



# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

## DARK PATTERNS IN DIGITAL CONTRACTS: THE FINE LINE BETWEEN UX AND MANIPULATION

*Sneha Chauhan*

### INTRODUCTION

In the modern digital economy, each click, scroll, and tap on a website or app is defined by design. As user experience (UX) seeks to make things easier, there's a sinister side, a "dark pattern", interface design practices deliberately designed to trick or push users into behaviour they may not otherwise adopt.<sup>1</sup> These include such practices as pre-checked boxes for subscriptions, surreptitious charges at checkout, or intentionally obfuscating opt-out procedures. Such manipulative designs are particularly problematic when applied to digital contracts, where consent from users is the legally foundational basis for contracts.

First coined by UX designer Harry Brignull in 2010, the term "dark patterns" refers to design patterns that profit the service company at the cost of the user, usually through manipulating free, informed consent. Dark patterns have grown from annoyance strategies over the last decade to full-blown consumer rights violations, particularly in industries such as e-commerce, fintech, and SaaS platforms. Studies indicate that such designs have a major impact on consumer behaviour, usually without their complete consciousness, deciding on data sharing, buying, and even subscription for years.<sup>2</sup> In online contracts, such patterns arouse serious questions regarding the authenticity of consent, making such agreements legally dubious.

As world regulators from the FTC in America to the European Commission under GDPR and the Digital Services Act, clamp down on these tactics, India has also entered the fray. The Central Consumer Protection Authority (CCPA) released specific Guidelines to Prevent Dark

---

<sup>1</sup> *Dark Patterns in Digital Contracts: Consumer Exploitation*, LexTalk, <https://www.lextalk.world/post/dark-patterns-in-digital-contracts-consumer-exploitation> (last visited Aug. 1, 2025)

<sup>2</sup> *Contract Law and Persuasive Design: Dark Patterns, AI and the Concept of Free Choice*, Eric Tjong Tjin Tai, Feb. 1, 2023, 16 pp., available at SSRN: <https://ssrn.com/abstract=4537170> (last accessed Aug. 1, 2025)

Patterns in 2023, focusing on 13 deceptive design patterns across digital platforms. The Digital Personal Data Protection Act, 2023 also strengthens the imperative of free and informed consent in every digital transaction

The article discusses the nature of dark patterns, their legal treatment in India and around the world, their effect on consent in digital contracts, and provides regulatory recommendations for a better digital ecosystem.

## **WHAT ARE DARK PATTERNS?**

Dark patterns are misleading design features in user interfaces that deceive, coerce, or manipulate users into making unintended or non-consensual choices. They take advantage of cognitive biases, information overload, or uncertainty to propel actions that profit the service provider, e.g., subscribing to a service, divulging personal information, or signing up for terms unknowingly. Unlike conventional fraud or misrepresentation, dark patterns work subtly in the confines of digital design, frequently taking the form of innocuous UX features.

These behaviours assume numerous guises, such as:

- Pre-checked boxes that sign up users for subscriptions or transmit personal information unless explicitly cleared
- Hidden or buried conditions and terms, which bury essential contractual terms behind dropdowns or multi-click routes
- Interface interference, whereby the design or layout highlights some buttons such as "Accept All" more than others such as "Reject" or "Manage Preferences"

It was first used in 2010 by Harry Brignull, who explained dark patterns as "tricks used in websites and apps that make you do things that you didn't mean to". As they expanded over time across the digital space, particularly in online commerce, travel reservation, and technology services they have come under growing legal and ethical attention.<sup>3</sup>

In India, the CCPA 2023 Guidelines call dark patterns "any practice or misleading design pattern through user interface or user experience interactions on any platform to mislead or

---

<sup>3</sup> *Dark Patterns Outlawed: Online Platforms to Watch Out*, SCC Online, Feb. 27, 2025, <https://www.sconline.com/blog/post/2025/02/27/dark-patterns-outlawed-online-platforms-to-watch-out/> (last accessed Aug. 1, 2025)

manipulate users"<sup>4</sup>, and directly prohibit methods such as pre-selected checkboxes, hidden advertisements, and confirm-shaming.

These patterns extend the boundary between persuasive design and manipulative intent, and their application in digital contracts can undermine the very basis of informed, voluntary consent

## **LEGAL RESPONSE TO DARK PATTERNS: ENFORCEABILITY IN INDIA AND BEYOND**

Dark patterns can start off as design choices, but their legal consequences go deep, particularly when employed to prompt user consent or bind people into digital contracts. Judges and regulators across the globe are slowly coming to realize such manipulative tactics as abuse of consumer rights, privacy regulations, and even elementary contract law concepts. Here is an organized examination of how India and other jurisdictions have reacted.

### **ARE THEY LEGALLY ENFORCEABLE?**

Fundamentally, online contracts are enforceable only if user consent is voluntary, informed, and free. Dark patterns subvert this premise by designing consent through deception instead of actual agreement.

According to Indian jurisprudence, where consent is obtained by misrepresentation, coercion, or undue influence, it could be deemed legally defective. According to Section 19 of the Indian Contract Act, 1872, such contracts are voidable at the discretion of the aggrieved party. Where dark patterns are present, such as concealed clauses or default opt-ins, they can be invalidated due to a lack of valid consent.

Additionally, Indian courts would turn to "unconscionable contract" laws, particularly in form contracts (contracts of adhesion), where the consumer has no or minimal negotiating capability and where misleading interfaces create a power imbalance.<sup>5</sup>

## **INDIAN CONSUMER PROTECTION ACT AND IT RULES, 2021**

---

<sup>4</sup> *Dark Patterns in Digital Contracts: Consumer Exploitation*, LexTalk, <https://www.lextalk.world/post/dark-patterns-in-digital-contracts-consumer-exploitation> (last visited Aug. 1, 2025)

<sup>5</sup> *Dark Patterns Outlawed: Online Platforms to Watch Out*, SCC Online, Feb. 27, 2025, <https://www.sconline.com/blog/post/2025/02/27/dark-patterns-outlawed-online-platforms-to-watch-out/> (last visited Aug. 1, 2025)

India's Consumer Protection Act, 2019 and the regulations thereto have taken on the role of addressing outright digital impropriety explicitly<sup>6</sup>. Section 2(47) makes the use of dark patterns potentially constitute an "unfair trade practice," particularly where it acts to conceal material facts, mislead by representations, or fail to disclose prices or terms of cancellation.

The Consumer Protection (E-Commerce) Rules, 2020 require transparency of terms and conditions, ban misleading representations, and insist that platforms make cancellation and refund policies clearly known to them. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate intermediaries to maintain transparency and due diligence, such as refraining from manipulative interface design, particularly with respect to consent, profiling, or targeted advertising.<sup>7</sup>

The biggest step was taken in November 2023, when the Central Consumer Protection Authority (CCPA) put out Guidelines for Prevention and Regulation of Dark Patterns. These guidelines enumerate and prohibit 13 dark patterns in particular, such as:

- Pre-ticked checkboxes
- Confirm-shaming
- Bait-and-switch
- Forced continuity

Infringements can attract heavy penalties under Section 21 of the CPA, up to ₹50 lakhs for false advertisements and up to 5 years of imprisonment for egregious infringement (Bar & Bench Analysis).

## **RECENT GLOBAL CRACKDOWNS (EU, US FTC)**

### European Union:

In GDPR, consent is "freely given, specific, informed and unambiguous" (Article 4(11)). The European Data Protection Board (EDPB) has established that consent based on misleading or confusing design features is not GDPR compliant, and thus such digital contracts are unenforceable.

---

<sup>6</sup> *Dark Patterns in Digital Contracts: Consumer Exploitation*, LexTalk, <https://www.lextalk.world/post/dark-patterns-in-digital-contracts-consumer-exploitation> (last accessed Aug. 1, 2025)

<sup>7</sup> *Contract Law and Persuasive Design: Dark Patterns, AI and the Concept of Free Choice*, Eric Tjong Tjin Tai, Feb. 1, 2023, 16 pp., available at SSRN: <https://ssrn.com/abstract=4537170> (last accessed Aug. 1, 2025)

The Digital Services Act (DSA) of 2024 also prohibits misleading interfaces that manipulate or disable user autonomy, especially where algorithmic personalization is involved (EDPB Consent Guidelines).<sup>8</sup>

#### United States:

The Federal Trade Commission (FTC) has fought dark patterns as "unfair or deceptive trade practices" under Section 5 of the FTC Act aggressively. Some significant actions include:

- Epic Games (Fortnite): Fined \$245 million for employing misleading UX to facilitate accidental purchases.
- The 2022 FTC Staff Report on Dark Patterns also presents a taxonomy of deceptive design categories and indicates more assertive enforcement in the future.

### **IMPACT ON CONSENT IN DIGITAL CONTRACTS**

Consent is the foundation of digital contracts, particularly in e-commerce, fintech, data protection, and app services. For a contract to be legally effective, the agreement of the user should be freely given, informed, specific, and clear.<sup>9</sup> Dark patterns consistently subvert these requirements by designing behavior from users through manipulation instead of free choice.

For example, research has established that:

- Opt-out removal or concealment increases consent rates by 22–23 percentage points.
- Providing users more detailed choices (which enhance clarity) decreases acceptance rates by 8–20%, demonstrating the ability of design to bias choice (Arxiv Study on Consent and UX Design).

In India, this is in direct contrast with the definition of free consent in the Digital Personal Data Protection Act, 2023, which requires that consent be free, specific, informed, and unambiguous.

Worldwide, the EU's GDPR and US FTC both mandate that consent gathered under misleading circumstances, e.g., concealed terms or opt-out resistance, has no valid legal basis.<sup>10</sup> The EDPB and courts have repeatedly held that consent from misleading or coercive user experience does not meet Article 7 of the GDPR (EDPB Guidelines on Consent).

---

<sup>8</sup> *Demystifying the Dark Patterns*, Lakshmikumaran & Sridharan, Jan. 3, 2024, <https://www.lakshmisri.com/insights/articles/demystifying-the-dark-patterns/> (last accessed Aug. 1, 2025)

<sup>9</sup> *Contract Law and Persuasive Design: Dark Patterns, AI and the Concept of Free Choice*, Eric Tjong Tjin Tai, Feb. 1, 2023, 16 pp., available at SSRN: <https://ssrn.com/abstract=4537170> (last accessed Aug. 1, 2025)

<sup>10</sup> *Demystifying the Dark Patterns*, Lakshmikumaran & Sridharan, Jan. 3, 2024, <https://www.lakshmisri.com/insights/articles/demystifying-the-dark-patterns/> (last visited Aug. 1, 2025)

Accordingly, contracts based on dark patterns can:

- Be unlawful because of faulty consent,
- Harm consumers,
- Injure data privacy law, creating civil and criminal liability.

Although India has made groundbreaking strides particularly with the 2023 Guidelines by CCPA banning 13 dark patterns more needs to be done to introduce uniform enforcement and regulatory clarity. Following are significant recommendations:

#### 1. Design Audits as a requirement

Periodic audits of digital platforms to identify and remove dark patterns must be demanded by regulators, particularly in high-risk domains such as financial apps, edtech, and e-commerce. The CCPA in June 2025 mandated that platforms perform a self-audit within three months.

#### 2. Enhance Penalties for Repeat Offenders

Institutionalize tiered penalties with repeat and high-value offenses eliciting higher fines and even license cancellations. <sup>11</sup>Section 21 of the CPA presently provides up to ₹50 lakh fines, but enforcement varies.

#### 3. Coherence with Data Protection Law

Enforce the Digital Personal Data Protection Board (DPDPB) to be harmonious with the CCPA so that UX-based consent manipulation is dealt with, particularly in data collection and sharing habits.

#### 4. Consumer Complaint Mechanisms

Improve current platforms such as Jago Grahak Jago and add a special portal through which consumers can report potential dark patterns. Screenshots, design flows, and complaint tracking can be provided.

#### 5. UX Design Ethics Education

Encourage or require ethics UX training for tech teams and product designers. Interventions from government agencies and tech universities can facilitate instillation of privacy by design and fair interface tenets

---

<sup>11</sup> *Demystifying the Dark Patterns*, Lakshmikumar & Sridharan, Jan. 3, 2024, <https://www.lakshmisri.com/insights/articles/demystifying-the-dark-patterns/> (last visited Aug. 1, 2025)

## **CONCLUSION**

Dark patterns can appear to be small changes to interface design, but their impact on consent, privacy, and contractual justice is significant. Under digital contracts, they threaten to invalidate user consent, contravene consumer protection law, and undermine trust in digital ecosystems. India's regulation of response, particularly the 2023 CCPA Guidelines and the DPDP Act, 2023, is an important step in the right direction. But as design innovation speeds up, so too must regulatory vigilance. Through enhanced enforcement, making design audits mandatory, incorporating cross-sectoral monitoring, and developing consumer literacy, India can guarantee digital contracts are grounded in fairness, not deception.

A forward-looking legal system must incentivize good design and discourage deception and so create a digital economy built on informed consent and user age.