DARK PATTERNS AND CONSUMER BEHAVIOUR: A STUDY MAPPING THE MINDSET OF THE CONSUMER THROUGH CRITICAL ANALYSIS

DR. MARIA GORETTI SIMOES
Assistant Professor (Selection Grade) and Officiating Principal, G. R Kare College of Law, Margao Goa

Abstract
The term' dark patterns' refers to elements that tend to deliberately mislead, coerce, and, most of the time, deceive users or visitors of websites into making harmful decisions and making unintended choices. Dark patterns are found on many websites and are used by almost all organisations. They are deceptive labelled buttons/tabs on the system that are difficult to 'undo' once into it. How the elements appear on screen in attractive colours, designs, shades, and labelling draws the users' attention away from confident choices or options. These dark patterns are a common sight for online subscriptions offering free trials for all kinds of goods and services. The use of dark patterns in advertising and its onslaught on the advertising sector makes it extremely difficult, sometimes impossible, for a customer to unsubscribe from the use of the service or eventually convert a free trial into a paid subscription.
To illustrate the kinds of design practices and to demonstrate the harmful effects caused on the consumers, the author, through the hypothesis, placed on record the different kinds of designs, the impact that it has on consumers, a brief analysis of the laws internationally and the empirical data to substantiate what could be done to protect consumers getting lured into such elements is effectively explained.
Keywords: *Dark patterns, meaning, kinds, protection of consumers, measures to regulate, data collection and its analysis.*

1. INTRODUCTION

Dark patterns refer to online user interfaces that intentionally undermine, manipulate, or hinder user autonomy, decision-making, or choice[1]. These are utilized in electronic commerce, mobile applications[2], online shopping platforms, social networking sites[3], and for privacy notifications[4]. Dark patterns commonly encompass deceptive tactics, such as the utilization of misleading statements like "Only 1 left!" (known as Exploding offers), the employment of trick questions that manipulate individuals into providing unintended answers (Trick questions), interfaces that deliberately impede users from exiting a screen, declining an offer, or canceling a subscription (Roach motel), and manipulative techniques that induce feelings of shame or guilt in users for not accepting or opting into a service (Confirm shaming).
The influence of dark patterns extends beyond the simple manipulation of online shopping decisions. Individual autonomy can be compromised by diminishing privacy and a decline in decision-making authority[5]. In a broader sense, economic and societal inefficiencies can occur when individuals and

[1] "Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces. Queue, 18(2), 67-92."
[2] "Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020, April). UI dark patterns and where to find them: a study on mobile applications and user perception. In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-14).
[3] Mathur A, A Narayanan, and M Chetty, 2018. 'Endorsements on Social Media: An Empirical Study of Affiliate Marketing Disclosures on YouTube and Pinterest' (2018) Proceedings of the ACM on Human-Computer Interaction
[4] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-13).
[5] Spencer, S. 2020. 'The Problem of Online Manipulation' (2020) U Ill L Rev 959, 990.

consumers do not effectively express their preferences or are compelled to undertake expensive and unproductive self-protection actions that reduce overall well-being.

Dark patterns can be distinguished from other innocuous or beneficial online nudges by their explicit goal and major beneficiary. Online nudging, also known as benign 'patterns', aims to help consumers overcome decision-making biases to increase their well-being and achieve their long-term goals. In contrast, dark patterns are designed to confuse or hide consumers' decision-making processes to benefit the merchant or online service provider, typically at the user's expense.

Scholars and authorities have used competing classifications to distinguish dark patterns from positive nudges. We focus on a few dark patterns used by online sellers to influence customers' decisions in this study.

The current body of research does not provide a definitive response to this inquiry. Several studies have shown that individuals with lower levels of education are more vulnerable to dark patterns[6]. However, other studies have found no association between the ability to detect dark patterns and factors such as age, employment status, or level of education. Various regions throughout the globe are currently implementing distinct policies that exhibit divergent stances towards individuals requiring safeguarding. Dark patterns, as seen by the US Federal Trade Commission[7], can disproportionately affect lower-income customers or other vulnerable demographics, leading to a more significant impact[8]. In contrast, the recently implemented Digital Services Act[9] (DSA) in the European Union operates under the assumption that all users are vulnerable to dark patterns and therefore completely bans them.

2. LITERATURE REVIEW

2.1 Decision-making biases

An extensive range of work explores the ways in which customers might be controlled and affected by commercial techniques that aim to exploit biases in decision-making or capitalize on commonly used decision-making shortcuts[10]. Research in the field of behavioral economics has demonstrated that these biases are both systematic and predictable[11]. Occasionally, these techniques are intended to enhance consumer well-being, such as when a business or government agency attempts to subtly influence a consumer to make a decision that benefits them in the long run[12]. However, when it comes to dark patterns, the main goal of the manipulations is typically to weaken consumer choice in a manner that harms their well-being and broader interests. This research specifically addresses the detrimental manipulation that occurs in the internet environment.

Research shows that decision-making biases or heuristics are constant and predictable, although they are often hard to spot. Thus, studies on consumer vulnerability to harmful manipulation have focused on easily apparent qualities including age, income, education, and other demographic factors connected to such biases. Specific consumer groups, such as the elderly or those in financial need, are thought to have biases and are more susceptible to negative manipulation. Consumer groups with unique characteristics have different levels of 'vulnerability' The 'victim approach' holds that certain

[6] Luguri J and LJ Strahilevitz, 2021. 'Shining a Light on Dark Patterns' (2021) 13 Journal of Legal Analysis 43."

[7] "Federal Trade Commission | Protecting America's Consumers

[8] FTC, 2022. 'Bringing Dark Patterns to Light' (Staff Report: September 2022) https://www.ftc.gov/reports/bringing-dark-patterns-light

[9] Digital Services Act, Regulation (EU) 2022/2065

[10] Hanson J and D Kysar, 1999. Taking Behvioralism Seriously: The Problem of Market Manipulation' 74 NYU L Rev 630.

[11] Ariely, D. 2009. Predictably Irrational: The Hidden Forces That Shape our Decisions (Harper Collins, 2009)

[12] Thaler RH and Sunstein CR, 2008. Nudge: Improving Decisions About Health, Wealth, and Happiness (Yale Univ. Press)"

groups of people need special protections due to their fragility and/or inability to advocate for themselves.[13].

However, the idea that only some client categories are prone to biases and decision-making characteristics is being challenged. An thorough survey of US panel data by Stango and Zinman[14] (2020) found that biases are frequent. The median consumer has 10 of 17 biases, and most people have multiple biases. They also find that demographic factors cannot explain cross-consumer bias variation. The fact that bias was more variable within classical sub-groups often utilized as indicators of consumer susceptibility than across them is noteworthy for our investigation. For instance, Stango and Zinman found higher bias variation within the highest-education group than between it and the lowest-education group. This survey shows that all consumers have preconceptions that can be used and influenced.

2.2 Online consumer vulnerability

The advancements in the digital economy, the emergence of big data analytics, and the capacity to specifically target internet users have sparked a discussion about the appropriate extent of consumer protection in the online realm.

Several studies suggest that our perceptions of time and space are altered in the online environment. Additionally, the excessive amount of information available online increases the likelihood of consumers relying on heuristics to make decisions, opting for simplified choices, and paying less attention compared to offline settings[15]. Contrary to consumer perception, others suggest that the online world actually offers a limited selection of choices, despite the illusion of greater possibilities[16]. This is due to the fact that the consumer's experience is influenced by a regulated environment consisting of customized buttons to activate, checkboxes to select, swipeable alternatives, and information to quickly read. The progress in data gathering, processing, and analytics is leading to a change in the way time is perceived. In today's day of constant exposure to screens, any offer or opportunity is readily accessible through algorithms[17].

The online environment is characterized by stealth and personalization. Research has shown that many online consumers are often unaware of the degree to which their online experiences are customized to them and can be modified to align with a 'persuasion profile'[18]. Although certain studies indicate that consumers perceive online environments as safer than offline ones[19], a significant number of consumers remain unaware of the deliberate manipulation and influence on their decision-making process[20].

The emerging dynamics on the internet provide a substantial obstacle to the conventional comprehension of customer susceptibility. Indeed, in digital markets, consumer vulnerability is perceived as a state of defencelessness and susceptibility to power asymmetries, which strongly

[13] "Cole, A. (2016). All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an ambivalent critique. Critical Horizons, 17(2), 260-277.

[14] Stango, V and J Zinman, 2020. We are all Behavioral, More or Less: A Taxonomy of Consumer Decision Making' NBER Working Paper No. 28138 (November 2020)

[15] CMA, 2020. 'Online Platforms and Digital Advertising.– Appendix Y: choice architecture and Fairness by Design' Market study final report (1 July 2020)

[16] Costa, E., & Halpern, D. (2019). The behavioural science of online harm and manipulation, and what to do about it. The Behavioural Insights Team."

[17] "Calo, R. 2014. 'Digital Market Manipulation', 82 Geo. Wash. L. Rev. (2014).1018

[18] Susser, B Roessler and H Nisssenbaum, 2019. Online Manipulation: Hidden Influence in a Digital World' (2019) 4 Geo L Tech Rev 1, 33

[19] Moran, N. 2020. 'Illusion of safety: How consumers underestimate manipulation and deception in online (vs. offline) shopping contexts' (2020) 54 J Consum Aff 890.

[20] Marchiori, D. R., Adriaanse, M. A., & De Ridder, D. T. (2017). Unresolved questions in nudging research: Putting the psychology back in nudging. Social and Personality Psychology Compass, 11(1), e12297.

favour the digital choice architects[21]. According to Calo[22] (2014), internet commerce is equipped with data-driven, dynamically configurable, and personalized decision architectures that are designed to deduce or even fabricate vulnerabilities. Essentially, consumers may mistakenly believe that they have control and are safer in an online setting, but this perception may be deceptive as online service providers exploit technical improvements to achieve their own objectives.

2.3 Dark patterns and online consumer vulnerability

There is a limited yet expanding corpus of empirical research that has investigated the utilization and impacts of dark patterns on customers. Several research have aimed to establish a classification system for various categories of dark patterns or have focused on determining the frequency of dark patterns[23]. Although the prevalence and characteristics of dark patterns may differ among websites, apps, and countries, collective research indicates that black patterns are not limited to a certain niche but rather are widespread in practice[24]. Another series of studies has specifically examined the efficacy of dark patterns, including certain sorts of dark patterns, in influencing customer decision-making.

The developing evidence is pertinent to our study since it examines whether dark patterns can have varying effects on customers, based on common variables such as income, age, education, and so on. The existing research, however scarce, provides a few (sometimes contradictory) observations. Several research examine the impact of age on a consumer's vulnerability to dark patterns, specifically youngsters and older consumers. Bongard-Blanchy[25] et al. (2021) discovered that individuals with lower levels of education are particularly susceptible to dark patterns. In contrast, the European Commission[26] (2022) determined that vulnerable consumers are more prone to making inconsistent choices compared to average consumers when they encounter dark patterns. Conversely, Di Geronimo et al. (2020) discovered no indication of a correlation between the capacity to identify dark patterns and factors such as age, employment situation, or educational attainment.

To understand the lack of consistency in these developing findings, it is crucial to examine the methodological approaches used in these research and their resemblance to a real-world choice and decision-making setting. Bongard-Blanchy[27] et al. (2021) conducted studies where they administered online surveys to evaluate participants' capacity to identify various forms of dark patterns. They also sought participants' opinions on the usefulness of different dark patterns. The study conducted by the European Commission in 2022 utilized a survey methodology and incorporated an online experiment in which participants were tasked with selecting between two distinct digital entertainment service bundles. If their selection aligned with their explicitly stated preferences, they were awarded a specific quantity of points.

We prefer this method to 'lab tests' that don't correctly imitate dark patterns. However, while Luguri and Strahilevitz's experimental design is similar to ours, our methods differ in one critical area for understanding both studies' results. In a study, participants were informed that they had been enrolled in an expensive identity theft protection program without their agreement and would have to pay unless they declined. Participants were told the website used their IP address and zip code to accurately determine their postal address. They also learned that after six months of free theft

[21] Helberger, N., Lynskey, O., Micklitz, H. W., Rott, P., Sax, M., & Strycharz, J. (2021). EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets, A joint report from research conducted under the EUCP2. 0 project. X

[22] Ibid 18

[23] Mills, S., Whittle, R., Ahmed, R., Walsh, T., & Wessel, M. (2023). Dark patterns and sludge audits: An integrated approach. Behavioural Public Policy, 1-27."

[24] "OECD, 2022. 'Dark Commercial Patterns' OECD Digital Economy Papers, October 2022 No. 336

[25] Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021, June). " I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!"-Dark Patterns from the End-User Perspective. In Designing Interactive Systems Conference 2021 (pp. 763-776).

[26] European Commission, 2022. 'Behavioural study on unfair commercial practices in the digital environment'. Final Report

[27] Ibid 26"

protection, they would be paid monthly to the same address. In our trial, individuals had to voluntarily purchase the service using a credit card or PayPal. The offer required an instant payment and did not include free subscription time. Since a payment page better resembles real-world settings, the design difference greatly affects the experiment's legitimacy and strength.

3. How do the Dark Pattern Guidelines Interface with the Existing Scheme of Regulations in India?

The Consumer Protection Act in India serves as the comprehensive legislation that safeguards the welfare and rights of customers.[28] The primary objective of the Consumer Protection Act[29] is to safeguard consumers from 'unfair trade practices'[30] and 'restrictive trade practices'[31], as well as to address issues related to product liability[32] (where applicable) and provide remedies for consumer concerns.[33] CCPA (The Central Consumer Protection Authority) has published numerous laws and recommendations to regulate various aspects, such as e-commerce and misleading ads.

Despite India's strong consumer protection framework, dark pattern practices have persisted and grown, requiring targeted action. The Dark Pattern Guidelines have tried to match with Indian consumer protection laws, however their influence and legality may be disputed. The Dark Pattern Guidelines highlight the use of purpose to deceive a user, which is subjective and cannot be objectively measured. Additionally, the Dark Pattern Guidelines appear to cover all 'users' rather than just 'consumers', which may be important at present. When examined closely, these guidelines, especially the definition of 'dark patterns' that links deceptive design practices to consumer interests, reveal that they are designed and implemented solely to protect 'consumers'. Primary legislation may limit this. The Dark Pattern Guidelines[34] may not cover all dark patterns in the digital age. Only design practices that contribute to deceptive ads, unfair commercial practices, or consumer rights violations are covered by these standards.

The Dark Pattern Guidelines do not provide the CCPA with the authority to take action against any violation of the Dark Pattern Guidelines, as outlined in the Consumer Protection Act. This is a departure from the previous draft, which allowed for stakeholder feedback. While the Consumer Protection Act[35] grants the CCPA significant authority to take actions for the safeguarding of consumer rights[36], the rules and guidelines that are issued as a result usually include specific penalties that empower the CCPA to take action against any violation of these rules or guidelines. The inclusion of such punitive measures is necessitated by the lack of residual authority afforded to the CCPA under the Consumer Protection Act to take action in instances of such violations. The omission of this particular section from the final version of the Dark Pattern rules may imply a lack of legal repercussions for failing to adhere to these rules, thereby weakening the authority of the CCPA.

In order to effectively reduce the prevalence of dark patterns in the market and beyond, it is crucial for the government to address how these patterns can undermine the Information Technology Act, 2000[37] ("IT Act"), the Information Technology (Intermediary Guidelines and Digital Media Ethics Code)[38], 2021 ("Intermediary Rules"), and the recent Digital Personal Data Protection Act, 2023

[28] "Section 2(7) of the Consumer Protection Act
[29] The Consumer Protection Act, NO. 35 OF 2019
[30] Section 2(47) of the Consumer Protection Act
[31] Section 2(41) of the Consumer Protection Act
[32] Section 2(34) of the Consumer Protection Act
[33] Section 9(v) of the Consumer Protection Act.
[34] The Guidelines for Prevention and Regulation of Dark Patterns, 2023"
[35] "Ibid
[36] Section 18 of the Consumer Protection Act.
[37] Information Technology Act, 2000
[38] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Vide G.S.R. 139(E)."

("DPDPA"). The implementation and success of the Dark Pattern Guidelines should be ensured to achieve this goal.

Interministerial collaboration and a complete effect analysis on dark pattern management may be needed to attain this goal. To close dark pattern gaps, existing laws need more linkages. These include (i) restricting the use of dark patterns like nagging, confirm shaming, trick questions, interface interference, and forced actions, which can undermine the DPDPA's consent requirements; and (ii) preventing malicious software, as outlined in the Dark Pattern Guidelines, from disrupting or damaging computer networks, tampering with computer-sourced documents, etc.

Therefore, due to the interconnectedness of these laws, it is crucial to establish a connection and correlation between the Dark Pattern Guidelines and the DPDPA[39], IT Act[40], and their respective rules, including the Intermediary Rules, in order to comprehensively regulate Dark Patterns.[41]

Although the CCPA invited stakeholder opinion on dark pattern preliminary regulations, it appears that public criticisms on regulatory overlaps, lack of precision, and excessive restrictiveness have not been addressed. The Dark Pattern Guidelines' first draft was barely altered by the CCPA. These changes weaken the Dark Pattern Guidelines by linking 'commercial gains' only to specific dark patterns like confirm shaming and nagging, adding three new dark patterns (trick questions, SaaS billing, and rogue malware), and removing the guideline that the Consumer Protection Act will apply in cases of Dark Pattern Guidelines violations.

4. Comparison between the Dark Pattern Guidelines in India and Abroad?

When comparing the Dark Pattern Guidelines with similar guidelines in other jurisdictions, it is clear that there is still more to be explored in terms of legal principles and their implications for dark patterns in India. The European Union's Digital Services Act[42] of 2022 provides a definition of dark patterns as "practices that intentionally or unintentionally significantly hinder or impair the ability of service users to make independent and well-informed choices or decisions." These tactics can be employed to influence the recipients of the service to participate in undesirable behaviors or make unfavorable decisions that result in negative outcomes for them.[43] Similarly, a report published by the Federal Trade Commission ("FTC") of the United States defines dark patterns as "design strategies that deceive or manipulate users into making decisions they would not have made otherwise, potentially resulting in negative consequences." Both of the mentioned jurisdictions have considered the importance of including a materiality qualifier to address the effects of dark patterns on consumers/users. This inclusion can aid in more effective enforcement by objectively assessing the impact of these practices on the user.

Moreover, dark patterns have been considered to have a negative impact, specifically in relation to privacy, data security, and user autonomy as outlined in the California Consumer Privacy Act[44] of 2018. This act establishes guidelines for obtaining legal permission from users by forbidding the use of double negative wording, which might hinder a user's ability to choose privacy protection options or make the process of unsubscribing or canceling a sale burdensome.[45] Noncompliance with these criteria is indicative of the utilization of dark patterns by a firm. The California Consumer Privacy Act[46] defines a user interface as a dark pattern if it significantly undermines or hinders the user's autonomy, decision-making, or choice, as described earlier.[47] An intricate strategy to tackling privacy-related issues is important in India, especially considering the imminent implementation of the DPDPA[48].

[39] "ibid
[40] ibid
[41] Section 43(c) of the IT Act, 2000; Section 65 of the IT Act, 2000.
[42] The Digital Services Act (Regulation (EU) 2022/2065, DSA)
[43] Recital 67 of the EU Digital Services Act of 2022"
[44] "California Consumer Privacy Act of 2018, 1798.100
[45] section 7004(a), California Consumer Privacy Act Regulations, effective from March 29, 2023
[46] ibid
[47] section 7004(c), California Consumer Privacy Act Regulations, effective from March 29, 2023
[48] Ibid"

4. CONCLUSION

In spite of the fact that the CCPA's initiative to regulate dark patterns in India is unquestionably a step in the right direction, it is possible that more measures will be required to address the deeply ingrained and long-standing dark pattern habits. In order to effectively govern dark patterns, it is imperative that the data protection and e-commerce legislations in India be seamlessly integrated with the Dark Pattern Guidelines. This is a pressing demand. Due to the fact that this legislation is still in its infancy, it is reasonable to anticipate that it will develop over time and become more successful in addressing the concerns with dark patterns.

REFERENCES

ARTICLES

[1] Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M., Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces. (2020) Queue, 18(2), 67-92.

[2] Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A., UI dark patterns and where to find them: a study on mobile applications and user perception. (2020) In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-14).

[3] Mathur A, A Narayanan, and M Chetty, 'Endorsements on Social Media: An Empirical Study of Affiliate Marketing Disclosures on YouTube and Pinterest' (2018) Proceedings of the ACM on Human-Computer Interaction

[4] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L., Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. (2020) In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-13).

[5] European Commission, 'Behavioural study on unfair commercial practices in the digital environment' (2022). Final Report

[6] Spencer, S. 'The Problem of Online Manipulation' (2020) U Ill L Rev 959, 990.

[7] Luguri J and LJ Strahilevitz, 'Shining a Light on Dark Patterns' (2021) 13 Journal of Legal Analysis 43.

[8] FTC, 2022. 'Bringing Dark Patterns to Light' (Staff Report: September 2022) https://www.ftc.gov/reports/bringing-dark-patterns-light

[9] Digital Services Act, Regulation (EU) 2022/2065

[10] Hanson J and D Kysar, Taking Behvioralism Seriously: The Problem of Market Manipulation' 1999, 74 NYU L Rev 630.

[11] Ariely, D. 2009. Predictably Irrational: The Hidden Forces That Shape our Decisions (Harper Collins, 2009)

[12] Thaler RH and Sunstein CR, 2008. Nudge: Improving Decisions About Health, Wealth, and Happiness (Yale Univ. Press)

[13] Cole, A., All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an ambivalent critique. (2016) Critical Horizons, 17(2), 260-277.

[14] Stango, V and J Zinman, We are all Behavioral, More or Less: A Taxonomy of Consumer Decision Making' 2020, NBER Working Paper No. 28138 (November 2020)

[15] CMA, 'Online Platforms and Digital Advertising.– Appendix Y: choice architecture and Fairness by Design'2020, Market study final report (1 July 2020)

[16] Costa, E., & Halpern, D., The behavioural science of online harm and manipulation, and what to do about it. (2019) The Behavioural Insights Team.

[17] Calo, R., 'Digital Market Manipulation', 82 Geo. Wash. L. Rev. (2014).1018

[18]Susser, B Roessler and H Nisssenbaum, Online Manipulation: Hidden Influence in a Digital World' (2019) 4 Geo L Tech Rev 1, 33

[19] Moran, N., 'Illusion of safety: How consumers underestimate manipulation and deception in online (vs. offline) shopping contexts' (2020) 54 J Consum Aff 890.

[20] Marchiori, D. R., Adriaanse, M. A., & De Ridder, D. T., Unresolved questions in nudging research: Putting the psychology back in nudging. Social and Personality Psychology Compass, (2017) 11(1), e12297.

[21] Helberger, N., Lynskey, O., Micklitz, H. W., Rott, P., Sax, M., & Strycharz, J., EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets, (2021) A joint report from research conducted under the EUCP2. 0 project. X
[22] Mills, S., Whittle, R., Ahmed, R., Walsh, T., & Wessel, M., Dark patterns and sludge audits: An integrated approach. (2023) Behavioural Public Policy, 1-27.
[23] OECD, 'Dark Commercial Patterns' OECD Digital Economy Papers, 2022, October 2022 No. 336
[24] Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G.. " I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!"-Dark Patterns from the End-User Perspective. (2021) In Designing Interactive Systems Conference 2021 (pp. 763-776).

LAWS AND STATUTES

[1] Section 2(7) of the Consumer Protection Act
[2] The Consumer Protection Act, NO. 35 OF 2019
[3] Section 2(47) of the Consumer Protection Act
[4] Section 2(41) of the Consumer Protection Act
[5] Section 2(34) of the Consumer Protection Act
[6] Section 9(v) of the Consumer Protection Act.
[7] The Draft Guidelines for Prevention and Regulation of Dark Patterns, 2023
[8] Section 18 of the Consumer Protection Act.
[9] Information Technology Act, 2000
[10] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 20211, Vide G.S.R. 139(E).
[11] Section 2(k) of the IT Act, 2000
[12] Section 43(c) of the IT Act, 2000; Section 65 of the IT Act, 2000.
[13] The Digital Services Act (Regulation (EU) 2022/2065, DSA)
[14] Recital 67 of the EU Digital Services Act of 2022
[15] California Consumer Privacy Act of 2018, 1798.100
[16] section 7004(a), California Consumer Privacy Act Regulations, effective from March 29, 2023
[17] section 7004(c), California Consumer Privacy Act Regulations, effective from March 29, 2023