Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Dark Patterns and Digital Consumer Protection in India: Filling the Regulatory Gaps

Sneha Vijayvargiya[a]

[a]Indore Institute of Law, Indore, India

Received 10 June 2026; *Accepted* 10 July 2026; *Published* 13 July 2026

Dark patterns are manipulative user-interface design techniques that deceive or coerce consumers into decisions they would not otherwise make and have become endemic to the Indian digital economy. Despite the rapid growth of e-commerce, over-the-top platforms, and fintech services in India, the regulatory architecture addressing dark patterns remains fragmented and, in critical respects, non-existent. This paper examines the conceptual foundation of dark patterns, surveys their taxonomy and documented prevalence in the Indian context, and critically evaluates the adequacy of India's existing legal framework comprising the Consumer Protection Act 2019, the Information Technology Act 2000 and allied rules, and the Guidelines for Prevention and Regulation of Dark Patterns 2023 issued by the Central Consumer Protection Authority. The paper argues that the Guidelines, while a significant first step, suffer from definitional ambiguity, enforcement limitations, and a failure to address the asymmetry of cognitive harm that dark patterns produce. Drawing upon comparative experience from the European Union's Digital Services Act, the United Kingdom's Online Safety Act, and United States Federal Trade Commission enforcement, the paper proposes a set of legislative and institutional reforms to build a comprehensive, rights-centred framework for digital consumer protection in India.

Keywords: *dark patterns, digital consumer protection, deceptive design.*

INTRODUCTION

In 2010, the user experience researcher Harry Brignull coined the term 'dark patterns' to describe interface design techniques that trick users into taking actions they did not intend, such as subscribing to unwanted services, sharing personal data, or accepting unfavourable contractual terms.[1] While the phrase entered design discourse as a term of professional criticism, its legal salience has grown considerably as digital platforms have become the dominant arena of commercial exchange. A 2022 study by the Princeton Web Transparency and Accountability Project found that more than eleven per cent of popular shopping websites deployed at least one dark pattern, with manipulative tactics appearing disproportionately on platforms with larger user bases.[2]

India presents a particularly urgent site for analysis. With over 850 million active internet users, a burgeoning e-commerce sector projected to reach USD 350 billion by 2030, and a consumer base characterised by significant digital literacy disparities, the conditions for exploitative design are structurally embedded. The Indian consumer is confronted daily with countdown timers that manufacture artificial scarcity, pre-ticked consent boxes that silently enrol users into marketing lists, and subscription interfaces that make cancellation deliberately labyrinthine. These practices cause concrete, measurable harm: financial loss, erosion of privacy, and the suppression of genuine autonomous choice.

India's regulatory response has been incremental. The Consumer Protection Act 2019 introduced a broad prohibition on 'unfair trade practices' and 'misleading advertisements,' but did not anticipate the specific architecture of digital manipulation.[3] The Central Consumer Protection Authority ('CCPA'), exercising its powers under the Act, issued the Guidelines for Prevention and Regulation of Dark Patterns 2023 ('the Guidelines'), a noteworthy intervention that represented the first time an Indian regulatory body formally defined and categorised dark patterns.[4] Yet the Guidelines are not statutory instruments; they carry uncertain enforcement weight, their definitions contain material ambiguities, and

---

[1] Harry Brignull, 'Deceptive patterns trick people into doing things they didn't mean to.' (*Deceptive Patterns*) <https://deceptive.design/> accessed 07 June 2026

[2] Arunesh Mathur et al., 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (Proceedings of the ACM on Human-Computer Interaction, Association for Computing Machinery 2019)

[3] Consumer Protection Act 2019, ss 2(28), 2(47)

[4] Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns 2023* (Ministry of Consumer Affairs, Food and Public Distribution, November 2023)

they do not address the structural causes of dark-pattern proliferation: the advertising-revenue business model and the absence of privacy-by-design obligations.

This paper is organised as follows. Part II develops a working conceptual and taxonomic framework for dark patterns. Part III analyses the Indian legal landscape, examining both the existing statutory framework and the Guidelines. Part IV undertakes comparative analysis of regulatory approaches in the European Union, the United Kingdom, and the United States. Part V identifies the principal gaps in the current Indian framework. Part VI proposes reforms. Part VII concludes.

DARK PATTERNS: CONCEPT AND TAXONOMY

Conceptual Foundation: A dark pattern may be understood as a user interface design choice that exploits cognitive biases such as loss aversion, status quo bias, or anchoring to direct user behaviour towards outcomes that serve the platform's commercial interests at the expense of the user's informed autonomy.[5] The defining characteristic that distinguishes dark patterns from ordinary aggressive marketing is the deliberate exploitation of the architectural context of choice: the user's decision is structured, framed, and constrained by the interface designer in ways the user cannot readily perceive or correct.

Academics have located the conceptual roots of dark patterns in the broader literature on ‘choice architecture’ developed by Richard Thaler and Cass Sunstein.[6] Thaler and Sunstein argued that the design of choice environments is never neutral; every default, every framing, every ordering nudges decision-makers in a particular direction. Dark patterns weaponise this insight: where benign nudges aim to promote the chooser’s welfare, dark patterns aim to extract value from the chooser for a third party. Mathur et al. have argued, persuasively, that dark patterns represent a form of ‘asymmetric power in the digital choice environment,’

[5] Colin M Gray et al., ‘The Dark (Patterns) Side of UX Design’ (CHI Conference on Human Factors in Computing Systems, Montreal, 2018) 534 <https://dl.acm.org/doi/10.1145/3173574.3174108?__cf_chl_f_tk=qPOCOBPEz_rf93n0hXV3D3HXhKOCeTVOxMrISLg5z9k-1782828060-1.0.1.1-vn3nt5UyDJl9BMqRphiCzW6nsVuYcIPQ5UBUiKNvSbo> accessed 07 June 2026

[6] Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (Yale University Press 2008) 3–6

which markets cannot self-correct because the harm to any individual user is often diffuse and invisible.[7]

Taxonomic Overview: The literature has produced several competing taxonomies of dark patterns. The most influential for regulatory purposes is the typology developed by Grey et al., which identifies five meta-categories: nagging, obstruction, sneaking, interface interference, and forced action. The CCPA Guidelines adopt a somewhat different classification, enumerating thirteen specific dark patterns: false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, disguised advertisement, nagging, trick question, SaaS billing, rogue malware, and disguised advertisement.

For legal analysis, the following typology, which maps onto the harm-causation mechanisms most relevant to consumer protection law, is adopted in this paper:

Deceptive Urgency and Scarcity: false countdown timers and stock indicators designed to suppress deliberation (e.g., 'Only 2 left!' when stock is plentiful).

Hidden Costs and Basket Sneaking: the clandestine addition of charges or items to a consumer's basket without explicit consent.

Confirm Shaming: the use of emotionally laden language to stigmatise the opt-out choice (e.g., 'No thanks, I don't want to save money').

Subscription Traps and Roach Motels: interfaces designed to make enrolment trivially easy but cancellation unreasonably difficult.

Privacy Zuckering and Forced Data Sharing: consent flows designed to extract maximum data through confusing or deceptive presentation of privacy choices.

The Indian digital market has exhibited documented instances of all five categories. A 2021 investigation by the Software Freedom Law Centre India identified basket sneaking on at least fourteen major Indian e-commerce platforms, where insurance products or donation amounts were pre-ticked at the checkout stage. The Advertising Standards Council of India's

[7] Arunesh Mathur et al., 'What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods' (CHI Conference on Human Factors in Computing Systems, Yokohama, 2021) 1, 4 <https://dl.acm.org/doi/10.1145/3411764.3445610> accessed 07 June 2026

2022 report on digital advertising documented widespread false urgency on travel aggregator platforms.[8]

THE INDIAN LEGAL FRAMEWORK: AN ASSESSMENT

The Consumer Protection Act 2019: The Consumer Protection Act 2019 ('the Act') is the primary legislative instrument governing consumer rights in India. The Act defines 'unfair trade practice' under Section 2(47) to include practices that adopt 'unfair methods or unfair or deceptive practice for the purpose of promoting the sale, use or supply of any goods or for the provision of any service.'[9] Section 2(28) prohibits 'misleading advertisements,' defined as those that give a false description of goods or services or conceal material information. The Act also vests the CCPA with broad powers under Section 18 to protect, promote, and enforce consumer rights and prevent unfair trade practices.

On its face, these provisions appear capacious enough to capture dark patterns. A countdown timer falsely representing scarcity could constitute a misleading advertisement; basket sneaking could constitute an unfair trade practice. However, several structural limitations prevent the Act from functioning as an effective regulatory instrument against dark patterns.

First, the Act's enforcement architecture is complaint-driven. Consumer disputes are resolved through a three-tier commission structure District, State, and National that requires individual consumers to initiate proceedings.[10] This architecture is ill-suited to the systemic, diffuse, and often low-value harm caused by dark patterns, where the per-consumer loss may be trivial, but the aggregate harm across millions of users is substantial. The class-action mechanism introduced under Section 35(1)(c) theoretically addresses this, but in practice, consumer class actions in India have remained nascent, beset by procedural complexity and limited legal aid.

Second, the Act predates the digital era in its conceptual framing. Its definition of 'goods' and 'services'does not specifically address free-at-point-of-use digital platforms where the consumer pays with data rather than money.[11] Dark patterns on social media platforms, which are technically free but commercially extractive, fall into a regulatory gap that the Act

[8] *Annual Complaints Report 2021–22* (Advertising Standards Council of India 2022) 34–36
[9] Consumer Protection Act 2019, s 2(47)(i)
[10] *Ibid* ss 34, 47, 58
[11] *Ibid* s 2(7)

does not explicitly address. The Supreme Court in State of Tamil Nadu v K Balu observed that consumer protection legislation must be interpreted purposively,[12] but purposive interpretation has limits where the textual gap is structural rather than semantic.

Third, the Act does not impose any positive design obligations on platforms. It prohibits certain outcomes (deception, unfair practice) but does not require that interfaces be designed to a standard of clarity, transparency, or accessibility. This negative framing cannot prevent dark patterns prospectively; it can only penalise them after consumers have already been harmed.

The Information Technology Act 2000 and Data Protection: The Information Technology Act 2000 ('the IT Act') addresses cyber-related offences and electronic contracts. Section 43A imposes liability for negligent handling of sensitive personal data. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 require significant social media intermediaries to establish grievance redressal mechanisms and appoint grievance officers.[13] However, neither the ITA nor the 2021 Rules address dark patterns as a distinct category of harm.

The Digital Personal Data Protection Act 2023 ('DPDPA') represents the most significant recent development in India's digital regulatory landscape.[14] The DPDPA requires that consent to data processing be 'free, specific, informed, unconditional, and unambiguous.' This standard, if enforced rigorously, would invalidate most privacy dark patterns, including pre-ticked consent boxes and bundled consent flows. However, the Act's consent framework has been criticised for its significant exceptions: consent is not required for 'legitimate uses' broadly defined, and the central government's exemption powers are wide.[15] Furthermore, the Act is not yet fully operationalised; its implementing rules are still under development, and the Data Protection Board, the enforcement body, has not been constituted.

The CCPA Dark Patterns Guidelines 2023: In November 2023, the CCPA issued the Guidelines for Prevention and Regulation of Dark Patterns 2023, applicable to all platform sellers, advertisers, and service providers operating in India. The Guidelines represent the

[12] *State of Tamil Nadu Rep By Secy and Ors v K Balu and Anr* (2017) 2 SCC 281 [48]
[13] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rr 3 and 4
[14] Digital Personal Data Protection Act 2023
[15] *Ibid* ss 7(b)–(j), 36

most direct regulatory engagement with dark patterns to date. They define 'dark patterns' as 'any practices or deceptive design patterns using UI/UX interactions on any platform that are designed to mislead or trick users into doing something they didn't intend to,' and enumerate thirteen prohibited categories.

The Guidelines are a significant regulatory achievement. They demonstrate awareness of the specific technological mechanisms through which consumers are manipulated, provide a vocabulary for regulatory action, and signal to industry that dark-pattern practices carry legal risk. However, several limitations reduce their effectiveness. First, the Guidelines are issued under Section 18 of the Consumer Protection Act 2019, which empowers the CCPA to issue directions and guidelines. Whether such guidelines carry the force of law and whether non-compliance attracts the penalties prescribed under the Act is not unambiguously established. The CCPA has the power to impose penalties up to Rs 10 lakh on first instance under Section 88, but this may be disproportionately low to deter large platforms whose revenue from dark patterns vastly exceeds potential fines.

Second, the definitional language of the Guidelines is imprecise. The definition of 'false urgency,' for example, encompasses 'creating a false sense of urgency to pressure consumers into making purchases' but does not specify the evidentiary threshold for establishing falsity, leaving platforms room to argue that their urgency indicators are based on real demand data. Comparative experience suggests that regulatory effectiveness is enhanced by concrete, measurable thresholds such as the EU's requirement under the Omnibus Directive that platforms display only verified reviews.[16]

Third, the Guidelines do not address the underlying business model incentives that drive dark-pattern adoption. Platforms operating on advertising-based revenue models have structural incentives to maximise engagement and data collection regardless of user preference; design manipulation is a rational commercial response to these incentives. Regulatory prohibition without structural market intervention addresses symptoms rather than causes.

[16] Directive (EU) 2019/2161 of the European Parliament and of the Council amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU [2019] OJ L328/7 art 7a

COMPARATIVE REGULATORY APPROACHES

The European Union: The European Union has developed the most comprehensive multi-instrument approach to dark pattern regulation. The Digital Services Act ('DSA') 2022, applicable from February 2024, imposes direct obligations on online platforms to refrain from designing, organising, or operating interfaces that deceive, manipulate, or impair users' ability to make free and informed decisions.[17] Article 25 of the DSA prohibits 'deceptive or manipulative' interface design that exploits cognitive biases. Critically, the DSA applies this prohibition to all online platforms, including social media and search engines, not merely e-commerce operators.

The DSA is complemented by the General Data Protection Regulation ('GDPR') 2016, under which the European Data Protection Board issued Guidelines 05/2020 on consent, specifying that consent obtained through dark-pattern interfaces is invalid as a matter of data protection law.[18] This creates a dual-track enforcement mechanism: dark patterns that involve data processing attract GDPR liability (up to four per cent of global annual turnover) in addition to DSA sanctions. The GDPR's 'cookie wall' jurisprudence developed through decisions of the Irish Data Protection Commission and the French CNIL has been particularly effective in dismantling dark-pattern consent flows on major platforms.[19]

The Unfair Commercial Practices Directive 2005, as amended by the Omnibus Directive 2019, further prohibits misleading commercial practices, and the Consumer Rights Directive imposes transparency requirements at the point of digital contracting.[20] Together, these instruments constitute a layered framework that addresses dark patterns as violations of consumer rights, data protection rights, and general commercial fairness norms simultaneously.

The United Kingdom: Following its departure from the European Union, the United Kingdom has pursued a partly divergent regulatory path. The Competition and Markets Authority ('CMA') launched a programme of enforcement action against dark patterns under

---

[17] Digital Services Act 2022, art 25

[18] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679* (EU 2020)

[19] Dan Milmo, 'France fines Google and Facebook €210m over user tracking' *The Guardian* (06 January 2022) <https://www.theguardian.com/technology/2022/jan/06/france-fines-google-and-facebook-210m-over-user-tracking-cookies> accessed 09 June 2026

[20] Directive 2005/29/EC of the European Parliament and of the Council concerning Unfair Commercial Practices [2005] OJ L149/22; Directive 2011/83/EU on Consumer Rights [2011] OJ L304/64

the Consumer Protection from Unfair Trading Regulations 2008.[21] Its 2022 report on 'subscription traps' documented the systematic use of difficult cancellation mechanisms and recommended a 'no-fault easy exit' requirement an obligation that cancellation be no more difficult than subscription which was subsequently adopted in the Digital Markets, Competition and Consumers Act 2024.[22]

The Online Safety Act 2023 adds a further dimension by imposing duties of care on platforms regarding user protection, with the communications regulator Ofcom empowered to issue codes of practice on design standards.[23] The UK approach is notable for its reliance on sector-specific expert regulators the CMA for commercial practices, Ofcom for online safety- rather than a single consumer protection authority, an institutional design that produces more technically sophisticated enforcement but risks coordination gaps.

The United States: In the United States, dark patterns are regulated primarily through the Federal Trade Commission's ('FTC') general authority to prohibit 'unfair or deceptive acts or practices' under Section 5 of the FTC Act.[24] The FTC's 2022 report, Bringing Dark Patterns to Light, documented the prevalence of manipulative design across digital commerce and issued industry guidance specifying the characteristics of dark patterns that the agency would treat as deceptive.[25] The FTC has brought several enforcement actions, including a USD 375 million settlement with Epic Games in 2022 arising in part from dark-pattern practices in the Fortnite game interface.[26]

The American approach is enforcement-led rather than statutory, which gives it flexibility but also creates unpredictability. The absence of a dedicated regulatory framework analogous to Europe's DSA means that enforcement priorities shift with administration changes, and small and medium platforms face less consistent scrutiny than major players.

IDENTIFYING THE GAPS IN INDIA'S FRAMEWORK

Absence of Positive Design Standards: The most fundamental gap in India's regulatory architecture is the absence of positive design obligations. Both the Consumer Protection Act

[21] The Consumer Protection from Unfair Trading Regulations 2008 (UK)
[22] Digital Markets, Competition and Consumers Act 2024 (UK), ss 253–256
[23] Online Safety Act 2023, s 10 (UK)
[24] Federal Trade Commission Act 15 US C s 45(a)(1)
[25] *Bringing Dark Patterns to Light* (Federal Trade Commission 2022)
[26] *United States of America v Epic Games Inc* [2023] Civil Action No 5:22-cv-00518-BO

and the CCPA Guidelines are framed in prohibitory terms: they specify what platforms must not do, but not what they must do. A robust framework would require that digital interfaces meet minimum standards of clarity, accessibility, and transparency at the design stage; that consent mechanisms be presented in equal-weight visual formats; or that subscription cancellation pathways be no more complex than subscription pathways. The DPDPA's consent requirements move in this direction for data processing, but they are not yet operationalised and do not extend to non-data commercial practices.

Inadequate Deterrence Through Penalties: The penalty structure under the Consumer Protection Act is ill-calibrated to large digital platforms. The maximum penalty of Rs 50 lakh for misleading advertisements under Section 21, and Rs 10 lakh for unfair trade practices under Section 88, represents a trivial cost relative to the revenue generated by dark-pattern practices at scale.[27] The EU's approach of calibrating maximum penalties to a percentage of global annual turnover four per cent under the GDPR and six per cent under the DSA provides a proportionality mechanism that India's fixed penalties cannot replicate. Legislative reform should introduce turnover-based penalties for large platforms, defined by reference to user numbers or revenue thresholds.

Enforcement Architecture and Expertise: The CCPA's enforcement capacity is constrained by limited technical expertise and investigative resources. Dark pattern identification requires interface analysis, user testing, and data analytics capabilities that the CCPA currently lacks. The separation of consumer protection (CCPA), data protection (Data Protection Board, not yet constituted), and competition regulation (Competition Commission of India) creates coordination gaps: a dark pattern that simultaneously violates consumer protection norms, data protection requirements, and competition law may fall between regulatory stools. The CCI has engaged with digital market design in the context of anti-competitive practices,[28] but a formal coordination mechanism between the CCPA, the Data Protection Board, and the CCI for dark-pattern enforcement does not exist. The CCPA has power under Section 22 of the Act to investigate unfair trade practices suo motu; a programme of proactive, technology-assisted platform audits — analogous to the CMA's market study methodology — would significantly enhance enforcement effectiveness.

[27] Consumer Protection Act 2019, ss 21(1), 88
[28] *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users* (2021) SM Case No 01/2021 (CCI)

Exclusion of Free Digital Services: A significant structural gap is the uncertain application of the consumer protection framework to free-at-point-of-use digital services. The CCPA Guidelines apply to all 'platforms,' which would include social media and search services, but the Consumer Protection Act's definition of 'consumer' in Section 2(7) requires payment of 'consideration.' The Supreme Court has not yet definitively resolved whether the provision of personal data constitutes 'consideration' for the Act. Until this is authoritatively settled, whether by judicial decision or legislative amendment, free-tier digital services operate in a state of regulatory uncertainty that platforms may exploit.

No Redress for Behavioural and Psychological Harm: Dark patterns cause a form of harm that standard consumer protection frameworks are not designed to remedy: the suppression of autonomous choice and the exploitation of cognitive vulnerability. Traditional remedies-compensation, refund, and injunction address financial loss and unlawful conduct, but do not address the structural psychological harm of accumulated manipulation. Behavioural economics research has documented that repeated exposure to dark patterns degrades users' epistemic confidence and reduces their willingness to exercise choice, an effect sometimes described as 'learned helplessness' in digital environments. A comprehensive regulatory framework would need to develop remedies, including mandatory consent restoration, data deletion rights, and periodic re-consent requirements that address this distinctive form of harm.

PROPOSED REFORMS

Legislative Amendment to the Consumer Protection Act 2019: The Consumer Protection Act should be amended to introduce a dedicated Part addressing digital commercial practices. The amendment should:

(i) define dark patterns with reference to specific manipulative mechanisms, rather than the general definition in the current Guidelines;

(ii) expressly extend the Act's coverage to digital services provided in exchange for personal data, resolving the 'consideration' uncertainty;

(iii) introduce a 'design transparency' obligation requiring platforms to maintain and disclose records of A/B testing, user-interface experiments, and default settings; and

(iv) introduce turnover-based penalties for large digital platforms, with a minimum threshold of two per cent of Indian annual turnover.

Elevation of the CCPA Guidelines to Statutory Rules: The CCPA Guidelines should be elevated to statutory rules under Section 101 of the Consumer Protection Act, which empowers the central government to make rules prescribing prohibited unfair trade practices.[29] Statutory rules, unlike executive guidelines, carry unambiguous legal force and create clear obligations that courts and enforcement authorities can apply. The rules should be developed through formal public consultation, including technical input from user-experience researchers, platform engineers, and civil society organisations.

Establishment of a Digital Markets Regulatory Council: India should establish a cross-regulatory Digital Markets Regulatory Council, comprising representatives of the CCPA, the Data Protection Board, the Competition Commission of India, and the Telecom Regulatory Authority of India (TRAI), with a mandate to coordinate enforcement on digital harms including dark patterns that span the jurisdictions of multiple regulators. The Council should be empowered to issue joint enforcement notices, undertake coordinated audits, and develop shared technical standards for interface design compliance. This model draws on the EU's Digital Regulation Cooperation Forum and the UK's Digital Regulation Cooperation Forum, both of which have demonstrated the value of regulatory coordination in complex digital markets.

Positive Design Standards and Privacy-by-Design Requirements: The DPDPA's implementing rules should incorporate 'consent-by-design' standards specifying minimum visual, linguistic, and structural requirements for consent interfaces. These should include:

(i) equal-prominence requirements for accept and decline options;

(ii) a prohibition on pre-ticked consent boxes;

(iii) a requirement that layered privacy notices be genuinely layered rather than cosmetically so; and

[29] Consumer Protection Act 2019, s 101

(iv) a prohibition on making service access conditional on consent to processing unnecessary for the service's core function. These design standards should be extended, through amendment to the Consumer Protection Act, to commercial consent flows that do not involve personal data processing.

Technical Capacity Building at the CCPA: The CCPA should establish a dedicated Digital Consumer Protection Cell with technical expertise in user-experience research, interface analysis, and digital market monitoring. The Cell should be funded through a levy on large digital platforms and empowered to commission independent audits, maintain a public register of dark-pattern enforcement actions, and publish annual reports on dark-pattern prevalence in the Indian digital market. This model draws on the UK CMA's Digital Markets Unit, established in 2021, which has developed significant in-house technical capability for digital market investigation.

Access to Justice for Digital Consumers: The class-action mechanism under Section 35(1)(c) of the Consumer Protection Act should be reformed to reduce procedural barriers to collective consumer actions in digital disputes. A simplified 'collective complaint' procedure should be established for digital consumer harms with per-consumer losses below a specified threshold, enabling consumer organisations and the CCPA itself to bring representative actions without the procedural requirements of standard class litigation. Consumer legal aid should be extended to digital consumer protection cases, and a small-claims digital consumer tribunal, building on the existing consumer commission structure but with dedicated online dispute resolution infrastructure, would reduce the transaction costs that currently deter individual claims.

CONCLUSION

Dark patterns represent one of the most pervasive yet under-regulated harms in the contemporary Indian digital economy. The gap between the sophistication of the manipulative techniques that major platforms deploy and the capacity of India's regulatory framework to address them is wide and growing. The CCPA's 2023 Guidelines represent a meaningful first step; the recognition that dark patterns constitute a category of legally cognisable harm is itself significant, but they are insufficient to address the structural causes of dark-pattern proliferation or to provide meaningful redress for the millions of Indian consumers who are their targets.

This paper has argued that a comprehensive response requires intervention on at least four fronts: legislative reform to the Consumer Protection Act to introduce positive design standards and proportionate penalties; institutional reform to build regulatory coordination and technical capacity; operationalisation of the DPDPA's consent framework to address privacy dark patterns; and procedural reform to make collective redress genuinely accessible to digital consumers. The comparative experience of the European Union, the United Kingdom, and the United States demonstrates that purposive, technically informed, and institutionally coordinated regulation can meaningfully reduce dark-pattern prevalence.

The broader normative stake is this: the right to free and informed consumer choice recognised in the Consumer Protection Act, derived from the constitutional guarantee of personal liberty, and affirmed in India's obligations under the United Nations Guidelines for Consumer Protection cannot be meaningful if the digital environments in which most commercial choices are made are systematically designed to subvert it. The law's task is to restore the conditions in which genuine choice is possible. That task remains unfinished.