DARK PATTERNS AND BEHAVIOURAL MANIPULATION IN DIGITAL MARKETPLACES

by

Reathiga Ravi R.K

Dhanalakshmi Srinivasan University

&

Asaikavin A

Dhanalakshmi Srinivasan University

&

Naveendran B

Dhanalakshmi Srinivasan University

&

Selva Harinesh C

Dhanalakshmi Srinivasan University

ABSTRACT:

In the hyper and competitive arena of digital marketplaces and dark patterns it is a deceptive interface designs that exploit cognitive vulnerabilities that have become insidious tools of behavioral manipulation, eroding consumer autonomy and skewing market dynamics. The CCPA Guidelines for Prevention and Regulation of Dark Patterns 2023 prohibit 13 patterns including subscription traps and disguised ads under section 3,4, and 5. In digital marketplaces where platforms such as amazon, flipkart, and meesho deploy tactics like drip pricing, false urgency, basket sneaking, and confirm shaming to drive unintended consumer actions. The Consumer Protection Act 2019 defines the unfair trade practices under section 2(47). Section 4 of the Competition Act 2002 provides that dark patterns enabling behavioral lock-in that can distort the competition which is to be seen in CCI probes against amazon and flipkart. In India while the CCPA fines remain modest relative to Big Tech revenues, global benchmarks offer sharper tools like the EU Digital Services Act article 25 of it which bans dark patterns outright with fines up to 6% of global turnover. The CCPA in June 2025 mandated the self-audits across 50+ platforms with compliance declaration. The National Cyber and AI Center framework has introduced risk-based AI assurance that is targeting manipulative nudges in digital

marketplaces while harmonizing with India AI missions. It advocates a unified digital fairness authority with mandatory behavioral audits, public pattern registries, and turnover that is linked with the penalties to deter A/B tested manipulations that is ensuring platforms prioritize ethical design over exploitative nudges.

Keywords:

Cognitive vulnerabilities, CCPA Guidelines for Prevention and Regulation of Dark Patterns 2023, EU Digital Services Act, National Cyber and AI Center, 6% of global turnover

INTRODUCTION:

Dark patterns represent a deceptive method in the digital market world where they have been used as a profit prioritizing platform. This has been coined by Harry Brignull in 2010[1] where it has various tactics such as ads mimicking, legitimate buttons for hiding subscription traps and exploit cognitive biases like loss aversion and default inertia. The e-commerce platform eroded the informed consent, inflate impulse buys, and perpetuate data extraction. This trend is well documented in the Indian market: a 2025 audit by LocalCircles, a citizen engagement platform that works with the Department of Consumer Affairs, found that ninety-seven per cent of two hundred and ninety major Indian online platforms continued to deploy at least one prohibited dark pattern nearly two years after the CCPA notification, with only three per cent of platforms found free of such practices. This persistence suggests that voluntary compliance and self-audit mechanisms alone have proven insufficient to curb manipulative design in the Indian digital economy.[2] These online platforms activities have been governed by the DPDP Act 2023 and the EU's Digital Services Act. These has behavioral manipulation play an important role over the psychological vulnerabilities, boosting seller revenues which is an undermining the consumer rights. It is calculated as a behavioral nudge, drawing from nudge theory[3] but twisted into "sludges" that impose friction on rational choices.

[1] Harry Brignull dark patterns: Deception vs. Honesty in UI Design Dark patterns (2010) https://darkpatterns.org (last visited may 4, 2026)

[2] LocalCircles, 'From Streaming to Shopping, Dark Patterns Rampant in Digital Services, Says LocalCircles' (NewsMeter, 27 September 2025) <https://newsmeter.in/entertainment/from-streaming-to-shopping-dark-patterns-rampant-in-digital-services-says-localcircles-755697> accessed 2 July 2026.

[3] Richard H. Thaler & Cass R Sunstein Nudge: improving decisions about health, wealth and happiness 3-6 (2008)

LEGAL FRAMEWORK:

The legal framework that targets the dark patterns integrate the consumer protection statutes, data privacy rules and platform regulations to curb manipulative designs in digital marketplaces. The CCPA issued guidelines for prevention and regulation of dark patterns 2023[4] which is to be provided under section 18(2)(j) of the Consumer Protection Act 2019. This Act has listed 13 prohibited tactics of the e-commerce they are 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 malware were these tactics has been used to do manipulation in the UI and UX designs.[5] Under Art.25(1) of the EU Digital Services Act which prohibits the dark patterns and requires a transparency design for systemic risks where large online platforms would face a fine of 6% of the global turnover with the enforcement via the commission since 2024.[6] Under section 5 of the Federal Trade Commission Act 2018 and the restore online shoppers confidence Act (ROSCA) which is targeting deceptive interface has proposed the click to cancel option which it to be the mandated rule for easy cancellation of the order. Domestic enforcement under the 2023 Guidelines has also gathered pace: in mid-2026 the CCPA imposed monetary penalties on the ed-tech platform PhysicsWallah and the software firm McAfee for practices classified respectively as basket sneaking, confirm shaming and forced action, and for a misleadingly asymmetric subscription renewal interface, marking a shift from earlier voluntary compliance orders toward direct financial penalties. These orders indicate that Indian regulators are beginning to treat interface design itself, rather than only advertising content, as a locus of unfair trade practice.[7] In the FTC v. Amazon[8] the prime subscription trap and confirm shaming

---

[4] Cent. Consumer Prot. Auth Guidelines for Prevention & Regulation of Dark Patterns,2023(nov30,2023) https://consumeraffairs.nic.in

[5] Consumer Prot. Act No 35, Acts of the Parliament 2019 (India) Ch V

[6] Regulation EU 2022/2065 of the Eur. Parliament & of the council of 19 Oct 2022 on a Single Mkt for Dig. Servs,2022 O.J (L 277) 1, arts 25, 52-55

[7] 'Consumer Protection Authority Fines PhysicsWallah and McAfee for Dark Patterns: What Counts as Consent Now?' (MediaNama, 3 June 2026) <https://www.medianama.com/2026/06/223-consumer-protection-authority-fines-physicswallah-and-mcafee-for-dark-patterns-what-counts-as-consent-now/> accessed 2 July 2026.

[8] Complaint Fed Trade Comm’n v. Amazon.com Inc., No 23-cv-132 (W.D. Wash June 21, 2023)

has violated section 5 of the FTC Act & ROSCA generating $1.7B unintended charges from 75M+ users.

BEHAVIORAL MANIPULATION AND COGNITIVE BIASES IN DIGITAL MARKETS:

Digital marketplaces the most frequently used platform for dark patterns that exploit cognitive biases using systematic mental shortcuts which would destroy the consumer psychological balance. For example: a platform deploy scarcity cues that only 3 stocks are left and in the urgency of buying or fear of missing it out which would lead to scarcity bias. Often the other terms and conditions are more in exploit status and it is quo bias which makes the users accept data sharing which would be otherwise rejected by themselves. These designs choices would amount to behavioral manipulation when they are systematically steer users toward choices that would benefit the consumer's expenses[9]. In India courts and other regulators are started to treat some of these acts as unfair trade practices under the CPA2019 and also the CCPA has laid down the guidelines of the deceptive designs of the dark patterns. So all these acts and design would affect a consumer's both physical and mental health of a wellbeing. In the Italian Competition Authority v. Amazon[10] the regulator found that amazon's ranking and default selection mechanisms on its marketplace platform exploited consumers cognitive biases such as default bias and limited attention by systematically steering them toward amazon favored listings thereby constituting unfair commercial practices under National Consumer Protection Law. Empirical research on India's digital marketplaces corroborates these doctrinal findings: LocalCircles's eighteen-month, AI-assisted audit of 228 Indian platforms found that forced action was the single most prevalent manipulative pattern, appearing on fifty-four per cent of platforms surveyed, followed closely by drip pricing at forty-eight per cent, with sectors such as edtech, online banking, quick commerce and OTT services recording seven or more distinct dark patterns each. Such consistency across otherwise unrelated sectors indicates that the exploitation of cognitive biases identified above is not incidental but a structural feature of platform design in India.[11]

[9] Live law "dark patterns and deep manipulation: regulating psychological exploitation in Indian digital markets" (2025)
[10] Italian Competition Authority amazon logistics (nov.4,2021) http://www.agcm.it.
[11] LocalCircles, 'LocalCircles Summarises Its Dark Pattern Findings After 18 Months of Research' (LocalCircles, 24 September 2025) <https://www.localcircles.com/a/press/page/ccpa-dark-patterns-survey> accessed 2 July 2026.

CONSUMER AUTONOMY AND INFORMED CONSENT:

In Indian law systems the consumer autonomy means that the consumer are free and they have the freedom to rational choices without manipulation as it is provided under article 21 of the Indian constitution that everyone has the right to privacy and dignity. On the other hand informed consent means were the consumers has the right to know and understand the key terms, risk, and consequences of a transaction in the digital markets before giving confirm or procced with a particular transaction[12]. When the digital platforms use the deceptive designs to collect uncharged fees, forced continuity and others the consent and autonomy are structured as undermined. In the Samira Kohli v. Dr Prabha Manchanda[13] the SC held that consent must be specific and informed emphasizing bodily autonomy as a core element of dignity under article 21. In digital markets, default settings, pre ticked boxes and dark patterns tilt the decision architecture in favor of the platform turning the consumer's choice into a procedural façade rather than a real exercise of autonomy[14]. For instance the CCPA's guidelines for Prevention and Regulation of Dark Patterns 2023 has explicitly link with the deceptive design which is to be covered under unfair trade practices were it is to mislead the consumers and impair their autonomy and restrict their freedom of choice[15]. Further in Vinod Khanna v. RG Stone Urology and Laparoscopy Hospital & Ors. The NCDRC has ruled that pre-printed generic consent forms with vague disclaimers do not amount to informed consent and may constitute unfair trade practice[16].

DARK PATTERNS IN E-COMMERCE AND SUBSCRIPTION MODELS;

In the e-commerce the design is user interface which means that they intentionally steer consumers into purchases, subscriptions or data sharing choices they would not make in a neutral environment. These includes the sneak into baskets, add on, hidden or late fees, pre ticked add on and prominent accept and tiny decline buttons which would countdown timers

[12] Justice K.S Puttaswamy (retd) v. union of India (2017) 10 SCC 1 holding that consent must be informed, specific, and freely given and rejecting opaque or "bundled" consent forms under the data privacy framework

[13] Samira Kohli v. Dr Prabha (2008) 6 SCC 430 emphasizing that consent must be specific and informed and treating patient autonomy as a facet of dignity under article 21

[14] See generally Neha Mishra Manipulation Under the click: Unravelling Dark Patterns in Digital Consumerism and the Indian Consumer Protection Act (2019) 4 Manu Law (2024) at 1-20 arguing that behavioral design in e-commerce systematically skews consumer choice

[15] Central Consumer Protection Authority Guidelines for Prevention and Regulation of Dark Patterns 2023 Consumer Protection Act 2019 (India)

[16] Vinod Khanna v. RG Stone Urology and Laparoscopy Hospital & Ors NCDRC (comp) No.186/2019(2020)

and fake scarcity and opaque or difficult cancellation flows (the roach motel)[17]. Further the e-commerce sites use different layouts, colors, and have some default settings were it is to exploit the scarcity, status-quo, and anchoring biases and the subscription model further rely on forced continuity buried renewal terms and hard to use opt outs to maximize retention and recurring revenue[18]. The e-commerce presentation as unfair is said in the Tribhuvan v. Facebook India Online Servs Pvt Ltd the NCDRC has held that misleading presentation of advertisements and offers on a digital platform could constitute deficiency of service and an unfair trade practice implicating interface presentation as a source of consumer harm[19].the CCPA enquiries and advisories have flagged prime enrolment flows and auto subscription conversions as deceptive enrolment practices requiring remedial measures. Empirical evidence bears out these subscription-related concerns across sectors beyond e-commerce: the Reserve Bank of India's February 2026 draft amendments to its Responsible Business Conduct Directions, later finalised, formally define and prohibit dark patterns such as basket sneaking and forced action in digital banking journeys, citing a LocalCircles survey in which fifty-seven per cent of respondents reported encountering basket sneaking and fifty-one per cent reported forced action on online banking platforms. The extension of dark pattern regulation from e-commerce into financial services signals a broader regulatory recognition that subscription and renewal architecture is a cross-sectoral consumer protection concern rather than one confined to online retail.[20]

ECONOMIC AND PSYCHOLOGICAL HARMS:

The dark patterns and manipulative behavior produce both the economic harm like unexpected charges, drain of household resources and switching costs and in case of psychological harm it leads to loss of trust, anxiety, decision regret and learned helplessness. The economic imbalance like sneak basket hidden fees at checkout all these would lead to a cancellation of the orders which is made up of UX designs. In the psychologically there will be a repeated exposure to the manipulative interfaces fosters mistrust reduces perceived agency and can cause anxiety or reactance when consumers discover they were misled the outcomes

---

[17] NDTV Dark patterns in e-commerce: why it matters to Indian consumers (may 27,2025) https://www.ndtv.com/india-news/dark-patterns-in-e-commerce-why-it-matters-to-indian-consumers-8526645.

[18] Arya Ramteke et al Detecting Deceptive Dark Patterns in e-commerce platforms(may 27,2024)

[19] Tribhuvan v. Facebook India Online Servs Pvt Ltd. complaint No CC-117/2020 (NCDRC) (June 30,2022)

[20] 'Compulsory Bundling, Dark Patterns Banned: Why the RBI Wants Banks to Stop Mis-Selling Financial Products' (MediaNama, June 2026) <https://www.medianama.com/2026/06/223-compulsory-bundling-dark-patterns-banned-rbi-financial-products-misseling/> accessed 2 July 2026.

documented in the behavioral economics and consumer psychology studies of the deceptive design[21]. National Consumer fora have treated the misleading presentation like digital ad and layout issues that have defective disclosure as constituted under the deficiency of service under CPA. In such a case the commission aim at restitution cancellation of unfair charges and corrective measures to the UX platforms. The courts and tribunals also use the traditional consumer law traps when assessing remedies for entrapped subscriptions. the remedies recommended are mandatory clear disclosure of the total price, the renewal terms, prohibiting the pre ticked paid options, straight forward cancellation and required notice before auto renewal and to provide periodic statement of recurring charges and fines or remedies where repeated harms has been displayed[22]. These measures aim to repair both the economic injury and the autonomy and psychological harms that deceptive design inflicts on consumers[23]. The financial scale of these harms in India is considerable: a 2026 analysis estimated that dark patterns cost Indian online shoppers approximately twenty-eight thousand crore rupees annually through hidden fees, forced upsells and drip pricing, with sixty-three per cent of surveyed users reporting exposure to hidden fees or drip pricing during checkout, a rise from fifty-two per cent the previous year. Such figures suggest that the economic harm caused by deceptive design has grown rather than diminished since the 2023 Guidelines came into force, underscoring the gap between regulatory notification and effective enforcement.[24]

DATA DRIVEN PERSONALIZATION AND AI NUDGING:

The personalization data driven is a user behavioral data where they have clicks, searches, purchase history, session timing, profiling, and predictive models to tailor recommendations, prices, and interface elements to individuals in real time[25]. When such personalization is designed to steer the choice of the consumer rather than informing them there occurs the algorithmic nudges which is selectively amplifying scarcity cues anchoring frames or social proof signals for users predicted to be susceptible with the aim of increasing conversion, retention, or monetized actions. Often the algorithmic nudges considers both the

---

[21] Tommaso Rebonato et al Dark patterns and consumer vulnerability behavioral public policy (2020) "the psychological traps of online shopping " (dec 14 2022)

[22] OECD Data Standards Body Patterns in the Dark Report (2024) (recommending remedies such as conspicuous pre renewal notices and one-click cancellation) Central Consumer Protection Authority guidelines

[23] UU Rebo Working Paper R. Basu Vulnerable Consumers and Dark Patterns in Digital Platforms Indian Journal in Consumer Law (2025)

[24] 'How Dark Patterns Are Quietly Costing Indian Online Buyers ₹28,000 Crore Annually' (The Logical Indian, June 2026) <https://thelogicalindian.com/how-dark-patterns-are-quietly-costing-indian-online-buyers-%e2%82%b928000-crore-annually/> accessed 2 July 2026.

[25] ACR Journal AI-Powered Personalization vs. consumer privacy striking the balance (2025)

economic and autonomy harms were it can extract the disproportionate value from the vulnerable consumers through the targeted up-sells, dynamic pricing, which erode the meaningful consent of the consumer by disclosing their personalizing data which often leads to discriminatory impacts when models use proxies for socio economics status and which creates a opacity that prevents effective challenges. Under the Indian Consumer Protection and Privacy frameworks these harms would implicate unfair trade practices, defective disclosure and data-protection duties and the regulators will have a signaled that personalization which materially misleads or the traps of the consumers may be actionable[26]. The National Commission has made many measures for the algorithmic impact assessments and independent audit focusing on consumer harm and has heightened protection for children, elderly, and low-literacy users. These are legitimate personalization benefits while preventing manipulative nudging that undermines autonomy and fairness[27]. The regulatory backdrop for such personalization practices shifted materially in late 2025, when the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules 2025 alongside the establishment of the Data Protection Board of India, bringing the consent, notice and data minimisation obligations of the 2023 Act into force on a phased basis through May 2027. Once fully operative, these obligations will require data fiduciaries engaged in behavioural profiling to justify the specificity and necessity of data collected for personalization, adding a distinct data protection layer to the unfair trade practice and consumer protection remedies discussed above.[28]

NEED FOR ETHICAL DESIGN STANDARDS:

Ethical design standards are the necessary measure to ensure that the digital platforms respect user autonomy, prevent exploitation and balance commercial goals with public interest. These standards translate the abstract value into autonomy, non-maleficence, transparency, and fairness into a concrete on design rules that reduce consumer harm while preserving legitimate product improvements. Standards require the interference of the consumer choice to decide what is their wants. By limiting the manipulation tactics standards would reduce the financial

---

[26] Central Consumer Protection Authority Guidelines for Prevention and Regulation of Dark Patterns (2023) and CCPA Advisory on self-audit by e-commerce Platforms (2025)

[27] Cambridge handbook and legal scholarship recommending algorithmic impact assessments and targeted safeguards for vulnerable users.

[28] Shahana Chatterji and Kirti Mahapatra, 'Enforcement of the DPDP Act and Notification of the DPDP Rules' (Shardul Amarchand Mangaldas & Co, 27 November 2025) <https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/> accessed 2 July 2026.

extraction, discrimination, and psychological harms that disproportionately burden vulnerable users. The CCPA's Guidelines for Prevention and Regulation of Dark Patterns (2023) and its 2025 self-audit advisory operationalize ethical norms into compliance requirements for e-commerce platforms which is in effective treating certain UX choices as unlawful which would be constituted under unfair trade practices when they mislead or trap the consumers[29]. The Reserve Bank of India's February 2026 draft Responsible Business Conduct directions, which propose mandatory user testing and periodic internal audit of banking interfaces for dark patterns alongside full refunds and compensation for proven mis-selling, illustrate how ethical design obligations are increasingly being written into binding sectoral regulation rather than left to indicative guidance. This regulatory convergence across the CCPA and the RBI suggests an emerging consensus that interface-level audit requirements, rather than after-the-fact grievance redressal alone, are necessary to operationalise ethical design standards.[30]

IMPACT ON VULNERABLE CONSUMERS:

Dark patterns and AI driven personalization are disproportionately harm to the vulnerable groups were the children, elderly people who belong to a low literacy level with digital skills and those who are economically constrained users are being exploiting to only a limited attention, lower digital literacy, cognitive biases, and financial fragility. Vulnerable users are to be less likely to detect the manipulative design and are less able to navigate the complicated opt-out procedures and more likely to comply with the authority or urgency signals where the personalization amplifies this by targeting the most susceptible individuals with the tailored nudges. In some decisions recognizing the digital access and the inclusion as aspects of fundamental rights. The courts have further emphasized that platforms must ensure access and non-discrimination for persons with disabilities and older users were the principles that support stronger obligations on the platforms to avoid designs that exploit vulnerabilities[31]. The remedies that is provided to these group of the peoples are the faster grievance redressal, presumptive refunds for subscription entrapment, and enhanced penalties in the cases of repeated harm to the vulnerable users. The scale of this vulnerability among elderly Indians is significant: survey data drawing on National Crime Records Bureau trends found that forty-

[29] Central Consumer Protection Authority Guidelines for Prevention and Regulation of Dark Patterns (2023) central consumer protection authority advisory on self-audit by e-commerce platforms for detecting dark patterns (June 5,2025) reporting CCPA's compliance push and platform self-audit initiative

[30] 'RBI to Regulate Dark Patterns in Banking Apps and Websites' (MediaNama, 26 February 2026) <https://www.medianama.com/2026/02/223-rbi-dark-patterns-draft-2026/> accessed 2 July 2026.

[31] Amar Jain v. Union of India (2025) (court recognising aspects of digital access and KYC accessibility as part of right to life and liberty).

five per cent of senior citizens struggled to identify online scams and that cybercrimes targeting the elderly rose by eighty-six per cent between 2020 and 2022, even as mobile phone usage among those aged sixty to sixty-nine climbed to sixty-one per cent over the same period. This widening gap between digital participation and digital literacy among older users heightens their exposure to the manipulative design practices discussed throughout this paper.[32]

CONCLUSION:

The dark pattern which is to be the most viral one among the digital market world were in the current society all the consumers are based on the e-commerce for buying the goods they want. So the deceptive designs used in the online platforms like Amazon, Flipkart, Meesho, etc were many consumers are being forced to unwanted charges and experiencing deficiency in service. Dark patterns are not mere UX quirks but deliberate choice cognitive biases to produce outsized commercial gains when eroding the consumer autonomy, privacy, and trust. Because these techniques work across all the demographic groups and often persist where the enforcement is weak and tackling them for the demands coordinated action. It has legally outlaw the most manipulative practices, require transparency and design audits, which push over the platform to adopt ethical defaults and equip consumers with a clearer information and easier remedies. Only by combining regulation, corporate governance changes and design ethics can digital marketplaces become both innovative and fair for preserving the benefits of online choice without sacrificing user rights.

[32] '45% of Indian Seniors Struggle to Identify Online Fraud, Cybercrimes on the Rise' (Storyboard18, 4 March 2025) <https://www.storyboard18.com/digital/45-of-indian-seniors-struggle-to-identify-online-fraud-cybercrimes-on-the-rise-58331.htm> accessed 2 July 2026.