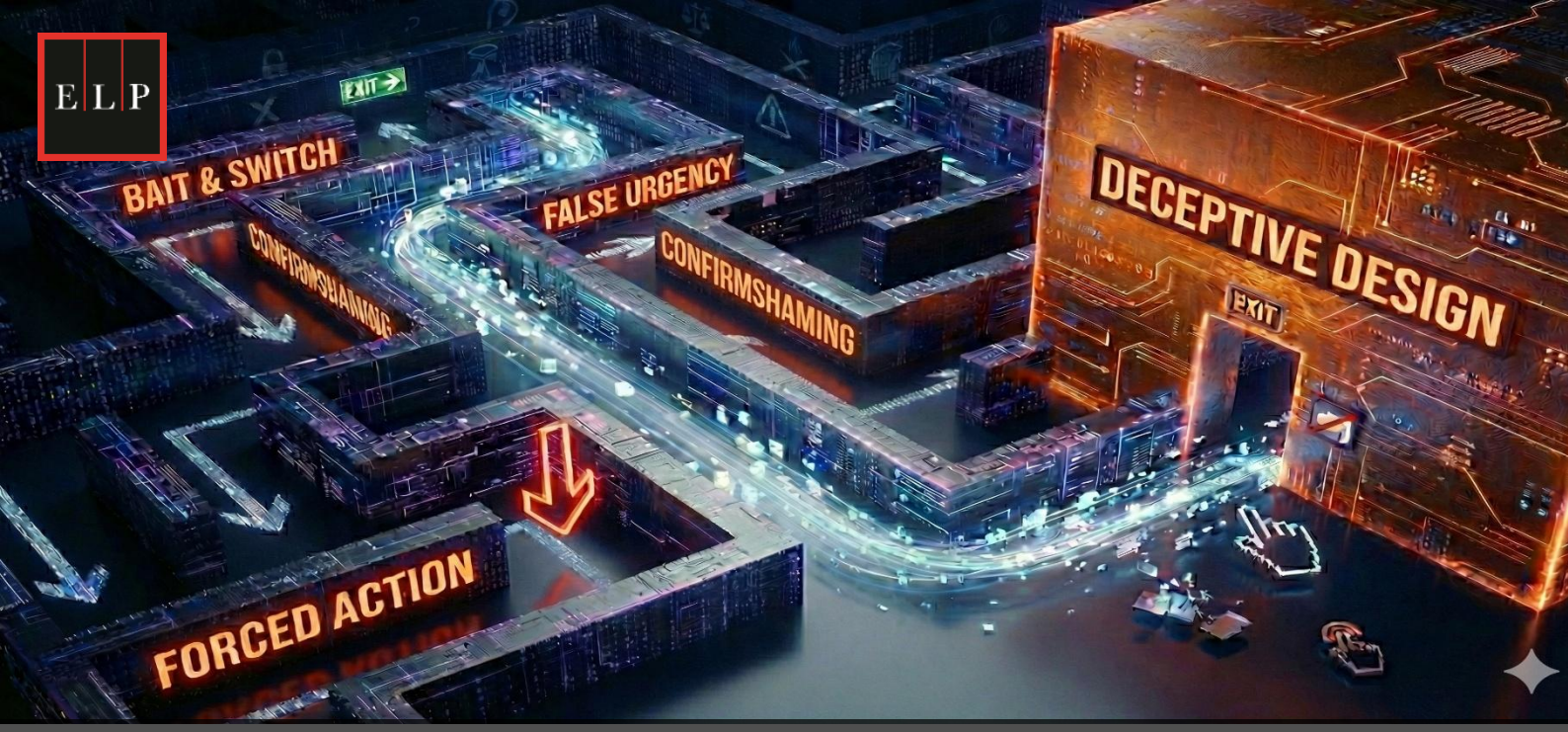

Dual Regulation of Dark Patterns: What Businesses Need to Know

As India's digital economy scales, regulators are increasingly focused on how online platforms shape user behaviour. A key concern is the rising use of "dark patterns", *i.e.,* manipulative interface designs that essentially nudge, steer, or pressure users into actions they may not have freely made. With the Digital Personal Data Protection Act, 2023 (**DPDP Act**) set to become fully operational by May 13, 2027, and the Consumer Protection Act, 2019 (**CP Act**) read with the Consumer Protection (E-Commerce) Rules, 2020 (**E-Commerce Rules**) and the Central Consumer Protection Authority's (**CCPA**) Dark Patterns Guidelines, 2023 (**Dark Patterns Guidelines**) already regulating dark patterns, businesses must rethink how they structure consent flows, display disclosures, and shape user journey on their platforms.

This primer outlines what constitutes a dark pattern, how it is currently regulated under the CP Act, and how a dual regulatory regime is likely to emerge as the DPDP Act comes into full force.[1]

WHAT ARE DARK PATTERNS?

Simply put, a "dark pattern" is any deceptive or manipulative user interface design that misleads, tricks, or pushes users into doing something that they did not originally intend to do. It works by undermining the user's **autonomy** or ability to make a **free choice**, and may amount to a misleading advertisement, an unfair trade practice, or a violation of consumer rights.[2] A common dark pattern is creating a false sense of urgency to push a user into a quick purchase. For instance, a hotel booking site may falsely claim "*Only 2 rooms left! 30 people are viewing this right now*" to pressure the user into booking immediately. Since dark patterns mislead users to act in a manner that they otherwise would not have provided they had complete and true information, free and informed **consent** is at the core of regulation of dark patterns.

REGULATION OF DARK PATTERNS UNDER THE CONSUMER PROTECTION LAW FRAMEWORK

The CP Act aims to offer a framework to address, amongst others, unfair trade practices by businesses and grievances of consumers through a multi-tier grievance redressal mechanism. It widely defines concepts such as "unfair trade practices", "misleading advertisements"[3] and "consumer rights"[4] such that practices such as dark patterns can be

---

1 This primer is limited to the CP Act and the DPDP Act and does not cover other laws that may also apply to dark patterns. For example, the Information Technology Act, 2000 does regulate certain aspects of dark patterns as defined and identified under the Dark Patterns Guidelines.

2 Guideline 2(e) of the Dark Patterns Guidelines.

3 Broadly, a misleading advertisement is any advertisement that falsely describes a product or service, makes misleading or false claims about its key features, conveys a representation that would amount to an unfair trade practice if made by the seller, or deliberately hides important information (Section 2(28) of the CP Act.

4 Broadly, consumer rights include the right to safe products and services, to accurate information about them, to access a variety of options at fair prices, to be heard and have concerns considered, to seek redress against unfair practices, and to be informed and aware as a consumer (Section 2(9) of the CP Act).

regulated under the CP Act. For example, an unfair trade practice broadly means any business practice that **uses unfair or deceptive methods** to promote the sale, use, or supply of goods or services and includes a non-exhaustive list of specific practices.[5] The CP Act puts the onus on the CCPA to ensure, amongst others, prevention of unfair trade practices and misleading advertisements.[6] It also empowers the central government to frame rules[7] and the CCPA to issue guidelines.[8]

In 2020, the central government issued the E-Commerce Rules, which, amongst others, prohibit e-commerce entities from adopting unfair trade practices and requires them to obtain explicit, affirmative consent from consumers and expressly prohibit practices like pre-ticked checkboxes or auto-recorded consent.[9] These obligations strike at the heart of dark patterns, *i.e.,* preventing platforms from nudging users into unintended actions.

Subsequently, in 2023, the CCPA issued the Dark Patterns Guidelines, expressly prohibiting all persons including platforms from engaging in any dark pattern practice. It widely defines dark patterns and identifies a list of illustrative dark pattern practices.[10]

IMPLICATIONS OF VIOLATIONS OF THE CONSUMER PROTECTION FRAMEWORK

As per the CP Act, conduct involving dark pattern practices could trigger investigations[11] and subsequent imposition of monetary penalties (which increase significantly for repeat offences) and in certain cases, imprisonment.[12] Based on media reports, earlier this year the CCPA issued notices to 11 platforms for non-compliance with the Dark Pattern Guidelines[13] and as recently as last month, 15 additional notices were issued.[14] The CCPA has also issued an advisory,[15] advising all e-commerce platforms to ensure compliance with the Dark Pattern Guidelines and carry out a self-audit and submit self-declarations stating compliance with the guidelines. So far, based on media reports, ~26 platforms have submitted their declarations.[16]

REGULATION OF DARK PATTERNS AND THE DPDP ACT

While the CP Act focuses on protection of consumer rights, the DPDP Act is primarily concerned with the processing of digital personal data without consent. While the DPDP Act does not explicitly regulate or prohibit dark patterns, it is likely to apply to practices involving dark patterns considering it undermines user consent for processing digital personal data.[17]

---

5 Section 2(47) of the CP Act.
6 Section 18 of the CP Act.
7 Section 101 of the CP Act.
8 Section 18 of the CP Act.
9 Rule 4(9) of the E-Commerce Rules.
10 Annexure 1 to Guideline 5 of the Dark Patterns Guidelines.
11 Section 15 r/w Section 18(2)(a) of the CP Act.
12 As per the CP Act (Section 20-21), the CCPA can order businesses to discontinue an unfair trade practice or modify misleading advertisements within a specified time. The CCPA may also impose penalties of up to INR 1 million (~ USD 11,200) for a first offence and INR 5 million (~ USD 56,200) for subsequent offences. As per Section 88 of the CP Act, non-compliance with the CCPA's direction can attract imprisonment of up to six months and/ or fines up to INR 2 million (~ USD 22,400). Section 89 of the CP Act lays down punishment for publishing false or misleading ads, which is imprisonment of up to two years (five years for repeat offences) and fines of up to INR 1 million (INR 5 million for repeat offences).
13 *Govt issues notices to 11 firms including Zepto, Uber for using dark patterns to sway consumers, warns action*, the Times of India, available at https://timesofindia.indiatimes.com/business/india-business/govt-issues-notices-to-11-firms-including-zepto-uber-for-using-dark-patterns-to-sway-consumers-warns-action/articleshow/121470779.cms.
14 *E-commerce firms asked to explain dark patterns*, Financial Express, available at https://www.financialexpress.com/business/news/e-commerce-firms-asked-to-explain-dark-patterns/4060990/.
15 The CCPA's 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* dated June 5, 2025, available at https://doca.gov.in/ccpa/files/Advisory-7.pdf.
16 *26 e-commerce firms say platforms are dark pattern free, govt nudges rest to comply*, CNBC TV18 available at https://www.cnbctv18.com/business/26-e-commerce-firms-swiggy-zomato-blinkit-declare-dark-pattern-free-govt-nudges-rest-ws-l-19774282.htm.
17 Indeed, dark patterns are also regulated under the EU's General Data Protection Regulation (**GDPR**), which like the DPDP Act, does not expressly regulate or prohibit dark patterns. However, certain key principles underlying the GDPR and in particular fair and transparent processing, data minimisation, purpose limitation, and accountability along with the stringent conditions for valid consent and obligations relating to data subject rights come into play. The EU regulators therefore assess dark patterns through multiple GDPR provisions, reflecting a similar overlap between design practices and data protection obligations. (European Data Protection Board's adoption of Guidelines on Art. 60 of GDPR: *Guidelines on dark patterns in social media platform interfaces: How to recognise and avoid them*, available at https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf).

Under the DPDP Act, a data fiduciary, barring few exceptions, can process (or get processed) digital personal data only upon obtaining **consent** of a user (*i.e.,* a data principal) and for a specified purpose.[18] **Consent**, under the DPDP Act, must be **free**, **specific**, **informed**, **unconditional** and **unambiguous** with clear affirmative action. As explained above, dark patterns precisely undermine this idea of free consent. Therefore, a data fiduciary that engages in dark pattern practices is likely to also infringe the obligations cast under the DPDP Act to the extent the dark pattern practices at issue also involve processing digital personal data. For example, if a ticket booking platform makes a false statement regarding ticket inventory for a show such that a user is nudged to purchase a ticket on priority through the platform by sharing personal data, this could be viewed as processing of digital personal data by the platform without valid consent. Or say that an online gaming platform prompts a user that he/ she is "one step away from losing rewards!" unless they immediately verify their identity through a phone number which in turn nudges the user to share personal data with the gaming platform. Both these illustrations essentially involve obtaining consent from a data principal which is not free and processing of personal data obtained, triggers consequences under the DPDP Act.

IMPLICATION OF VIOLATIONS OF THE DPDP ACT

Violation of the DPDP Act can lead to enforcement action by the Data Protection Board of India, including the initiation of inquiries and imposition of monetary penalties in cases of breach. Depending on the nature and gravity of the breach, these penalties can be significant, reaching up to INR 2.5 billion (~USD 30 million).

DUAL REGULATORY REGIME

Both the CP Act and DPDP Act operate in addition to and not in derogation of each other.[19] Specifically, the Dark Patterns Guidelines also state that they operate in addition to and not in derogation of any other law.[20] Simply put, a single conduct involving dark patterns may trigger enforcement under both the statutes.

WHAT SHOULD BUSINESSES DO?

Given the dual regulatory regime, where the same dark pattern-related conduct may trigger enforcement (including penalties) under both the CP Act and the DPDP Act, businesses should pro-actively ensure that their product and user interfaces do not employ manipulative design. Specifically, at a minimum, businesses should consider:

- ***Conducting a dark pattern audit***. Regularly evaluate interfaces, user flows, and communication to identify and remove elements that may mislead, pressure, confuse users or undermine the consent mechanism enshrined under the DPDP Act. This will also help in complying with the advisory issued by the CCPA.

- ***Filing of declarations with the CCPA***. The CCPA recently advised e-commerce platforms to file declarations outlining steps taken to remove dark patterns. Businesses must submit the required declaration explaining what steps they have taken to remove dark patterns.

- ***Embedding compliance within product and design teams***. Build compliance into the product itself, *i.e.,* legal, product, and design teams must collaborate and ensure that the design of websites, apps, and consent prompts prioritizes genuine user choice and does not bury or obscure important information.

- ***Ensure withdrawal processes are frictionless***. Make it easy for users to walk away. For example, one-click unsubscribe or simple account deletion may help mitigate risks.

---

18 Section 4 read with Section 6 of the DPDP Act. While the DPDP Act allows for processing of digital personal data without consent under certain circumstances (*i.e.,* legitimate use cases), those circumstances are narrow. Similarly, for legacy data, data fiduciaries are not required to obtain fresh consent and notice in terms of Section 5(2) of the DPDP Act would suffice.

19 Section 100 of the CP Act and Section 38 of the DPDP Act.

20 Guideline 6 of the Dark Patterns Guidelines.

- ***Internal training***. Equip relevant teams including product and design team with clear dos and don'ts guidelines to avoid accidental adoption of dark patterns.

- ***Monitoring enforcement trends***. Since both the consumer protection and personal data protection laws are at an early stage and evolving, tracking legal developments is essential to continuously update internal compliance measures.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email -*ravisekharnair@elp-in.com*

Parthsarathi Jha, Partner – Email - *parthjha@elp-in.com*

Ketki Agrawal, Principal Associate – Email *- ketkiagrawal@elp-in.com*