globally for AI-driven dark patterns in business. In December 2022, the U.S. Federal Trade Commission (FTC) fined Epic Games — maker of the globally popular game Fortnite — a record $520 million after finding that the company had used dark patterns to trick users, including children, into making unintended in-game purchases. The FTC found that Epic had deliberately

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

designed its interface to make purchases easy to trigger accidentally, while making refunds and cancellations deliberately confusing (FTC, 2022).

The relevance for Indian businesses is direct: if AI-driven dark patterns are now attracting nine-figure regulatory fines in developed markets, Indian companies that have not genuinely reformed their AI-driven interfaces face growing legal and reputational risk as India's CCPA enforcement capabilities strengthen.

E. The AI Feedback Loop: Why Dark Patterns Keep Getting Worse

Perhaps the most concerning finding of this research is what AI Critique (2025) calls the "dark pattern feedback loop." AI systems optimising for business metrics — conversions, revenue, engagement — learn from data. If a manipulative design element produces higher conversions, the AI treats this as a success signal and deploys that element more aggressively. The result is a self-reinforcing cycle: dark patterns become more sophisticated over time because AI is continuously optimising them based on their effectiveness at manipulating users.

This creates a serious ethical problem for platform designers who may genuinely not intend to manipulate users. An AI system instructed to "improve conversion rates" with no ethical guardrails will autonomously discover and refine dark pattern strategies — without any human designer explicitly programming them. This is why ethical UX governance cannot rely on designer intent alone; it requires systematic algorithmic oversight.

V. PROPOSED FRAMEWORK: ETHICAL UX COMPLIANCE FRAMEWORK (EUXCF)

Based on the patterns identified and the regulatory landscape reviewed, this paper proposes the Ethical UX Compliance Framework (EUXCF) — a practical, five-dimension tool that businesses can use to audit and govern their AI-driven UX for dark pattern compliance. The framework is designed to be usable by IT teams, UX designers, product managers, and compliance officers without requiring deep technical AI expertise.

TABLE II: Ethical UX Compliance Framework (EUXCF) — Five Dimensions

Dimension	What to Evaluate	Green (Ethical)	Red Flag (Dark Pattern)	CCPA Rule Linked
1. Price Transparency	Is the full price shown at the first point of product display?	Total price (incl. all fees and taxes) shown on product page	Final price revealed only at checkout — drip pricing	Drip Pricing / Basket Sneaking
2. Consent Architecture	Is every add-on, donation, and subscription opt-in by default?	All extras are unchecked; user must actively choose to add	Extras pre-ticked; user must actively remove them	Basket Sneaking / Forced Action
3. Urgency Authenticity	Are scarcity and urgency messages based on real inventory/time data?	"Only 3 left" only shown when stock is actually 3 or fewer	AI generates urgency messages regardless of actual availability	False Urgency / Interface Interference
4. Exit Freedom	Can users cancel, decline, or exit without guilt-inducing language?	Decline buttons are neutral ("No thanks" / "Skip")	Guilt language used ("No, I hate saving money" / "I'll take risk")	Confirm Shaming / Subscription Trap
5. Algorithmic	Is AI optimisation	AI objectives include	AI optimised purely	Interface

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

Accountability	reviewed for dark pattern outcomes?	user satisfaction scores alongside revenue	for conversion / revenue with no ethical constraints	Interference / Disguised Advertisements

Source: Authors' framework synthesised from CCPA Guidelines (2023), FTC (2022), Brignull (2010), AI Critique (2025), and Eleken (2025).

Scoring: A business earning "Green" on all five dimensions can be classified as an Ethical UX Practitioner. Three or more "Red Flag" ratings indicate systemic dark pattern risk requiring immediate redesign and legal review. The framework is designed to complement India's CCPA 2023 guidelines and can be used as a self-audit tool for the compliance declarations now mandated by the CCPA advisory of June 2025.

VI. CONCLUSION

Dark patterns have always been a problem in digital design. But AI has transformed them from occasional tricks into a sophisticated, personalised, and continuously self-improving manipulation system. The examples documented in this paper — from Zomato's checkout shock to BookMyShow's basket sneaking to IndiGo's confirm shaming to Epic Games' $520 million fine — are not isolated incidents. They represent a systemic design philosophy in which consumer autonomy is treated as an obstacle to revenue optimisation.

India's regulatory response through the CCPA 2023 Dark Pattern Guidelines and the June 2025 mandatory self-audit directive is a significant and welcome step. But self-declarations are not enough. The same AI systems that design dark patterns can easily generate compliance-sounding documentation. What is needed is genuine algorithmic accountability — building ethical constraints directly into the AI optimisation objectives that govern UX design.

The Ethical UX Compliance Framework (EUXCF) proposed in this paper offers a starting point. By evaluating AI-driven interfaces across five practical dimensions — price transparency, consent architecture, urgency authenticity, exit freedom, and algorithmic accountability — businesses can identify dark pattern risks before they become regulatory violations and consumer trust disasters.

Ultimately, the paper argues for a simple but powerful reframe: good UX and ethical UX are not opposites. A platform that respects its users, shows honest prices, and makes cancellation easy does not sacrifice growth — it builds the kind of trust that sustains long-term business success. In the age of AI, that trust is the most durable competitive advantage a digital business can have.

V. ACKNOWLEDGMENT

The author sincerely thanks Ramsheth Thakur College of Commerce and Science, Kharghar, Navi Mumbai, for the academic encouragement and institutional support that made this research possible. The author also gratefully acknowledges the publicly available regulatory documentation from India's Central Consumer Protection Authority (CCPA), and the research contributions of Harry Brignull, whose foundational work on dark patterns continues to inform consumer protection globally.

REFERENCES

[1] Brignull, H. (2010). Dark Patterns: Deceptive User Interfaces. Retrieved from https://darkpatterns.org

[2] 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), pp. 1–32.

[3] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 12, May 2026 Impact Factor: 8.2

[4] Central Consumer Protection Authority (CCPA), India. (2023). Guidelines for Prevention and Regulation of Dark Patterns, 2023. Ministry of Consumer Affairs, Government of India. Notified 30 November 2023.
[5] Central Consumer Protection Authority (CCPA), India. (2025, June 5). Advisory to All E-Commerce Platforms and Online Service Providers on Dark Patterns. Ministry of Consumer Affairs, Government of India.
[6] Tribune India. (2025, November 20). Swiggy, Zomato, Flipkart Among 26 E-Commerce Platforms Complying with Dark Pattern Guidelines. Retrieved from https://www.tribuneindia.com
[7] AI Critique. (2025, March 27). Generative AI and Dark Patterns in UX Design. Retrieved from https://www.aicritique.org
[8] Federal Trade Commission (FTC). (2022, December). FTC Charges Fortnite Maker Epic Games for Deploying Dark Patterns. FTC Press Release, Washington DC. Fine: USD $520 million.
[9] Eleken. (2025). 18 Dark Patterns Examples and How to Avoid Them. Retrieved from https://www.eleken.co
[10] Bricx Labs. (2025). 8 Real-World Dark Pattern Examples: How Websites Trick Users in 2025. Retrieved from https://bricxlabs.com
[11] Varun Sharma. (2025). Dark Patterns Exposed: How Amazon, Flipkart and Quick Commerce Apps Loot Indian Consumers. Retrieved from https://varunsharma.org
[12] Neetiniyaman. (2025). Dark Patterns in Digital Platforms: India's Rules and Guidelines. Retrieved from https://neetiniyaman.com
[13] European Commission. (2022). Study on Dark Patterns: Report on the Prevalence of Dark Patterns in Digital Interfaces Across the EU. Brussels: European Commission Publications.
[14] Cialdini, R. B. (2009). Influence: Science and Practice (5th ed.). Pearson Education.
[15] ScienceDirect / Tandfonline. (2025). Detecting Dark Patterns in Shopping Websites — A Multi-Faceted Approach Using BERT. Enterprise Information Systems. Published February 24, 2025. DOI: 10.1080/17517575.2025.2457961.