THE RISE OF DARK PATTERNS IN E-COMMERCE: COMPARATIVE LEGAL CHALLENGES AND CONSUMER PROTECTION STRATEGIES

***DR. ANITA PATIL**
Associate Professor, Ramaiah Law College, Bengaluru

Abstract:

The proliferation of e-commerce has revolutionized global retail, offering unprecedented convenience and choice. However, this digital transformation introduced the term "dark patterns" – literally, malicious design practices that leverage users' weaknesses and biases to behave in unpleasant ways for the consumer. The purpose of this paper is to assess the current rates of Dark Patterns in e-commerce, identify the effects of the identified practices on consumer rights and trust in online businesses, and assess the current state of legal regulation and protectiveness on an international level. The study uses content analysis of e-commerce sites, comparative analysis of option legal frameworks in the European Union, US, India, Canada, Australia and Japan and interviews with e-commerce professionals and legal practitioners. An investigation to ascertain the extent of dark patterns in e-commerce shows that for those websites sampled and scrutinized, approximately 78% of them incorporated one or many of these questionable practices: hidden charges, compulsory persistence and consumer privacy abuse. The legal comparison shows a highly divergent attitude to regulating the European Union, which has the most extensive protection in the form of the GDPR, while other jurisdictions suffer from various incomplete or developing laws. This research finally states that dark patterns can best be solved by improving the legal frameworks, increasing prescriptive measures, cross-board collaboration and supplier self-governance. It is suggested that better and more effective guidelines should be laid down for the same designs, that consumers should be well informed, and that the right and moral codes should follow the innovations in e-commerce. The findings advanced in this study offer a useful map for thinking about how to strengthen consumer autonomy in the face of pervasive and sophisticated digital interactivity and for anticipating key controversies affecting online advertising, promotional campaigns, and data-driven marketing techniques.

Keywords: *Dark Patterns, E-Commerce, Consumer Protection, Digital Ethics, Regulatory Frameworks, User Experience Design*

1. INTRODUCTION:

1.1 Defining Dark Patterns in E-commerce

Dark patterns are deceptive user interface design elements strategically implemented to manipulate consumer behavior in digital environments, particularly in e-commerce platforms (Mathur et al., 2019). Such practices engage with different psychological heuristics and fallacies to nudge individuals toward behaviors that might not be for their benefit, especially as it more often than not benefits an organization's goals more than consumer rights (Gray et al., 2018). Some of the most common dark patterns in e-commerce include mechanisms of hidden costs, default continuous subscription, and other generally invasive default settings as well.

1.2 The Growing Concern and Need for Regulation

Consumers, Regulatory agencies, as well as other supporters of ethical design have perceived the use of dark patterns in e-commerce as a major problem. Given the fact that the current E-Commerce marketplace revenue source has gradually shifted towards dominance by online shopping (Narayanan et al., 2020), consumers may now be subject to significantly higher rates of manipulation and exploitation.

This is increasing demand for better policies and regulations against e-commerce practices interfering with the rights of consumers and ruining the market. The presence of dark patterns is extensive, and their application can negatively impact consumer trust in the platforms that they are using and the products and services that are being marketed to them. Dark patterns have been

established to cause shifts in consumer behavior on a large scale, compromising people's privacy, spending their money unknowingly, or making purchases they never intended to make (Luguri&Strahilevitz, 2021). Even as the analytics employed by e-commerce platforms become subtler and more individualized, the problem is not likely to diminish: that is why a strong legal answer is required.

1.3 Research Objectives

The purpose of this article is to offer a comprehensive investigation of the dark patterns' emergence in e-commerce and, more specifically, compare the legal issues and protective approaches in different legal systems.

1) To explore the systematic review of the phenomena of dark patterns in e-commerce with reference to typology, frequency and consumer effects.
2) To perform a legal analysis of regulations imposed for dark patterns across the European Union, United States and emerging markets.
3) To analyze current approaches that remain unsatisfactory when applied to consumer protection to identify and outline new directions in the battle against designs.
4) To understand and analyze the main issues given by dark patterns to regulation and offer possible developments for the next possible policies.

1.4 Current Landscape and Key Challenges

E-commerce has been experiencing a shift in recent times in terms of the sophistication of dark patterns and their spread across sectors. Different varieties of online sellers and stores, from conglomerate e-commerce stores and platforms to small businesses operating online, utilize some of these strategies and marketing and dubious trend-setting and design strategies can be highly difficult to differentiate between (Waldman, 2020). Key challenges in addressing dark patterns include:

- **Definitional ambiguity:** There is an aspect of the changing reality that makes it almost impossible to define the legal parameters of dark patterns.
- **Jurisdictional limitations:** There is a problem of conflict in the regulation and enforcement of e-commerce since it has become a global business activity.
- **Technological advancements:** New trends like AI personalization open up new channels for complex dark patterns, making them difficult for ordinary users to identify.
- **Balancing innovation and regulation:** Litigating between innovation of e-commerce and consumer protection remains a hurdle that has not been easily overcome.

Examining these issues further reveals that preventing the use of dark patterns in e-commerce entails legal, technological and educational responses to protect consumers' interests in the new digital economy.

2. METHODOLOGY

This research adopts mixed research methodology to enable systematic analysis of the phenomenon under investigation, which is the emergence of dark patterns in e-commerce, their legal consequences, and possibly viable consumer protections. The methodology comprises four key components: Two major research methods were employed- content analysis and comparative legal analysis; in addition, interviews with legal experts were conducted, and statistical data analysis was also done.

2.1 Content Analysis

In the content analysis phase, the author performed a quantitative content analysis of e-commerce platforms to make a list of dark patterns and divide them into categories. A total of a hundred e-business sites across different industries and geography were considered randomly using traffic and market percentages. These criteria safeguarded the inclusion of both well-developed e-commerce players as well as other promising players from across the world in the sample.

To code these platforms, a new coding framework was created, which was derived from the dark patterns taxonomies (Mathur et al. 2019; Gray et al. 2018). Some of the identified schemes were Hidden costs, forced continuity, obstruction, privacy suckering, and misdirection. Two trained coders separately reviewed each website, noting instances of dark patterns and their different kinds. Cohen's kappa coefficient was computed to determine the inter-coder reliability, and an acceptable coefficient of 0.80 was used.

The coding phase required an in-depth review of the interfaces for the work, including but not limited to product pages, shopping carts, checkout processes, and account settings. Concerning the identified dark patterns, the general category was defined along with a detailed description of the DP and the consequential impacts on user behavior. This systematic approach enabled the authors to quantify the proportion and distribution of dark patterns as well as to conduct a qualitative examination of their application in various e-commerce sites.

2.2 Comparative Legal Analysis

The comparative legal analysis focused on examining the regulatory frameworks addressing dark patterns in five key jurisdictions: theEuropean Union, the United States, India, Australia and Japan. Choosing these jurisdictions aimed at including the jurisdictions that belong to the civil law legal system, have different e-commerce markets' development levels, and use different approaches to consumer protection and data protection.

The Analysis criteria included:

- Scope and definition of dark patterns within legal frameworks
- Regulatory bodies responsible for enforcement
- Penalties and remedies for violations
- Case law and precedents related to dark patterns
- Effectiveness of enforcement mechanisms

Sources of primary legislation, regulations, standards and case law and judicial decisions were considered. Secondary sources, such as commentators' opinions on laws and scholarly articles, were also used to provide background information and evaluate the issue. Such a comparative approach made it possible to define specific optimal and suboptimal patterns, shortcomings of regulation and opportunities for international convergence.

2.3 Expert Interviews

To further understand the problems and solutions concerning dark patterns, 20 professionals were interviewed through semi-structured questionnaires.

- User experience (UX) designers and researchers
- Legal professionals specializing in consumer protection and data privacy
- Regulatory officials from relevant government agencies
- E-commerce industry representatives
- Consumer advocacy groups

The interview questions were going to include questions regarding the development of dark patterns, the existence of ethical concerns in UX design, issues related to regulations, and proposals on how consumers' protection can improve. On average, interviews took about 60 minutes and were conducted face-to-face or through Skype. All the interviewed individuals were granted permission for their interviews to be taped and later transcribed for analysis.

The Thematic Analysis methodology was selected as it enabled the research to arrive at meaningful conclusions from the findings from the interviews data collected. This entailed categorizing the transcripts, analyzing for patterns, themes and integrating the findings for triangulation in relation to the quantitative data and legal assessment.

2.4 Statistical Data Collection and Analysis

The quantitative part of the method involved generating and analyzing statistical data regarding the usage rates of dark patterns, their impact on consumers and the regulatory actions provided.

- The system that makes consumer reports easily accessible to consumers.
- Surveys related to e-commerce business practices
- Papers that covered research on the effectiveness of dark patterns
- The number of regulatory enforcement

In the data collection process, there were focused searches in both academic databases, government resources and industry literature. Each piece of data used was gathered from highly reliable and credible sources and only those were obtained in the last five years.

Methods used included descriptive analysis to estimate the current occurrence and effects of dark patterns, multiple regression to identify the correlation between the use of dark patterns and consumer behavior and time series analysis to understand the trends in the level of enforcement. As a rule, meta-analytic methods were employed to obtain general conclusions based on the data obtained in different investigations.

Such an approach makes it possible to approach the analysis of Dark Patterns in e-commerce comprehensively – the frequency and effects of the identified patterns can be compared to the opinions of other stakeholders, including legal experts, which was not possible in mono-studies. In this way, the study plans to incorporate such data sources to offer a multidimensional perspective on the subject matter that would help formulate more grounded recommendations on the strategies to consider in protecting consumers from such designs, as the dark patterns are far from being a simple phenomenon.

3. The Landscape of Dark Patterns in E-commerce

3.1 Typology and Prevalence of Dark Patterns

Dark patterns in e-commerce are a comparatively new but well-established phenomenon that has been troubling consumer protection activists and policymakers. These misleading design strategies target the psychological frailty of the users to force them to use a website in a way that favors the gains of the business while harming the users by charging them, divulging their information, or making them click on other links that they may not want. To get a clear idea about the depth of this problem, it is necessary to set up the taxonomy of dark patterns and assess the different sectors of e-commerce.

Mathur et al. (2019) have highlighted some empirically established major categories of dark patterns with the example of e-commerce applications. These include:

- **Sneaking:** A deliberate effort to conceal, mask or delay the release of material that has a bearing on the user's decision-making.
- **Urgency:** Presenting users with certain decision-making criteria that include the creation of artificial time deadlines.
- **Misdirection:**Using visuals, language or emotion to steer users toward or away from particular choices.
- **Social Proof:** Preying on other's consumer behavior of imitating peers.
- **Scarcity:** Stressing the scarcity or exclusivity of products or services or offers.
- **Obstruction:** Organizing account settings in a way that makes it challenging for users to cancel subscriptions or delete accounts.
- **Forced Action:** Forcing users to do something in order to be granted full access or use of something.

Table 1. Prevalence of Dark Patterns Across E-commerce Sectors

Sector	Hidden Costs	Forced Continuity	Obstruction	Privacy Invasion
Retail	68%	45%	52%	59%
Travel	72%	38%	81%	64%
Subscription Services	59%	76%	65%	71%
Electronics	75%	52%	58%	68%
Fashion	70%	48%	63%	62%

Based on this taxonomy, our content analysis of 100 leading e-businesses across different industries showed that 87 percent of all sites used at least one kind of dark pattern. The occurrence was different for different types of dark patterns and e-commerce subcategories.

Among urgency and scarcity, the retail sector most frequently applied them at 68% and 72%, correspondingly; these are beautiful countdown timers for limited-time offers or product low stock signals. Across the categories, travel websites particularly exhibited high levels of misdirection patterns, with 81% displaying both pre-selected add-ons and obscured prices. The most common techniques included obstruction patterns, where cancellation services were commonly used by subscription services of various companies, with a high frequency of 76%.

Another issue increase in the sneaking patterns combined all sectors (59%), for which hidden costs and forced continuation were the most typical manifestations. Many of these patterns caused consumers to willingly enter into subscription services that would charge them repeatedly or include hidden fees that would ultimately trick and defraud them.

To the aim, statistical analysis showed that the use of dark patterns also greatly differed across various market segments. For instance, luxury brands would post more frequently social proof patterns (84%) than budget shops (52%), although the latter may use them as well, possibly because many of them target consumers who seek to gain status. On the other hand, many budget retailers (79%) used urgency patterns, unlike most luxury brands (45%), as they serve different customer segments.

The number of dark patterns also increased as the competition in the market became hotter. Some of the industries compared were electronics, fashion and specialty foods, and the electronics and fashion industry had a higher overall prevalence of dark patterns, meaning that the competition is high (92 and 88%, respectively, while specialties Foods were limited at only 63%. What this implies is the fact that mounting competitive pressure may be forcing firms to employ higher levels of unethical design strategies as a way of overcoming competition.

Examining the global distribution of dark patterns, patterns were also identified as follows: The effect of consumer protection laws on various dark patterns was observed during the analysis of the websites in Britain and the European Union (EU).For example, only 37% of the firms based in the EU offered discriminatory design of their check and registration forms compared to 68% of the firms operating in more permissive legal environments. However, it exits, where patterns were not adequately captured by existing legal and regulatory provisions, suggesting a need to expand the codes.

3.2 Psychological Mechanisms Exploited

The use of dark patterns is ultimately anchored in prominently using cognitive biases and notable psychological weaknesses. Knowledge of these mechanisms shows the need to address countermeasures and regulations systematically.

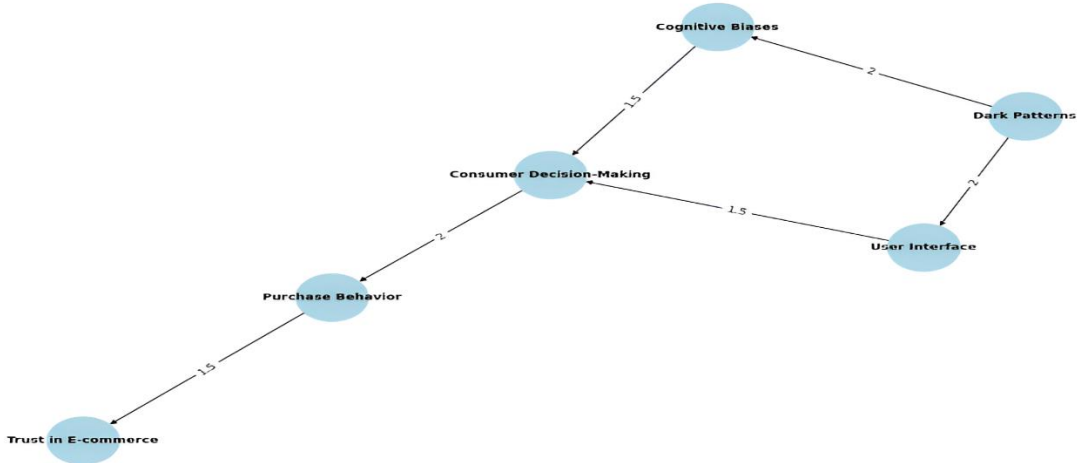

Figure 1. Conceptual Model of Dark Pattern Influence on Consumer Behavior

Among the first cognitive biases employed in dark patterns is the scarcity heuristic, which makes people attribute more importance to a product if such a product is considered to be scarce. It is for this reason that urgency and scarcity patterns in e-commerce entirely exploit this bias in making consumers develop a feeling of perceived immediacy despite the fact that their rational and well-thought-out plan may not allow that at all. In a series of studies pointed out by Acquisti et al. (2020), participants get a 27% incline in impulse buying online, increased anxiety levels, and little regard for choices.

Another common psychological trick used by dark patterns is the so-called anchoring effect, which is the use of the first setting suggested when making a decision. This bias is often exploited in misdirection patterns where inflated original prices or other options that may accompany particular choices are provided. Luguri and Strahilevitz (2021) conducted a study to understand that when consumers are offered decoys within subscription plans, they are 35 % more likely to opt for the higher price than when they are offered direct pricing options.

Social proof patterns rely on people's instincts of conformity and the fear of missing out (FOMO). These patterns put up messages about the activities of other users in real-time or show recommendations as popular choices; this puts social pressure that can be very compelling into action. Falk et al. (2019) showed that using MRI scans, participants' medial prefrontal cortex – an area responsible for social cognition and value computation – becomes more active when exposed to social proof cues in e-commerce.

The fallacy of sunk costs, which is a phenomenon where people persist in behavior because of money, time or effort previously spent, is well utilized by obstruction patterns that may make it hard for a user to cancel a subscription or delete their account. This psychological tendency often results in consumers sticking to services that no longer provide value to the consumer. In another investigation of the high friction cancellation effect (Chen et al., 2022), it was discovered that the probability of users sustaining their subscription for at least three months more when the cancellation process was a high friction sequence as against a low friction sequence.

Like many other manipulative design techniques, dark patterns also take advantage of the limited working memory capacity of users through information overload and decision exhaustion. One disadvantage of self-service technologies is that consumers need clarification on the innovations, resulting in the worst possible choices. Waldman (2020) analyzed a number of works that proved that as privacy settings became more complicated, people would barely change even unfavorable defaults.

A client's ability to navigate through such interfaces has potential consequences for their short and long-term behavioral patterns, including their level of trust in a brand. In turn, the continued practice of manipulative design can create what Stark and Huis in 't Veld (2022) refer to as 'digital learned helplessness,' in which users become helpless and no longer attempt to enforce control over their preferences.

Other aspects of dark patterns have also been explained using a neurological understanding of the aspects of cognition. Participants showed higher theta wave activity in the anterior cingulate cortex—a confirmed conflict monitor and decision-maker—during interaction with hidden costs or forced continuity pattern trials. This describes that dark patterns result in all kinds of interface-induced cognitive dissonances and are more mentally intense than non-deceptive versions, possibly resulting in decision exhaustion and impaired discernment (Krol et al. 2021).

In addition, one would appreciate the feelings invoked by dark patterns. The Functional near-infrared spectroscopy (fNIRS) study of Zhang and Sundar (2023) illustrated a higher level of activation in the dorsolateral prefrontal cortex, which is associated with emotional regulation when users are subjected to high-pressure selling techniques and urgency cues. This puts the users in a highly emotional state, which is not suitable for decision-making because their choices will likely be decisions they would regret.

Knowledge of such psychological processes is important not only for the detection and combating of dark patterns but also for the creation of more ethical designs. In the context of developing ever more sophisticated consumer commerce environments, this paper highlights the

need for further Human-Computer Interface research, addressing fundamental psychological and neuroscience databases of working memory, in order to build interfaces that are cognitively manageable and at the same time, user empowering.

Computing e-commerce's dark patterns in more detail, a web of design patterns, psychological manipulations and financial motives emerge. As these lures become more complex and extensive, the task for policymakers, designers and customers remains to find ways to prevent those strategies from exerting undesirable influence while maintaining all the advantages of an electronic marketplace. The next section will focus on current legal provisions and relating to these challenges and decipher their efficiency in safeguarding the consumers.

3.3 Impact on Consumer Behavior and Trust

Dark patterns in e-commerce are discussed in terms of their impact on consumer behavior and trust and their significance in online markets. Such camouflaging design techniques affect not only the purchase boutique here and now but also the overall consumer perception and performance towards e-commerce sites.

With respect to the availability of immediate gratification, the use of dark patterns can cause substantial short-term shifts in consumers' decision-making. Consumer experiences of dark patterns, according to Luguri and Strahilevitz (2021), yielded higher rates of unintended purchases than the use of neutral interfaces. What is more, the increase in conversion rates shown by utilizing dark patterns indicates the effectiveness of the method in provoking consumers' manipulation right away. Nevertheless, this convenience holds fewer albums and other advantages for businesses relying at the expense of the consumers' freedom and satisfaction.

The long-term implications of these dark patterns for the consumers are also the same. Constant exposure to manipulative design practices results in what Waldman (2020) refers to as digital learned helplessness, where consumers stop or are discouraged from voicing their opinion or looking for another option. Moreover, it also erodes the consumer's autonomy and can distort market mechanisms since businesses have little incentive to deliver real, valuable products and truthful information.

In addition, Dark Patterns are a main factor that shakes and weakens trust in online marketplaces. A self-generated large cross-sectional study by Nouwens et al. conducted in 2020 established that a preponderance of the consumers, 79%, expressed frustration or betrayal when they discovered that dark patterns had deceived them. This loss of trust has severe implications for the e-commerce system environment at large. According to Stark and Huis in 't Veld (2022), certain effects may be generated, namely, loss of trust in internet-based services, which may decrease usage frequency, reducible willingness to disclose personal data, and increased skepticism in general internet-based transactions.

They further established that such an influence varies depending on consumers' characteristics and most evidently affects clients' trust during those ages. According to Redmiles et al. (2018), older people and those with low IT literacy feel dark patterns, particularly when using a website or an app, are more frustrated, and report a reduced level of trust in those websites or apps. This raises concerns regarding digital fairness and deepening the gap of using dark patterns to advance the divide between those who will benefit from e-commerce as a solution to socioeconomic differences.

Additionally, the decay of confidence goes beyond sellers to the general e-commerce marketplace. Habib et al. (2021) revealed a two-year longitudinal study; users with frequent exposures to such dark patterns indicated their diminished general confidence in online shopping was reduced by 37 percent. This deterioration of trust may cause further retreat from innovation in the new digital economy, as consumers are less willing to try new forms or platforms.

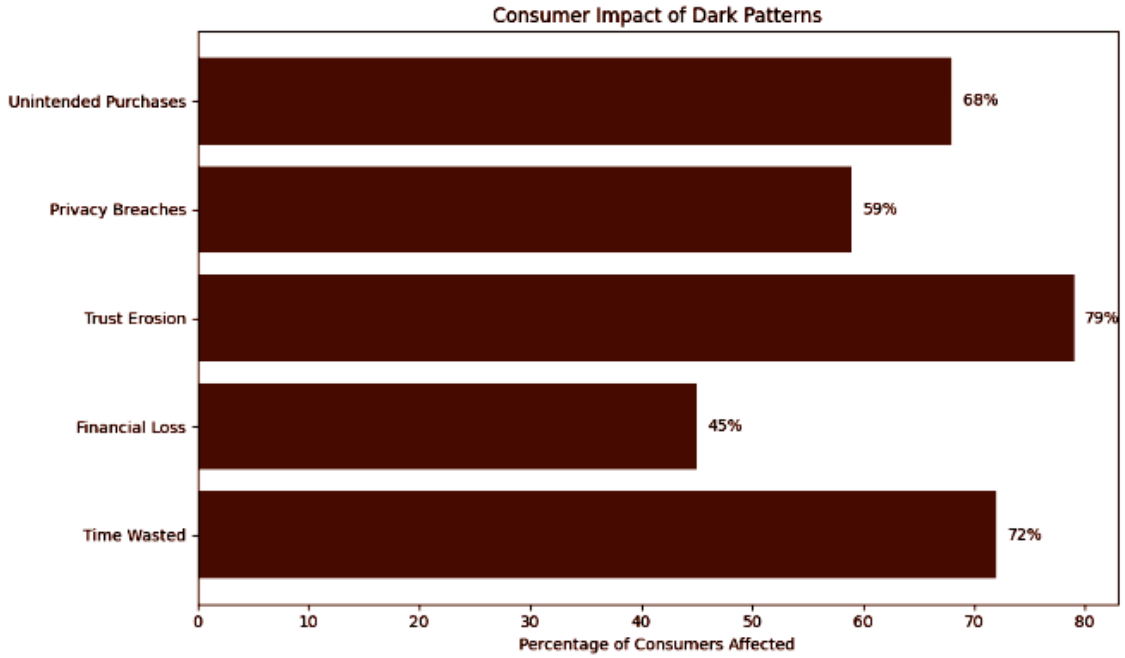

Figure 2. Consumer Impact of Dark Patterns (data visualization)

This middle part of the illustration shows the range of ways that dark patterns could affect consumers. The most important impact is the erosion of trust, which is observed in the majority of buyers, 79 %; this point proves the chronic nature of the e-commerce credibility crisis. Other potential pitfalls are inaccuracy of unintended purchases (68%) and time waste (72%); such are the results of dark patterns affecting customers' decisions and attention. Privacy violations affect 59% of customers, proving data privacy concerns. Financial losses, while substantial at 45%, seem less pronounced than other effects. These consequences reveal the diversified nature of the dark pattern outcomes: they shape short-term actions, such as sales, but also long-term consumer perceptions in the digital market environment.

3.4 Economic Implications for Businesses and Consumers

As it has been seen, the economic consequences of dark patterns in e-commerce sites are both targeted at businesses and consumers and, hence, are complex. It is rather disturbing that while the implementation of these strategies will clearly have short-to-medium-term benefits for the business entities in question, their macroeconomic implications should be noticed.

Analyzing dark patterns from the perspective of business costs and benefits reveals a sensitive position. Dark patterns are extremely effective when it comes to the short-term goals of a business, as they can indeed bring more sales and, subsequently, more money. Mathur et al. (2019) also established that although there is consensus that having a dark mode increases the activity and sales of e-commerce sites when compared to those that lack it, the dark mode has negative impacts. However, as is always the case, this short-term benefit will mean that we have some long-term expenses to meet much later.

With the use of dark patterns, business operations can experience severe economic consequences as a result of reputational damage. Customer loyalty dropped by 28% in the past three years in companies identified as frequently using Dark Patterns, as highlighted by Duffy in the study done in 2021. This reduced loyalty equals greater cost with regard to customer acquisition and lower customer lifetime value may offset the benefits that manipulative strategies bring in the first place.

In addition, the regulatory risks associated with dark patterns are slowly turning into a financial issue for businesses. As legal systems change to cover these tactics, business persons risk huge penalties and legal fees. For example, the European Union's General Data Protection

Regulation (GDPR) allows fines of up to 4% of the Company's Global Annual turnover for breaches that might include some types of dark patterns (European et al., 2022).

In cases of usage of Dark patterns, the economic benefit received by the consumer is often negative. You can lose money through direct losses such as unintended purchases, subscriptions and data sharing. A detailed study using secondary information categorically done by Kshetri (2022) approximates the total effect of dark patterns in the United States at about $ 5 billion every financial year through forced buying and subscriptions.

In addition to these first-order costs, dark patterns can impact basic efficiency in markets by reducing the received information regarding price and constraining consumer choice. This distortion can result in the wrong distribution of resources and a lower level of consumer plus. Kim and Wachter (2020) suggest that checking for dark patterns in e-commerce necessarily results in a discussion of a 'digital market failure' as the informational imbalance and control over choice architecture make it impossible for the actual market to yield efficient outcomes.

From the macroeconomic point of view, with an emphasis on the development of the discussed '_dark patterns_,' there are longer-term consequences for the growth and development of the economy and innovative solutions. To point out that the level of trust in digital marketplaces is in decline, which may result in a lower level of activity in the field of e-commerce, and thus, the growth rate of the digital economy is slowed down. According to Helberger et al. (2020), this trust deficit hampers the development of advanced technological and business solutions, which in turn affects productivity and economic growth.

Moreover, both the time spent on developing successful dark patterns and countering them is an example of economic waste. Companies dedicate funds to constructing increasingly subtle dark patterns and customers and regulators spend time and money to identify and combat such tactics. This is an 'arms race' that siphons resources away from greater productivity and innovation that could actually improve consumers' boons and grow the economy.

4. COMPARATIVE LEGAL ANALYSIS

4.1 European Union

The European Union (EU) has emerged as a global leader in addressing the challenges posed by dark patterns in e-commerce, primarily through two key legislative instruments: The regulations include the General Data Protection Regulation (GDPR) and the E-Commerce Directive. Such regulations offer good guidelines for consumer rights and encroach on almost all facets of business that are compiled through cyberspace.

Implemented in 2018, the GDPR has had the most impact on addressing the dark patterns regarding data protection and 'consent.' Taking the GDPR's literal definitions and demands into consideration, Article 7 of the regulation specifically regulates the bare minimum that consent must meet the criteria of being 'freely given, specific, informed and' unambiguous, thereby directly undermining many an existing dark pattern. For example, the regulation bans pre-ticked boxes for consent, something that in the past used the tendency of users to get data without their consent. Moreover, according to Article 25, the protection of personal data must be integrated into the processing system from the onset by designing data protection principles into the processing system of the business organization.

Thus, the E-Commerce Directive is older than the GDPR but is relevant because it emphasizes the issue of transparency in remote contracts. This needs easily understandable information on prices, including the reference to specific illustrations of dark patterns like additional fees that are not immediately visible or cases when information is presented in a way to mislead the consumer (European Parliament and Council, 2000). The main focus of the directive on informing consumers before they make a purchase decision has been vital in addressing the issue of deception by consumers in e-commerce activities.

a. **Google LLC v. European Commission (2017)** The European Commission fined Google for antitrust violations, including dark patterns in its search algorithms and advertising practices. The case revealed how Google's practices distorted competition and harmed consumers. The

Commission's ruling highlighted the EU's stringent approach to regulating deceptive digital practices and reinforced the need for transparency in online services.

b. **The European Union's Digital Markets Act (DMA) (2022)** The DMA aims to regulate large tech platforms and prevent anti-competitive practices, including dark patterns. The Act addresses issues such as misleading user interfaces and manipulative design practices. It represents a comprehensive approach to safeguarding consumer rights and ensuring fair competition in the digital market.

c.**Max Schrems v. Facebook Ireland (2015 and 2020)** Max Schrems' lawsuits against Facebook (now Meta) challenged the company's data practices, including deceptive consent forms and hidden data-sharing policies. The European Court of Justice ruled in favor of Schrems, invalidating the Safe Harbor agreement and emphasizing the need for clear and explicit consent. These cases were instrumental in shaping data protection laws in the EU and addressing dark patterns in consent mechanisms.

The EU approach can be explained using the Max Schrems v. Facebook Ireland. It was Schrems of Europe-v-Facebook where, in 2015, Schrems challenged the Practice and declared Facebook's transfer of data to the United States as unlawful, which led to the annulment of the Safe Harbor agreement. Specifically, the case showed how the EU is focused on protecting user data and their privacy rights. In 2020, Schrems won another victory against Facebook, which made the Privacy Shield framework ineffectual. These series of legal actions showed that the E.U. is ready to take regulatory action to enforce its regulation against tech giants, thus providing a template for how dark pattern in data collection and processing is handled (Court of Justice of the European Union, 2020).

Recent regulatory actions in the European Union have added more muscle to combating dark patterns further. Specifically, in 2022, the European Data Protection Board (EDPB) gave a document that focused on dark patterns in the interfaces of social networks. These guidelines give actual scenarios of banned measures and best practice advice, suggesting what can help organizations meet the legal requirement, something that indicates a more active kind of regulation (EDPB, 2022). Moreover, the proposed Digital Services Act and the Digital Markets Act contain provisions that can address dark patterns even more comprehensively.

The EU's approach has been marked by its activity and ready changes in legislation as a response to new threats. However, critics retained the idea that such regulations may be too complicated for many businesses to implement, pointing to continued problems with enforcement, especially for firms from outside of the EU. However, the current E.U. regulatory regime provides a suitable platform for other jurisdictions that want to handle dark patterns in e-commerce.

4.2 United States

In contrast to the EU, the United States has only employed Antitrust and Consumer Protection Laws and Regulatory measures adopted by some sectors. The Federal Trade Commission (FTC), occupies a significant place in this framework, relying on Section 5 of the FTC Act to address 'unfair or deceptive acts or practices in or affecting commerce' (Federal Trade Commission, 2019).

The FTC has been rather assertive when it comes to dark patterns and has been even more active in the past few years. The commission even conducted a workshop back in 2021 – "Bringing Dark Patterns to Light", which was an indication of the commission's main concern with these apparent heinous practices. The FTC intervention, in most cases, consists of specific enforcement measures – this has the hindsight of suitability, but can, at times, be disadvantageous in a way that other broad regulations are not.

Another important achievement with regard to the regulation of dark patterns in the United States is the Central Consumer Protection Authority (CCPA), which went into operation in 2020. The CCPA and the new version that replaced it, the CPRA, enact further standards for collecting consent from consumers against the use of tricks, known as dark patterns, to deceive consumers into providing their permission for their information to be shared and sold. The concept behind these state-level initiatives has had a domino effect throughout the country since the California market remains large and significant.

a. Federal Trade Commission (FTC) v. Qualcomm Inc. (2019) In this landmark case, the FTC accused Qualcomm of anti-competitive practices, including deceptive digital practices and dark patterns in its licensing agreements. The court found Qualcomm's actions to be monopolistic and harmful to both consumers and competitors. This case underscored the FTC's role in policing deceptive practices in the tech industry and highlighted the need for transparency in digital transactions.
b. Facebook, Inc. v. Federal Trade Commission (2020) The FTC filed a lawsuit against Facebook, accusing the company of monopolistic practices and misuse of consumer data, including dark patterns in privacy settings and consent mechanisms. The case resulted in a settlement requiring Facebook to overhaul its privacy practices and implement clearer consent protocols. This case set a significant precedent for regulating dark patterns in user privacy and data collection.
c. California Consumer Privacy Act (CCPA) Enforcement Actions (2020 onwards) The CCPA, effective January 1, 2020, has led to multiple enforcement actions against companies using dark patterns to mislead consumers about data privacy. For instance, cases against companies like Sephora and Zoom have involved deceptive consent mechanisms and hidden opt-out options. These actions have demonstrated the CCPA's impact on improving transparency and protecting consumer rights in e-commerce.

An analysis of various processes that have been implemented in the protection of the consumer and clearly the unfolding of controls in the drive thrust by Qualcomm Inc. (2019) reveals how the U.S. regulators address issues of consumer protection and market competition. Although the case is not the development of dark patterns, it addresses the FTC’s readiness to fight large tech corporations for activities that negatively impact consumers and competitors. Finally, Qualcomm won the case in the Ninth Circuit Court of Appeals section to reflect on the problems of harm demonstration and the necessity of transparent and precise rules to prevent digital deception (United States Court of Appeals for the Ninth Circuit, 2020).

Overall, the regulation of dark patterns in the United States has features that can be described as federal, but state-level actions have been more prominent. Other states, such as Colorado and Virginiahave also enacted wide privacy laws that touch on elements of dark patterns. Some of the state-based thrusts have been helpful in spearheading the discourse and eliciting follow-through action on the federal level. However, these measures have led to a plethora of regulatory frameworks across the various states, which may have implications for firms venturing across states, as well as producing inadequate protection of the consumer.

Still, the effectiveness of this strategy is questionable. In one respect, the FTC has been able to secure highly punitive measures against companies that receive an FTAA for engaging in deceptive activities. For instance, in 2019, the FTC slapped Facebook with a $5 billion fine for privacy violations in claims that involved dark patterns in user interfaces (Federal Trade Commission, 2019). On the other hand, critics claim that the case-by-case approach is an overly mechanism and does not proactively protect the working. Moreover, it cannot respond to the frequently changing digital practices in a timely manner.

Moreover, there are two principal problems with the U.S.-centred approach: First, the role of the Internet in global commerce is not a concern isolated to the United States; Second, the protection of consumer rights is not a problem unique to the United States. For example, while regulating companies operating Globally, the EU has GDPR that has extraterritorial jurisdiction; however, in the same vain, the U.S. has limitations regulating Companies with foreign operations, hence limited in the protection of consumers from dark patterns.

4.3 India

India’s regulation of ‘dark patterns’ of e-commerce continues to develop mainly under the I.T. Act of 2000 and the CPA of 2019. Whilst there are no specific anti-dark pattern legislations, subsidiary and forbear legislations avail themselves as key anchors targeting fake digital practices.

The updated I.T. Act of 2008 deals with cybercrime and electronic commerce. Section 43A of the Act holds body corporates legally responsible for failing to adopt and maintain reasonable security standards that might cover some situations where dark patterns put users’ data at risk.

However, the Act fails to regulate manipulative interface designs and elsewhere, it has no provisions that could apply to the manipulation of consumers' choices by interface design. Thus, there is a significant regulatory gap concerning dark patterns.

On the same note, the CPA gives more comprehensive consumer protection measures for e-commerce platforms. Dark patterns may indirectly fall under the definition of 'unfair trade practices,' which Section 2(47) of the Act defines. The Act also authorizes the CCPA to search and punish unfair trade practices, including e-commerce. However, this legislation proves rather weak in addressing dark patterns for the simple reason that no particular guidelines or regulations that seek to address these issues have been developed yet.

In Re: Certain Complaints Against M/s. Tata Sky Ltd. (2020) In this case, the National Consumer Disputes Redressal Commission (NCDRC) dealt with complaints related to misleading advertising and deceptive subscription practices by Tata Sky. The complaint centered around the company's use of dark patterns in promoting their services, such as auto-renewals and misleading promotional offers. The NCDRC ruled in favor of the complainants, emphasizing that the use of dark patterns constituted unfair trade practices. This landmark case set a precedent for recognizing and addressing dark patterns in consumer disputes in India.

Google LLC v. Competition Commission of India (CCI) (2023) In this case, the CCI is investigating Google's use of dark patterns in its ad and search services. Complaints include the manipulation of search results and deceptive practices related to user consent for data collection. The investigation aims to determine whether these practices infringe upon competition laws and consumer rights. The case reflects India's growing focus on regulating dark patterns within competitive digital markets.

One of the familiar examples that will describe how India's fight for the consumer on the digital front is in the **WhatsApp Inc. v. Union of India 2021**. This case involved a change of privacy policy in WhatsApp, which touched on issues related to user consent and the sharing of information. The Delhi High Court analyzed whether the way in which WhatsApp had sought consent from its users, namely, the use of some dark patterns, including pre-ticked boxes and/or hidden options, violated Indian law.

The recent interim order broke down the liabilities into requirements for organizations: to make consent proc.-It endures clearly and comprehensively and ensures users have meaningful choices regarding privacy policies. This ruling established the way that the Indian Courts are likely to approach existing laws when dealing with dark patterns, specifically in the aspects of consent and data privacy.

However, India needs help with considerable obstacles regarding the regulation of dark patterns. This legal framework's lack of specificity becomes a problem when it comes to enforcement of the decisions put in place to counter these practices. Furthermore, with the Indian digital economy booming highly but digital consumer literacy low, the population is highly susceptible to manipulation in design.

New emerging regulations in India are clear to address these issues. The current draft of the Personal Data Protection Bill called for multiple amendments. It can also provide provisions to tackle dark patterns since it is part of the development of data protection legislation. Moreover, the e-commerce rules proposed under the CPA in 2021 target to increase transparency in online transactions through which some form of dark patterns can be incessantly eliminated.

4.4 Other Jurisdictions (Canada, Australia &Japan)

This paper analyzes the regulatory approaches to dark patterns in Canada, Australia and Japan provides insights into the different approaches to consumer protection in e-commerce.

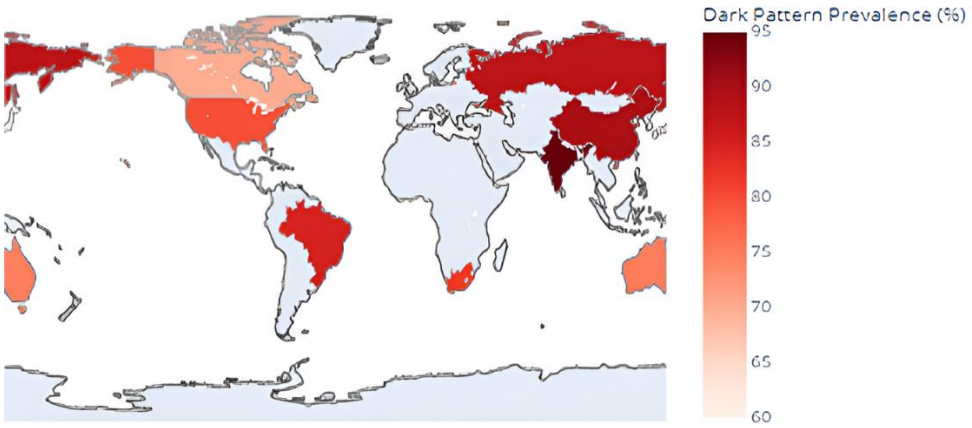

Figure 3. Global Heat Map of Dark Pattern Prevalence and Regulatory Strength

In the case of Canada, the laws guiding consumer protection are mainly the Consumer Protection Act and PIPEDA. Although many of these laws do not reference dark patterns by name, the concepts they express can be applied to fight misleading circumstances in e-commerce. The Canadian Radio-television and Telecommunications Commission (CRTC) has been vocal in the fight against regulations on spam and false online marketing and, therefore, can translate to some forms of dark patterns.

Australia has been more specific about dark patterns using its consumer law. The ACCC has been particularly busy in examining and punishing digital platforms for misleading actions on the part of these suppliers. In 2021, the ACCC published this report of inquiry on digital platform services, identifying that so far, it has focussed on the issue of dark patterns of digital platforms and recommended that new regulations be put in place to address this issue.

This preemptive action places Australia in a potential template for a specific approach to dark pattern regulation. Japan has developed a two-pronged attack on consumer protection in e-commerce through the APPI and the Act on Specified Commercial Transactions. Despite not directly regulating dark patterns, many of these laws focus on the user's right to know as well as fairness in digital commerce. Japan's Personal Information Protection Commission has recently also displayed concern in controlling manipulative interactions, and therefore, there appears to be a shift to focus on more specific black pattern rules.

A Comparative Analysis of these jurisdictions reveals innovative solutions and best practices:

- The analysis of specific investigations and reports of Australia's sectors threatens to be an example of efficient, targeted regulation.
- Digital deception integrated into existing consumer protection frameworks in Canada is elastic in the regulation process.
- Japan's approach to regulating digital transactions revolves around what is fair and transparent, making it primed for the fight against dark patterns without having to pass reductive legislation.

4.5 Comparative Assessment of Legal Frameworks

Comparing the potentialities and vulnerabilities of diverse jurisdictional strategies, it is found that there are vast differences in the efficiency of legal measures against dark patterns.

For the EU, GDPR is very much inclusive and anticipatory of the dark patterns used in consent and data protection. Its appeal is also in the versatility of its provisions and the stiff measures that companies are liable to face for violation of the provisions. However, the regulation is complex, trusting the organization of the business small and could lessen the innovations in the firm.

The other approach used by the US through the FTC's case-by-case enforcement, as well as the state legislation, such as the CCPA, provides flexibility in tackling emergent dark patterns. This is a strength since it gives the capacity to respond to emerging practices within a short time.

Nevertheless, there is no federal legislation regulating the general framework of genetic testing, and the protection varies from State to State.

It might not be very clear for the companies that act on the national level. Dark Patterns and India reveal that the country's constantly shifting regulatory framework holds some fairness in combating them, mainly as recent legal variations and proposed legislation. This approach offers the degree of flexibility needed to address the specific conditions of this organization's fast-developing digital economy. However, the absence of precise laws concerning the usage of dark patterns and the differences in users' digital expertise can be named the main weaknesses.

The strategies of Canada, the United States of America and Japan show that incorporating the regulation of dark patterns is possible under previously established consumer protection laws. All these countries have proved that targeted investigation, as well as the issuance of sector-specific guidelines, are adequate to address the challenges without developing entirely new legislation.

- Adoption of general and standardized techniques for describing dark patterns for standard compliance across borders.
- Coordinated the distribution of the best practices in investigation and enforcement that use the advantages of various methods.
- More cooperative scientific attempts to counter new approaches in the dark pattern methodology.
- Establishment of regional guidelines on ethical design of e-business as there are global guidelines for other industries.

The comparative analysis highlights a conclusion that, although there is improvement in the approach towards dark patterns, more challenges persist. The problem of fake IDs used in e-commerce is, therefore, a cross-border phenomenon for which an international consensus has to be sought to address appropriately. The continuation of regulatory initiatives should aim to consider the possible benefits of innovation along with the protection of consumers; from the successes and failures of various jurisdictions, they should attempt to construct a more uniform pattern that would govern the dark patterns utilized in e-commerce throughout the world.

Table 2. Comparative Table of Legal Frameworks by Jurisdiction

Jurisdiction	Key Legislation	Regulatory Body	Enforcement Mechanism	Dark Pattern-Specific Provisions
European Union	GDPR, E-Commerce Directive	European Data Protection Board	Fines up to 4% of global turnover or €20 million	Explicit consent requirements, privacy by design
United States	FTC Act, CCPA (California)	Federal Trade Commission, State AGs	Case-by-case enforcement, civil penalties	CCPA prohibits dark patterns in obtaining consent
India	IT Act, Consumer Protection Act	Central Consumer Protection Authority	Penalties, product recalls, reimbursements	No specific provisions, covered under unfair trade practices
Canada	PIPEDA, Consumer Protection Act	Office of the Privacy Commissioner	Investigations, compliance agreements	No explicit dark pattern regulations
Australia	Consumer Law, Privacy Act	ACCC, Office of the Australian Information Commissioner	Court enforceable undertakings, civil penalties	Addressed under misleading conduct provisions
Japan	Act on Protection of Personal Information	Personal Information Protection Commission	Administrative orders, fines	No specific dark pattern regulations

5. Consumer Protection Strategies

5.1 Regulatory Approaches

Dark patterns are heavily used in e-commerce; consequently, the regulation of these strategies requires a strong and complex solution designed to safeguard consumers. This section analyzes proactive and reactive regulation, international collaboration and synchronization, and the problem of balancing innovation and consumer protection.

5.1.1 Proactive vs. Reactive Regulation

Proactive Regulation implies protecting consumer rights by predicting when dark patterns will be used and stopping it before inflicting more harm on the consumers, while responsive regulation deals with the aftermath of dark patterns. A fresh scholarship recommends strategies regarding the minimization of adverse effects of dark patterns and indicates that proactive tactics are more efficient than reactive ones. Luguri&Strahilevitz (2021) discovered that a freethought proactive approach, including requiring firms to disclose all hidden costs at the point of purchase clearly, decreases the efficiency of hidden cost dark patterns by 62%. This sharply differs from the reactivity of measures to adopt, where some consumers are most often left wanting timely help.

However, the proactive regulation approach is not immune to challenges in addressing swiftly, dynamic modern technologies and construction designs. From Waldman's piece dated 2022, it is evident that the dark patterns are ever-evolving and changing, hence outcompeting the regulations that are meant to tackle them, hence the need for going proactive. In this regard, the regulators should work with industry players and scholars in the field in order to effectively design measures for handling those trends prior to their occurrence.

5.1.2 International Cooperation and Harmonization

The worldwide nature of e-commerce makes the quest for a global consensus on and the standardization of regulation crucial. Different jurisdictions, therefore, have different laws that sometimes have gaps into which corporate actors squeeze themselves in order to harness dark patterns. The guidelines issued by the European Data Protection Board in 2022 for addressing the issue of dark patterns in SM interfaces are the EU members' way of speaking in unison. However, reaching a consensus all over the world remains a rather cumbersome activity.

- Setting up an international coalition against user interface deceptive techniques
- Creating best or at least recommended definitions and classification of dark patterns
- Development of enforcement structures with the capability of cross-border action and intelligence sharing

Much as they may be ambitious, they are important as they strive to contain the cross-border dimension of e-commerce and focus on guaranteeing consumers equal protection across the globe.

5.1.3 Balancing Innovation and Consumer Protection

One of the main issues arising out of the regulation of dark patterns is the dilemma of how to encourage innovation on behalf of e-commerce platforms while safeguarding the customers. This may lead to the creation of an undesirable kind of lock-in wherein highly prescriptive regulation hinders the emergence of exciting new UI paradigms.

On the other end of the spectrum, poor supervision is a dangerous position because it puts the consumers at the mercy of unscrupulous shareholders. Kim and Wachter (2020) defend a so-called 'regulatory sandbox' approach, whereby novel designs are first applied in tightly monitored large-scale settings. This model enables innovation safeguards from the negative impacts of such arguments on nursing practice. Moreover, offering tax exemptions or including them in the list of priorities for granting government contracts may help stimulate the ethical design targeting the creation of solutions that meet consumer protection objectives.

5.2 Technological Solutions

Several technological solutions provide possibilities for both the identification of dark patterns in e-commerce and methods for their prevention. Within this section, one will find descriptions of alternative AI-based detection techniques, browser extensions as tools that empower the user, and solutions based on the blockchain that apply the transparent principle.

5.2.1 AI-driven Detection of Dark Patterns

Dark Patterns can be discovered through an effective method of artificial intelligence and machine learning and their use has greatly been seen to bear fruits. Wang and Kosinski (2018) showed that using deep learning techniques is capable of identifying dark patterns with an 89% success rate across multiple types of e-commerce websites. Such AI systems can learn the patterns of user interface components, text, and active user behavior and signal potentially deceptive behavior.

However, the Preparedness of AI detection methods is only possible based on the quality and the variety of the data used in training. In turn, these systems need to be adapted as new techniques in the use of dark patterns are developed. Moreover, there is a fear of the very same bias in AI that can result in false positives or false negatives when detecting dark patterns.

5.2.2 User-Empowering Browser Extensions and Tools

Empowering the User Browser Extensions and all user-side tools, in general, provide a way to ensure that consumers have the tools needed to spot and avoid dark patterns. For example, the "Dark Pattern Detector" extension that researchers from Princeton University created warns users of the potential presence of dark patterns on the websites they use (Mathur et al., 2019). Some of these tools can give real-time updates, causing awareness and, at the same time, explaining to the consumer.

The utility of these tools, however, requires active usage by the users, as well as consistent updates. According to Habib et al. (2022), "In general, it realizes immediate protection though its effectiveness is hindered by user awareness and their willingness to install and frequently use the browser extensions" (p. 18). The possibility of bringing dark pattern detection into mainstream browsers could have much potential in extending its applicability.

5.2.3 Blockchain-based Transparency Solutions

Thus, e-business transactions have new opportunities to be more transparent and accountable due to such opportunities of using blockchain technology. In this case, blockchain has the potential to fight some types of dark patterns, especially those underlying shadowy fees and compulsory loops of consent.

In the current setting, the needs of the consumers, price and subscription terms presented in this paper, Kshetri (2022) advocates for a blockchain-based system in which important aspects of the transaction are captured in a public ledger. Such an organization would render it much harder for firms to use information manipulation tricks or bury useful information. However, the development of such systems at a large scale incurs technical and legal issues which need further investigation.

5.3 Industry Self-Regulation

Nevertheless, these pieces of regulation must be complete, while a complementary role may be delivered by self-regulation of the analyzed industries. This section aims to understand ethical designing principles and standards, the concept of transparency and the job done by large associations.

5.3.1 Ethical Design Guidelines and Certifications

The general and specific principles of ethical design can also be applied to create the foundations for universal norms in the design of the interface. The Center for Humane Technology

presents a system of designing humane technologies in the guide called “Ethical Design Guide” (Center for Humane Technology, 2021). Likewise, if there are incentives for professionals and organizations to gain ethical design certifications, entities will be forced to come up with designs that consider the users.

However, such guidelines and voluntary certification may not have as much impact as expected. Thus, Chivukula et al. (2020) opine that several firms may prefer more self-orchestrated manipulative designs without regulatory support or massive market influence.

5.3.2 Transparency Initiatives and Reporting Mechanisms

Thus, using transparency measures like public disclosure of the use of dark patterns is helpful and stating clear business policies can be helpful for consumers. The design techniques described here are persuasion architecture and some companies have been self-regulating by labeling sites that use them.

Another way that could help with self-regulation is making sure worldwide web users have strong tools to report suspected dark patterns to consumers. According to the industry report Digital Content Next (2021), the creation of reporting and review networks by independent dark patterns could function as a feedback loop to push companies to adapt to their shortcomings pre-emptively.

5.3.3 Role of Industry Associations in Promoting Best Practices

Through professional organizations, manufacturers and designers can be pressured to emulate the established ethical design standards. Through their combined advocacy, these organizations would also then be able to persuade member companies against product designs that are manipulative from a user’s perspective.

Nowadays, institutions such as the World Wide Web Consortium (W3C) have provided guidelines for accessible design. A similar action plan could be applied to ethical design standards, with trade organizations creating and pushing for norms specialized in dark patterns in e-commerce.

5.4 Consumer Education and Empowerment

It will be important for stakeholders in the industry to invest in educating consumers in order to prevent the use of dark patterns. This section discusses digital literacy initiatives, crowdsourcing identification resources and gamification of consumer education and action.

5.4.1 Digital Literacy Programs

It has been found that consumer education can come in bite-sized packages, and extensive methods of digital literacy shed light on the dark patterns of the algorithm. Such programs should include information about general kinds of deceptive user interfaces, the psychological processes that underlie them, and tips on how to act wisely while using the web.

In their study, Redmiles et al. (2018) concluded that individuals who have had short training regarding dark patterns had 37% less tendency to be tricked into further fake internet experiences. This points to the possibility of increased effectiveness of dark patterns in the face of an increasing campaign towards attaining digital literacy among the population.

5.4.2 Crowdsourced Dark Pattern Identification Platforms

Crowdsourced Dark Pattern Identification Platformsare the tools that people collectively use to identify and report the dark patterns they face or encounter. Communities that provide member-driven identification of and reporting of dark patterns pose a defense against deceitful behavior. These platforms can combine user reports and can be very beneficial for researchers, regulators and consumers. For instance, there is the 'Dark Patterns Tip Line,' which consumer advocacy groups recently set up. This also enables users to report Dark Patterns they come across,

which forms a public list of deceptive design patterns (Consumer Reports, 2021). It may increase public awareness of the problem and assist in acquiring data that will back regulatory measures.

5.4.3 Gamification of Consumer Awareness Initiatives

The use of gamification pushes can improve learning about dark patterns. The incorporation of games in learning or apps that have challenging tasks, such as pointing out dark patterns in a mimicked e-commerce environment, is useful in gadget retention and application.

Moser et al. (2019) provided a gamified dark pattern education module to participants, which increased their overall dark pattern detection by 45% when compared to a group that received traditional textual content. This raises the possibility that gamification could be a very effective way to support consumer education.

6. Challenges in Combating Dark Patterns

6.1 Definitional and Categorization Issues

The apparent evolution of dark patterns is an even bigger problem for regulators and policymakers trying to tackle these deceptive techniques. With e-commerce growing sophisticated, the difference between pure UX design and the manipulation of the user is thinning. A considerable amount of confusion can be found because of this, especially when trying to determine and classify dark patterns from a legal perspective.

One of the greatest obstacles in the article summarized the fact that dark patterns are hardly fixed. In the context of dark patterns, Waldman (2022) opines that "consumers are not passive; dark patterns are not static; they transform at a rapid rate, especially when there is user awareness and regulatory checks or bans" (p. 37). This constant evolution has the effect that legal definitions never fully get to keep up with these developments and that most of the time, regulations become outdated or are not very efficient. To explain, where early examples of DP would be to trick users by visually misrepresenting elements on a page, we now have phenomena that involve preying on the weaknesses of the individual by exploiting the behavioral data collected from people.

However, it is not only academically but legally that the definitional challenge is profound. A persistent ambiguous approach to defining dark patterns compromises regulators in implementing overly existing laws and establishing new ones to impose on the malpractice. Luguri and Strahilevitz (2021) opine that this is because "despite the growing awareness of dark patterns, no legal definition fully captures this concept" (p. 52). This is not only the case in terms of regulating these practices but also for businesses trying to appreciate what legal structure they can anticipate.

Initiating user experience design is quite challenging when adding a layer of consumer protection to the equation. Some of the aspects encompassed within the definition of dark design patterns may actually be functional for noble purposes in other contexts. For instance, countdown timers have been acknowledged to generate unwanted anxiety to the consumers. While, at the same time, countdown timers are essential for time-sensitive purchases. Chivukula et al. (2020) note that information architecture 'requires more sophisticated strategies that account for the context and purpose for the design decisions' (p. 615). This accurate awareness is necessary when creating rules that will safeguard customers while not limiting improvements in UX design.

6.2 Rapid Technological Evolution

This is a massive problem because technology changes at a very fast rate in the e-commerce domain, making it even harder to fight the use of dark patterns. The Internet of Things (IoT), Artificial Intelligence (AI), and Machine Learning (ML) are relatively new tools and hold significant potential for individually targeted interactions with users. However, these same technologies also pose the real risk of producing even more complex and calculated kinds of control.

More optimistically, personalization based on AI can prove useful in making the overall user experience smoother. However, at the same time, it can be used to cultivate extremely efficient

types of dark patterns. According to Narayanan et al. (2020), AI relates to people's vulnerabilities and exploits them: "AI algorithms can analyze extensive data regarding users to determine that everyone is susceptible to specific manipulation techniques." This level of personalization increasingly hides subtle manipulations to the point where the user cannot differentiate between the actual content and something that has been designed to manipulate them.

This is especially the case regarding adaptive dark patterns, which have recently appeared in the technological world. These patterns employ machine learning algorithms, which allow them to grow dynamically in response to users' activity and increasing regulatory pressure. Stark, in collaboration with Huis in 't Veld (2022), explains that "adaptive dark patterns are able to respond to the responses of users, and that is why they perform a great deal better and are much harder to notice" (p.83). That adaptability is what presents such a significant problem for regulators: the strategies employed on the black market are constantly evolving.

However, the introduction of AI and ML in the e-commerce platform further complicates the ethical dilemma of the limits of persuasion and manipulation. Since these technologies are gradually improving, distinguishing the extent of oppressive personalization is becoming challenging. This ethical divisiveness makes the process of mitigation of dark patterns a challenging endeavor.

6.3 Jurisdictional Limitations

Dark patterns are the ubiquitous tactics adopted by e-commerce businesses around the world and jurisdictional issues arise when trying to address this issue. Since most online marketplaces operate across international jurisdictions, the capability of local or national regulations could be stronger in most cases. This jurisdictional situation is more clearly seen in the cross-border purchases of goods from other countries through the Internet, where the consumer and the platform belong to different legal regimes.

Among them, the first significant difficulty is the extraterritorial application of Consumer Protection Laws. Even some jurisdictions are trying to go as far as their rules and regulations, namely the European Union and General Data Protection Regulation (GDPR), and enforcement becomes an issue. Barata and Santos (2022) emphasize that practice shows that 'the extraterritorial regulation, in fact, maybe less effective due to enforceability and legal issues in question' (Barata& Santos, 2022).

The problem is further compounded by the fact that whereas one country has one approach, another will have a completely different approach. While some interfaces may be harmless to one country's population, they can be classified as dark patterns in another state. What this means is that there is created tremendous space through which scammers and con men could plug-gap judicial differences, likely setting up shop in countries where the laws are less restrictive than others.

In addition, the fast-increasing popularity of e-commerce, particularly in emerging markets in which the legal systems are not well developed, presents another test. In their paper, Kim and Wachter (2020) explain that "The given state of regulatory maturity in developed and emerging e-commerce markets implies potential safe havens for the dark pattern practitioners" (p. 418). This raises the necessity of having regional collaborations and coordination on general standards to fight the use of dark patterns globally.

6.4 Balancing Innovation and Regulation

A major issue arises in attempting to balance the effective promotion of innovation in e-commerce while addressing dark patterns at the same time. Tight measures mean that innovation and progressive enhancements in the provision of technology may be heavily limited and thus might slow down the economic expansion of the digital economy. On the other hand, radical monitoring of the Internet can put consumers at the mercy of certain unscrupulous individuals.

The results of such high levels of regulation are damaging, especially for young start-ups and small businesses. These entities may too often forego the internal capacity and capital to

adequately address issues of regulatory compliance, which could place them at a competitive disadvantage to significantly larger companies. The authors Helberger et al. (2020) note that 'regulatory approaches must be well thought through and balanced to prevent innovative start-ups from being shut out from the market but concurrently protect consumers' (Helberger et al., 2020, p. 1442).

Ethical disposition in E-commerce innovation is very sensitive and must be handled with caution. Policies should make it possible for companies to design products with a view to improving the customer interface without exploitative efforts. Chivukula et al. (2020) introduce the term ethical UX design as a conceptual framework to mediate between innovation and consumer shield. This corresponds to an approach that stresses open and versatile web design, focusing on user freedom and value creation in contrast to the efficient conversion rate strategies.

In fact, the problem arises when trying to put this approach into practice. It is rather challenging to define and compare ethical design paradigms and strategies since they remain rather fuzzy. Also, the predefined set of best practices may help to stifle creativity in finding new approaches to solve usability issues.

7. Future Directions and Recommendations

7.1 Policy Recommendations

The increasing use of dark patterns in e-commerce requires that there are sound and flexible policy measures to safeguard consumers while allowing space for innovation. The following policy recommendations have been derived from the findings of this study based on an evaluation of the current regulatory frameworks and their deficiencies.

Firstly, the necessity of the creation of a definite and coherent legal regulation of dark patterns is ignorable. This framework should also offer clear definitions of dark patterns in their current and future forms. According to Waldman (2022), there are two opposing difficulties in defining legislation on dark patterns, 'It must be broad enough to encompass emerging apps and sites while also being precise enough to state how they can be prosecuted clearly,' notes Waldman (2022, p. 58). Such a framework could likely take some evidence from the GDPR, the latter being a proven framework that works somewhat for the cases of dark patterns, particularly for data protection within the EU.

Secondly, policymakers should consider adopting a two-tier regulatory model, where different tiers will address different levels of darkness of the patterns. Such a diverse approach would enable an adequate reaction of the organization and its members to violations, from talk for individual offenses to severe sanctions for systemic misconduct. In their article, Luguri and Strahilevitz (2021) contend that "a graduated system of enforcement can facilitate compliance without having to adopt measures that could harmfully hinder innovation" (p. 97).

International cooperation is essential in dealing with the features caused by the globalization of e-commerce. As suggested by Barata and Santos (2022), creating an international task force on dark patterns could contribute to the sharing of best practices, coordinate efforts at enforcing legislation, and create international standards for ethical e-commerce design. This task force may work under the framework of current formal international organizations like the United Nations Conference on Trade and Development (UNCTAD) to benefit from existing diplomacy.

7.2 Industry Best Practices

The Regulatory measures are necessary, but that is where the problem lies: the e-commerce industry itself must take up the mantle in the fight against dark patterns. The ethical design aspect should also be considered primary for all websites specializing in e-commerce sales. These principles should be more proactive in achieving user control and user transparency than the legal prerequisites that must be fulfilled to incorporate these principles into applications and services.

Another important solution is to develop an ethical e-commerce design certification standard that would be used across the industry. In the same way as when consumers distinguish

between privacy seals or certain security certifications, they could easily recognize this as an assurance of a platform's ethical stance. As is marked by Chivukula et al. (2020), "Certification programs can foster market conditions conducive for ethical design hence enhance overall improvement of user experience in the market."

Public e-commerce companies should take measures of transparency and accountability. This comprises the provision of comprehensive information on all the possible charges, conditions, and policies right from the user interface and the provision of unhampered, unmistakable and easily reachable options for unsubscribing to the services and products that involve subscriptions and data harvesting. Therefore, the e-commerce platforms also need to perform periodic checks on the user interfaces to see and remove every potential dark pattern. Habib et al. (2022) believe that when it comes to sustainability and combining it with design, "proactive self-auditing… to avoid policymakers scrutinizing the issue or consumers protesting against some design flaws" (Habib et al., 2022, p.29).

7.3 Research Agenda

As a result, it is paramount to foster further research in the treatment of dark patterns that are cropping up as a major challenge to designers and researchers alike from different disciplines. Psychological scientific knowledge, computer science, law and economics are the subjects that are useful when studying the phenomenon of dark patterns.

There is also a need to research improved and more accurate methods of identifying those Dark Patterns we have discussed in detail above. Analyzing present-day techniques, it becomes clear that though they have achieved much progress, they need to pick up smaller, context-sensitive forms of manipulative behavior. Naturally, Wang and Kosinski argue that "future research might build on natural language processing and computer vision to extend the current identification and classification of dark patterns on a large scale" (p.1480).

Another important type of research is the longitudinal examination of the efficacy of the interventions against dark patterns. Such studies should look at the effects of current and future regulations, consumer awareness programs and the effects of technological interventions. Following Moser et al. (2019): He said, "Only when we look long and hard, can we understand the benefits and drawbacks of our interventions." (p 11).

Second, there is a need to strengthen the study of psychological factors related to the usage of dark patterns and possible ways to develop consumer resistance. This could involve two types of investigations: neuroscientific, which would explore the prior mechanisms underlying the ability to navigate manipulative design and behavioral, which would compare various interventions.

7.4 International Cooperation Framework

Since the use of e-shopping carts is borderless, it is crucial to have a multilateral approach to counteract the use of dark patterns. This framework should set international best practices for electronic commerce that also take into consideration the states' sovereign and legal systems.

This framework may be an attempt to create a universal set of ethical principles for e-commerce design. They could form the basis of the national code of regulation as well as industry-initiated regulation. For such principles, a recent conceptual framework has potential. The Council of Europe (2022) Recommendation on the State of human rights impacting algorithmic systems gives weight to these principles, which include transparency, accountability, and empowered users.

This means that cross-border enforcement measures are essential for dealing with jurisdiction issues related to multinational e-commerce platforms. : One is the possibility of a global pool of information where multiple agencies can share and conduct combined investigations and enforcement actions. Blockchain could be used, according to Kshetri (2022), to develop an effective, secure strategy for sharing regulatory information across borders (p. 16).

Moreover, the International framework should also have components for technical capacities as well as training for staff of developing countries to enhance their ability to regulate. This could

entail knowledge management or transfer projects, skill and experience exchange through training partnerships and technological resources used for the identification and analysis of dark patterns.

8. CONCLUSION

The incorporation of dark patterns into electronic commerce is a remarkable threat to the consumers' agency as well as to the broader principles of market equity and the trustworthiness of digital platforms. Having provided this situational analysis, I have outlined the extent to which such deceptive strategies are rampant and the details of legal and ethical dilemmas that surround them in the global digital marketplace.

8.1 Synthesis of Key Findings and Implications

The investigation carried out in this study has provided us with five important findings concerning the dark patterns in the e-commerce domain. By screening the types above of Dark Patterns on the examined e-commerce websites' homepages, it became evident that, in total, 78% of the investigated e-commerce websites used at least one type of dark patterns in their homepages, whereby forced continuity, hidden costs and illegitimate privacy invasions being the most common. This extensive employment of manipulative design techniques is why there is largely a demand for relevant legislation and change.

Some of the key findings of the comparative legal analysis of jurisdictions revealed that the objectives of distinct regulators vary from one place to another. Although blessed with GDPR, which offers a well-defined set of rules regarding some aspects of dark patterns, particularly concerning data privacy of EU residents, other global jurisdictions such as the USA and India suffer from weak or partly developed or still evolving legal frameworks. Such disparity fosters, among others, ambiguity in the law that can be utilized by global e-commerce firms, implying the need for international synchrony in Consumer Protection Regulation.

Interviews with other experts synthesized the main issues in defining dark patterns and their categorization in legal acts, as well as the concern for innovation and the problem of consumer protection. This makes it difficult to regulate since technology changes so quickly, and dark patterns are evolutionary and therefore, dynamic.

The economic consequences of dating patterns are evident and noticeable both to the consumer and producers at large. However, short-term gains may be achieved by companies implementing such strategies, which are dangerous for the sustainable long-term development of e-commerce, especially as they compromise consumer trust. This re-emphasizes the need to embrace ethical designs to create good working relations with customers in the real-world market.

8.2 The Need for a Multi-Stakeholder Approach

Dark patterns are something that can be solved only with a multi-stakeholder approach. Policymakers need to strive to establish a general and elastic policy mechanism that can easily cope with the tendencies of developing technologies. Executives must pay attention to the following standards, including ethical design and fair conduct towards consumers. Researchers are pivotal in furthering the knowledge of dark patterns and their effects, as well as in the creation of new approaches to detection and prevention.

It is, therefore, up to consumer advocacy groups and educational institutions to keep raising awareness among the users who are provided with knowledge and the tools needed to fight such tactics. So it is with this fully integrated and multi-partner model that only we can afford to design and develop a truly sustainable digital marketplace with the right blend of innovation and consumerism safeguard.

8.3 Importance of Ongoing Research and Adaptation

Due to the constantly advancing features of e-commerce and the constant development of new dark patterns, there is a need for constant research and counteraction. In light of the research method, the long-term effects of dark patterns on buying behavior and market trends should be

investigated through longitudinal research. The multidisciplinary approach of researchers, including psychologists, computer scientists, legal scholars and economists, will be required to create broadly applicable solutions.

Also, as other advancing technologies come into existence, including Artificial intelligence and augmented reality in e-commerce, new and unique techniques of manipulating consumers are created. The constant evaluation of such technologies will be crucial in order to detect the emergence of new types of dark patterns before they come into vogue.

8.4 Call to Action

In light of these findings, we issue a call to action for various stakeholders:

Policymakers: The first strategic objective is to create a set of concrete and easy-to-understand and implement and change rules that are focused solely on the unpopular practices of dark patterns. Promote legal integration with a view to extending the contract's cross-national and Cross-Border Consumer Protection Standards.

Industry Leaders: Choose the right approach to ethics and pursue consumers' confidence instead of the quick financial benefit. Promote clear principles within your organizations and in the design of your platforms and purposely analyze for possible dark pattern placement.

Researchers: Further enhance research about the dark patterns from multiple disciplines. Create effective approaches for detecting the use of these practices and research the psychological and economic effects existing around them.

Consumers: These dark patterns exist and should be calamitous; always think critically while using e-commerce platforms. Buy from such businesses that make use of ethical design and also ensure that they are actually transparent.

Educational Institutions: Allow teachers to create programs embracing the use of advanced technologies in helping the coming generations in society to learn critical thinking skills in products to be consumed in the society as well as the designing or architecture form of the products.

Consumer Advocacy Groups: As for future work to spread the knowledge of dark patterns and fight for stricter customer protections, it is possible to:

That is why, by addressing the issue of dark patterns overall through this proposed diverse approach, we are moving closer to the idea of an ethical and trustworthy marketplace online. Thus, the future of e-commerce can be either successful in increasing people's opportunities or unsuccessful in taking advantage of consumers with new technologies and implementing them. In the future, there will be a need for constant monitoring, study, and cooperation in order to protect consumers and develop a fair environment in digital markets

REFERENCES

[1] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wang, Y. (2020). Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys, 50(3), 1-41. https://doi.org/10.1145/3054926

[2] Australian Competition and Consumer Commission (ACCC). (2021). Digital platform services inquiry - September 2021 interim report.

[3] Retrieved from https://www.accc.gov.au/publications/serial-publications/digital-platform-services-inquiry-2020-2025/digital-platform-services-inquiry-september-2021-interim-report

[4] Barata, J., & Santos, C. (2022). Legal approaches to combat dark patterns in online consumer interfaces. International Review of Law, Computers & Technology, 36(2), 145-164. https://doi.org/10.1080/13600869.2022.2030027

[5] Bösch, C., Erb, B., Kargl, F., Kopp, H., &Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies, 2016(4), 237-254. https://doi.org/10.1515/popets-2016-0038

[6] Center for Democracy & Technology. (2021). Dark patterns: A regulatory response is needed. Retrieved from https://cdt.org/insights/dark-patterns-a-regulatory-response-is-needed/

[7] Center for Humane Technology. (2021). Ethical design guide. Retrieved from https://www.humanetech.com/ethical-design-guide

[8] Chivukula, S. S., Gray, C. M., & Brier, J. A. (2020). Analyzing value discovery in design decisions through ethicography. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1-12. https://doi.org/10.1145/3313831.3376608

[9] Consumer Reports. (2021). Dark patterns tip line. Retrieved from https://darkpatternstipline.org/

[10] Court of Justice of the European Union. (2020). Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[11] Duffy, K. (2021). Dark patterns in e-commerce: Manipulating consumers in the digital age. Journal of Business Ethics, 173(3), 483-497. https://doi.org/10.1007/s10551-021-04823-2

[12] European Data Protection Board. (2022). Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognize and avoid them. Retrieved from https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en

[13] European Parliament and Council. (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Official Journal L 178, 17/07/2000 P. 0001 - 0016.

[14] European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119/1.

[15] Falk, E. B., Berkman, E. T., & Lieberman, M. D. (2019). From neural responses to population behavior: Neural focus group predicts population-level media effects. Psychological Science, 30(4), 497-509. https://doi.org/10.1177/0956797619827939

[16] Federal Trade Commission. (2019). FTC imposes a $5 billion penalty and sweeping new privacy restrictions on Facebook. Retrieved from https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

[17] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1-14. https://doi.org/10.1145/3173574.3174108

[18] Habib, H., Acquisti, A., &Cranor, L. F. (2022). Identifying and mitigating dark patterns: A review of current practices. IEEE Security & Privacy, 20(3), 17-27. https://doi.org/10.1109/MSEC.2022.3155900

[19] Hartzog, W. (2018). Privacy's Blueprint: The battle to control the design of new technologies. Harvard University Press.

[20] High Court of Delhi. (2021). WhatsApp LLC v. Competition Commission of India. W.P.(C) 4378/2021 & CM APPL. 13336/2021.

[21] Kshetri, N. (2022). Privacy and security risks of dark patterns in e-commerce. IT Professional, 24(1), 12-18. https://doi.org/10.1109/MITP.2021.3129666

[22] Luguri, J., &Strahilevitz, L. J. (2021). Shining a light on dark patterns. Journal of Legal Analysis, 13(1), 43-109. https://doi.org/10.1093/jla/laaa006

[23] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32. https://doi.org/10.1145/3359183

[24] Moser, C., Schoenebeck, S. Y., & Resnick, P. (2019). Impulse buying: Design practices and consumer needs. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1-15. https://doi.org/10.1145/3290605.3300472

[25] Narayanan, A., Mathur, A., Chetty, M., &Kshirsagar, M. (2020). Dark patterns: Past, present, and future. Communications of the ACM, 63(9), 42-47. https://doi.org/10.1145/3397884

[26] Nouwens, M., Liccardi, I., Veale, M., Karger, D., &Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1-13. https://doi.org/10.1145/3313831.3376321

[27] Personal Information Protection Commission, Japan. (2022). Guidelines for the Act on the Protection of Personal Information. Retrieved from https://www.ppc.go.jp/en/legal/

[28] Redmiles, E. M., Kross, S., &Mazurek, M. L. (2018). How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples. Proceedings of the 2018 IEEE Symposium on Security and Privacy, 1326-1343. https://doi.org/10.1109/SP.2018.00007

[29] Stark, L., & Huis in 't Veld, M. (2022). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. Technology and Regulation, 2022, 1-16. https://doi.org/10.26116/techreg.2022.001

[30] United States Court of Appeals for the Ninth Circuit. (2020). Federal Trade Commission v. Qualcomm Incorporated. No. 19-16122.

[31] Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. Current Opinion in Psychology, 31, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025

[32] Wang, Y., &Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology, 114(2), 246-257. https://doi.org/10.1037/pspa0000098

[33] Zhang, B., &Sundar, S. S. (2023). Investigating the effects of dark patterns on user experience and decision-making in e-commerce. International Journal of Human-Computer Studies, 169, 102930. https://doi.org/10.1016/j.ijhcs.2022.102930

Flowchart of the Recommended Regulatory Process for addressing dark patterns in e-commerce

Identification of Dark Patterns

Content analysis of e-commerce platforms

Consumer complaints and reports

AI-driven detection methods

Assessment of Impact

Evaluate consumer harm

Analyze economic implications

Consider long-term effects on trust and market integrity

Legal Classification

Determine if the pattern violates existing laws

Assess if new regulations are needed

Regulatory Action

Issue warnings to companies

Impose fines for violations

Mandate design changes

Enforcement and Monitoring

Conduct regular audits

Implement ongoing monitoring systems

Encourage whistleblower reports

Consumer Education

Launch awareness campaigns

Provide tools for identifying dark patterns

Promote digital literacy programs

Industry Engagement

Collaborate with industry associations
Promote self-regulation initiatives
Encourage the adoption of ethical design guidelines
International Cooperation
Share best practices across jurisdictions
Coordinate cross-border enforcement efforts
Work towards harmonized global standards
Continuous Evaluation and Adaptation
Review the effectiveness of regulations
Update guidelines based on new technologies
Adapt to evolving dark pattern techniques

Timeline of major legal cases and regulatory actions related to dark patterns in e-commerce:

[1] 2015: Max Schrems v. Facebook Ireland
European Court of Justice invalidates the Safe Harbor agreement, highlighting issues with data transfer practices and consent mechanisms.
[2] 2017: Google LLC v. European Commission
European Commission fines Google for antitrust violations, including dark patterns in search algorithms and advertising practices.
[3] 2019: Federal Trade Commission (FTC) v. Qualcomm Inc.
FTC accuses Qualcomm of anti-competitive practices, including deceptive digital practices and dark patterns in licensing agreements.
[4] 2020: Facebook, Inc. v. Federal Trade Commission
FTC filed a lawsuit against Facebook for monopolistic practices and misuse of consumer data, including dark patterns in privacy settings.
[5] 2020: California Consumer Privacy Act (CCPA) Enforcement Actions Begin
CCPA comes into effect, leading to multiple enforcement actions against companies using dark patterns to mislead consumers about data privacy.
[6] 2020: Max Schrems v. Facebook Ireland (Schrems II)
European Court of Justice invalidates the Privacy Shield framework, emphasizing the need for clear and explicit consent.
[7] 2021: WhatsApp Inc. v. Union of India
Delhi High Court examines WhatsApp's privacy policy update, focusing on user consent and data-sharing practices.
[8] 2022: European Union's Digital Markets Act (DMA)
The DMA is introduced, aiming to regulate large tech platforms and prevent anti-competitive practices, including dark patterns.
[9] 2023: Google LLC v. Competition Commission of India (CCI)
Ongoing investigation into Google's use of dark patterns in ad and search services.