WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Consent and Coercion in the Digital Economy: Legal Perspectives on Dark Patterns in India

[1]Rishabh Agarwal, [2]Dr. Ramakant Tripathi

[1 2] Law college Dehradun, India.

ABSTRACT:

There is a rapid evolution of an expanding digital economy in India that is anticipated to touch $350 billion by 2030. It can witness the invasive growth of dark patterns-hiding behavior manipulation by user interface/front-end design. False urgency promos, subscription traps, dripping pricing and other such darkness practices consent undermine and exploit cognitive biases. It affects the 350 million online consumers in India from whom a majority are novice, casual users with little digital literacy. Dark patterns infringe the foundational principles of consent provided for in Section 13 of the Indian Contract Act, 1872. Dark patterns are today coming under the purview of burgeoning acts such as the Consumer Protection Act, 2019, the 2023 Guidelines on Dark Patterns by the CCPA, the Digital Personal Data Protection Act, 2023, and the Competition Act, 2002. While the legal frameworks describe dark patterns as unfair trade practices, misleading advertisements, and violations of privacy, the mechanism to enforce these provisions has remained overly reactive against fragmented institutions, constraining resources, and delays in courts. A few of the major cases against Amazon, MakeMyTrip, and Paytm, which have shown increasing legal scrutiny, still are pending as of March 2025. The present paper presents an account of those psychological and behavioral mechanisms by which coercive design occurs, an indication of the blurry line between persuasion and manipulation, and exposes the compelling immediate need for regulation reform. Suggested remedies include forming an integrated task force, refinement of enforcement capabilities, launching digital literacy campaigns, and establishing ethical UI design standards. India is propelling its digital market; therefore, it becomes all the more important to ensure that systemic interventions happen to maintain the informed consent and ethical digital relations.

Keywords: Dark pattern investigation, Digital agreement, UI or UX manipulation, Consumer Protection Act 2019, Data Privacy India, Coercion in design, Indian Contract Act, Regulation in the digital economy.

Introduction

Digital transformation in the Indian economy stands before its most significant transformation, waiting to explode at $350 billion by 2030, powered by a broad digital infrastructure with widespread adoption of Internet technologies. By 2025, the nation is likely to have over 936 million Internet subscribers, of which 350 million will be online transaction-using individuals reflecting an enormous shift towards digital adoption. All this will take place because of the meteoric rise of e-commerce behemoths like Flipkart and Amazon India, social media giants such as Instagram and WhatsApp, and fintech innovators such as Paytm and PhonePe. Only e-commerce recorded sales of $60 billion in 2023, while the UPI has seen growth in digital payments processing over 100 billion transactions in a year. However, the immediate concern for the business sector here is that these platforms do not only change how business is carried out but also how the people of India interact, purchase, and manage budgets thereby creating a vibrant yet complex digital ecosystem. Adding to this rapid transformation is another set of challenges that deal mostly with user freedom and consumer protection in an increasingly digitalized interface where interaction mediates many conditions.[1]

Emergence of Dark Patterns

In this digital age, dark patterns of UI and UX come as one common stray in the dgital world. Defined intentionally chosen manipulative designs and behavioral patterns by users for favoring platform interests instead of individual agency, dark patterns manipulate user actions tricking them into doing something they would not do otherwise.4Examples include false urgency reminders like “Only 2 left in stock” appearing on the e-commerce sites to pan and induce a kind of impulsive purchase, subscription traps that hide cancellation within a twisted menu, and drip pricing to expose fees at the time of check out, like MakeMyTrip does in travelling. Such practices were introduced in India for the first time by the UX designer Harry Brignull in 2010 and reported on by the Advertising Standards Council of India (ASCI) in 2024 for their prevalence across online buying, social networking, and financial services. With such designs in a marketplace common to digital transactions, an immediate investigation surface to address their legality and morality in India’s digital landscape.

Significance of Consent and Coercion

The contemporary emergence of dark patterns assaults the very essence of consent, defining it as the agreement to be informed, voluntary, and free from coercion. It does not cease here; in India law, notably Section 13 of the Indian Contract Act, 1872, real living persons must consensus according to tamper-proof understanding and untainted by manipulative influences.7Dark patterns drag it down into duress for ultimate decisions regarding sharing private data, agreeing to subscriptions, or undergoing unanticipated charges without full awareness or intent. This kind of autonomy is, of course, a reflection of very strong ethical implications, especially in India, which has millions living in very low digital literacy in rural areas.8Almost 60% of the Internet population are defined as novices, not able to solve difficult interfaces; hence, the exploitation from such interfaces to such populations will be amplified in disparity. Legal as well, these practices challenge the very bond of digital contracts and consumer rights; while ethically, they create a crack in the trust of a market much more dependent on online platforms. This is the need for stricter laws and mechanisms to cover consent and limit the possibility of coercion as India struggles with this tension.[2]

Understanding Dark Patterns: Concept, Types, and Implications

Harry Brignull, a British UX designer, invented the term “dark patterns” in 2010, referring to the intentional design choices made in digital interfaces that cause users to take action against their best judgment, for the benefit of the platform rather than the user. Dark patterns counter the spirit of ethical design, which seeks to provide clarity and enhance usability by, for example, providing clear navigation or simple opt-out options. Dark patterns, on the other hand, serve to manipulate behavior for commercial gains. An ethical design website would reveal the stock level of its products accurately and allow the user to change items in the shopping cart easily; in contrast, a website rife with dark patterns would employ exaggerated scarcity tactics or sneak selected items into the user’s shopping cart at checkout. This difference becomes important in India’s digital economy, where platforms like Amazon India, Flipkart, and Paytm govern user interactions. Since Brignull’s framework has emerged as a global standard and increasingly represents the ethical and legal issues these designs raise with the advent of digital commerce, in India the rise of these patterns has kept pace with the exponential growth in online engagement, thus demanding an in-depth understanding of their workings and associated effects.

Taxonomy of Dark Patterns

The Guidelines for Prevention and Regulation of Dark Patterns, 2023, issued by the CCPA, have coined some lethal terms which give us robust taxonomy for dark patterns, with 13 specifically noted in their use against consumer choice. Some of the more apparent examples include: (1) False Urgency: the act of manufacturing faux scarcity (ex: “Only 2 left” from Flipkart); (2) Basket Sneaking: adding items to carts without consumer consent (ex: charity donations on Amazon); (3) Confirm Shaming: the act of applying guilt to pressure users into compliance (ex: “I’ll risk it” on declining insurance from travel websites); (4) Forced Action: the unnecessary actions forced (ex: app download to make purchases); (5) Subscription Trap: the act of making cancellation impossible (ex: Netflix’s many-step opt-out); (6) Interface Interference: these dark patterns obscure options (for example, on a visual spectrum they make the “No” button look faded); (7) Bait and Switch: they are substituting the offerings (e.g., In Myntra, the cheap deals never existed;); (8) Drip Pricing: hiding fees until the moment of payment (ex: airline surcharges on MakeMyTrip); (9) Disguised Advertisement: ads masked as content (ex: fake reviews on Instagram) (10) Nagging: e.g. WhatsApp repeating requests for backup; (11) Trick Question: like misleading language; (12) SaaS Billing: automatic ongoing charges without notice, such as free trials turning into paid subscriptions on Adobe; and (13) Rogue Malware: misleading users into downloading malware, such as fake virus alerts.

India has real-world examples. E-commerce platforms now advertise “Only 2 left” to create urgency purchase, generally unverifiable, travel sites like Yatra.com hiddenly charge to the consumer such that their costs increase by up to 20-30% under “additional fees”. Cataloged in their 2024 ASCI report, such practices are not only present in any specific sector but run from online retail to social media, therefore the need for the regulatory scrutiny being emphasized here.[3]

Psychological Mechanisms

On the contrary, cognitive biases that dark patterns leverage - manipulating psychological triggers to bypass rational decision-making - were described using Daniel Kahneman’s dual-process theory of System 1 (impulsive) versus System 2 (deliberative) thinking.4False urgency taps into the fear of missing out (FOMO), prompt rash purchases; confirm shaming brings guilt to bear, pressure for conformity; and subscription traps play on inertia relying on user apathy to ensure inaction.14A 2021 study linked the streaks feature at Snapchat to dopamine-fueled engagement, suggesting how this kind of design prompts habitual behavior more like addicition.5It has a special potency in India by profile status that 60% of the 936 million Internet subscribers include novice users, frequently from rural settings, where digital illiteracy is high; hence, they are easy prey for such devices.6

According to a consumer survey conducted in 2023, 70% of Indian users of e-commerce sites succumbed to urgency prompts and ended up buying items that they later regretted, while nagging notifications on apps such as Instagram drained users into enabling unwanted features. This vulnerability accentuates the coercive influence of dark patterns which makes voluntary choices into forced actions especially for the uninitiated in digital navigation.[4]

Legal Implications

The legal implications of dark patterns are primarily those of their erosion of consent, and this is the bedrock of Indian law as per the Indian Contract Act of 1872. Section 13 defines consent as the mutual agreement of the parties, while Section 15 renders the same void when obtained through coercion; coercion is defined as any act causing injury or unlawful pressure. Dark patterns will manipulate user intent- be it through obscured options or psychological nudges-infringing this standard. For instance, a subscription trap that locks users into recurring payments without clear assent may render the resulting contract unenforceable, as it lacks the free agreement Section 13 mandates.

Such relevance holds very strongly for transactions done digitally. On the face of it, the very act of pressured choice in the presence of dark patterns—be it consenting to data sharing on Paytm or buying an extra on Amazon—raises questions about its validity. The Consumer Protection Act, 2019, calls them out explicitly as unfair trade practices under Section 2(47), while the Digital Personal Data Protection Act, 2023, emphasizes the necessity of consent (§ 6), both of which violations call dark patterns into consideration. This complicity renders a strong regulatory rampart quite necessary, because when choices are manipulated, these choices violate not just consumer rights but also cast doubts on the sanctity of the digital marketplace of India.

Legal Framework in India

The legal responses on dark patterns in India mainly integrate consumer protection law, competition law, and privacy law for a comprehensive approach to maintain the autonomy of users in digital economy engagement.

Consumer Protection Act, 2019, and Guidelines for Prevention and Regulation of Dark Patterns, 2023

The Consumer Protection Act of 2019 is another landmark legislation that gives a fresh lease to consumer protection in India, especially regarding the digital consumer. Section 2(9), defining consumer rights, speaks about protection against unfair trade practices, while Section 18 refers to establishing the Central Consumer Protection Authority (CCPA) as a regulatory body responsible for issuing guidelines and enforcing compliance.8While the new CPA has been introduced precisely in the context of India's booming digital economy, projected to reach $350 billion by the year 2030, it has also taken into account new-age challenges such as online frauds where dark patterns thrive. The role of the CCPA becomes important in this regard as it not only watches the market but also enforces laws in order to protect an immense population of 350 million active online users from exploitation in e-commerce, social media, and fintech.

2023 Guidelines

On November 30, 2023, after substantial stakeholder consultations, the CCPA proclaimed the Guidelines for Prevention and Regulation of Dark Patterns, 2023, becoming the first overt response targeting manipulative digital designs in India. These guidelines place dark patterns under UI/UX practices that "subvert or impair consumer autonomy, decision-making, or choice", thereby constituting misleading advertisements under Section 2(28) or unfair trade practices under Section 2(47) of the CPA. Largely, their ambit extends to platforms, advertisers, and sellers, who issue offers of goods or services systematically in India, with particular application to foreign entities like Amazon and Netflix; business to business (B2B) transactions are, however, expressly excluded. This delineation allows focus on consumer-facing digital interactions, which, as at 2025, are supported by India's 936 million Internet subscribers.

Specific Dark Patterns

Thirteen categories of deceptive behaviors have been delineated, rooted in principles of consumer protection.

- False Urgency: Misleads via scarcity claims (e.g., "Only 2 left" on Amazon), violating transparency (§ 2(28)).
- Basket Sneaking: Adds items without consent (e.g., donations on Flipkart), an unfair practice (§ 2(47)).
- Confirm Shaming: Guilt-trips users (e.g., "I'll pay more" on airline sites), manipulating choice.
- Forced Action: Mandates extras (e.g., app downloads on Myntra), breaching autonomy.
- Subscription Trap: Hides cancellation (e.g., Netflix's multi-step process), unfair retention.
- Interface Interference: Misleads via design (e.g., faint "No" on pop-ups), deceptive.
- Bait and Switch: Substitutes offerings (e.g., unavailable deals on Ajio), misleading.
- Drip Pricing: Conceals fees (e.g., MakeMyTrip's surcharges), violating disclosure.
- Disguised Advertisement: Masks ads (e.g., Instagram fake reviews), deceptive advertising.
- Nagging: Persistent prompts (e.g., WhatsApp backups), coercive.
- Trick Question: Confuses intent (e.g., opt-out traps), manipulative.
- SaaS Billing: Unnotified charges (e.g., Adobe trials), unfair.
- Rogue Malware: Deceives into downloads (e.g., fake alerts), fraudulent.
- Examples like Amazon's urgency prompts and Netflix's cancellation hurdles illustrate their real-world impact, often inflating costs or locking users into services.[5]

Enforcement Mechanisms

The CPA permits the CCPA to act either suo motu or based on complaints or government references. Section 21 imposes penalties: a fine of INR 20 lakhs for the first-time offence and INR 50 lakhs for subsequent misleading advertisements, along with imprisonment for a term that may extend to 6 months. Compensation may be awarded by District Consumer Commissions which comes under Section 39, which provides cover for consumer damage caused by dark patterns. However, enforcement is still in its infancy, with few investigations conducted so far-a March 2025 report mentioned a probe into Amazon on drip pricing in 2024 that might indicate resource or prioritization issues.

Case Law

Rakesh Sharma v. Amazon India[6]: The complainant alleged that drip pricing inflated the checkout prices by around 30% and that he was misled into paying a higher amount. This case, filed in 2023, tests the applicability of CPA with respect to dark patterns. The arguments were still ongoing as of 2025.

In Kumar's view, the hidden charges are coercive and violative of any consumer autonomy. The case is still pending since 2022, showing judicial concern for pricing strategies. The case is therefore significant since various elements of pricing strategies are being subjected to judicial scrutiny. These court cases signal an increasing awareness of laws. However, due to their unsettled outcomes, they limit the value of their precedents.

Competition Law

Legal Basis

The effect of Section 4 of the Competition Act, 2002 is to prohibit abuse of a dominant position, and this becomes the part of the framework the Competition Commission of India ("CCI") operates under for digital platforms. In that context, CCI has been appreciating data as a non-price metric of competition that relates manipulative UI/UX design to distortions in the market. Such dark patterns invoked by dominant players have been able to exploit consumers while erecting entry barriers for potential competitors.

Key Cases

The CCI Case No. 01/2021 on the WhatsApp Privacy Update: The CCI in 2021 began looking into the updates in privacy policy by WhatsApp, claiming coercive consent for sharing data with Facebook breaches Section 4(2)(a). This investigation, still continuing in 2025, is looking into whether abuse can be attributed to opt-in designs.

The Google Pay case (as CCI Case No. 07/2020) is an investigation into the UI of Google Pay, primarily regarding the elimination of Open Markets for competitors such as PhonePe, misusing dark patterns for its favorable standing. The matter is still unresolved.

The Amazon Marketplace (CCI Case No. 40/2019): The CCI opined that Amazon was liable for INR 202 crores in fines for being involved in anti-competitive practices in 2022, which included UI bias favoring certain sellers that could indicate dark pattern implications.

Analysis

The cases are the intersection between dark patterns and competition law where data is exploited and market barriers are created. For instance, WhatsApp's policy may interfere with the interface to compel consent, and the very design of Google Pay could present forced action. However, with the decisions still pending as of March 2025, their immediate influence is mitigated, serving to evidence the CCI's restrained stance towards new-age digital dilemmas.[7]

Data Protection and Privacy Laws

In Section 6 of the DPDP legislation, enacted in August 2023, consent is required to be "free, specific, informed, and unambiguous" for data processing purposes. Sections 7 and 8 impose transparency and notice requirements on data fiduciaries, ensuring that the users know how their data will be used. This relates to countering dark patterns that obfuscate consent.

Relevance to Dark Patterns

Dark patterns such as pre-ticked boxes (for example, Paytm's default for data-sharing consent) or annoying prompts (like the notifications of Instagram) are contrary to Section 6 so as to nullify the element of meaningful consent. In January 2025 in the Rahul Gupta v. Paytm8, it was alleged that the mandatory Aadhaar linking for obtaining basic services breached the right to privacy under the DPDP Act. Pending before the court, this case brings to the fore the privacy implications of dark patterns.

Implementation Status

The rules of the DPDP Act will still be under finalization and unavoidably delay the Act from fully coming to force. These delays will make it difficult for the Act to address dark patterns with timely rules, although those intentions are apparent.

Interplay and Gaps

Whereas CPA concerns deception, the CCI deals in market abuse, and the DPDP Act speaks to privacy, thus creating overlaps: actions that may be said to forcibly violate all of these three. Enforcement, however, is still facing challenges: the CCPA, CCI, and Data Protection Board work independently, and lack of resources hamper any proactive approach. The evident gaps are reflected in the fact that over 50 dark pattern complaints against the CCPA filed in 2024 remain unaddressed. This speaks to a necessity for a coordinated approach toward dealing with this diverse issue effectively.

Analysis of Consent and Coercion

The essence of dark patterns is to apply some form of psychological manipulation to interfere with legal notions of consent and coercion.

Psychological Underpinnings

Dark designs capitalize on cognitive biases to counteract rational decision-making by exploiting the psychological weaknesses of their victims. The scarcity bias leads to an errant false sense of urgency, as with countdowns such as “Hurry! Sale ends in 10 minutes” on Flipkart, thereby triggering feelings of fear of missing out (FOMO). The phenomenon of confirm shaming puts social pressure in play whereby messages such as “I’ll risk my safety” for declining insurance manipulate users into compliance. An inertia-thriven fatigue directs subscription traps when users are reluctant to navigate through elaborate cancelation; think Netflix. An ASCI study done in India in 2023 notes that 70% of e-commerce users fall prey to urgency tactics and end up buying goods they later regret—this speaks to the strength of these designs in front of a market 350 million active online consumers.9

This kind of manipulation is revealed with the help of the dual-process theory of Daniel Kahneman the behavioral economist: dark patterns attack System 1 thought--automatic, impetuous responses-- and bypass the System 2 deliberate, reflective processes. The 2021 study about streaks on Snapchat, for example, revealed how such items trigger dopamine release, thus conditioning users to compulsive activity resembling addiction. Well, in a country like India, where 60% of the 936 million Internet subscribers are novice/inexperienced users, very often found coming from rural areas with limited digital sophistication, such conditions magnify exposure.: Clogging users on such apps to convert into allowing notifications is what nagging might mean in the general sense. The dishonest advertisement disguised as a review shows how dark patterns can turn voluntary into forced choices.

Legal Standards of Consent

Indian law prescribes severe thresholds of consent which are usually violated by dark patterns. Consent is defined in the Indian Contract Act, 1872, under Section 13, as an agreement between parties, and Section 15 renders it void when caused by coercion, such as any act which causes harm or unlawful pressure. The Consumer Protection Act, 2019 (CPA) also extends it into the digital domain to define unfair trade practices under Section 2(47) as voiding consent by deceiving or exploiting consumers. Under the Digital Personal Data Protection Act, 2023 (DPDP Act), it is additionally prescribed in Section 6 that “free, specific, informed, and unambiguous” consent has to be taken for data processing, which gets diluted by manipulative designs.

Subscription traps (example: requiring phone calls for canceling a service) or drip pricing (like hidden charges on MakeMyTrip) are actual dark patterns that curtail voluntariness making such agreements unenforceable as per Contract Act. These have now been explicitly linked to unfair practice in the 2023 Guidelines of the CPA, and the DPDP Act nullifies consents based on pre-ticked boxes and tricky questions as seen in some fintech apps like Paytm. This triad of law-Contract Act, CPA, and now DPDP Act-makes a neat sum of requirements about true intent from users for digital transactions, which, more often than not, dark patterns fail to satisfy.

Judicial Perspectives

Indian courts have always held true and favorable actions in favor of the consumers such that they had a special lens to see through dark patterns. In Consumer Education and Research Centre v. Union of India10, the Supreme Court required to keep autonomy as a basic right besides protection against exploitative practices. The issues raised in this precedent are thus to be extended to dark patterns where autonomy is sacrificed. Vinod Kumar v. MakeMyTrip11 has more direct effects, alleging coercive pricing through hidden costs inflated prices claiming violation of rights under the CPA. Though filed in 2022, it remains pending in 2025, still testing the judicial willingness to declare dark patterns equal to coercion.12

Subscription traps could potentially be prosecuted by the same light. If a user continues an unwanted subscription because he/she is misled by the intricacy of the cancellation process, the courts shall deem the same contract unenforceable under section 15 of the Contract Act on the grounds of coercion by design.

Tension Between Persuasion and Coercion

The gray line that separates persuasion and coercion is however fine, and critical. While marketing tactics like discounts or limited-time offers legitimately induce behavior, the dark side of persuasion transforms into manipulation in that it either obscures the truth or exploits vulnerabilities. A clear "50% off today" promotion persuades; whereas a fake claim that "only 1 left" coerces by deception.
The intent and effect form the legal line: practices are unfair under CPA if they "cause the consumer to take a transactional decision he would not have taken otherwise." Courts may ask whether a reasonable user would have acted differently without manipulation—e.g., have opted out of a subscription if cancellation had been more intuitive. This tension showcases the need for distinct judicial and regulatory lines in India to encapsulate the difference between good, ethical persuasion and bad, illegal coercion in the digital environment.

Recent Examples and Enforcement Trends

Dark patterns continue to pose their pernicious presence across sectors in India; although the legal framework permits swift and effective action, action appears to be slow. This section highlights some prominent examples across sectors and assesses the regulatory and judicial responses.[13]
Notable Instances (2024-2025)

E-commerce

- Sheer urgency is being manipulated via "Lightning Deals" (for example, "Ends in 2 hours") which are sometimes impossible to verify; meanwhile, drip pricing adds hidden fees at the checkout stage, raising prices by 20-30%.
- Flipkart: Hidden delivery costs sneak up later, leading customers to spending more, an ASCI report indicates in 2024.14

Social Media

- Instagram application: These relentless nagging notifications ("Turn on now!") wear down the user until they comply, while ads masquerading as user posts deceives the matrix into working for engagement.

Fintech

- Paytm: Compulsory linking of Aadhaar for base transfers portrays forced action, along with subscription traps in loan apps inherently trap users to make them pay

Travel

- On Yatra.com, claim "Just 1 seat left", as usually inaccurate, are seen to falsely propagate a sense of urgency and boost bookings.
- Enforcement Actions

CCPA Initiatives

- Amazon Probe (Dec. 2024): The CCPA launched an investigation into drip pricing, potentially facing INR 20-50 lakh fines under Section 21, though no ruling has emerged.
- Complaints: Over 50 dark pattern complaints were filed in 2024, ranging from false urgency to subscription traps, yet no major penalties have been imposed, signaling enforcement delays.

ASCI Role

- 2024 Recommendations: ASCL recognized significant concerns about hidden ads sold on Instagram and eCommerce sites promoting quick sales through disapprovals
- Limitations: With no sanction powers under the ASCI's supervision, the effectiveness of deterrents is thus limited.[15]

Enforcement Gaps

- The CCPA has been afflicted with resource constraints: investigations get prolonged due to understaffing (see, for instance, the sluggish progress in probing Amazon). Delay of judicial proceedings, as in some of the unresolved cases in the NCDRC, thus only builds onto this imbalance, suggesting a reactive, not proactive, take on these matters. With over 50 complaints pending, this signal of a backlog calls for stringent monitoring and faster redressal mechanisms to curtail dark patterns.

Suggestions

In order to efficiently counter dark patterns in India's digital economy, it would be important to bring about a holistic approach that amalgamates legal integration with better enforcement, user education, and design governance.

Integrated Legal Framework

The overlapping jurisdictions of the Consumer Protection Act, 2019, the Competition Act, 2002 and the Digital Personal Data Protection Act, 2023, therefore, create silos for enforcement, thereby diluting the potency of all three legislations with regard to dark patterns. One option that may seem useful in this situation is to create a joint task force of the Central Consumer Protection Authority, Competition Commission of India and the future Data Protection Board under the DPDP Act. This task force would harmonize investigations-for instance, confronting forced actions violations, which relate to consumer deception (CPA), market abuse (CCI), and privacy breaches (DPDP)-reducing duplication and speeding up redressal. [16] This would also need a unified set of guidelines, one that would be an expansion of the 2023 Dark Patterns Guidelines and ought to specifically define these overlaps as offenses, like drip pricing as both an unfair trade practice and tactic of data exploitation. This is akin to the coordinated enforcement by the EU under the GDPR, which encompasses the multidimensional nature of digital manipulation. Pooling expertise within the task force would give priority to high-impact cases involving the likes of the ongoing one into Amazon, thus improving efficiency in under-resourced systems.

Enhanced Enforcement

Strengthening enforcement mechanisms is critical to deter dark patterns. First, the CCPA requires a significant budget and staffing increase—current understaffing delays probes, with over 50 complaints from 2024 still pending. Allocating funds to hire digital forensics experts and investigators, akin to the U.S. FTC's specialized units, would expedite cases like the December 2024 Amazon drip pricing investigation. Second, empowering the Advertising Standards Council of India (ASCI) with penalty authority—beyond its current advisory role—would bolster deterrence. ASCI's 2024 advisories on disguised ads flagged violations, but without fines, compliance remains voluntary. Granting ASCI powers akin to the CCPA's (e.g., INR 20 lakh fines) could target smaller-scale offenders, complementing the CCPA's focus on major platforms.

And, a dark patterns complaint portal should be launched, both mobile and web-based, for easy reporting especially for rural users. The structure can be replicated from the California CPPA portal to register all the complaints- say Paytm linking their services with Aadhaar as complaint-example-and automatically trigger a CCPA review to reduce the current backlog and improve responsiveness. These, complete in themselves, will orient law into aspiring practices of enforcement rather than putting it from the reactive to proactive category.

Digital Literacy

Digital literacy gives power to the people and acts as the preventive cornerstone of such an endeavor. Awareness campaigns should be nationwide but with a slice into rural India, where about 60% of India's 936 million Internet subscribers are novices. Learning dark patterns would include those bad examples such as false urgencies or nagging prompts. Through partnerships with NGOs and other platforms such as Doordarshan and regional radios, such campaigns could reflect the European Union's GDPR awareness drives to reduce the susceptibility of India's 350 million online users. Including such topics on digital rights into school curricula-fighting with consent manipulation and safe navigation, would prepare future generations. This could be piloted in states like Tamil Nadu that are comparatively more digital, and then ramp it up by 2030. Literacy not only reduces the levels of harassment but also heightens pressure on platforms to self-regulate augment legal measures.[17]

Design Regulation

Setting rules on transparent UI/UX design is a preventive fix awaiting the DPDP Act's regulations. In drawing from Article 7 of the GDPR, India's requirement for opt-in/opt-out mechanisms must allow equal prominence to all design elements-E.G., there shall be no faint "No" buttons-and pre-ticked boxes should be prohibited just as Paytm has set default data-sharing settings. To ensure compliance with such norms, monitoring is needed through annual audits to be conducted by third-party agencies on the likes of platforms such as Flipkart and Instagram. Building upon such penalties for non-compliance-fines based on an entity's revenue-would mirror the EU design requirements to tighten enforcement. Thus, this regime anticipates placing the burden on platforms, thus lessening reliance on post-violation enforcement and creating a user-friendly and responsive digital ecosystem.[18]

Conclusion

While dark patterns seriously threaten consent and autonomy in the digital economy of India, they exploit the user into performing undesirable actions like unwanted subscriptions or data sharing. The Consumer Protection Act, 2019, strengthened with the 2023 Guidelines, provides a solid platform to prevent deceptive UI/UX designs classified as unfair trade practices. The Competition Act, 2002, prevents distortion of the market by dominant players,

while the Digital Personal Data Protection Act, 2023, keeps privacy intact through rigorous consent enforcement. The very gaps in these mechanisms, including siloed enforcement, lack of resources, and delayed justice delivery, render these measures ineffective against the ever-present menace of dark patterns.

The legal advancements have not much assisted enforcement actions. The CCPA 2024 Amazon investigation and more than 50 pending complaints reflect a reactive approach rather than a proactive one. Given the slow case progress due to capacity constraints, cases such as Rakesh Sharma v. Amazon India and Rahul Gupta v. Paytm further suffer. The recent cases reflect the predominance of dark patterns across e-commerce, social media, fintech, and travel sectors: false urgency from Amazon; incessant nudging from Instagram; coercive nudging from Paytm; and scarcity claims by Yatra.com. The emergence of standing cases is a precursor to awareness, while enforcement stagnation devoid of any big fines leaves consumers exposed in an exponentially growing $60 billion e-commerce market.

India's way forward can be built on three pillars: integration, enforcement, and literacy. One way to fill enforcement gaps is a joint CPA-CCI-DPDP task force, enhanced CCPA resources and an empowered ASCI, with the help of a complaint portal. Digital literacy campaigns at the national level and in school curricula will add to users' power, while rules requiring UI/UX transparency, along with audits, will serve as a safeguard against violations. Embedding within the U.S. spirit for enforcement and clarity toward design from the EU, India will create its balanced model. India, with the potential and the need for ushering in ethical digital regulation for its digital economy worth $350 billion by 2030, must ensure that consent remains a foundational principle of the online ecosystem.

REFERENCES :

1. Dark Patterns and User Consent: Ethical Concerns in Digital Design, available at: https://thelegalschool.in/blog/dark-patterns (last visited on March 19, 2025).
2. Beni Chugh & Pranjal Jain, Unpacking Dark Patterns: Understanding Dark Patterns and Their Implications for Consumer Protection in the Digital Economy, available at: https://www.rsrr.in/_files/ugd/286c9c_3da4e758c4db40098ebe691004e90b71.pdf?index=true (last visited on March 22, 2025).
3. The Need for the Triangular Approach – Dark Patterns, available at: https://www.cdpp.co.in/articles/the-need-for-the-triangular-approach---dark-patterns (last visited on March 24, 2025).
4. Neelesh Sinha, Dark Patterns in Digital Business – A Legal Perspective in India, available at: https://www.linkedin.com/pulse/dark-patterns-digital-business-legal-perspective-india-neelesh-sinha-hfolf/ (last visited on March 25, 2025).
5. Manan Chhabra, Sameer Avasarala, et.al., Demystifying the Dark Patterns, available at: https://www.lakshmisri.com/insights/articles/demystifying-the-dark-patterns/# (last visited on March 21, 2025).
6. Delhi SCDRC, Consumer Case No. 456/2023.
7. Rohi Ray, Dark Patterns and India's Legal Battle for Ethical E-Commerce, available at: https://jolt.richmond.edu/2023/10/04/dark-patterns-and-indias-legal-battle-for-ethical-e-commerce/ (last visited on March 27, 2025).
8. NCDRC, Consumer Complaint No. 789/2024.
9. YAGAY and SUN, Regulations on Dark Patterns, available at: https://www.taxmanagementindia.com/visitor/detail_article.asp?ArticleID=13547 (last visited on March 20, 2025). 1995 AIR 922.
10. NCDRC, Consumer Complaint No. 123/2022.
11. Neha, Dark Patterns Outlawed: Online Platforms to Watch Out, available at: https://www.scconline.com/blog/post/2025/02/27/dark-patterns-outlawed-online-platforms-to-watch-out/ (last visited on March 25, 2025).
12. Sandeep J. Sharma, Ishita Sharma, et.al., "Dark Patterns in a Bright World: An Analysis of the Indian Consumer Legal Architecture", 11 International Journal on Consumer Law and Practice 7 (2023).
13. Nikhil Naren, "Dark Patterns: How Design Tricks Manipulate Users", The Hindu, January 17, 2024.
14. Renu Gupta, Akshat Bhushan, et.al., Looking at Dark Patterns in Light of the Competition Law in India, available at: https://blogs.law.ox.ac.uk/business-law-blog/blog/2021/11/looking-dark-patterns-light-competition-law-india (last visited on March 24, 2025).
15. Hayati AN, "The Issue of Dark Patterns in Digital Platforms: The Challenge for Indonesia's Consumer Protection Law", 11 Asian Journal of Law and Society 453 (2024).
16. Aarushi Jain, Krishnangi Bhatt, et.al., Dark Patterns: An (Un)Fair Trade Practice?, available at: https://corporate.cyrilamarchandblogs.com/2023/08/dark-patterns-an-un-fair-trade-practice/ (last visited on March 27, 2025).
17. Raja Sengupta, Contracts, Clicks, and Compliance: The Invisible Hands of Dark Patterns, available at: https://complianceandethics.org/contracts-clicks-and-compliance-the-invisible-hands-of-dark-patterns/ (last visited on March 27, 2025).