Chapter 12

Consumer Manipulation With Artificial Intelligence: Dark Patterns and Hidden Techniques

Kadir Deligöz[1]

Abstract

Technological advancements and artificial intelligence (AI)-assisted digital transformation offer significant opportunities to consumers, while at the same time paving the way for the development of manipulative design strategies. Among these strategies, ***'Dark Patterns'*** are deceptive UI/UX (User Interface / User Experience) design techniques that direct users to perform certain actions without their awareness. Artificial intelligence makes these techniques more complex, personalized and effective, thus guiding users' decision-making processes.

Artificial intelligence-supported ***Dark Patterns*** have negative effects on individual and social levels. These techniques undermine consumer autonomy, leading to financial losses, privacy violations, and reduced trust in digital platforms. In terms of social justice, low-income users may be exposed to more hidden costs and dynamic pricing. Therefore, it is crucial to adopt ethical design principles, increase user awareness and strengthen legal regulations. Raising consumer awareness, promoting transparent digital marketing practices and tightening algorithmic controls by regulatory bodies will be critical steps in the fight against Dark Patterns.

Introduction

The digitalization process, together with technological developments, offers unprecedented opportunities to consumers, while at the same time paving the way for the emergence of new manipulation (manipulation, influence, deception) techniques One of the most prominent examples of these techniques is defined as "Dark Patterns", which are used in user

1 Associate Professor, Atatürk University, kadir.deligoz@atauni.edu.tr, ORCID ID: 0000-0003-3247-9223

https://doi.org/10.58830/ozgur.pub710.c3029

interface (UI) design and direct users to perform certain actions with deceptive or manipulative methods Dark patterns are deceptive design strategies designed to manipulate users on digital platforms These strategies can cause users to unwittingly sign up for subscriptions, make unwanted purchases or share personal data Artificial intelligence technologies are increasingly being used to enhance, personalize and scale the effectiveness of these patterns This raises important debates about consumer rights and digital ethics (Ducato & Marique 2018)

In this section, a comprehensive analysis of AI-powered dark patterns will be presented First, the main types of dark patterns and AI integration will be examined, and then the ethical and social implications of these practices will be discussed Legal regulations and technological solutions will also be discussed in detail, and finally, potential future developments will be evaluated This study aims to take an in-depth look at what AI-driven dark patterns are, how they work, their impact on consumers and the measures that can be taken against them

1. The Concept of Dark Patterns

Today, as digital transformation accelerates, consumers are increasingly engaging with online platforms and digital services. These interactions are largely realized through interface designs that shape the user experience. However, it is observed that these designs do not always serve for the benefit of the user, on the contrary, they can be used for manipulative purposes. These manipulative design patterns, called "dark patterns" or "dark patterns" in Turkish, are defined as insidious tactics that direct users to make decisions against their own interests (Brignull & Darlo, 2019).

Dark patterns are deceptive elements that are intentionally crafted to make the users do actions that they wouldn't do otherwise. Those techniques are used for the benefit of various stakeholders and are included in web products that are used world-wide, such as social media platforms, some popular apps or web services. The concept is well known among practitioners (Cara, 2019: 105). With the development and proliferation of artificial intelligence technologies, the effectiveness and sophistication of dark patterns has also increased significantly. Machine learning algorithms are able to develop personalized manipulation strategies by analyzing user behavior, thereby guiding consumers more effectively (Zhang et al., 2021). Dark patterns tactics are user interfaces that benefit an online service by leading consumers to make irrational decisions they might not otherwise make (Narayanan et al., 2020) or tricking or manipulating consumers into purchasing products

or services (Federal Trade Commission, 2022). This raises serious concerns about digital ethics and consumer rights, and calls for new regulations in this area.

2. Historical Development of Dark Patterns

Dark patterns are defined as manipulative design strategies that direct users to perform certain actions. This concept was first introduced in 2010 by User Experience designer Harry Brignull, who drew attention to the ethical risks of such design patterns (Brignull, 2010). Brignull systematically categorized dark patterns and emphasized the aspects of these practices that negatively affect the user experience. Therefore, Brignull's contribution to the concept is important.

With the development of digital platforms, the use of dark patterns has become more sophisticated and widespread, especially in electronic commerce, social media and mobile applications. In this process, machine learning and artificial intelligence-supported algorithms analyze user behavior to develop personalized manipulation strategies and increase the impact of dark patterns.

Understanding the history of dark patterns helps us better understand how these techniques have evolved and their impact on user experience. Table 1 below provides a detailed overview of the development and milestones of dark patterns.

Table 1. Historical Process of Dark Patterns

Year	Milestone	Description
1990s	**The Emergence of Digital Manipulation**	Early e-commerce platforms, such as Amazon and eBay, introduced basic manipulative techniques, including targeted product placements, dynamic pricing, and early-stage pop-up ads (Nielsen, 1994; Wilson, 1997).
2000s	**Privacy Policy Complexification & Hidden Consent Strategies**	Websites began implementing complex, lengthy privacy policies that obscured data collection practices, making it easier for users to give implicit consent (Cranor, 2000). Subscription traps and forced continuity techniques also became more prevalent.
2010	**Introduction of the Term "Dark Patterns"**	UX researcher **Harry Brignull** coined the term "Dark Patterns" and categorized deceptive UI/UX tactics on his website *darkpatterns.org* (now *deceptive.design*) (Brignull, 2010).
2012-2015	**Expansion of Dark Patterns in Social Media & Mobile Apps**	Social media algorithms and mobile apps began integrating dark patterns, such as manipulative notifications, in-app purchase traps, and personalized engagement techniques (Gray et al., 2018).
2016-2019	**AI-Driven Dark Patterns & Algorithmic Manipulation**	The rise of artificial intelligence enabled highly personalized dark patterns. Machine learning algorithms began predicting user behavior, optimizing engagement tactics, and reinforcing compulsive digital habits (Anderson et al., 2020).
2018	**Regulatory Intervention: GDPR & Consumer Protection Debates**	The European Union's **General Data Protection Regulation (GDPR)** took effect, addressing dark patterns related to privacy, data transparency, and user consent (European Commission, 2018).
2020s	**Ethical Design, Legal Reforms & AI Transparency Debates**	Growing awareness of AI-driven manipulation prompted legal and ethical discussions on banning deceptive practices. Countries and regulatory bodies introduced laws against dark patterns in digital marketing (Federal Trade Commission, 2022; Zuiderveen Borgesius, 2018).
2023 & Beyond	**Future Directions: AI Ethics & Transparent User Experience**	Ethical design principles and AI transparency guidelines emerged to counteract dark patterns. Researchers and policymakers continue to advocate for fair, user-centric digital environments (Weinberg, 2018).

The development of dark patterns started with the spread of the internet and the birth of e-commerce platforms, and became more complex with the development of digital marketing techniques. Combined with artificial intelligence and big data analytics, algorithmic manipulation techniques

have become increasingly effective. Important milestones in this process can be summarized as follows;

1990s: First Traces of Techniques - The Beginning of Digital Manipulation

With the widespread use of the Internet, online commerce platforms have started to develop strategies to influence users' purchasing behavior. Pioneering e-commerce sites such as Amazon and eBay have transferred product placement, price display and promotion techniques used in traditional retailing to the digital environment (Nielsen, 1994). The manipulation techniques that emerged in this period are as follows:

- Ensuring that users see specific products with product placement algorithms,
- Offering different prices to different user groups with dynamic pricing strategies,
- The first pop-up ads were developed to direct users' attention to specific actions (Wilson, 1997).

2000s: Complexification of Privacy Policies and Commercial Use of User Data

With the rapid spread of the Internet, users' data privacy has become an increasingly big issue. Websites and digital service providers have developed complex privacy policies that allow users to give unconscious consent to collect personal data (Cranor, 2000). In this period;

- User agreements and privacy policies were made long and complex, allowing users to give consent without careful reading.
- "Forced continuity" and subscription traps have been developed to make it easier for users to sign up for services while making the cancellation process more difficult.

2010: Emergence and Systematization of Dark Patterns

Harry Brignull introduced the concept of dark patterns into the literature and began to systematically analyze such manipulative design strategies. He established the website darkpatterns.org (now updated as https://www.deceptive.design/) and contributed to raising awareness (Brignull, 2010). During this period, common examples of dark patterns include:

- "Roach Motel" strategies are methods that allow users to subscribe easily and make it difficult to unsubscribe,

- "Privacy Zudging" techniques, interface designs that encourage users to share more data,

- "Social Proof" manipulations are strategies that encourage users to imitate the behavior of others.

2012-2015: Spread of Dark Patterns and the New Era of Digital Marketing

The rapid growth of social media platforms and mobile applications has enabled dark patterns to reach a wider user base. In particular, personalized recommendation systems and algorithms have been used more effectively to direct users to specific content (Gray et al., 2018). During this period;

- Dark patterns became widespread in mobile apps (e.g., in-app purchase traps).

- Social media algorithms have developed manipulative strategies to ensure that users are exposed to certain content.

2016-2019: Artificial Intelligence Assisted Algorithmic Manipulation

Machine learning and artificial intelligence have led to more advanced techniques for predicting and guiding user behavior. Algorithms that analyze user data have started to create personalized dark patterns strategies at the individual level (Anderson et al., 2020). The prominent developments in this period are as follows;

- Dynamic pricing strategies started to be optimized according to individual purchase history.

- Algorithmic content recommendations included guidance mechanisms that encouraged users to spend more time.

2020 and Beyond: Legal Regulations and Ethical Debates

The proliferation of dark patterns has necessitated the development of legal regulations to protect user rights. Regulations such as the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) aim to limit dark patterns (Zuiderveen Borgesius, 2018).Today:

- Ethical design and transparency requirements are on the agenda.

- Laws have been developed to protect consumer rights.

- User awareness has increased and platforms containing dark patterns have been criticized.

Dark patterns have become more complex with the development of the internet and digital commerce, and have evolved into personalized manipulation techniques with artificial intelligence-supported algorithms. Although legal regulations and ethical design principles aim to limit these manipulations, the increasing sophistication of artificial intelligence leads to the emergence of new types of dark patterns.

3. Types of Dark Patterns and Artificial Intelligence Integration

Dark patterns are manipulative design strategies that direct users to perform certain actions without their awareness. These strategies usually target the weak points of human psychology and aim to prevent conscious decision-making processes. Today, artificial intelligence is being used to make these manipulative techniques more effective, analyzing user behavior and developing tailored manipulation strategies. Below, we examine common types of dark patterns in the literature and how AI optimizes these patterns.

3.1. Privacy Zudging

Privacy undermining is a type of dark pattern that relies on encouraging individuals to share their personal data or manipulating them into unconsciously giving up their privacy rights. This strategy involves design techniques and persuasion methods that induce users to unwittingly share more data. Social media platforms, e-commerce sites, and mobile apps use methods such as making default privacy settings less protective, presenting permission requests in ambiguous language, or deliberately complicating the process of changing privacy settings to carry out this manipulation (Böhm, 2018).

Artificial intelligence uses various algorithms to make privacy mitigation techniques more effective and personalized. Behavioral analysis, timing optimization, and personalized persuasion strategies are among the frequently used methods in AI-assisted privacy manipulation.

- ***Behavioral Analysis:*** By analyzing users' privacy preferences, previous decisions, and sensitivities, AI algorithms can determine which privacy settings certain individuals are more sensitive to. This analysis enables the creation of personalized manipulative strategies.

- ***Personalized Persuasion***: Customized privacy policies or persuasive messages are offered based on the user's profile and past interactions. For example, a social media platform may display tailored and emotionally-charged alerts to encourage a user to change their privacy settings.

- ***Timing Optimization:*** Artificial intelligence analyzes user behavior to determine the optimal moment to ask for privacy permissions. For example, privacy consent requests can be shown when the user is busy or making a purchase, increasing the likelihood that the user will accept without paying attention to the details.

Facebook's facial recognition feature can be examined from the perspective of privacy undermining. The messages Facebook uses to enable facial recognition are considered an example of AI-assisted privacy undermining. For example, users are presented with a statement such as "Your friends can tag you more easily in photos", aiming to minimize privacy concerns. Such messages encourage individuals to share more data by making the process of changing privacy settings seem user-friendly and advantageous (Waldman, 2020).

As a result, privacy undermining is an ethically controversial manipulation strategy that can lead users to unwittingly violate their right to protect their data. The role of artificial intelligence in this process is to analyze individuals' personal preferences to persuade them at the most opportune moments and develop customized techniques to induce them to share more data voluntarily. This raises serious ethical and legal questions in terms of protecting user privacy and necessitates the tightening of regulatory frameworks.

3.2. Forced Continuity

Coerced sign-up is a type of dark pattern that involves inadvertently steering users into paid subscriptions and deliberately complicating the cancellation process. This usually involves initiating automatic payments after a free trial period, complicating the cancellation process, and developing dynamic strategies that encourage users to continue their subscription. For example, a digital publishing platform may automatically charge users after the trial period expires by requesting their credit card information in advance and deliberately complicate the cancellation process (Følstad, 2020b).

Artificial intelligence uses advanced data analysis methods to make forced registration strategies more complex and effective. Techniques such as predicting user behavior, providing personalized offers, and making the cancellation process harder for the individual are widely used in AI-assisted subscription manipulation (Zuboff, 2019).

- ***Churn Prediction***: AI algorithms analyze previous usage habits and interactions to predict which users tend to unsubscribe. For example, by identifying users who frequently check settings for unsubscribes or who are less interested in content, specific interventions can be planned for them.

- ***Dynamic Retention Strategies:*** AI tries to keep users who tend to unsubscribe by offering them special offers and incentives. For example, a video streaming platform can show a user who wants to unsubscribe a message saying "You got a special 50% discount this month!" or try to keep the user's interest alive by offering special recommendations based on content that the user was previously interested in.

- ***Optimization of the Cancellation Process***: Artificial intelligence can make the subscription cancellation process more complex for the user. For example, some users may be presented with cancellation processes that include more steps, while others may be presented with different screens or distracting surveys such as "Why do you want to cancel your subscription?". At times when the user is impatient or tends to make quick decisions, deliberately lengthening the process may cause them to delay their decision to cancel (Cara, 2019; Coussement, and Van den Poel, 2006; Gkikas, and Theodoridis, 2022).

Research shows that AI-assisted forced persistence techniques cause 67% of users to continue their unwanted subscriptions (Chen et al., 2021). This shows how effective manipulative subscription strategies are and that users tend to continue their subscriptions without realizing it. In particular, services that initiate automatic payments at the end of the trial period, platforms that require users to contact a customer representative at certain hours to cancel subscriptions, or user interfaces that hide cancellation buttons are examples of forced registration techniques.

In digital broadcasting platforms, we can see forced recording manipulation supported by artificial intelligence. In particular, video streaming platforms use artificial intelligence to personalize unsubscribe processes and offer suggestions that encourage users to continue their subscription. When a user tries to unsubscribe before completing a movie, the system may display messages such as "Your subscription will remain active until you complete the content you are watching" as a strategy to delay the cancellation process.

As a result, forced sign-up strategies are an ethically questionable way of deliberately manipulating the user experience in order to keep people subscribed. Artificial intelligence makes these processes more effective by analyzing users' habits and weaknesses, and creates personalized challenges for individuals when unsubscribing. This situation raises important debates in terms of consumer rights, ethical design and digital marketing principles, and is among the issues that regulatory authorities should carefully address.

3.3. Social Proof

Social proof is a psychological and social phenomenon wherein people copy the actions of others in an attempt to undertake behavior in a given situation (Wikipedia, 2025). The peer pressure technique takes advantage of consumers' tendency to follow the decisions of their social circles to encourage them to take certain actions. For example, an e-commerce platform can influence users' purchasing decisions with statements such as "1000 people have bought this product" or "One of your friends liked this product". Artificial intelligence-supported systems analyze individuals' social networks and offer personalized content and recommendations, thereby increasing social pressure and strengthening the tendency to purchase (Cialdini, 2009). This strategy is commonly applied through the following methods.

- ***Popularity Indicators***: By using phrases such as "1000 people have bought this product" or "500 people have made a reservation in the last 24 hours", users develop a positive perception of the product or service.

- ***Friend Recommendations***: By showing users that their friends have purchased a certain product or used a service, social network pressure is created.

- ***Real-Time Notifications***: Notifications such as "Elanur just bought this ticket!" or "10 people are currently reviewing this hotel" encourage users to make quick decisions (Convertize, 2025; Deceptive Design, 2025).

Today, many online shopping sites offer dynamic recommendations that show which products similar users have purchased using an AI-powered system that triggers peer pressure. For example, when a user wants to buy a particular book, the system will suggest other products with the statement "Users who bought this book also bought this book". This technique influences the user's individual decision-making process and creates the perception that "If people like me are buying it, it's probably a good choice".

Digital movie streaming sites have developed recommendation systems that emphasize popular content, especially by using artificial intelligence-supported algorithms. They utilize social proof principles by showing users messages such as "This series is currently the 5th most watched content in Turkey" or "Your friends have watched this content". Furthermore, when the user wants to cancel their subscription, the system can encourage them to continue their subscription by increasing the social proof effect with messages such as "Don't miss the most watched content this month!".

Peer pressure strategies are a powerful manipulation technique based on the principle that people make decisions under the influence of their

social environment. Artificial intelligence makes this process more complex, allowing users to be manipulated through their social circles. While some of these techniques aim to improve the user experience, they carry risks of personal data misuse and unethical manipulation. When consumers are unconsciously manipulated into making a purchase decision or encouraged to use a service under social pressure, it is necessary to question the ethical limits of these techniques. Adopting transparency and ethical design principles in the digital marketing world and developing legal frameworks to protect users from deceptive or manipulative manipulation is of great importance.

3.4. Scarcity Principle

The scarcity principle is a type of dark pattern that forces users to make quick decisions by creating the perception that products or services are limited. Human psychology tends to perceive scarce resources as more valuable and desirable. Therefore, digital platforms use scarcity strategies to accelerate users' rational decision-making processes, forcing them to make hasty purchases or reservations (Nodder, 2009). This technique is particularly common in electronic commerce, hotel booking sites and ticketing platforms. Users are shown messages such as "Last 2 rooms left!", "This product is about to run out of stock!" or "10 people are currently looking at this ticket!" to make a quick and impulsive purchase decision.

Artificial intelligence uses advanced data analysis methods to reinforce the sense of scarcity and manipulate users' decision-making process. These techniques are as follows:

- ***Dynamic Scarcity Perception:*** By analyzing the user's previous searches, past purchase data and location information, AI can create personalized scarcity messages. For example, a hotel booking site may show the message "90% occupancy is now reached!" to a user who has previously searched for a hotel in a specific city, but this message may be different for another user.

- ***Real-Time Scarcity Simulation:*** AI algorithms can optimize scarcity messaging by analyzing the amount of time a user spends looking at a particular product and page interactions. For example, when an airfare search site notices that a user has looked at a flight several times, it can show the message "Last 3 tickets left!", thus making the user hurry.

- ***FOMO (Fear of Missing Out) Triggers:*** By taking advantage of users' "fear of missing out" (FoMO) psychology, the perception of scarcity is increased by informing them that other users have already purchased the product. For example, a fashion e-commerce site shows messages such as

"20 people have bought this product in the last 15 minutes!" to help the consumer make a quick decision.

- ***Fake or Exaggerated Stock Information:*** By analyzing the past behavior of the user, artificial intelligence can present stock information in a personalized manner. For example, when an online shopping platform notices that a particular user frequently makes price comparisons, it can display the message "Only 1 product left at this price!", thus enabling the user to make a quick purchase decision (Kim et al., 2023; Deceptive Design, 2025).

Booking websites, in particular, use scarcity tactics to speed up users' accommodation search processes by using artificial intelligence algorithms. When a user enters a hotel page, messages such as "Last 2 rooms left!" or "50 people booked this hotel today!" are displayed.

AI-powered scarcity strategies are a powerful manipulation tool that uses consumer psychology to help users make quick decisions. Unlike in real scarcity situations, these strategies put users under pressure, causing them to make unnecessary or hasty purchasing decisions. Raising consumer awareness of these manipulative techniques and forcing platforms to provide transparent inventory information can create a fairer digital trading environment against scarcity illusion tactics (Cialdini, 2009).

3.5. Hidden Costs

Hidden costs are a type of dark pattern that manipulates consumers by exposing them to additional fees, taxes or service charges that they did not initially see during the purchase process. This strategy is particularly prevalent in online shopping platforms, airline ticketing systems and subscription-based services. It is used to deliberately steer the decision-making process by exposing the user to additional costs that are not predetermined during the purchase process (Weinberg, 2018). For example, on an online shopping platform, the price of the product is attractively displayed, but at the checkout stage, shipping fees, transaction fees or additional taxes are added. In another example, an airline may initially offer a low-priced ticket, but then add additional costs such as seat selection, baggage allowance or transaction fees later in the ticketing process.

By analyzing users' price sensitivity, purchase history and payment trends, AI can dynamically determine which hidden costs to apply to which customers. This may result in some customers facing more hidden costs, while others may see different discounts.

Artificial intelligence-assisted hidden cost manipulation is realized through the following methods:

- ***Price Sensitivity Analysis:*** Artificial intelligence analyzes a user's past purchase data to determine how price sensitive they are. Customers with less price sensitivity may be charged more hidden costs, as they are predicted to be more inclined to complete the transaction.

- ***Dynamic Pricing:*** By analyzing the user's geographic location, previous shopping habits and browsing history, different surcharges can be displayed for each customer. For example, a customer who has previously shopped in the luxury category may be charged a higher shipping fee.

- ***Timing and Buying Psychology:*** Adding surcharges at the last stage, when the user is most likely to make a purchase, can reduce the likelihood of changing the purchase decision. For example, hidden costs can be added to users who are shopping during a sale period, as they are less likely to cancel the purchase because they think they've already gotten a deal.

- ***Cross-selling and Adding Additional Fees:*** Once users are in the buying process, "additional services offered with this product" can be offered to increase the total price unnoticed. For example, a user buying an airplane ticket is told that "it is recommended that you buy extra baggage allowance with this ticket", thus gradually increasing the additional fees (Deceptive Design, 2025; Binns, 2018).

Hidden costs are a manipulative technique that weakens the consumer's control over the shopping process and is becoming more complex with artificial intelligence. When faced with hidden costs, users are often manipulated into accepting additional charges rather than returning, thus making them spend more.

3.6. Roach Motel (Cockroach Motel) Technique

The Roach Motel technique is a type of manipulative dark pattern that allows users to easily sign up for services or subscriptions, while deliberately making the cancellation process difficult. The basic logic of this strategy is based on making the user's entry process simple and fast, but the exit process complex and cumbersome. It is widely used especially in subscription-based services, digital platforms and applications that require membership (Brignull, 2010). The most common applications of this technique are as follows:

- ***Easy online registration, but complex cancellation procedure***: While signing up for a gym membership or digital streaming service can be done

in a few clicks, canceling can only be done through a phone call to customer service, visiting the office at certain hours, or filling out lengthy forms.

- ***Intentionally hiding or redirecting the cancel button***: The user may have to navigate through multiple menus and sub-pages to find the cancel option. For example, when trying to cancel a subscription, messages such as "Are you sure you really want to cancel?" or "Keep your subscription to continue enjoying special offers" may appear.

- ***Applying psychological pressure to get the user to back down:*** Users who want to unsubscribe are shown phrases such as "You will lose these great benefits!" or "Most users are happy with our service, why are you leaving?" to create indecision (Deceptive Design, 2025).

By analyzing users' tendency to cancel, AI develops personalized strategies to get them to postpone their decision or abandon the cancellation process altogether. These techniques aim to keep the user connected to the service by making the cancellation process more difficult:

- ***User Behavior Analysis:*** Artificial intelligence algorithms can predict which users are inclined to cancel. For example, users who have not used the service for a long time or who have changed their payment methods may be perceived as more likely to cancel, and specific intervention strategies can be implemented for these people.

- ***Personalized Persuasion Messages***: By analyzing the user's previous behaviors and interests, artificial intelligence can present the most appropriate messages to persuade them. For example, when a music listening platform notices that the user's favorite artist has just released a new album, it can say "Your favorite artist's album will be released soon! Don't cancel your subscription!".

- ***Deliberately Prolonging the Cancellation Process***: When the user wants to cancel, AI-powered systems can guide them through a multi-step process. For example, a digital publishing platform may require the user to fill out a questionnaire during the cancellation process, so that the user may get tired and leave the process halfway through.

- ***Last Minute Special Offers:*** When AI algorithms realize that a user is about to complete the cancellation process, they can offer them a special discount. For example, "You just received a 50% discount! Do you want to continue canceling your subscription?" (Deceptive Design, 2025).

Some online movie streaming and music streaming platforms try to keep users on the service by deliberately complicating the unsubscribe process.

For example: The user may have to click through multiple submenus to find the cancel option. When the user tries to cancel, they may be presented with special discount offers or suggestions for future content. At the final stage, additional steps such as "Please fill out a survey before canceling your membership" can be added to prolong the cancellation process.

To counter this manipulative tactic, it is crucial that more transparent consumer policies are developed, users are made aware of their rights, and digital service providers adopt ethical design principles. Making users more aware of such manipulations and applying to regulatory bodies when necessary will be one of the most effective defenses against unethical marketing strategies such as Roach Motel.

3.7. Bait and Switch

Bait and switch is a type of manipulative dark pattern that lures users to take a certain action by tempting them with an attractive offer, but results in a worse option being offered later in the process instead of the promised one. This strategy, which is based on deliberately misleading consumer expectations, is widely used in various digital domains, especially e-commerce, financial services, subscription-based platforms, and mobile applications (Gray et al., 2018).

While traditional bait-and-switch techniques target the general user audience, artificial intelligence makes this process much more personalized and offers manipulative content based on users' individual tendencies.

AI-powered bait and switch strategies include the following:

- ***Behavioral Data Analysis:*** By analyzing users' past shopping habits, price sensitivities and interests, AI can identify the most attractive offers that will attract them the most.

- ***Dynamic Content Manipulation***: AI can show attractive offers or discounts when a user logs into the platform, only to remove them at the point of purchase and offer higher prices. For example, an airline ticket platform may show the ticket the user is looking for at a low price at the first login, but claim that the price has increased later in the purchasing process, allowing the user to make a quick decision.

- ***Customized Alternative Presentation:*** When it is determined that the user wants to buy a specific product, AI-powered systems can direct them to a more expensive alternative by indicating that stocks are out of stock or the discount period has expired.

- ***Timing and Urgency Manipulation:*** By detecting the moments when the user tends to make urgent decisions, AI can create a manipulative time pressure with messages such as "Don't miss this opportunity!".

An online shopping site may announce a campaign such as "Big discounts! Deals up to 70%!". However, when the user visits the site, it may turn out that the actual discount rates are much lower or that the most demanded products have been excluded. The user is attracted to a service with a free trial period, but later in the process may be hit with mandatory subscription fees or unexpected additional costs.

Dark patterns are strategies that manipulate the user experience and direct individuals' conscious decision-making processes. Artificial intelligence increases the effectiveness of these techniques, analyzing user behavior more precisely and taking the manipulation to a personalized level. This situation poses a significant problem in terms of consumer rights and ethical debates and reveals the need to update regulatory frameworks and raise awareness (Brignull, 2010; Gray and Kou, 2021; Deceptive Design, 2025).

4. Ethical and Social Implications of Artificial Intelligence-Powered Dark Patterns

AI-driven dark patterns stand out as manipulative design strategies that undermine consumers' autonomy, freedom of choice and privacy. Digital platforms use artificial intelligence algorithms to analyze user behavior, influence individuals' decision-making processes and direct them to perform certain actions. These manipulative approaches have important consequences not only on an individual level, but also on social and ethical dimensions (Zuiderveen Borgesius, 2018). We can summarize these consequences as follows:

- ***Declining Trust in Digital Platforms:*** As users encounter misleading and manipulative experiences, they may lose trust in digital platforms and online services. In the long run, this can undermine customer loyalty in the e-commerce, digital media and online service sectors (Koops, 2018).

- ***Impacts on Digital Literacy:*** When users are unwittingly exposed to manipulative strategies, they may struggle to understand how to act in the digital world. This can undermine their ability to use the internet responsibly and safely.

- ***Damage to Social Justice:*** AI-powered dark patterns can increase social and economic inequalities. For example, some consumers may be subjected to dynamic pricing strategies, while individuals with lower income levels

may face higher prices. Such practices are contrary to the principles of fairness and equality in terms of consumer rights.

AI-driven dark patterns raise serious ethical concerns, violating users' rights and influencing individuals' decision-making processes through manipulation (Bostrom, 2019). From an ethical perspective, the problems that these applications may create are as follows:

- ***Invasion of Privacy***: By analyzing users' online behavior, AI algorithms can identify their weakest moments and use this information for manipulative purposes. Users' consent without knowing exactly what data is being collected and how it is being used points to an unethical data management process.

- ***Restriction of Consumer Freedom:*** AI-powered dark patterns can disrupt users' rational and informed decision-making processes, causing them to suffer economically and psychologically. Deliberately restricting individuals' freedom of choice should be considered an unethical practice.

- ***Normalization of Manipulation:*** The proliferation of AI-assisted manipulation techniques may lead to the normalization of manipulative user experiences. This may lead to social acceptance of systems that unconsciously manipulate users' decisions.

The fight against dark patterns requires a multifaceted approach. Raising consumer awareness, adopting ethical design principles, establishing legal regulations and developing technological solutions are of great importance in this struggle.

In this context, consumer awareness raising activities can be carried out first. Consumers' knowledge about dark patterns will enable them to recognize these manipulative techniques and act consciously against them. Digital literacy trainings and public awareness campaigns can play an important role in this regard.

In addition, having ethical design principles will enable consumers to have a more transparent and fair user experience. User-friendly privacy settings and clear information processes should be implemented instead of techniques such as "Privacy Thinning".

Legal regulations together with ethical design principles can limit dark patterns (European Commission, 2020). In particular, banning manipulative practices that do not obtain the explicit consent of the consumer, forcing digital platforms to increase their transparency policies, and auditing and criminalizing unethical algorithms are among the measures that can be taken on these issues.

Conclusions And Recommendations

While the process of digitalization and the rapid development of artificial intelligence technologies provide many advantages by personalizing the user experience, they also offer new tools for consumer manipulation. Manipulative design strategies, referred to as dark patterns, are deceptive techniques that lead users to unconsciously perform certain actions. Today, AI-powered dark patterns have become more sophisticated and effective, leading to negative consequences such as forcing consumers into subscriptions, encouraging them to share their personal data, leading them to unwanted purchases, and causing financial losses.

The ethical and social consequences of dark patterns jeopardize the credibility of the digital ecosystem. These AI-powered manipulative practices reduce trust in digital platforms, cause consumers to suffer economic losses, and violate individuals' personal privacy. In addition, the creation of personalized manipulations using artificial intelligence algorithms causes especially low-income individuals to be more at risk. For all these reasons, consumer rights need to be protected, ethical design principles need to be adopted, and regulatory frameworks need to be strengthened.

Consumers, designers, regulators and technology companies have a shared responsibility to minimize the harms of dark patterns. The following measures should be taken to create a more conscious, ethical and transparent digital ecosystem against these manipulative techniques:

Ø Consumer Awareness and Increasing Digital Literacy

One of the most effective measures against dark patterns is to raise consumers' awareness and digital literacy. If users can recognize which manipulative techniques they are exposed to and make informed decisions, the effectiveness of such strategies will decrease.

Ø Adoption of Ethical Design Principles and Transparency in UX/UI Practices

In order to prevent the spread of dark patterns, ethical design principles should be adopted and transparency policies should be implemented in UI/UX. Digital platforms should prefer transparent and user-friendly designs instead of techniques that manipulate user experiences.

Ø Strengthening Legal Regulations and Establishing Audit Mechanisms

In order to bring dark patterns in line with ethical and fair trade rules, consumer protection laws need to be developed and regulators need to conduct effective audits.

Ø Establishing Ethical Standards for Artificial Intelligence Developers

To prevent the proliferation of AI-enabled dark patterns, AI developers should fulfill their ethical responsibilities and create user-friendly algorithms.

Ø Detecting and Preventing Dark Patterns with Technological Solutions

New technological solutions should be developed and offered to consumers in the fight against dark patterns.

Artificial intelligence-supported dark patterns are manipulative techniques that undermine consumers' free will and pose serious ethical problems. In the fight against such practices, it is critical to raise consumer awareness, adopt ethical design principles, establish legal regulations, ensure that artificial intelligence developers fulfill their ethical responsibilities, and prevent these manipulations with technological solutions. All stakeholders need to take responsibility to create a more fair, transparent and ethical digital ecosystem.

References

Anderson, J., Sarma, K. M., & Borning, A. (2020). Deceptive Design. *Communications of the ACM*, 63(10), 126-133.

Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency,* 149–159. https://doi.org/10.1145/3278721.3278722

Bostrom, N. (2019). *Süper zekâ: Yapay zekâ uygulamaları, tehlikeler ve stratejiler* (F. B. Aydar, Çev.). Alfa Yayıncılık. (Orijinal eser 2014'te yayımlanmıştır)

Böhm, K. (2018). Privacy by Design. *In: Encyclopedia of Big Data Technologies*. Springer, Cham.

Brignull, H. (2010). Dark patterns: Deception vs. honesty in UI design. Dark Patterns. Retrieved January 10, 2025, from https://darkpatterns.org/

Brignull, H., & Darlo, C. (2019). *The Dark Patterns Tip Sheet*. Retrieved from https://darkpatterns.org/

Cara, C. (2019). Dark patterns in the media: A systematic review. *Network Intelligence Studies*, 7(14), 105.

Chen, L., Lee, K., & Nissenbaum, H. (2021). Bias in Algorithmic Transparency. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1), 1-32.

Cialdini, R. B. (2009). *Influence: Science and practice*. Pearson Education.

Convertize. (2025). Social proof & dark patterns: How marketers manipulate consumers. Convertize. Retrieved January 7, 2025, from https://www.convertize.com/social-proof-dark-patterns/

Coussement, K., & Van den Poel, D. (2006). Churn prediction in subscription services: An application of support vector machines while comparing two parameter-selection techniques. Expert Systems with Applications, 34(1), 313–327. https://doi.org/10.1016/j.eswa.2006.09.038

Cranor, L. F. (2000). Internet privacy. *Communications of the ACM*, 43(9), 29-31.

Deceptive Design. (2025). Dark Patterns. Retrieved February 7, 2025, from https://www.deceptive.design/

Ducato, R., & Marique, E. (2018). Come to the dark side: We have patterns. Choice architecture and design for (un)informed consent. Choice Architecture and Design for (Un) *Informed Consent*.

European Commission. (2018). *General Data Protection Regulation* (GDPR).

European Commission. (2020). *Shaping Europe's Digital Future*. Retrieved from https://ec.europa.eu/digital-single-market/en/shaping-europes-digital-future

Federal Trade Commission. (2022). Available at: Bringing dark patterns to light. Assessed on September 26, 2022 https://www.ftc.gov/reports/bringing-dark-patterns-light.

Følstad, A. (2020a). Dark Patterns in UX Design. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. ACM.

Følstad, A. (2020b). What do users consider as dark patterns?. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1-14).

Gkikas, D. C., & Theodoridis, P. (2022). AI in consumer behavior. In Advances in artificial intelligence-based technologies (Chapter 10). Springer Cham. https://doi.org/10.1007/978-3-030-80571-5_10

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM.

Gray, C., & Kou, Y. (2021). "The Ethics of Dark Patterns in UX Design." *Journal of Business Ethics*, 169(3), 425-440. doi:10.1007/s10551-020-04443-3.

Kim, K. (K.), Kim, W. G., & Lee, M. (2023). Impact of dark patterns on consumers' perceived fairness and attitude: Moderating effects of types of dark patterns, social proof, and moral identity. Tourism Management, 98, 1–14. https://doi.org/10.1016/j.tourman.2023.104763

Koops, B. J. (2018). The Concept of Privacy in the Digital Age. In: Proceedings of the 2018 International Conference on Information Systems. AIS.

Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark patterns: Past, present, and future: The evolution of tricky user interfaces. ACM Queue, 18(2), 67–92.

Nielsen, J. (1994). Usability engineering. Morgan Kaufmann. https://www.nngroup.com/books/usability-engineering/

Nodder, C. (2009). Evil by Design: Interaction Design to Lead Us into Temptation. Wiley.

Waldman, M. (2020). Privacy as Trust. Cambridge University Press.

Weinberg, B. D. (2018). The Dark Side of UX Design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM.

Weinberg, G. (2018). Dark patterns in the design of digital interfaces.

Wikipedia. (2025). Social proof. Wikipedia, The Free Encyclopedia. Retrieved March 7, 2025, from https://en.wikipedia.org/wiki/Social_proof

Wilson, B. (1997). The Annoying Pop-Up Ads.

Zeller, W. (2014). Mobile application usability. Morgan & Claypool.

Zhang, Y., & Liu, Z. (2021). The Addictive Nature of Social Media. Journal of Computer-Mediated Communication, 26(5), 325-342.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Zuiderveen Borgesius, F. J. (2018). Dark Patterns in the Digital Economy. In: Proceedings of the 2018 International Conference on Information Systems. AIS.