DARK PATTERNS AND CONSUMER PROTECTION: A SHIFT FROM HARM-CENTRIC TO DESIGN-BASED REGULATION IN INDIA

Shivesh Aggarwal & Ishaa Mahajan[*]

ABSTRACT

The proliferation of dark pattern practices in digital markets has raised significant concerns regarding consumer autonomy and transparency in the operation of e-commerce and digital platforms and in the offering of goods and services through them. These practices, which are subtly integrated into the UX and UI design architecture of the platforms, manipulate users and influence their decision-making behaviour. In India, dark patterns are primarily regulated under the Consumer Protection Act, 2019, and the Guidelines for Prevention and Regulation of Dark Patterns, 2023 issued by the Central Consumer Protection Authority. This article analyses the nature and classification of dark patterns, examines the existing Indian legal framework governing dark patterns, and evaluates recent regulatory actions and governing frameworks established in the US and EU. This article aims to argue that the current Indian framework remains predominantly harm-centric and is therefore insufficient to address the design-based nature of dark practices. It is argued that a shift towards a principle-driven regulatory approach is needed, along with targeted policy measures to strengthen consumer protection in digital markets.

Keywords: Dark Patterns, Consumer Protection, Digital Markets, Regulatory Framework, User Experience Design.

[*] Shivesh Aggarwal is Counsel at Trilegal, and Ishaa Mahajan is a Senior Associate at Trilegal. The authors also wish to acknowledge the research assistance provided by Shoptorishi Dey of RGNUL. The views stated in this paper are personal.

I. DARK PATTERNS: INTRODUCTION AND CHARACTERISTICS

As widely reported for the past decade, the term 'dark patterns' was coined by Mr. Harry Brignull, a UK based user experience ('**UX'**) and user interface ('**UI'**) designer in 2010, who defines it, in simple terms, as 'tricks used in websites and apps that make you do things you didn't mean to, like buying or signing up for something.[1] In other words, dark patterns refer to business practices commonly found in UX or UI design elements of digital platforms, which steer, manipulate, deceive or coerce users by exploiting consumer bias, to make choices which may not be in their best interest.[2]

As an end goal, these practices intend to get consumers to purchase, or purchase more of, or continue to purchase, a product or service; to overspend on a purchase; or to divulge more personal data than desired, resulting in increased business revenue for the platforms.[3] These practices are particularly harmful as they tend to impact consumers cumulatively, and pose a real threat to children, first time users and individuals with limited digital literacy.

---

[1] Justin (Gus) Hurwitz, 'Designing a Pattern, Darkly' (2020) 22(1) North Carolina Journal of Law & Technology <https://ssrn.com/abstract=4583587> accessed 1 April 2026.

[2] Organisation for Economic Co-operation and Development, *Dark Commercial Patterns* (OECD 2022) <https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf> accessed 2 April 2026.

[3] ibid.

Dark pattern practices operate through subtle design choices that influence consumer behaviour without resulting in immediately recognisable harm. Remember coming across the following: "*Only 1 item left!*"; "*Are you sure you want to unsubscribe? You might regret this decision.*"; "*No thanks, I prefer to pay full price.*"; "*20 people are viewing this right now.*"; and "*Oh! The price just increased.*"? In essence, such practices qualify as dark patterns that impair consumer autonomy and transparency, thereby justifying regulatory intervention.

II. BEHAVIOURAL ECONOMICS

Behavioural economics provides an important framework for understanding and predicting human behaviour in digital markets.[4] The concept of 'choice architecture', which was developed by Richard Thaler and Cass Sunstein highlights that the way in which choices are presented can significantly influence consumer decision-making.[5] Similar to designing a physical environment, elements of a digital interface including layout and wording, tend to guide consumer reactions and outcomes.[6]

Within this framework, certain concepts are often used to analyse dark patterns and their effects on consumers. 'Nudging' refers to the use of human tendencies or cognitive biases to influence consumer behaviour towards outcomes intended to be 'welfare enhancing' and in their long term interest.[7] In contrast, 'sludging' refers to frictions which make it harder for individuals

[4] Michele Fang and Marcela Mattiuzzo, 'Online Choice Architecture and Behavioural Economics – The Role for Antitrust Law' (*Yale University, May* 2023) <https://som.yale.edu/sites/default/files/2023-05/TAP_Consumer_Protection_Paper_3.1.pdf> accessed 10 April 2026.
[5] ibid.
[6] ibid.
[7] Ryan Calo, 'Digital Market Manipulation' (2014) 82 The George Washington Law Review <https://ssrn.com/abstract=2309703> accessed 1 April 2026.

to undertake beneficial actions and 'dark nudges' describe design features that are intended to steer users towards decisions that may leave them worse-off.[8] While 'nudging' is premised on welfare enhancing architecture, the concept of 'sludging' and 'dark nudges' highlight the manner in which design elements can also be used to undermine consumer decision-making autonomy, and erode consumer trust, while benefiting the digital platform, and thus creating a necessity for stronger consumer protection safeguards.

Behavioural insights can also play a crucial role in strengthening the enforcement of consumer protection laws and informing policy design. They enable regulators to better identify misleading, unfair and deceptive business practices, which may not be immediately visible from a traditional legal perspective.

At the same time, businesses increasingly rely on data driven technologies including machine learning to predict human behaviour, patterns and habits and employ strategic practices such as personalised advertising. This creates significant information asymmetry, allowing businesses to target consumer's vulnerabilities and subtly influence their decision making.

Several behavioural biases are especially relevant in digital marketplaces. Consumers may continue using existing products or services despite better alternatives due to the endowment effect (overvaluing what they already possess), default bias (sticking to pre-selected options) and loss aversion (preferring to avoid losses rather than acquiring equivalent gains).[9] Platforms

[8] Stuart Mills and others, 'Dark patterns and sludge audits: an integrated approach' (2023) 10(1) Behavioural Public Policy <https://www.cambridge.org/core/journals/behavioural-public-policy/article/dark-patterns-and-sludge-audits-an-integrated approach/8675A269B8FE79D2ECE0A8952D182C0B> accessed 12 April 2026.

[9] Organisation for Economic Co-operation and Development, *Integrating Consumer Behaviour Insights in Competition Enforcement* (OECD 2022) <

can exploit these tendencies by designing user interfaces in a strategic manner, such as relying on default settings or displaying pre-ticked options.

Similarly, salience bias and framing effect may cause users to focus on the salient features of an offer, thereby impairing the consumer's ability to make decisions effectively.[10] Overconfidence and time inconsistency may also lead consumers to underestimate future costs and overestimate their own ability to manage such increased costs.[11] In addition, information overload arising from abundant options may overwhelm consumers and lead them to selecting the most visible or popular option, or lead to avoiding decision making, altogether.[12]

The strategic use of such biases by platforms may also distort competition by permitting businesses to capture consumer attention and drive sales through manipulative design, rather than through improvement in the quality of products or services. In some cases, platforms may adopt dark pattern practices simply to remain competitive in a market where such strategies are widespread.[13] While businesses may exploit such consumer tendencies for commercial gain, policy makers can also leverage these insights to develop a more effective regulatory framework.

III. INDIAN LEGAL FRAMEWORK

The Consumer Protection Act, 2019 (**'Act'**) (which came into force on 20 July 2020) was enacted to provide for protection, promotion and enforcement of rights of consumers, to ensure fair trade practices and to establish

http://www.oecd.org/daf/competition/integrating-consumer-behaviour-insights-in-competition-enforcement-2022.pdf> accessed 12 April 2026.

[10] ibid.

[11] ibid.

[12] ibid.

[13] ibid.

authorities for timely and effective administration and settlement of consumers' disputes and related matters. It has been formulated as a social benefit legislation to provide better protection to consumers from unfair and exploitative trade practices and to provide speedy, inexpensive and accessible remedy.[14]

The Central Consumer Protection Authority (**'CCPA'**), the primary regulatory authority under the Act, was established to regulate consumer rights violation matters including false and misleading advertisements, unfair trade practices and exploitation, which are adverse to consumers' interests.[15] The powers and functions of the CCPA include reviewing, enquiring and investigating matters (including taking suo moto actions) relating to violation of consumer rights, protecting consumers' interest, promoting awareness on consumer rights and issuing necessary guidelines, advisories and directions to prevent violation of consumers' interests and timely redressal of consumer complaints, including imposition of penalties.[16]

The present consumer protection regulatory framework is enforced through statutory provisions under the Act and through guidelines, directions and advisories issued by the CCPA.

A. Guidelines for Prevention and Regulation of Dark Patterns, 2023

The CCPA *via* a notification dated 30 November 2023 issued the Guidelines for Prevention and Regulation of Dark Patterns, 2023 ('**2023 Guidelines'**) under Section 18 of the Act, to prevent unfair trade practices and protect consumer's interest.[17] The 2023 Guidelines which are applicable

[14] Consumer Protection Act 2019.
[15] Consumer Protection Act 2019, s 10.
[16] Consumer Protection Act 2019, s 18.
[17] Guidelines for Prevention and Regulation of Dark Patterns 2023.

to all platforms systematically offering goods or services in India, advertisers, and sellers, prohibit all persons including platforms from engaging in any dark pattern practice.[18]

Under the 2023 Guidelines, dark patterns are defined as "*any practices or deceptive design pattern using user interface or user experience interactions on any platform that is designed to mislead or trick users to do something they originally did not intend or want to do, by subverting or impairing the consumer autonomy, decision making or choice, amounting to misleading advertisement or unfair trade practice or violation of consumer rights*."[19]

Dark patterns as defined under the 2023 Guidelines impose an additional condition for such practices to be classified as a dark pattern, namely that such practices or patterns must also amount to a misleading advertisement, or unfair trade practice, or violation of consumer rights.[20] The requirement that dark pattern practices satisfy the threshold of existing legal categories of 'misleading advertisement' or 'unfair trade practice' or 'violation of consumer rights' attempts to subsume such practices within traditional legal jurisprudence, rather than recognising them as an independent category of harm.

In terms of article 5 of the 2023 Guidelines, a person shall be considered to be engaging in a dark pattern practice if it engages in any practice specified in Annexure 1 (Specified Dark Patterns) of the guidelines.[21] Annexure 1 (Specified Dark Patterns) of the 2023 Guidelines contains an illustrative list of dark patterns ('**Specified Dark Patterns'**), which serves only as a guidance

[18] Guidelines for Prevention and Regulation of Dark Patterns 2023, art 3.
[19] Guidelines for Prevention and Regulation of Dark Patterns 2023, art 2(e).
[20] ibid.
[21] Guidelines for Prevention and Regulation of Dark Patterns 2023, art 5.

and may be interpreted differently basis different facts or conditions.[22] Any other dark patterns specified by the CCPA from time to time or otherwise will also be construed to be a Specified Dark Pattern.[23] While the illustrative list of dark patterns enables CCPA to capture new and emerging dark patterns and resolve ambiguity in favour of consumers, it also creates a gap in clarity for businesses regarding prohibited conduct and may also result in uneven enforcement.

The illustrative list of Specified Dark Patterns includes the following practices, which can broadly be grouped into three categories, i.e., manipulative design techniques, barriers to user autonomy and lack of transparency.

1. MANIPULATIVE DESIGN TECHNIQUES

These techniques introduce design elements in digital platforms that exploit human emotions, including fear, shame, ridicule, or guilt, which direct consumers to take such actions that they may originally not have intended to take, and which benefit the platforms by resulting in commercial gains.

(i) *False Urgency*: falsely creating a sense of urgency or scarcity, misleading user to take immediate action.[24]

(ii) *Confirm Shaming*: creating a sense of fear or shame or ridicule or guilt in the mind of the user, and nudging them to purchase a product or continue with a service.[25]

---

[22] ibid.
[23] Guidelines for Prevention and Regulation of Dark Patterns 2023, art 2(i).
[24] ibid.
[25] ibid.

2. BARRIERS TO USER AUTONOMY

These practices restrict, force, or create hurdles for users, preventing them from making an independent choice while using and undertaking transactions on digital platforms.

(i) *Basket Sneaking*: inclusion of additional products, services, or charity/ donation payments at the time of checkout, without the user's consent[26];

(ii) *Forced Action*: forcing a user into taking an action which would require the user to buy any additional goods or subscribe or sign up for an unrelated service or share personal information[27]; and

(iii) *Subscription Trap*: involves making the cancellation of a subscription impossible or a complex and lengthy process.[28]

3. LACK OF TRANSPARENCY

These techniques signal a lack of transparency in the manner in which business is conducted on digital platforms, where key terms such as pricing are not revealed upfront in a clear manner, or certain information is highlighted or masked, to benefit digital platforms.

(i) *Drip Pricing*: practices where elements of prices are not clearly revealed upfront[29];

(ii) *Disguised Advertisement*: posing and masking advertisements to trick customers into clicking on them.[30]

---

[26] ibid.
[27] ibid.
[28] ibid.
[29] ibid.
[30] ibid.

(iii)*Interface Interference*: highlighting specific information and obscuring other relevant information, to misdirect a user from a desired action.[31]

B. Advisory

Further to the 2023 Guidelines, the CCPA also issued an advisory on 5 June 2025, on a self-audit to be carried out by e-commerce platforms for detecting dark patterns on their platforms to create a fair, ethical, and consumer-centric digital ecosystem ('**Advisory'**). As per the Advisory, CCPA has advised all e-commerce platforms to take necessary steps to ensure that the platforms do not engage in such deceptive and unfair trade practices in the nature of dark patterns.[32]

The platforms were advised to conduct such self-audits within three months of the issue of the Advisory. In addition to the self-audits, the platforms have also been encouraged to issue self-declarations that the platform is not indulging in any dark patterns.[33] The Advisory is only in the nature of a recommendation, and there is no mandatory requirement for platforms to comply with the Advisory. Lack of a mandatory requirement to conduct self-audits weakens the regulatory framework being established against dark patterns, and results in uneven compliance, limits transparency and accountability and weakens enforcement.

---

[31] ibid.

[32] Central Consumer Protection Authority, *Advisory in terms of Consumer Protection Act, 2019 on Self Audit by E-Commerce Platforms for detecting the Dark Patterns on their platforms to create a fair, ethical, and consumer-centric digital ecosystem* CCPA-1/1/2023-CCPA (5 June 2025) <https://doca.gov.in/ccpa/checkuploaddocs.php?updocs=./uploads/1766468507Zepto_Final_order__1___1_.pdf&unique_id=> accessed 3 April 2026.

[33] ibid.

While the move is beneficial, it also lacks clarity in terms of the manner in which the audit must be conducted, the standards to be achieved by the platforms, requirement of an audit to be conducted by an expert third party, the manner of issue of declaration, its contents and frequency. Inclusion of these aspects alongside the current Advisory would ensure that the process is not treated as a mere formality, and a systematic approach is followed in conducting such an audit and issuing a self-declaration, thereby strengthening the intent of the 2023 Guidelines.

As on the current date, the CCPA has received self-audit declarations only from twenty-four organisations, which have been published on its website. In the declarations, the companies have confirmed their compliance with the 2023 Guidelines and the Advisory, and have stated that they have conducted self-audits or audits through independent auditors, to ensure adherence with the Advisory.[34]

The Advisory signals a preference for soft, self-regulatory compliance mechanisms rather than prescribing binding behavioural requirements. However, making such audits compulsory, especially through a prescribed methodology issued by the CCPA, would help ensure that the platforms proactively comply with the 2023 Guidelines and remain free of deceptive dark patterns. This move would also provide further clarity to the platforms on the parameters to be considered while conducting their self-audit, thereby creating uniformity and promptness in compliance across the digital ecosystem.

[34] Press Information Bureau, Government of India, '26 Leading E-Commerce Platforms Declare Compliance with Self-Audit to Eliminate Dark Patterns' (20 November 2025) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2191948&reg=3&lang=2> accessed 5 May 2026.

C. Misleading Advertisement and Unfair Trade Practice

Traditionally, 'misleading advertisement' under Section 2(28) of the Act has been understood to primarily cover advertising content.[35] However, with the increasing dependence on digital platforms, interface design practices such as drip pricing and false urgency may also *mislead consumers as to the nature, substance, quantity and quality of products and services*.

Further, 'unfair trade practice' under Section 2(47) of the Act is defined broadly to include "*trade practice which, for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive practice…*."[36] Such wide definition enables regulatory authorities to subsume dark patterns within the ambit of unfair trade practices, as was seen in the proceedings against BookMyShow.[37]

Unlike traditional misleading advertisements, which rely on false or incomplete representations, dark patterns operate through user interface design to influence consumer behaviour, without necessarily altering the substantive terms of the offer. This creates a regulatory challenge as consumers may be influenced through behavioural manipulation in the absence of explicit misrepresentations, thereby creating a need to revisit what may be considered 'deceptive' and 'misleading' under the Act, in the context of classifying such practices as misleading advertisements or unfair trade practices. Recent adjudicatory developments further indicate that regulatory authorities are increasingly interpreting these provisions to include design-

[35] Consumer Protection Act 2019, s 2(28).
[36] Consumer Protection Act 2019, s 2(47).
[37] Central Consumer Protection Authority, Order in the case of *Big Tree Entertainment Pvt Ltd* CCPA-2/20/2023-CCPA (11 February 2025) < https://doca.gov.in/ccpa/checkuploaddocs.php?updocs=./uploads/bookmyshow.pdf&unique_id=> accessed 10 April 2026.

based forms of manipulation, extending traditional consumer protection principles to digital markets.

D. E-commerce Rules

The Consumer Protection (E-Commerce) Rules, 2020 (‘**E-Commerce Rules’**) issued by the Indian government under the Act, are aimed at regulating goods and services bought or sold over digital networks and are applicable to all forms of unfair trade practices across e-commerce platforms. While the Act provides a broad framework for preventing unfair trade practices, the E-Commerce Rules give effect to these principles in the context of digital commerce, by imposing targeted obligations relating to transparency, disclosure, and consumer redressal.[38]

The E-Commerce Rules require clear and upfront disclosure of total price and e-commerce entities must also ensure that consumers are informed of the full consideration payable, including all mandatory charges such as delivery fees, handling charges, and taxes.[39] This requirement directly addresses concerns associated with drip pricing, where costs are revealed in an incremental manner during the purchase process, thereby distorting informed consumer choice.

The E-Commerce Rules also require platforms to explain the most significant parameters which are utilized to determine ranking of goods or sellers on the platform, along with relative importance of each such parameter.[40] This transparency requirement may act as a deterrent for platforms against manipulation of search results or rankings, thereby

[38] Consumer Protection (E-commerce) Rules 2020, rule 2.
[39] Consumer Protection (E-commerce) Rules 2020, rule 6(5)(b).
[40] Consumer Protection (E-commerce) Rules 2020, rule 5(3)(f).

indirectly discouraging unjustified preference being given to specific sellers or product listing. This provision addresses interface-driven influences on consumer attention and choice.

In addition, the E-Commerce Rules mandate the establishment of grievance redressal mechanisms, including the appointment of grievance officers and prescribed timelines for resolution of consumer complaints.[41] This provides consumers with a formal mechanism to challenge unfair or deceptive platform practices.

The E-Commerce Rules also require clear disclosure of return, refund, exchange, warranty, and cancellation policies.[42] This is particularly relevant in the context of subscription-based models, where cancellation mechanisms are often designed to be complex or non-transparent, thereby indirectly addressing subscription traps.

However, despite these safeguards, the E-Commerce Rules do not explicitly recognise or regulate behavioural manipulation through UX or UI design. Their focus remains primarily on transparency and procedural fairness rather than user interface architecture. As a result, practices such as confirm shaming, interface interference, and urgency-based manipulation are not directly addressed within the rules, even though they materially affect consumer autonomy. Accordingly, while the E-Commerce Rules strengthen the regulatory architecture for digital commerce, they do not adequately address the design-based nature of dark patterns, thereby reinforcing the need for a more explicit, principle-driven framework under the broader consumer protection regime.

[41] Consumer Protection (E-commerce) Rules 2020, rule 4(4) and 4(5).
[42] Consumer Protection (E-commerce) Rules 2020, rule 5(3)(c).

IV. US AND EU REGULATIONS

In the United States, Section 5 of the Federal Trade Commission Act, 1914 (‘**FTC Act’**) prohibits the use of unfair or deceptive practices in or affecting commerce and serves as the primary legislation against dark pattern practices.[43] The Federal Trade Commission (‘**FTC’**) has increasingly relied on this provision to challenge a wide range of manipulative dark pattern practices, including subscription traps, trick-questions, and pre-selected options, by bringing them within the ambit of “unfair’ or ‘deceptive’ conduct. FTC recognises that interface design by itself may be used as a vehicle to deceive consumers, even in the absence of explicit misrepresentations.[44]

This approach is reflected in several recent judicial case laws. In the case of *FTC vs Amazon.com, Inc*., the FTC has alleged that Amazon deployed “Iliad Flows”, a manipulative interface design which made it easy for consumers to subscribe to Amazon Prime, while making it difficult to cancel the subscription, due to the deliberately lengthy and time-consuming cancellation process.[45] Similarly, in the case *FTC vs Age of Learning, Inc.* **(‘ABC mouse’)**, it was found that the company failed to clearly disclose automatic renewal terms and made the cancellation difficult, resulting in a settlement through monitory relief of USD 10 million and the company was also required to change its subscription practices.[46] In another notable case

[43] Federal Trade Commission Act 1914, s 5.
[44] OECD, *Integrating Consumer Behaviour Insights in Competition Enforcement* (n 9).
[45] Federal Trade Commission, 'FTC Takes Action against Amazon for Enrolling Consumers in Amazon Prime without Consent and Sabotaging Their Attempts to Cancel' (25 June 2023) <https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their> accessed 18 June 2026.
[46] Federal Trade Commission, ‘Age of Learning, Inc’ (*ABCMouse*, 18 September 2021) <https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3186-age-learning-inc-abcmouse> accessed 15 April 2026.

involving *FTC vs. Epic Games, Inc*, the use of deceptive interface designs which led to unintended in-app purchases, particularly by children, highlighting the need to protect vulnerable stakeholders such as children.[47]

The FTC Act is supplemented by The Restore Online Shoppers' Confidence Act, 2010 (**'ROSCA'**), which specifically targets online subscription practices and online negative option billing features.[48] It mandates clear and conspicuous disclosure of all material terms, express informed consent prior to charging and a simple and accessible cancellation mechanism to stop recurring charges.[49] FTC has specifically invoked ROSCA in conjunction with Section 5 of the FTC Act to address subscription based dark pattern practices.

At the state level, the California Privacy Rights Act, effective 1 January 2023 ('**CPRA'**) which amended the California Consumer Privacy Act 2018 is particularly significant and is widely recognised as the first legislation to explicitly define and regulate dark patterns. The CPRA provides that user consent obtained from employing dark patterns does not constitute as valid consent. The CPRA defines dark patterns as "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice" and also prescribes illustrative examples to identify non-compliant interface designs.[50] The CPRA adopts an effects-based approach, where the focus in not on the intent of the business, but on whether the design materially undermines the user's ability to make a

[47] Federal Trade Commission, 'Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges' (19 December 2022) <https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations > accessed 15 April 2026
[48] Restore Online Shoppers' Confidence Act 2010.
[49] Restore Online Shoppers' Confidence Act 2010, ss 3-4.
[50] California Consumer Privacy Act 2018.

free and informed decision. This represents an important shift towards recognising interface design as the subject of regulatory scrutiny.

The U.S. framework reflects a hybrid approach, where broad, principles-based prohibitions under the FTC Act are combined with targeted statutory measures such as under the ROSCA and state-level privacy laws, however, the structure's consequences are double edge. The enforcement of these regulations remains largely reactive in nature, producing no clear ex ante standards and leaving platforms unable to determine in advance which design choices attract liability. However, the recent developments indicate an increasing trend to examine digital interface design as a tool of consumer deception and manipulation, gradually moving towards a design-based regulatory approach. While the Central and the State laws together create a stronger framework for consumer protection, it also creates regulatory inconsistencies and ambiguities across jurisdictions.

The European Union regulates dark pattern practices by adopting a multi-layered and cross sectoral approach, through consumer protection, data protection and regulation of digital markets.

The Unfair Commercial Practices Directive ('**Directive'**) which lies at the core of EU consumer protection laws, prohibits misleading and aggressive commercial practices and includes a limited 'blacklist' of practices which are deemed unfair in all circumstances. Although the Directive does not expressly refer to dark patterns, its broad scope enables regulators to address several such practices within the existing categories of deception and coercion.[51]

[51] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices [2005] OJ L149/22.

However, its framework remains largely effects-based and does not fully capture the design-oriented nature of dark patterns.

The General Data Protection Regulation complements this by addressing manipulative design practices in the context of personal data processing. Its provisions on consent, transparency, purpose limitation, and privacy by design imposes substantive obligations on platforms to ensure that user consent is freely given, is informed, and is unambiguous.[52] The European Data Protection Board's Guidelines on Deceptive Design Patterns in Social Media Platform Interface further develops this approach by identifying categories of 'deceptive design patterns', with a particular focus on social media interfaces.[53]

Further, the Digital Services Act ('**DSA'**) introduces a direct prohibition on deceptive or manipulative interface design. It provides that online platforms must not design or operate interfaces in a manner that deceives or materially distorts users' ability to make free and informed decisions.[54] This provision targets practices such as confirm-shaming, interface interference, and making cancellation processes more complex than subscription. Additionally, the act imposes systemic risk assessment obligations on very large online platforms, including risks arising from interface design.[55]

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.
[53] European Data Protection Board, *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: how to recognise and avoid them* (14 February 2023) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en> accessed 6 April 2026.
[54] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2022] OJ L277/1.
[55] ibid.

The Digital Markets Act (**'DMA'**) includes provisions preventing designated gatekeepers from deploying manipulative design techniques to circumvent regulatory obligations[56] and the Artificial Intelligence Act prohibits certain AI systems that employ subliminal or manipulative techniques capable of materially distorting user behaviour.[57]

Enforcement within the EU is decentralised, involving the European Commission (particularly under the DSA), national data protection authorities under the GDPR, and national consumer protection authorities under the Directive. Notable enforcement actions such as significant fines imposed on major technology platforms for manipulative cookie consent mechanisms demonstrate an increasing willingness to scrutinise interface design practices.[58]

The EU framework is often criticised for its fragmentation, as different legislations address dark patterns through distinct definitions, thresholds, and enforcement mechanisms. This is further reinforced by the interaction between the DSA and the Directive, as DSA excludes practices covered under the Directive, meaning that many business-to-consumer interface manipulation practices are primarily assessed under the Directive rather than the DSA, creating overlap and uncertainty in applicable standards and enforcement.[59] The European Commission has initiated steps toward a more

[56] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L265/1.
[57] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L1689/1.
[58] CNIL (France), 'Cookies and advertisements inserted between emails: Google fined 325 million euros by the CNIL' (3 September 2025) <https://www.cnil.fr/en/cookies-cnil-fines-google-and-facebook-non-compliance-consent-rules> accessed 7 April 2026.
[59] Unfair Commercial Practices Directive 2005/29/EC (n 51).

harmonised approach, including consultations on a proposed Digital Fairness Act, which is expected to introduce a more unified and coherent regulatory framework.[60]

Taken together, the EU approach reflects a progressively evolving model that moves beyond a purely harm-based analysis towards recognising interface design itself as a site of regulatory concern. However, the absence of a single, consolidated framework continues to pose challenges in ensuring consistency and clarity in enforcement.

The U.S. model is ill-suited to jurisdictions such as India where consumer litigation infrastructure remains underdeveloped. India's framework, operating through the 2023 guidelines and proactive CCPA-led enforcement such as mandatory self-audits, is closer to the EU model than the U.S. model. Both the EU and Indian frameworks prefer regulatory action over consumer litigation, and India is best placed to develop its framework along similar lines as the EU.

V. WIDENED SCOPE OF DARK PATTERNS ENFORCEMENT UNDER THE ACT

Indian courts have in the past consistently focused on the overall impression created on a reasonable consumer while adjudicating matters, recognising that consumers may be deceived by the manner in which goods or services are presented.[61]

---

[60] Commission, 'Review of EU consumer law' (4 October 2022) < https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en> accessed 5 April 2026.

[61] *Colgate Palmolive Company v Anchor Health and Beauty Care Pvt Ltd* [2003] 108 DLT 51 (Delhi HC) 68-69.

The Indian courts have been prompt in identifying dark pattern practices and applying the 2023 Guidelines in relevant cases. The State Consumer Disputes Redressal Commission, U.T. Chandigarh ('**Chandigarh Commission'**) in its order dated 28 December 2023, recognised that forcing a consumer to share his personal details without his consent is a dark pattern of 'forced action' under the 2023 Guidelines.[62] Further, the Chandigarh Commission, in its order dated 20 February 2024, categorised the practice of issuing two separate bills for a single transaction on the pretext of an offer handling fee as a dark pattern under the 2023 Guidelines and unfair trade practice under the Act.[63] Also, the Chandigarh Commission in its order dated 12 March 2024, held that the supply of a different, lower quality brand than the one advertised on the digital platform constitutes as a dark pattern practice, and further categorised such conduct as a deceptive, unfair and restrictive trade practice.[64]

While these cases illustrate that the Indian courts have begun to engage with and identify dark pattern practices, they do not yet articulate any coherent set of guiding principles or framework that may be applied systematically in the future. In the absence of such structured principles, enforcement of the 2023 Guidelines remains largely fact specific and reactive, and may result in limiting the evolution of jurisprudence in this area. This also creates an uncertainty regarding permissible and non-permissible design

[62] *Pankaj Chandgothia v The Coffee Bean & Tea Leaf*, State Consumer Disputes Redressal Commission, UT Chandigarh, Complaint Case No 99 of 2023 (28 December 2023) [14].
[63] *Mr Ashwani Chawla v Flipkart Internet Pvt Ltd*, State Consumer Disputes Redressal Commission, UT Chandigarh, Consumer Complaint No CC/113/2023 (20 February 2024) [17].
[64] *Jatin Bansal v M/s Amazon Reseller Services Pvt Ltd and Others State Consumer Disputes Redressal Commission* (UT Chandigarh) Appeal No 192 of 2023 (12 March 2024) [23].

practices, which may result in uneven enforcement under the consumer protection framework.

The CCPA has also adopted a proactive enforcement approach, including initiating suo moto proceedings further to its routine investigation of e-commerce platforms regarding prevalence of dark pattern practices. CCPA has taken suo moto actions against Zepto Marketplace Pvt. Ltd. ('**Zepto'**), Axelia Solutions Pvt. Ltd. ('**PharmEasy'**), Big Tree Entertainment Private Limited ('**BookMyShow'**) and InterGlobe Aviation Ltd. ('**Indigo Airlines'**).

In the case involving Zepto, CCPA concluded that Zepto was involved in the use of dark pattern of drip pricing (where the final payable amount is significantly higher than the initial price displayed to the consumer) and basket sneaking (which involved pre-selection or automatic addition of paid products or services at checkout, without the consent of the consumer). CCPA was of the opinion that such practices resulted in violations of Sections 2(28) and 2(47) of the Act read with the 2023 Guidelines, falling within the ambit of existing doctrines of misleading advertisements and unfair trade practices. These practices led to misleading representation of the final price and induced consumers to pay charges they did not knowingly agree to, thus undermining consumer autonomy.[65]

With respect to PharmEasy, which had previously conducted an internal self-audit and had come to the conclusion that its practices were in compliance with the 2023 Guidelines, similar to the above case, it was observed that PharmEasy was engaged in the practice of 'basket sneaking'.[66]

---

[65] Central Consumer Protection Authority, Order in the case of *Zepto Marketplace Pvt Ltd* Case No Z-10/1/2025-O/O US(CCPA) (4 December 2025).

[66] Central Consumer Protection Authority, *Order in the case of Axelia Solutions Pvt. Ltd.* CCPA-2/20/2024-CCPA (20 November 2025).

These cases demonstrate that dark patterns are being subsumed within the scope of existing doctrines of misleading advertisement and unfair trade practices. This reflects a judicial tendency to interpret traditional consumer protection doctrines in an expansive manner, to accommodate emerging forms of digital manipulation, deception and coercion. However, it also raises questions regarding dark patterns as an independent regulatory category.

Further, in the inquiry involving BookMyShow, CCPA as part of its preliminary enquiry stated that the practice of basket sneaking includes not only goods or services, but also extends to charitable contributions.[67] This case illustrates that the scope of scrutiny while investigating dark patterns is not strictly confined to commercial transactions or profit-driven conduct of platforms, but also extends to non-commercial elements which are integrated into design architecture. This showcases the broader interpretive approach adopted by judicial authorities, wherein the focus is on the design element and its impact on the consumer, rather than the underlying commercial nature of such activity.

In the suo moto case involving Indigo Airlines, CCPA in its order stated that during the web check-in process, Indigo Airlines does not inform the consumers that they can complete the check-in process without choosing a preferred seat, in a distinct, clear and unambiguous manner. CCPA instructed Indigo Airlines to examine the feasibility of introducing a distinct, clear and unambiguous message to the consumers.[68]

[67]Central Consumer Protection Authority, *Order in the case of Big Tree Entertainment Pvt. Ltd.* CCPA-2/20/2023-CCPA (11 February 2025).
[68] Central Consumer Protection Authority, *Order in the case of InterGlobe Aviation Ltd.* CCPA-2/10/2024-CCPA (19 June 2024).

The CCPA continues to adopt the consumer perception based approach developed by Indian courts in its suo moto orders, extending its application to digital platform designs. It is actively enforcing the 2023 Guidelines through suo moto investigations across digital platforms and industries. Notably, the CCPA's approach also reflects a shift towards identifying deficiencies in the design architecture of platforms and its role in steering consumer behaviour, rather than focusing solely on a pre-dominantly effect-based enforcement approach.

VI. LIMITS OF HARM-CENTRIC APPROACHES IN BEHAVIOURAL DESIGN

There are certain limitations to the present harm-centric approach when applied to digital markets. Such an approach is premised on demonstration of consumer harm, typically in the form of economic loss or misleading representation. However, dark patterns operate in a significantly different manner, whereby they influence the process of decision-making itself.

Firstly, the impact of dark pattern practices is often cumulative in nature, in that it collectively impacts user behaviour over time, and may not be immediately or easily identifiable. It may not result in a single, identifiable instance of harm. Further, repeated exposure to such practices over time gradually erodes consumers' capacity for independent decision-making.

At times, dark patterns are subtle in nature and structurally invisible within the design architecture of platforms. As dark patterns influence the decision-making process of the consumer, rather than directly resulting in a tangible loss or injury, the identification and assessment of harm caused to the consumer may be subject to interpretation. In such a case, it becomes imperative to question whether the consumer would have acted differently in

the absence of design manipulations, making it difficult to establish clear regulatory thresholds.

Additionally, relying on a harm-based approach may allow such practices to persist until regulatory intervention, thereby delaying their identification and enforcement of applicable regulations. Such a reactive enforcement framework allows manipulative practices to persist unchecked for significant periods of time.

It is also quite challenging for authorities to regulate such practices, while striking an appropriate balance between consumer protection and the compliance burden on business, in order to avoid over-regulation. Absence of clear, enforceable indicators of harm, may result in under-enforcement. Conversely, overly broad interpretations of harm may create disproportionate obligations on businesses, resulting in over-regulation.

In addition, a consumer with limited information on consumer rights may not even be aware of an enforcement mechanism against dark patterns. While he/she may reprimand to another consumer or a third person, they may refrain from approaching the authorities in light of the effort to be put in and lack of a prompt resolution.

The above limitations indicate that a harm-centric framework is insufficient to address dark pattern practices, due to the unique manner in which they influence consumer behaviour. In light of the above regulatory challenges, a shift from a harm-centric approach towards regulating user interfaces becomes necessary. Such a shift would be more effective in addressing dark patterns, as it would address the issue proactively at its source, at the stage of development of UX or UI design elements, rather than regulating outcomes once consumer harm has already been caused.

VII. RECOMMENDATIONS

While the current framework prescribes guiding principles for the e-commerce/digital platforms, it lacks a clear and definite set of regulations governing platform design, and accordingly, may not stand the test of time (in light of the evolving technological advancements).

It is the authors' recommendation that the following key principles may be added, to complement and strengthen the current framework. Inclusion of these principles to the current framework would mandate that consumer autonomy is embedded within platform designs, rather than relying only on reactive enforcement measures.

(i) Platforms should ensure that users are able to choose between different options with equal ease. Both "yes" and "no", or "accept" and "reject" options should be presented in the same manner, with equal visibility and without any technological impediments (such as extra clicks for a particular choice). Further, any default setting of the platform should not be structured in a manner that advantages the platform over the user.

(ii) Platforms should enable users to exit, unsubscribe, cancel or withdraw consent with the same ease as entering, subscribing, or providing consent. Consent for all user action should be obtained through clear, affirmative user action, and should not be inferred from inactivity, pre-selections, or bundled acceptance.

(iii) Information and instructions should be presented in a clear, simple and unambiguous manner, with all key terms (such as pricing, subscription terms, auto-renewal, cancellation conditions) disclosed upfront, and supported with clear reminders. The total cost payable by the consumer

should also be clearly disclosed upfront to prevent the addition of hidden costs at the final stage.

(iv) Platform design should not emotionally or psychologically manipulate users by exploiting feelings of guilt, shame, or fear including through urgency cues such as low stock indicators or countdown timers.

(v) Advertised or sponsored products and services should be clearly distinguishable from products and services organically offered on the platform.

(vi) Data collection practices of the platforms should be aligned with applicable data protection laws, ensuring that personal data is collected only when necessary and used strictly for the stated purpose.

(vii) Platforms should be able to conduct regular UI and UX design audits to guarantee that the platform does not enable any dark patterns.

Adopting such principles would ensure a proactive stance against dark patterns, thereby reducing ambiguity for businesses by creating clear obligations, placing a higher responsibility on businesses, and would aid compliance and enforceability. The Consumer Protection Act 2019 and the CCPA's Guidelines on Dark Patterns 2023 prohibit specific manipulative practices, but neither imposes affirmative design obligations on platforms. This matters because the current model requires the CCPA to demonstrate deceptive intent on the facts of each complaint, a demanding evidentiary threshold.

Symmetry requirements under Recommendations (i) and (ii) would replace that with an objective, auditable standard. Recommendation (iii) addresses drip pricing more directly than the existing framework does. Recommendations (vi) and (vii) raise a further issue of interface designs that nudge users toward broader data permissions through asymmetric choice

architecture may simultaneously constitute a dark pattern and a consent violation under the Digital Personal Data Protection Act 2023.

In addition, the implementation of UX and UI audits introduces certain practical constraints, given their highly technical nature. Such audits require expertise in behavioural sciences, design architecture and legal analysis. Regulatory authorities such as the CCPA, in their present capacity, may face a limitation in undertaking detailed technical evaluation of interface designs, which may impact the effectiveness of enforcement measures. This challenge could be addressed by involving individuals with expertise in behavioural designs and by constituting specialised technical advisory committees, to assist in evaluation of design interfaces.

While robust regulatory oversight and platform accountability play a central role in addressing dark patterns, enhancing consumer awareness may also serve a supplementary role in addressing the issue. Consumers should be encouraged to critically engage with digital interfaces. Increased digital literacy along with accessible grievance redressal mechanisms would enable users to better identify and report potentially manipulative practices. Additionally, while the CCPA has introduced e-Jagriti and National Consumer Helpline services for the consumers to file complaints online, in light of the lack of general awareness about such facilities, CCPA may consider organizing periodic education camps (through offline and online sources) to ameliorate the enforcement system.

Such improvements will not only strengthen the existence of consumer rights, but will also enhance the consumer experience on such platforms, thereby promoting a more transparent and trustworthy online commercial environment and fostering greater consumer engagement.

VIII. CONCLUSION

The current Indian statutory framework governing dark pattern practices continues to rely on a harm-centric model, even as recent regulatory actions indicate an emerging shift towards recognising design architecture itself as a source of consumer harm.

Dark patterns primarily operate through interface design choices that influence consumer behaviour and undermine consumer autonomy, often prior to recognition of any legally actionable harm. As a result, reactive enforcement by itself is insufficient to address the issue of dark patterns at its core.

In order to bridge this gap, Indian regulations must move from reactive adjudication and towards a principle-driven governance framework. This would require formulation of clear design standards that integrate consumer autonomy, transparency and informed consent within the design architecture. Further, the audit requirement under the Advisory should also be made mandatory and should be supported by a standardised methodology prescribed by the CCPA, to ensure continuous, effective compliance.