# POLICING THE INVISIBLE: DARK PATTERNS, CYBER FRAUD AND THE LEGAL CHALLENGES OF DECEPTIVE UX DESIGN IN INDIA AND BEYOND

Pragati Bajpai, Research Scholar, Faculty of Law, University of Lucknow[1]

Utkarsha Singh, Research Scholar, Dr. Ram Manohar Lohiya National Law University, Lucknow[2]

## ABSTRACT

The rapid expansion of digital markets in India has concurrently exposed users to subtle and manipulative digital design strategies known as "dark patterns." These patterns, often embedded within user interfaces, exploit cognitive biases to mislead, coerce, or deceive individuals into unintended actions, such as giving consent, sharing personal data, or spending money inadvertently. While jurisdictions such as the European Union and the United States have adopted robust regulatory stances, India currently lacks an explicit legal framework to comprehensively address this pervasive form of cyber manipulation.

This paper posits that dark patterns are not merely facilitators of cyber fraud; rather, in their deliberate subversion of user autonomy and informed consent, they constitute a unique and insidious form of deceptive UX Design that fundamentally blurs the lines with fraud itself. The analysis delves into the conceptual, ethical, and legal underpinnings of dark patterns, critically examining how existing Indian laws address, or fail to address, these practices. A comparative analysis of international regulatory responses provides valuable lessons for India.

Drawing upon real-world examples, interdisciplinary research, and legal scholarship, this paper asserts the urgent necessity for India to formally recognize dark patterns as a distinct category of cyber fraud and consumer harm. It concludes by proposing clear legislative and regulatory strategies to effectively combat this evolving threat to digital consumer welfare.

**Keywords:** Dark patterns, cognitive-biases, autonomy, deceptive, UX Design

[1] The author is a research scholar at Faculty of Law, University of Lucknow

[2] The co-author is research scholar at Dr. Ram Manohar Lohiya National Law University, Lucknow

## 1. Introduction: The Pervasive Threat of Deceptive UX in India's Digital Landscape

*"Those who won our independence believed that the final end of the state was to make men free to develop their faculties, and that in its government the deliberative forces should prevail over the arbitrary. They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty."*

**- Justice Brandeis**[3]

India's digital landscape has undergone a remarkable transformation in recent years, marked by an exponential surge in internet usage and a corresponding increase in online commercial transactions and reliance on digital platforms. This profound digital shift, while fostering unprecedented connectivity and economic growth, has simultaneously given rise to sophisticated deceptive design practices, colloquially termed "dark patterns." These patterns, though often subtle in their manifestation, are meticulously crafted to manipulate users into making decisions they might not have otherwise intended, encompassing actions such as sharing personal data, subscribing to paid services, or making unintended purchases.

Unlike more other scams or traditional forms of cyber fraud, dark patterns operate through the very architecture and design of user interfaces. Their deceptive power lies in their inherent subtlety, which allows them to gradually effect user autonomy and blur the thin line distinction between legitimate persuasive design and outright digital coercion.[4] These patterns are engineered to exploit cognitive biases, misleading, coercing, or deceiving users into giving consent, sharing personal data, or spending money unintentionally. They are defined as "deceptive tools" or "user interfaces carefully crafted to trick users into doing things". These designs "prey on human psychology" and are "designed to gear users into performing certain actions on the interface" without the user's knowledge.[5] Any application using dark patterns must first address users' fears and misunderstandings.

Despite their pervasive nature, India currently lacks a proper legal framework to effectively tackle this form of cyber manipulation. While existing statutes, such as the Information

[3] Whitney v. California, 71 L. Ed. 1095
[4] Arunesh Mathur, Jonathan Mayer and Mihir Kshirsagar, 'What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods' (*CHI Conference on Human Factors in Computing Systems 2021*) https://doi.org accessed on 07 June 2025.
[5] Anika Atluri, 'The Psychological Effects of Dark Patterns' (Research Archive of Rising Scholars, 2023) https://research-archive.org/index.php/rars/preprint/download/263/514/351 accessed on 08 June 2025.

Technology Act, 2000[6] (IT Act), and the Consumer Protection Act, 2019[7] (CPA), provide foundational legal frameworks, they prove insufficient in explicitly addressing the complexities and nuances of dark patterns. These designs exploit legal loopholes and violate the fundamental right to informed consent, thereby casting doubt on the authenticity of digital consumer freedom. This situation necessitates a redefinition of the scope of "cyber fraud" within legal frameworks, moving beyond policing individual fraudulent transactions or overt deceptive messages to regulating the fundamental design principles and user experience architecture of digital platforms.

## 2. Defining Dark Patterns and Their Manipulative Typology

Dark patterns are precisely defined as user interface designs intentionally crafted to manipulate users into taking actions they would not otherwise undertake. The term was originally coined by user experience designer Harry Brignull on July 28, 2010, coinciding with the launch of darkpatterns.org, a "pattern library with the specific goal of naming and shaming deceptive user interfaces".[8]

Brignull, who possesses a PhD in cognitive science, further elaborated on this concept in his 2023 book, "Deceptive Patterns"[9]. Broadly, "dark patterns" consist of design practices used to deceive, steer, or manipulate user behavior, primarily to serve the interests and financial objectives of an online service, often to the detriment of users or contrary to their original intent. A core characteristic of dark patterns is their exploitation of human psychology and inherent cognitive vulnerabilities. They are meticulously engineered to leverage various cognitive biases, such as the default effect, urgency bias, and loss aversion, thereby making choices that primarily benefit the platform or designer appear inevitable, desirable, or even the only logical option. The effectiveness of dark patterns lies precisely in their unpredictable and the unconscious nature of the manipulation.[10]

Users are frequently unaware that they have been manipulated, often attributing their actions to

[6] Information Technology Act 2000
[7] Consumer Protection Act 2019
[8] Harry Brignull, '*Dark Patterns: Deception vs. Honesty in UI Design*' (1 November 2011) https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design/ accessed 18 June 2025.
[9] Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023)
[10] A Mathur, J Mayer and M Kshirsagar, '*What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods'* (2021) CHI Conference on Human Factors in Computing Systems https://doi.org/10.1145/3411764.3445610 accessed 16 June 2025

their own choices rather than to external design coercion. This poses a huge challenge for traditional legal remedies, which often rely on proving misrepresentation or conscious intent to defraud. It necessitates a shift towards design-centric regulation that can infer manipulative intent from the demonstrable effect of the design on user behavior, rather than requiring subjective proof of a designer's malicious intent.

The specific cognitive biases that dark patterns exploit include:

- **Framing Effects:** Presenting choices in a manner that influences the user's decision, even if the underlying options are identical. For example, "confirm shaming" frames declining an offer in a way that makes it seem undesirable or morally wrong, convincing users towards accepting it.

- **Sunk Cost Fallacy:** Manipulating users into continuing with a service or purchase because they have already invested time or effort, even when it is not in their best interest.

- **Anchoring:** Setting an initial "anchor," such as a pre-selected default option, that influences subsequent decisions, making that choice appear natural or expected.

- **Hidden Information/Aesthetic Manipulation:** Obscuring important information, such as costs or terms, visually or by placing it in a less prominent location, making it difficult for users to notice or comprehend. This exploits the bias where users may not diligently seek out all information.

- **Obstruction:** Intentionally making it difficult for users to express their actual preferences by requiring them to navigate unnecessary hurdles to decline a service or cancel a subscription. This exploits user inertia and the desire to avoid effort.

- **Trick Questions:** Using intentionally confusing prompts that make it challenging for users to understand how to achieve their desired objective, leading them to make unintended choices.

- **Preselection/Default Bias:** Firms pre-selecting options that benefit them, with users often sticking to these defaults due to inertia or the assumption that the default is the recommended choice.

- **False/Misleading Messages (Social Proof, Scarcity, Urgency):** Presenting false or misleading information about others' actions (e.g., "1,657 other participants have accepted this") to create a bandwagon effect or fabricating a sense of limited quantities or time-limited offers (e.g., "only three trial memberships left") to pressure users into impulsive decisions.

The deployment of dark patterns is not accidental; it is a deliberate, data-driven strategy systematically made and implemented for corporate profit, often directly at the expense of user well-being, autonomy, and informed choice.[11] These designs are intended to "manipulate user behavior to align with the interests and goals of the business" and are "highly effective at influencing consumer behavior".[12] They are used for "optimizing online experiences to favor stakeholder requirements" where "user value is supplanted in favor of shareholder value." [13]

The various types of dark patterns, categorized by their manipulative tactics, are detailed in the table below:

**Table 1: Typology of Dark Patterns and Their Manipulative Tactics**

| Dark Pattern Type | Description | Manipulative Tactic/Cognitive Bias Exploited |
|---|---|---|
| **Bait and Switch** | Advertising one product or outcome but delivering another. | Misdirection, expectation violation |
| **Forced Continuity** | Tricking users into paid subscriptions after free trials, with intentionally difficult cancellation processes. | Inertia, cognitive load, hidden information |

[11] 'What are Dark Patterns?', Koley Jessen, https://www.koleyjessen.com/insights/publications/what-are-dark-patterns accessed on 14 June 2025.

[12] CM Gray and others, 'The Dark (Patterns) Side of UX Design' (2018) *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* https://doi.org/10.1145/3173574.3174108 accessed 5 June 2025

[13] Wang, R., Bush-Evans, R., Arden-Close, E., Bolat, E., McAlaney, J., Hodge, S., Thomas, S., & Phalp, K. (2022). Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications. *Computers in Human Behavior*, *139*, 107545. https://doi.org/10.1016/j.chb.2022.107545

| | | |
|---|---|---|
| **Roach Motel** | Designing a service to be easy to enter but intentionally hard to exit. | Inertia, cognitive load, obstruction |
| **Hidden Costs / Drip** | Charges are only | Information asymmetry |
| **Pricing** | Revealed or added at the very last step of a transaction, misleading consumers about the true cost | Cognitive load, default effect |
| **Confirmshaming** | Employing guilt-based prompts or language that makes opting out feel socially undesirable or morally wrong | Framing effects, social pressure, guilt |
| **Misdirection** | Drawing a user's attention to one element to distract them from another, often more critical, piece of information or option. | Attention bias, visual hierarchy manipulation |
| **Privacy Zuckering** | A practice that tricks users into sharing more personal information than they intended. | Information asymmetry, cognitive load, default bias |
| **Sneak into Basket** | Automatically adding extra items to a user's shopping cart without their explicit consent or clear notification. | Default effect, inertia, hidden information |
| **Urgency/Scarcity** | Creating a false sense of urgency or limited availability to pressure users into making quick, impulsive purchases. | Fear of Missing Out (FOMO), cognitive overload |
| **Disguised Ads** | Presenting advertisements in a way that deceives users into believing they are genuine content, such as news, articles or user reviews. | Cognitive bias, trust exploitation |
| **Nagging** | Repeatedly interrupting the user with persistent prompts, pop-ups, or requests, often without their consent, even after they have declined multiple times. | Persistence, annoyance, cognitive load |

| | | |
|---|---|---|
| **Preselection** | Automatically opting users into certain settings or services without their explicit consent, typically by pre-ticking checkboxes. | Default bias, inertia |
| **Forced Actions/Cookie Walls** | Preventing users from accessing content or services unless they agree to certain terms or perform unrelated actions, such as accepting all cookies. | Coercion, obstruction, limited choice |
| **Interface Interference** | Designing the user interface in a way that visually prioritizes certain actions or conceals others to subtly manipulate user decisions. | Visual hierarchy manipulation, attention bias |
| **Confusing Wording** | Using ambiguous or intentionally confusing language, such as double negatives, to trick users into formally accepting an option they believe has the opposite meaning. | Cognitive load, linguistic manipulation |

## 3. Dark Patterns as Digital Deception: A Conceptual Link to Cyber Fraud

The central argument of this report posits that dark patterns, through their deliberate subversion of user autonomy and informed consent, constitute a unique form of digital deception that blurs the lines with traditional notions of fraud.

It is important to note that the intent to deceive is not always strictly required; rather, the "overall net impression" of the communication being misleading is often sufficient for a finding of deception.[14] This reinterpretation could significantly lower the evidentiary bar for enforcement, making it substantially easier to hold digital platforms accountable for manipulative UI/UX designs.

In numerous severe instances, dark patterns themselves can directly constitute elements of "deceit" or "dishonest inducement," which are core components of the definition of "cheating" as outlined under Section 318, Bhartiya Nyaya Sanhita 2023 (BNS)[15]. A critical "Explanation"

[14] Kerstin Bongard-Blanchy, *et al.* (2021) 'I am definitely manipulated, even when I am aware of it. it's ridiculous! - dark patterns from the end-user perspective', *Designing Interactive Systems Conference 2021*, pp. 763–776 http://dx.doi.org/10.1145/3461778.3462086 accessed on 17 June 2025.
[15] Bhartiya Nyaya Sanhita 2023, Section 318.

within Section 318 clarifies that "A dishonest concealment of facts is a deception within the meaning of this section". This provision is particularly relevant to dark patterns, which frequently rely on obscuring or hiding material information, such as hidden costs or opt-out options, or coercing users into specific actions through manipulative design. This directly maps to how many dark patterns operate, providing a strong conceptual overlap. In *Reserve Bank of India v. Secure Value India Ltd*[16]. the Bombay High Court emphasized that financial intermediaries must adopt user-friendly and fraud-resistant designs

The critical linkage between dark patterns and broader cyber fraud lies in the manner these deceptive designs facilitate the harvesting of user data, enable "consent fatigue," and bypass informed decision-making processes, thereby creating ripe conditions for a spectrum of subsequent online frauds. For instance, Section 66C of the IT Act, 2000[17], specifically penalizes identity theft, defined as fraudulently or dishonestly making use of another person's electronic signature, password, or any other unique identification feature. Similarly, Section 66D of the IT Act, 2000[18], penalizes cheating by personation by using computer resources, which involves a person assuming a fake identity with a mala fide intention to deceive another. While there isn't a direct one-to-one mapping between a dark pattern and these specific crimes, dark patterns such as "Privacy Zuckering" directly lead to users unknowingly sharing more personal data than they intended or consented to. This illicitly obtained data can then be exploited as the raw material for subsequent identity theft, impersonation, or other forms of cyber fraud.

This establishes a critical causal chain: deceptive UI/UX design (dark patterns) leads to vitiated consent for data sharing, which in turn leads to unauthorized or unintentional data harvesting, ultimately increasing the risk and direct facilitation of identity theft and other cybercrimes.[19] Consequently, regulating dark patterns at the fundamental design stage could serve as a powerful preventative measure against a wider array of cyber frauds, effectively tackling the problem at its root rather than merely addressing its effect.

A particularly prevalent tactic in India, as highlighted by various reports, is the "subscription trap". This involves deceptive billing practices that lead to unauthorized payments, especially affecting users in Tier-2 and Tier-3 cities who often have limited digital literacy and are more

[16] Reserve Bank of India v Secure Value India Ltd (2020) SCC OnLine Bom 155
[17] The Information Technology Act, 2000, Section 66C
[18] The Information Technology Act, 2000, Section 66D.
[19] Arun Prabhu and Nivedita S, 'Digital Dark Patterns in India: A Regulatory Gap?' (2022) 5 NUJS L Rev 33

vulnerable to such opaque cancellation procedures. Beyond financial detriment, users experience emotional tolls such as frustration, annoyance, and a significant fall of trust in online platforms.

Dark patterns also induce a "Fear of Missing Out" (FOMO) and a feeling of being trapped or lacking genuine choice, leading to rushed and often regrettable decisions.[20] This is not merely about isolated instances of hidden fees or difficult cancellations; it represents a systemic problem where certain business models are built upon exploiting user and designing intentionally cumbersome cancellation processes.[21] The volume of complaints on various platforms indicates that such incidents are not rare or isolated, suggesting that regulatory efforts must be made addressing individual consumer complaints and instead focus on systemic audits of business models and design practices, especially within high-volume, recurring payment sectors.[22] This also underscores the urgent need for proactive regulatory intervention rather than a reactive, complaint-driven enforcement approach, given the huge scale of potential harm and the specific vulnerability of certain demographic segments in India.

## 4. India's Legal Framework: A Critical Assessment of Current Provisions

India's legal framework for regulating dark patterns is fragmented and often indirect. While existing statutes touch upon cybercrime, consumer protection, and data privacy, none explicitly define or directly target the nuances of manipulative UX design. In *Punjab National Bank v. Leader Tour & Travels*[23] the Delhi High Court held the bank liable for failing to prevent a phishing fraud. This judgment, while not directly about UI design, is instructive as it highlights a judicial expectation for digital platforms to implement strong security measures and a user-centric approach to prevent financial harm. Similarly, the case of *Swati Gupta v. Amazon India*[24] states that the judiciary's struggle to categorize UI manipulation within existing legal frameworks and highlights the need for legislative clarity and specialized judicial training to effectively address design-based deception.

[20] Alison Hung, 'Keeping Consumers in the Dark' (2021) 121 *Columbia Law Review* 2483.
[21] Caroline Sinders, *Designing Against Dark Patterns* (The German Marshall Fund of the United States 2021) https://www.gmfus.org/news/designing-against-dark-patterns imperceptibility and the unconscious nature of the manipulation." accessed on 5 June 2025.
[22] Dark Patterns in India's Subscription Economy: A Threat to Consumer Rights and Digital Trust - The Wire, https://m.thewire.in/article/ptiprnews/dark-patterns-in-indias-subscription-economy-a-threat-to-consumer-rights-and-digital-trust accessed on 15 June 2025.
[23] Punjab National Bank v Leader Tour & Travels (2022) SCC Online Del 1365
[24] Swati Gupta v Amazon India (2021) Complaint No. 112/2020, NCDRC

### 4.1. Information Technology Act, 2000

The Information Technology Act, 2000, primarily serves as India's significant step towards curbing cybercrime. It penalizes various forms of digital offenses, including hacking (Section 66), identity theft (Section 66C), and impersonation (Section 66D). However, a huge limitation of the IT Act is its notable silence on criminalizing deceptive design practices or UI manipulation, which are central to dark patterns.[25] While Section 43, pertaining to compensation for damage to computer systems (broadly interpreted to include unauthorized access), might extend to situations where dark patterns coerce consent, particularly if data is accessed or extracted without truly free will, its provisions are ultimately too broad and lack the specificity required to address digital coercion inherent in deceptive interfaces. The IT Act, primarily designed for overt cybercrimes, struggles to encompass the nuanced nature of design-based deception. Furthermore, Section 79 of the IT Act, which extends safeguards to intermediaries from third-party information or data, could potentially create an inconsistency with any future dark pattern guidelines, posing a huge implementation challenge.

### 4.2. Consumer Protection Act, 2019

The Consumer Protection Act (CPA), 2019, aims to safeguard consumer rights and includes provisions against "unfair trade practices," specifically defining "misleading advertisements"[26]. Dark patterns, by their very nature, involve misrepresentation and the concealment of material information, which directly leads to manipulated consumer choice. However, despite this conceptual overlap, the absence of specific terminology and clear guidelines within the CPA means that enforcement against dark patterns remains patchy and highly subject to interpretational ambiguities.[27] While dark patterns are indeed considered an "unfair commercial practice" and "misleading advertisement" under the broader consumer protection law framework , and existing legislation "offers protection against unfair trade practices and misleading advertisements by using similar tactics" , the CPA lacks the precision and explicit definitions necessary for consistent and direct enforcement against manipulative UI/UX

[25] Shreya Singhal v Union of India (2015) 5 SCC 1
[26] Consumer Protection Act (CPA), 2019, Section 2(47).
[27] Akhil Raj & Ekta Gupta, 'Illuminating the Shadows in India's Dark Pattern Guidelines: A Flawed Regulatory Attempt' (Centre For Business and Commercial Laws 2024) https://cbcl.nliu.ac.in/contemporary-issues/illuminating-the-shadows-in-indias-dark-pattern-guidelines-a-flawed-regulatory-attempt/ accessed 18 June 2025.

designs.

A significant development came with the Central Consumer Protection Authority (CCPA) Advisory dated September 2023.[28] For the first time, the CCPA explicitly acknowledged "dark patterns" and provided a list of specific practices, including "confirm shaming," "forced action," and "subscription traps," deeming them as violations. This advisory is a welcome and crucial step, indicating a growing regulatory awareness and a clear intent to address the issue. However, a primary problem of such advisories is their non-binding nature and the absence of direct penal sanction. They serve primarily as guidance or warnings, making it difficult to initiate direct punitive action based solely on advisory violations. The CCPA has encouraged e-commerce platforms to conduct self-audits to detect dark patterns and has issued notices to some platforms found violating the guidelines.[29] The guidelines themselves do not allude to the forum to be approached in case of violations, and establishing "intention," which the definition requires, is hard to ascertain, further complicating enforcement. The non-binding nature of the advisory and the lack of explicit statutory backing mean that while it raises awareness and provides guidance, its direct punitive power is limited, placing a burden on consumers or civil society to initiate complaints based on potentially ambiguous interpretations of "unfair trade practice."

### 4.3. Digital Personal Data Protection Act, 2023 (DPDPA)

The Digital Personal Data Protection Act (DPDPA), 2023, marks a significant advancement in India's privacy law, introducing stringent requirements for data fiduciaries. It mandates that consent for data processing must be "free, specific and informed," and delivered in "clear and plain language".[30] This Act, while notably silent on the term "dark patterns" itself, provides a powerful indirect tool against them, as dark patterns are designed to compromise the spirit and letter of this consent requirement. Techniques such as pre-checked boxes, misleading opt-out options, or obscured privacy settings (which act as "roach motels" for data consent) directly compromise the "free," "informed," and "unambiguous" nature of consent mandated by Section 6(1) of the DPDPA. However, critics rightly argue that without explicit provisions or specific regulatory guidelines that define how interface design influences consent validity, Sections 6

[28]Central Consumer Protection Authority, 'Advisory on Dark Patterns' (September 2023) https://consumeraffairs.nic.in accessed on 11 June 2025.
[29] 'CCPA issues advisory to e-commerce platforms for self-audit within 3 months to detect dark patterns', *The Economic Times* https://m.economictimes.com/industry/services/retail/ccpa-issues-advisory-to-e-commerce-platforms-for-self-audit-within-3-months-to-detect-dark-patterns/articleshow/121692130.cms accessed 14 June 2025
[30] Digital Personal Data Protection Act 2023, Section 6(1).

and 7 of the Act, governing consent and lawful processing, remain too abstract to effectively combat sophisticated design coercion. There is a crucial need for the Dark Patterns Guidelines to "incorporate elements from the DPDP Act, specifically, terms such as 'Data Fiduciary'," to comprehensively address the consent and data privacy aspects related to dark patterns. This points to a significant gap in legal linkage and enforcement mechanisms, making enforcement reliant on proactive regulatory interpretation that connects deceptive UX practices directly to the invalidation of consent under the DPDPA.

## 5. Global Perspective: What India Can Learn

After examining the approaches adopted by other jurisdictions that provide valuable lessons for India in crafting a robust legal framework against dark patterns. They highlight a growing global consensus on the need to regulate deceptive user interfaces.

### 5.1. United States

In the United States, the Federal Trade Commission (FTC) has been a proactive force in curbing deceptive UI. Section 5 of the FTC Act[31], which prohibits "unfair and deceptive acts or practices". A significant recent example is *In re Amazon.com, Inc. (2023)*[32] , where the FTC sued Amazon for allegedly enrolling users into Prime subscriptions without proper consent and making cancellation difficult—classic "forced continuity" and "roach motel" patterns. This demonstrates the U.S. approach's emphasis on penal enforcement and the use of broad consumer protection statutes to address manipulative design.

Furthermore, California's Consumer Privacy Rights Act (CPRA) explicitly bans obtaining consent via dark patterns, indicating a legislative recognition of the issue. Proposed federal legislation like the DETOUR Act also aims to prohibit interface designs that exploit behavioral biases to impair autonomy. The U.S. experience provides effectiveness of strong enforcement actions, even under general consumer protection laws, when regulators are aware of the nuances of digital manipulation.

### 5.2. European Union

The European Union has adopted a comprehensive and pioneering stance against dark patterns.

[31] Federal Trade Commission Act 1914, Section 5.
[32] In Re AMAZON.COM, INC., No. 23-104 (Fed. Cir. 2023)

The EU's General Data Protection Regulation (GDPR) mandates that consent must be "freely given, specific, informed, and unambiguous". The European Data Protection Board (EDPB) has issued clear guidelines clarifying that manipulative interfaces invalidate user agreement. In a landmark move in 2022, France's CNIL fined Google and Facebook over €150 million for cookie banners that made opting out significantly harder than accepting, a clear example of deceptive design. More recently, the EU has fortified its regulatory arsenal with the Digital Services Act (DSA) and Digital Markets Act (DMA). These acts explicitly ban deceptive design practices and require platforms to ensure neutral, accessible, and non-manipulative interfaces. The Norwegian Consumer Council's 2018 report titled "Deceived by Design" significantly influenced EU-level scrutiny, highlighting the importance of civil society research in driving regulatory change. The EU's multi-layered approach, combining broad data protection principles with specific legislative prohibitions and robust enforcement, provides a powerful model for addressing the systemic nature of dark patterns.[33] India, with its vast digital user base and diverse consumer vulnerabilities, could significantly benefit from a hybrid model, combining the EU's precise legal prohibitions and clear guidelines with proactive enforcement and educational outreach.

### 5.3. Other Jurisdictions

Beyond the US and EU, other jurisdictions are also taking note. The UK's Competition and Markets Authority (CMA) has issued reports on online choice architecture, signaling regulatory concern. The Organisation for Economic Co-operation and Development (OECD) published guidance on "dark commercial patterns" in 2021, contributing to a global standard-setting dialogue. These international trends collectively affirm that dark patterns are a recognized threat requiring dedicated regulatory attention.

## 6. Recommendations

To effectively combat dark patterns and safeguard consumer autonomy in India's rapidly expanding digital landscape, a multi-faceted and proactive approach is imperative.

1. **Statutory Recognition and Definition of Dark Patterns:** The most crucial step is to amend existing laws, particularly the Consumer Protection Act, 2019, and the

[33] M. R. Leiser and Cristiana Santos, 'Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation Beneath the Interface' (2023) SSRN https://ssrn.com/abstract=4431048 accessed on 13 June 2025.

Information Technology Act, 2000, to explicitly define and prohibit dark patterns. This would provide necessary legal clarity and reduce interpretational ambiguities, enabling direct enforcement actions against manipulative UX designs.

2. **Issuance of Sector-Specific UX Guidelines:** The Ministry of Electronics and Information Technology (MeitY) and the CCPA, in coordination with sectoral regulators like RBI, should publish detailed national standards and UX guidelines. These guidelines should clearly illustrate prohibited dark pattern types with examples relevant to the Indian digital context, providing clear benchmarks for platform compliance.

3. **Enhanced Enforcement Mechanisms and Tools:** Regulators must be equipped with specialized tools and technical expertise for UX detection and analysis. This includes investing in forensic UX analysis capabilities and empowering regulatory bodies (like the CCPA and Data Protection Board) to conduct proactive audits of digital platforms.

4. **Mandatory Design Audits and Transparency:** Large digital platforms, especially those in sensitive sectors like finance and e-commerce, should be mandated to submit annual independent UX audits to relevant regulators. Furthermore, platforms should be required to clearly disclose any A/B testing or design choices related to user engagement and conversion that could be interpreted as manipulative.

5. **Strengthening Digital Literacy and Consumer Awareness Campaigns:** The government and civil society organizations must collaborate on extensive, state-supported programs to educate users about manipulative design. These campaigns should be multilingual and accessible, empowering consumers to identify, report, and resist dark patterns.

6. **Establishing Clear Redress Mechanisms and Whistle-blower Incentives:** Create accessible reporting tools for consumers to lodge complaints specifically regarding dark patterns. Additionally, offer protection and incentives to designers and insiders who expose the use of deceptive design practices within their organizations.

7. **Judicial Training and Sensitization:** Conduct regular training programs for judges and members of consumer forums to sensitize them to the technical and psychological aspects of design-based deception. This will enable them to better evaluate evidence and deliver

informed judgments in cases involving dark patterns.

## 7. Conclusion

The battle against cyber fraud in India cannot be won solely through traditional enforcement methods. As the nature of digital deception evolves, so too must the legal system's ability to detect and deter it. Dark patterns represent a subtle yet powerful method of exploitation, often hidden beneath layers of interface and code. They fundamentally undermine consumer rights, data privacy, and the constitutional right to autonomy and informed consent recognized by the Supreme Court in *Justice K.S. Puttaswamy v Union of India*.[34]

In a country like India—where millions are newly connected and often digitally naïve—this manipulation can have serious financial and psychological consequences. It is time for Indian law to formally acknowledge and address the pervasive threat of dark patterns. This requires a multifaceted approach—robust statutory reform, proactive regulatory oversight, enhanced judicial recognition and understanding, and widespread public awareness. Only then can digital spaces become safer, fairer, and truly accountable for the users they claim to serve. By embracing a comprehensive strategy, India can position itself as a leader in protecting digital consumers from these insidious forms of online manipulation.

[34] Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1