Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2024 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Dark Patterns: The Need for Regulation

Lakshika Singh[a]

[a]Maharashtra National Law University, Aurangabad, India

Received 28 April 2024; *Accepted* 29 May 2024; *Published* 05 June 2024

Dark patterns encompass unethical UI/UX interactions that are deliberately deceitful or manipulative, aiming to compel users into executing undesired activities. They subsequently provide advantages to the organization or platform that adopts the designs. This article aims to examine the necessity of regulating Dark Patterns in modern times and emphasizes the requirement for clear and effective regulation in India. The article begins by providing a brief overview of Dark Patterns. Further, the necessity and rationale for regulating Dark Patterns are also examined, drawing upon scholarly surveys and contemporary illustrations. The work briefly discusses the rules and regulatory framework established by the European Union (EU), specifically the Digital Services Act (DSA), as well as those implemented by the United States i.e. California Consumer Privacy Act (CCPA). It also touches upon some current instances related to these regulations. Lastly, an analysis is conducted on the most recent guidelines issued by the Indian government (COPRA), specifically the rules for Prevention and Regulation of Dark Patterns 2023, and their implications for implementation.

Keywords: *dark patterns, dsa, ccpa, copra.*

INTRODUCTION

Dark patterns are manipulative user interfaces that use deceptive or coercive strategies to influence humans into engaging in undesirable actions. These patterns leverage cognitive

processes to exert influence on individuals, resulting in discontent and a decline in total consumer confidence. One may encounter these in the form of subscription email lists that are rigorous to unsubscribe from, or servers that persistently fail to revoke consent for actions that include data harvesting. Nevertheless, although they may seem inconspicuous at first sight, dark patterns pose enduring challenges to data privacy and online sovereignty.[1] Through the utilization of Dark Patterns, online services, including websites and applications, can effectively influence individuals into making choices they would not have otherwise chosen. Numerous instances of these misleading tactics can be observed in various places, ranging from prominent news platforms to the preferred meal delivery application. Most internet service companies commonly employ deceptive tactics or manipulate users to increase their profitability.

Dark Patterns are not a new phenomenon; they have existed for a considerable period. Previously, they took the shape of tangible patterns employed by actual businesses. According to one perspective, the use of deceptive tactics in physical objects in the past served as the driving force for the emergence of the modern design trend called dark patterns.

Harry Brignull coined the word in 2010. Brignull's research on dark patterns catalyzed scholarly exploration into the definition and characterization of these patterns. This analysis emphasized the importance of comprehending and surmounting these challenges in the creation of user interfaces. Brignull examined e-commerce and tourism websites to build a taxonomy for misleading design methods, also known as dark patterns. The experiences were categorized into twelve distinct groups, wherein individuals were compelled to make unwanted decisions and faced unpleasant outcomes. Furthermore, a multitude of other scholars, such as Conti and Sobiesk, Bosch, Zagal, and Mathur, have made significant contributions to the subject over time.

[1] Arushi Mukherji, 'India Steps Up Against Dark Patterns' (*Lexology*, 03 November 2023) <https://www.lexology.com/commentary/tech-data-telecoms-media/india/btg-advaya/india-steps-up-against-dark-patterns> accessed 20 April 2024

NEED FOR REGULATION

In recent times there has been a notable increase in the prevalence of dark patterns on numerous websites and applications. Dark Patterns can be present in many applications or across different categories, and they are not mutually exclusive. Instances may arise where a single app or website employs many dark patterns simultaneously.

As per a study done by the Department of Informatics, University of Zurich, Switzerland, where 240 apps were studied, Out of those 240 apps that were examined, a staggering 95% of them included one or more Dark Patterns in their user interfaces. A total of 1,787 instances of Dark Patterns were identified across all apps, resulting in an average of 7.4 deceptive designs per application. Approximately 10% of the apps surveyed had 0, 1, or 2 instances of Dark Patterns (N=33). 37% of the apps had between three to six (3 to 6) instances of Dark Patterns (N=89), while the remaining 49% had 7 or more instances (N=118).[2]

{'N' here means the number of apps surveyed}.

In their study, they presented two investigations that were conducted to evaluate the incidence of dark patterns in mobile applications and the user's impression of this issue. An analysis was conducted on the Google Play Store, specifically on 240 apps from 8 distinct categories. These apps were carefully examined and categorized, with a focus on identifying and classifying dark patterns. The results revealed that 95% of the analyzed apps had one or more instances of dark patterns. Subsequently, an online experiment was carried out with 584 participants who were tasked with evaluating the user interface (UI) of a specific group of applications that were previously examined in the initial study. The result revealed that people often fail to detect the existence of harmful designs.[3]

In another study conducted by Princeton University in 2019 where some of the most popular shopping websites were examined, it was discovered that over 11.1% of the analyzed websites contained at least one occurrence of a dark pattern. Significantly, 183 of the websites exhibited

[2] Linda Di Geronimo et. al., *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception* (Association for Computing Machinery 2020)
[3] *Ibid*

misleading statements. Moreover, it has been noted that popular websites are more prone to displaying dark patterns.[4]

A recent study examined the occurrence of 50 different types of deceptive user interface designs, known as dark patterns, across several platforms including desktop on the web, mobile web, and mobile apps. The study analyzed 105 different services.[5]

According to a paper published in October 2022 by the Organization for Economic Co-operation and Development (OECD), a majority of 57.4% of cookie consent notices on Europe's most popular websites employed interface designs that encouraged users to agree to options that posed a threat to their privacy. These companies employ deceptive strategies to undermine user experience and prioritize their interests.[6]

The aforementioned surveys conducted by numerous scholars and research done by researchers indicate the widespread occurrence of Dark patterns throughout various applications, websites, and industries, including social media as well as significant technology companies.

Other additional instances substantiate the widespread existence of dark patterns in numerous popular applications and websites. Amazon received backlash for its intricate termination process for Prime subscriptions in the European Union, but, it made significant enhancements in 2022. LinkedIn users frequently receive unwanted paid messages from influencers, and deactivating this feature necessitates a thorough comprehension of the platform's policies. Additional deceitful tactics encompass sponsored video commercials on Instagram, and invasive pop-up notifications on YouTube Premium.[7] Other examples are Google Workforce

[4] Arunesh Mathur et. al., 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 (CSCW) Association for Computing Machinery <https://doi.org/10.1145/3359183> accessed 20 April 2024
[5] Johanna Gunawan et. al., 'A Comparative Study of Dark Patterns Across Web and Mobile Modalities' (2021) 5(CSCW2) Association for Computing Machinery <https://doi.org/10.1145/3479521> accessed 20 April 2024
[6] Paritosh Chauhan and Rohan Verma, 'Regulation of Dark Patterns' (*Lakshmikumaran Sridharan Attorneys*, 19 December 2023) <https://www.lakshmisri.com/insights/articles/regulation-of-dark-patterns/> accessed 20 April 2024
[7] Jon Porter, 'EU forces Amazon to make it easier to cancel Prime subscriptions in Europe' *The Verge* (05 July 2022) <https://www.theverge.com/2022/7/5/23195019/amazon-prime-cancellation-europe-european-union-dark-patterns> accessed 20 April 2024

forcing users to sign up for the expensive free trial before downgrading to cheaper options then IndiGo manipulating the emotions of users when booking flights to opt for travel insurance.[8]

FOREIGN REGULATIONS AND CASES

The application of dark patterns has already been subject to regulatory and judicial scrutiny on a global scale. Recently, numerous jurisdictions worldwide have enacted laws to safeguard privacy and consumer rights in response to the dangers brought about by dark patterns. The EU Digital Services Act, implemented in 2022, forbids online platform providers from engaging in deceptive or manipulative practices through their interfaces. Furthermore, it forbids acts that greatly disrupt the psychological processes involved in users' decision-making. The Act incorporates dark patterns by strategically highlighting some options to manipulate decision-making and implementing a more arduous termination procedure in contrast to acceptance.[9]

'Dark patterns' are defined by the California Consumer Privacy Act (CCPA) and California Consumer Privacy Regulations (CCPR) as user interfaces that are deliberately created to hinder the independence, decision-making, or freedom of choice of users. These regulations also forbid obtaining consent using misleading design methods.

TikTok received a fine of €5,000,000 from the French DPA (Data Protection Act) in December 2022. The charge was imposed due to TikTok's unauthorized use of advertising identifiers and its inadequate cookie banner in terms of providing sufficient information. The banner facilitated the acceptance of all cookies with a single click, so obstructing the ability to decline them, and certain advertising cookies were installed even without the user's consent. [10]

In March 2023, Epic Games Inc., the creators of the popular online game 'Fortnite', was fined $245,000,000 by the U.S Federal Trade Commission. The penalty was imposed based on a complaint that accused Epic Games Inc. of violating the U.S. Federal Trade Commission Act of

[8] 'Hall of shame' (*Deceptive Patterns*) <https://www.deceptive.design> accessed 04 May 2024
[9] Chauhan (n 6)
[10] Hall of Shame (n 8)

1914. The complaint alleged that Epic Games Inc. used dark patterns to discourage users from cancelling or requesting refunds for specific in-game charges.[11]

INDIAN GUIDELINES

In India, the legislature has introduced similar initiatives for regulating dark patterns. The Department of Consumer Affairs, which operates under the Ministry of Consumer Affairs, Food and Public Distribution, has just put forth a draft called 'Guidelines for Prevention and Regulation of Dark Patterns, 2023'. The objective of these guidelines is to prohibit the utilization of dark patterns by platforms, advertisers, and dealers. The Central Consumer Protection Authority issued the final version of the guidelines under Section 18 of the Consumer Protection Act 2019 (COPRA) on 30 November 2023.

The Guidelines conform with the discussion paper titled 'Dark Patterns – The New Threat to Consumer Protection' published in November 2022 by the Advertising Standards Council of India (ASCI) and the Guidelines for Online Deceptive Design Patterns in Advertising published on June 15, 2023, by the ASCI.[12]

The Guidelines define 'dark patterns' as *'Dark patterns shall mean any practices or deceptive design patterns using UI/UX (user interface/user experience) interactions on any platform; 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 a misleading advertisement or unfair trade practice or violation of consumer rights.'*[13]

Annexure 1 of the guidelines mentions the following dark patterns along with their illustrations:[14]

---

[11] Chauhan (n 6)
[12] Ashima Obhan and Aparna Amnerkar, 'Dark Patterns Banned: Guidelines For Prevention And Regulation Of Dark Patterns, 2023' (*Mondaq*, 11 December 2023) <https://www.mondaq.com/india/advertising-marketing--branding/1399674/dark-patterns-banned-guidelines-for-prevention-and-regulation-of-dark-patterns-2023> accessed 20 April 2024
[13] Consumer Protection Act 2019, s 18(2)
[14] *Ibid*

False Urgency – It entails misleading customers into making immediate purchases or taking actions by promoting false popularity or asserting limited availability of a product or service. This may result in an inappropriate decision, potentially impacting their purchasing choices.

Basket Sneaking – This refers to the act of discreetly adding more things to the checkout process without the user's knowledge or agreement. This practice goes beyond the intended selection of products or services. However, it is important to note that free samples, complimentary services, or price information do not fall under the category of basket stealing.

Confirm Shaming – It is the act of employing phrase, video, or audio to induce fear, shame, or guilt in people, to persuade them to buy or subscribe to a product or service for the sake of commercial benefit.

Forced Action – It pertains to the act of compelling a user to make more purchases, subscribe to a service, or disclose personal information to acquire or subscribe to the desired product or service.

Subscription Trap – It is a system that intentionally complicates the process of terminating a paid subscription. It involves hiding the cancellation option, demanding payment details or authorization for automatic debits, or providing vague and confusing instructions for cancelling the subscription.

Interface Interference – This refers to a design feature that intentionally emphasizes certain information and hides other relevant data in the user interface, thereby diverting the user's attention away from intended activities.

Bait-and-Switch – It refers to the deceptive technique of advertising a specific result that is dependent on the user's action, but then providing a different consequence instead.

Drip Pricing – This pertains to the practice of not revealing prices in advance, discretely within the user experience, or after confirming a transaction. It also includes advertising something as free without adequately disclosing the requirements for in-app purchases or preventing access to paid services.

Disguised Advertisements – This entails the act of concealing adverts as either user-generated material or deceptive ones, seamlessly integrating them into an interface to deceive clients into clicking on them.

Nagging – It refers to the continuous and unpleasant act of users getting annoyed by requests, information, or interruptions that aim to facilitate transactions and achieve commercial benefits unless explicitly authorized.

Trick Question – This pertains to the utilization of ambiguous language, such as complex phrasing or double negatives, with the intention of misleading users or guiding them towards a particular action.

Saas Billing – It refers to the process of consistently gathering payments from users in a software as a service (SaaS) business model. This is achieved by using effective subscription strategies to acquire customers and generate revenue.

Rogue Malware – It uses ransomware or scareware tactics to defraud customers by falsely claiming the presence of a virus, and coercing them into purchasing a counterfeit malware removal solution that installs malware.

However, these guidelines pose some ambiguity, and loopholes and raise questions about its application. There are a few disquieting features of the standards.

Firstly, the concise nature of the guidelines, with the main part being quite brief, prompts the question of whether it was necessary to create a completely new regulation in this case. It is worth considering whether the desired outcome could have been accomplished by making amendments to the existing guidelines on e-commerce and advertising, which are extensively mentioned in the guidelines.[15]

[15] Arun Prabhu et. al., 'Dark Pattern Guidelines: Illuminating Or Illusory?' (*Cyril Amarchand Mangaldas*, 21 December 2023) <https://corporate.cyrilamarchandblogs.com/2023/12/dark-pattern-guidelines-illuminating-or-illusory/> accessed 20 April 2024

The primary content of the Guidelines is also somewhat contradictory and poses a potential threat of giving rise to conflicting interpretations, self-restraint, and disagreement. As instance:

- Although efforts have been made to expand the Guidelines to include sellers and advertisers, the practical limitations outlined in the Guidelines pertain to all persons (including platforms).
- Similarly, while text in the annexure mentions, *'The dark pattern practices and illustrations specified below provide only guidance and shall not be construed as an interpretation of law or as a binding opinion or decision as different facts or conditions may entail different interpretations'*[16] Guideline 5 continues to state that any person or platform *'shall be considered to be engaging in a dark pattern practice if it engages in any practice specified in Annexure 1 of the guidelines.'*[17]
- The inclusion of specific dark patterns in the Guidelines, which comprise the majority of the content, is useful for offering assistance. However, it may pose issues if regarded as absolute and final.

Although there has been an effort to make this list in Annexure 1 provide an example (possibly in response to feedback), it should be noted that any action falling within the defined specified dark patterns will likely face intense scrutiny and potentially frequent legal action. This is particularly true when considering Guideline 5, which undermines the intended illustrative nature of Annexure 1.

In addition, although several items in this list are evident and beneficial, various issues span from repetition and duplication to too broad limitations and subjective decision-making. These concerns have the potential to result in unforeseen repercussions in a developing digital environment. For instance:

- The purpose of the Guidelines is to restrict the occurrence of 'rogue malware' as a deceptive design, however, the illustration is superfluous and perplexing, as it combines malware attacks with deceptive advertising. This implies that the activity, which is not

[16] Consumer Protection Act 2019, s 18(2)(1)
[17] *Ibid*

commonly seen in product or service sales, should be governed by the Information Technology Act, of 2000.[18]

- The definition of a 'disguised advertisement' is clear, but the need for an additional restriction to regulate a practice that is already addressed by a specific regulation appears dubious, particularly in light of the Advertising Standards Council of India's proposed more detailed guidelines on advertising.[19]
- Business tactics that are commonly described as 'subscription traps' include requesting consumers to give payment data or granting auto debit authorization for free subscriptions. Several free trials necessitate 'penny drop' verifications of payment methods to validate the legitimacy of payment for prospective subscribers.

The aforementioned concerns go beyond regular drafting considerations; lack of accuracy would hinder the effective execution and compliance with the regulations, and place an undue burden on the standard appeals procedure—more specifically, the appeals to higher courts from CCPA (Central Consumer Protection Authority) decisions. To effectively address the issue of dark patterns, it is important to implement a fair and targeted strategy. This will help prevent any unintended repercussions on authentic content, market practices, and technological progress, in the fast-paced digital environment.

CONCLUSION

The phenomenon of Dark Patterns, as mentioned previously is not a recent concept and has been present in physical form for a prolonged time. In the current era of rapidly progressing technology and artificial intelligence, numerous studies indicate that dark patterns pose a substantial threat to consumers. Enacting laws is essential to safeguard the interests of consumers. Numerous countries globally have enforced steps to combat dark patterns, and India has recently proposed guidelines to tackle this problem as well. However, the regulations enforced by the Indian government seem to be relatively ambiguous and have various implications in terms of their implementation, which could potentially hinder advancement.

[18] Prabhu (n 15)
[19] *Ibid*

Hence, India needs to enact a concise, transparent, and pragmatic regulation to regulate dark patterns.

SUGGESTIONS

To create a comprehensive and influential policy and framework, policymakers and government officials should analyse foreign legislation and precedents that have shaped the implementation of Dark Pattern rules and regulations. This investigation will offer useful insights into the effective regulation of such practices in other nations. Moreover, it is crucial to review the present condition of dark patterns in India and determine the sufficiency of existing consumer protection regulations. This assessment will ascertain the necessity of implementing new rules and regulations. It is essential to conduct a thorough study of different online platforms to obtain a profound awareness of the existing situation and the threat of dark patterns in India. This will help in formulating or modifying rules effectively.