UCLouvain

LOUVAIN
School of Management

Louvain School of Management

# “Dark patterns” - To what extent are user attitudes and behaviors influenced by incentive and deceptive mechanisms in the user interface (UI)?

A comparative analysis based on a taxonomy.

Author(s): Romain Vandenschrick
Supervisor(s): Pr. Chantal de Moerloose

Academic year: 2023-2024

Master's thesis to obtain the title of Master (120) in management sciences, with a specialized focus.

Daytime schedule.

# Declaration Regarding AI Tool Usage in Master's Thesis

1. **Critical Evaluation :**
    - We critically assessed the AI-generated output, ensuring its alignment with our research objectives.
    - Any modifications or corrections were made based on our expertise and domain knowledge.
2. **Transparency :**
    - We acknowledge the use of ChatGPT and SCISPACE transparently, emphasizing that it contributed to our work but did not replace human judgment.
    - Our commitment to transparency ensures the integrity of this thesis.
3. **Ethical Considerations :**
    - We actively monitored for biases or unintended consequences introduced by the AI tool.
    - Our ethical responsibility guided our decisions throughout the research process.

During the preparation of this master's thesis, the author(s) utilized ChatGPT and SCISPACE for the following purpose:

**1. Find academic articles:** SCISPACE helps find academic articles based on a provided research question. The AI assists in retrieving many articles, including those in other languages, as it is able to translate them.

**2. Correct the writing style:** ChatGPT was used to correct grammatical errors and to enhance the coherence and readability of certain parts.

**3. Find the statistical methods:** ChatGPT was used to generate ideas on the statistical methods that could be employed for the analysis.

4**. Generate first ideas/drafts:** ChatGPT was used to generate ideas for certain parts, which were then critically reviewed and modified.

After using ChatGPT and SCISPACE the author(s) diligently reviewed and edited the content produced by the tool. We take full responsibility for the final content presented in this thesis.

By signing this declaration, we affirm that the content of this master's thesis reflects our original work, augmented by the responsible use of AI.

*Read and approved, August 7, 2024.*

*Romain Vandenschrick*

Abstract:

This study investigates the influence of dark patterns—manipulative design tactics in digital interfaces—on user attitudes and behaviors. The primary objective is to develop a comprehensive classification system for dark patterns and empirically validate their impact on users' self-reported decision-making, emotions, trust, and loyalty. By using a structured survey distributed to 159 participants, and by employing t-tests and ANOVA analysis, the research analyzes various examples of dark patterns to assess their effects. Findings reveal that dark patterns do not significantly impact overall decision-making, contradicting existing literature. However, they elicit strong negative emotional responses, undermine trust, and reduce user loyalty. The study also confirms that user awareness significantly mitigates the impact of dark patterns, though age and IT confidence do not play significant roles.

The proposed classification in this study differentiates dark patterns based on their degree of obligation, deception, and visibility, providing a refined framework for understanding these manipulative tactics. The study reveals that forced dark patterns are found to be more blameworthy compared to oriented ones, deceptive dark patterns are more blameworthy than manipulative ones, and hidden dark patterns are more blameworthy than visible ones.

Theoretical implications include advancing the understanding of dark patterns by validating their influence on user behavior. From a managerial perspective, the findings emphasize the ethical responsibility of designers and managers to avoid manipulative tactics that can harm user relationships and brand reputation. Practical recommendations include avoiding manipulative design practices, implementing ethical design training, incorporating user feedback mechanisms, and conducting regular audits. Despite some limitations, such as potential survey biases and a limited number of dark pattern examples, this research offers valuable insights and suggests future studies should explore broader variables, longitudinal effects, AI detection methods, trust recovery strategies, and the mental health impacts of dark patterns.

**UNIVERSITÉ CATHOLIQUE DE LOUVAIN**
**Louvain School of Management**
Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve
Boulevard Emile Devreux 6, 6000 Charleroi, Belgique
Chaussée de Binche 151, 7000 Mons, Belgique
**www.uclouvain.be/lsm**

# Acknowledgements

*I would like to express my sincere gratitude to my supervisor, Prof. Chantal de Moerloose, for her insightful guidance, both academically and personally. Her patience and confidence in the project's success, as well as her valuable feedback and expertise, have been crucial for the development of this work and for my personal growth. Thank you so much, Professor, and I wish you all the best for this new chapter of life that is soon opening for you.*

*I would also like to thank all the professors and assistants at the LSM for their exceptional dedication and generous sharing of expertise. Their passionate teaching has been a constant source of inspiration, significantly enriching my academic journey.*

*I would like to extend a special mention to the large number of participants in this study. Their contribution has been essential to the research, and their keen interest along with their numerous positive feedback have been a valuable source of encouragement.*

*Lastly, I'm deeply grateful to my family and close friends for their unwavering support throughout this journey, especially during challenging times. Your patience, encouragement, and constant presence have been invaluable sources of motivation and comfort.*

# Contents

List of Figures

List of Tables

# 1. Introduction

## 1.1. Context of the study

In today's digital world, user interface (UI) and user experience (UX) design are crucial in shaping how users interact with websites and apps (Hassenzahl, 2018). While these innovations aim to provide seamless and enjoyable experiences, they have also introduced ethical challenges, particularly the use of dark patterns. Dark patterns are manipulative design tricks that push users into making choices they might not want to make (Cara, 2019). The term "dark patterns" was first coined by Brignull in 2010 to describe these deceptive tactics that benefit companies at the user's expense (Kollmer & Eckhardt, 2023). These patterns exploit psychological weaknesses, leading users to take actions that favor designers rather than customers (Mathur et al., 2019).

This research, titled “Dark patterns: To what extent are user attitudes and behaviors influenced by incentive and deceptive mechanisms in the user interface (UI)?” aims to explore the influence of these manipulative design strategies on user behavior and attitudes. The increasing use of dark patterns has drawn attention from researchers and regulatory bodies, as studies have shown these patterns can lead to user frustration, loss of trust, and diminished autonomy (Gray et al., 2021). Regulatory bodies, such as those enforcing the European Union's General Data Protection Regulation (GDPR), have begun addressing these issues with stricter data protection laws (Kollmer & Eckhardt, 2023). Despite these efforts, a comprehensive and universally accepted classification system for dark patterns is lacking, hindering a full understanding and regulation of their use.

## 1.2.Research aim

Existing classifications of dark patterns often categorize them based on single dimensions, i.e. their operating design and motivations, and don't consider the ethical dimension, i.e. the extent to which users may find one dark pattern more "blameworthy" (reprehensible) than another. These classifications may not fully capture the complexity and diversity of dark patterns. For this purpose, this contribution addresses these gaps by proposing a multidimensional classification framework that considers the degree of obligation, deception, and visibility. This comprehensive framework will enhance the understanding of dark patterns by reflecting contemporary digital contexts and will highlight their ethical implications and impacts on user behavior. By providing

a more refined classification, this study offers a robust basis for analyzing dark patterns and supports the development of more effective strategies to identify and mitigate their negative effects on users.

Additionally, the study will explore the impact of these patterns on users' self-reported decision-making, emotions, trust, and loyalty, as well as the roles of age, confidence in using the internet, and awareness of dark patterns in susceptibility to manipulation. Through detailed analysis and empirical validation, this research seeks to provide valuable insights into the nature of dark patterns and offer practical recommendations for designers and regulators to mitigate their negative effects.

### 1.3.Research questions and objectives

Since evolving digital landscapes are characterized by an increased complexity in terms of user interactions, this study seeks to fill current research gaps by proposing a new classification of dark patterns, drawing primarily from Mathur et al. (2021) and other sources. Additionally, this contribution aims at understanding the influence that dark patterns exhibit on users' attitudes and behaviors. Therefore, research questions can be formulated as follows:

- How can dark patterns be classified differently from existing literature to capture the complexity and "blameworthiness" of different types of dark patterns?
- Is the proposed classification of dark patterns confirmed based on users' experience?
- How do different types of dark patterns influence user self-reported decision-making, emotions, trust, and loyalty?
- Does age, confidence in using IT, and awareness of dark patterns reduce their manipulation of users?

### 1.4.Research significance

This research is significant in the field of human-computer interaction as it aims to clarify the understanding of dark patterns and their impacts. The new classification system offers a detailed and practical framework for identifying and analyzing dark patterns in digital interfaces. This research, based on a quantitative study, provides empirical evidence on the influence of dark patterns on users, which is useful for drawing policy recommendations for designers and regulators.

The study's significance lies in its potential to guide the development of ethical standards and regulations to protect users from manipulative design practices, as understanding the emotional and psychological effects of dark patterns can help designers create more ethical and user-friendly interfaces.

### 1.5.Methods and results summary

To achieve the research objectives, this study employed a hypothetico-deductive approach, which used a structured survey to test the influence of dark patterns on user behavior and attitudes among 159 participants. Participants were asked to report their experiences related to decision-making, emotions, trust, and loyalty, alongside demographic information, awareness of dark patterns, and IT confidence.

Findings show that dark patterns do not significantly affect overall decision-making, contradicting existing literature. However, they elicit strong negative emotional responses and reduce trust and loyalty. Users aware of dark patterns are less likely to feel manipulated, but age and IT confidence do not significantly influence susceptibility. The study emphasizes that forced dark patterns are found to be more blameworthy compared to oriented ones, deceptive dark patterns are more blameworthy compared to manipulative ones, and hidden dark patterns are more blameworthy compared to visible ones.

These results underscore the importance of ethical design practices and regulatory measures to protect users. The empirical findings validate the proposed classification system of dark patterns, highlighting the varying degrees of perceived blameworthiness across different types of dark patterns.

## 2. Literature review

### 2.1.Theoretical framework

The rapid advancement of technology has transformed web products, shifting user expectations from basic functionality to immersive experiences (Hassenzahl, 2018). This shift has led to the widespread adoption of UX principles, which prioritize the quality of interactions between users and interfaces, moving beyond the traditional human-computer interaction (HCI) model that emphasized functional aspects (Hassenzahl & Tractinsky, 2006). Since 2010, there has been a shift

from focusing solely on interface functionality to considering users' subjective emotions and experiences, emphasizing how interfaces affect user feelings and responses.

While enhancing user experience has led to personalized and engaging interactions, it has also raised concerns about manipulation, where users are subtly guided or misled into actions against their best interests (Cara, 2019). This practice, known as a dark pattern, is increasingly discussed in the literature (Gray et al., 2023). For this, the next subsection will define dark patterns in detail and examine their historical development.

### *2.1.1. Historical development and definition of dark patterns*

The concept of dark patterns emerged alongside modern digital technologies that increasingly influence user behavior and decision-making processes (Kollmer & Eckhardt, 2023). Before the digital age, manipulative strategies were used in traditional retail advertising to boost sales and collect information, such as using customer data for marketing calls without consent (Mathur et al., 2021; Troisi et al., 2020). With the rise of digitalization, these tactics migrated to the web, evolving into sophisticated techniques that manipulate users' choices (Narayanan et al., 2020).

Brignull coined the term "dark patterns" in 2010 to describe manipulative design tricks in websites and apps that lead users to take unintended actions (Narayanan et al., 2020). These designs exploit psychological vulnerabilities, such as preselected default options that prompt users to subscribe to newsletters or consent to data sharing (Mathur et al., 2021; Schneider et al., 2018). While Brignull's definition suggests dark patterns weaken user intention, Lukoff et al. (2021) note that some tactics, like infinite scrolling, align with user intentions but increase dependency and addiction (Monge Roffarello & De Russis, 2022).

Kollmer and Eckhardt (2023) provide a comprehensive definition of dark patterns, building on Mathur et al. (2021), Weinmann et al. (2016), and Sunstein (2015), describing them as design elements that undermine user autonomy by obstructing informed decision-making, potentially leading to privacy breaches and financial losses (Kollmer & Eckhardt, 2023). This definition highlights dark patterns' ability to manipulate users through visible and hidden means (Leiser & Yang, 2022).

While initial research focused on defining dark patterns, recent studies have explored taxonomies and ethical considerations (Fansher et al., 2018; Nouwens et al., 2020). Additionally, the growing

body of literature still underscores the need to understand dark patterns to protect users from their adverse effects (Lukoff et al., 2021). To note, current efforts of many regulatory bodies like the European Union's GDPR is to enforce the implementation of laws requiring user consent before data collection (Kollmer & Eckhardt, 2023), while the US Federal Trade Commission educates the public and explores ways to ban these deceptive practices (Obi et al., 2022).

### *2.1.2. Choice architecture and psychology behind dark patterns*

While the definition and evolution of dark patterns underscore the critical role of choice architecture in influencing user behavior, it is important to highlight that the presentation of choices on websites and apps plays a significant role in shaping users' decision-making processes (Day & Stemler, 2019). This concept, known as choice architecture, is rooted in behavioral economics and has fundamentally shaped digital interface design. While a later section will explore the specific relationship between dark patterns and decision-making, this section introduces choice architecture as a foundational theory informing digital design (Zhao, 2018).

According to Johnson et al. (2012), no web interface is neutral; each is designed with an underlying intent. Many developers craft platforms to subtly guide users toward specific decisions under the guise of free will. Zhao (2018) notes that while users aim to maximize their utility, the context and environment of decision-making, especially in digital spaces, heavily influence their choices.

Choice architecture exploits cognitive biases to shape decision-making. By definition, cognitive biases are tendencies for individuals to deviate from rational thinking, often resulting in perceptual errors. One common strategy is the use of preset and default setting, where preselected options require effort to change, leading users to comply (Bösch et al., 2016). For example, pre-checked boxes are frequently used in subscription services to enroll users in newsletters or gain consent for data usage (Figure 1). This strategy leverages the default effect, whereby users tend to accept preset options rather than altering them.

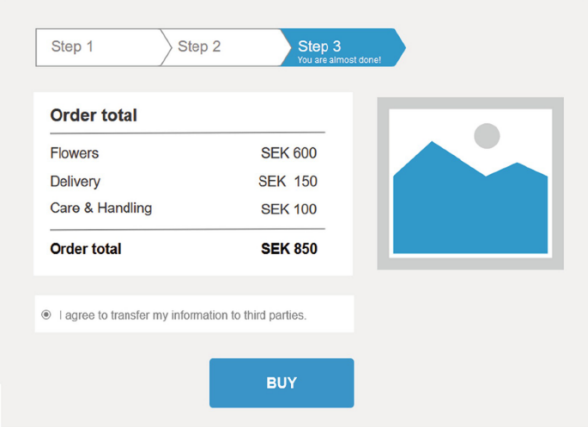



***Figure 1: Last minute pre-checked consent box***

***Source: (Kitkowska, 2023)***

Another technique is framing effects, which influence perception by presenting information strategically. Johnson et al. (2012) find this method highly effective; for example, service websites often highlight cost savings with annual plans over monthly ones, encouraging long-term commitments. Furthermore, when users face information overload, as in online shopping, they rely on heuristics and cognitive shortcuts (CNIL, 2019). Sunstein (2019) suggests that offering a single choice can create an illusion of control, even when the decision is influenced by how options are structured.

Choice architecture includes other tactics like misdirection, forced continuity, scarcity, and social proof (Bogliacino et al., 2023). For misdirection, it diverts attention from crucial information, leading to uninformed decisions (OECD, 2022). However, forced continuity traps users in ongoing commitments by complicating cancellation processes, exploiting aversion to effort (Figure 2). Gray et al. (2018) describe hidden cancellation options requiring multiple steps. Additionally, scarcity and social proof create urgency (e.g., "Only 1 item left!") or pressure (e.g., "12 people are viewing this item"), exploiting the fear of missing out (FOMO) and social conformity, driving hasty decisions (Cialdini, 2006).

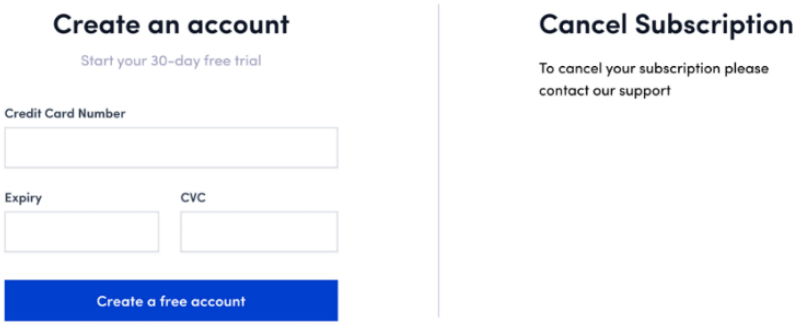



***Figure 2: Forced continuity dark pattern by making subscription cancelation difficult***

***Source: (Wolfgang, 2023)***

### *2.1.3. Nudging theory*

Concerning the nudging theory, which is one of the most common one when talking about dark patterns, it was introduced by Thaler and Sunstein (2008), and refers to subtly guiding users toward specific decisions without limiting their freedom of choice. Nudges can be beneficial when used ethically to promote positive behaviors. However, in the context of dark patterns, nudging techniques are often exploited to serve corporate interests at the user's expense. For instance, Mathur et al. (2019) highlight how e-commerce sites make the "Agree" button for additional purchases prominent while making "Opt-out" options less visible. This visual nudge manipulates users into making choices that benefit the platform.

### *2.1.4. Dark patterns and A/B testing*

The relationship between dark patterns and choice architecture cannot be fully understood without examining the role of A/B testing in their development.

A/B testing, commonly called "split testing," involves a between-subjects experimental approach in which participants are exposed to either variant A or variant B of a UI design. The goal is to evaluate which version is more effective based on predefined Overall Evaluation Criteria (OEC). (Vanderdonckt et al., 2019).

While this method enhances user experience and boosts conversion rates, it is often used to create and refine dark patterns. Narayanan et al. (2020) suggest that many dark patterns stem from A/B tests, where developers identify the most effective manipulative designs to influence user behavior and achieve goals like increasing newsletter subscriptions. By analyzing how users respond to different designs, developers continuously refine strategies to guide users toward specific actions (Figure 3).

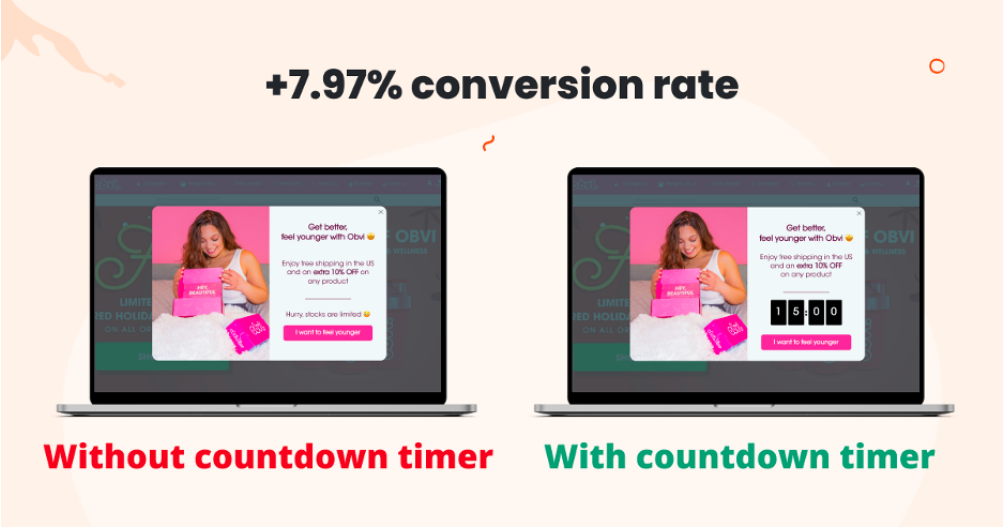



***Figure 3: A/B testing for enhanced conversion rate when implementing a count down in the design***

***Source: (Lorincz, 2024)***

For example, A/B testing can help determine the best placement for subscription offers to maximize unintentional sign-ups or identify which pre-checked box design minimizes opt-outs for additional services. E-commerce sites often use this approach to make "Agree" buttons for add-ons more prominent while obscuring "Opt-out" options (Mathur et al., 2019). This iterative method exploits insights from human cognition studies to fine-tune manipulative designs, thereby maximizing their impact.

The next subsection will explore the relationship between dark patterns and user emotions, further examining how these designs influence user behavior and experience.

### *2.1.5. Dark patterns and user emotions*

Many studies have demonstrated the significant impact of dark patterns on users' emotions and behavior (Lewis, 2014; Yada et al., 2022). These deceptive strategies exploit psychological

vulnerabilities, resulting in negative emotional reactions such as frustration, distrust, and feelings of manipulation (Gunawan et al., 2022). Dark patterns evoke strong emotional responses through deceptive design techniques, causing users to feel manipulated, frustrated, or deceived (Singh et al., 2023).

Emotional manipulation is a core aspect of dark patterns, with the goal of benefiting organizations. Research suggests that mild dark patterns (e.g., hidden information and costs) can generate profits without significant backlash, whereas aggressive dark patterns provoke strong user resentment (Luguri & Strahilevitz, 2021). This highlights the complex relationship between the severity of dark patterns and the emotional reactions they provoke.

#### *2.1.5.1.Emotional Distress and Loss of Autonomy*

Dark patterns can lead to emotional distress and a loss of autonomy among users. Manipulative designs impose cognitive burdens and foster addiction, intensifying negative emotional states (Gunawan et al., 2022). For instance, dark patterns in video streaming services exacerbate addictive behaviors, impacting users' emotions through specific UI designs and contextual factors (Chaudhary et al., 2022). Temporal dark patterns, which waste users' time and create a sense of obligation, particularly manipulate emotions, causing frustration and annoyance (Lewis, 2014; Voigt et al., 2021).

Similarly in social media, resistance to dark patterns is growing, with users increasingly aware and emotionally reactive against these tactics, especially in regions with regulatory measures. This shift highlights the importance of awareness and resistance to dark patterns.

#### *2.1.5.2.Perceptions, awareness, and dark patterns manipulation*

The psychological effects of dark patterns are evident in studies on user perceptions. Users perceive manipulative designs as sneaky and dishonest, contributing to frustration and distrust towards organizations using these tactics (Maier & Harr, 2020). This perception impacts brand trust and consumer loyalty, as users feel manipulated and are less likely to trust brands employing dark patterns (Voigt et al., 2021).

Interestingly, despite awareness of dark patterns, users find it difficult to resist their influence, often adopting a resigned attitude (Bongard-Blanchy et al., 2021). In social robotics, dark patterns manipulate users' emotions through deceptive design, raising ethical concerns about their use in

intimate settings. Recommendations for ethical practices in designing emotional social robots emphasize the need for awareness and regulation to protect vulnerable users from emotional manipulation (Dula et al., 2023).

Overall, the literature underscores the significant emotional impact of dark patterns on users, ranging from frustration and annoyance to distrust and manipulation (Voigt et al., 2021; Yada et al., 2022). These emotional effects call for greater awareness, ethical considerations, and regulatory actions to mitigate their negative consequences. To further support this last statement, the next subsection will further explore how they influence decision making, and the business objectives from using them.

#### *2.1.6. Dark patterns and users' decision-making*

Dark patterns significantly impact decision-making by subtly manipulating user choices through deceptive designs. These techniques exploit cognitive biases, leading to decisions that often benefit service providers at the expense of users. For example, in online shopping, dark patterns can drive impulse buying by pushing users to make hurried decisions (Sin et al., 2022). Similarly, in cookie consent requests, dark patterns increase consent rates by nudging users toward actions they might otherwise avoid (Graßl et al., 2021).

Dark patterns frequently exploit cognitive biases to manipulate decisions. Scarcity and urgency tactics leverage FOMO to prompt immediate actions (OECD, 2022). Video streaming services use autoplay features to exploit users' tendencies to continue watching beyond their initial intentions, highlighting how dark patterns can extend user engagement (Chaudhary et al., 2022).

Even when users recognize dark patterns, this awareness does not always enable them to resist effectively. Recognizing manipulation does not always translate to avoiding it, as the subtlety and pervasiveness of dark patterns often lead users to act against their best interests (Bongard-Blanchy et al., 2021). This underscores the need for regulatory and design interventions alongside user education.

Addressing dark patterns is crucial for enhancing user autonomy and trust. Implementing ethical design practices that prioritize user welfare can mitigate the adverse effects of dark patterns. Developing automated tools to detect and flag dark patterns can empower users to make more informed decisions (Hausner & Gertz, 2021; Raju et al., 2022).

### *2.1.7. Business objectives of dark pattern and consequences for users*

The implementation of dark patterns is often driven by various business objectives. The primary goal is to enhance conversion rates and maximize financial revenues. This is typically achieved through tactics like forced continuity, where customers are automatically subscribed to a service after a free trial without clear reminders. Companies frequently exploit such tactics to boost revenues, particularly during peak sales seasons.

Another objective is to enhance user engagement using strategies like endless scroll and deceptive countdown timers. Social media companies, for instance, use infinite scroll to maximize engagement, which is directly linked to increased ad revenue streams (Runge et al., 2023).

Dark patterns also aim to maximize data collection by manipulating users into sharing more information than they might initially intend. Tactics such as pre-checked boxes encourage users to share data, which is then used for targeted advertising and personalized content.

However, these business objectives can have serious implications for users, including decreased trust in platforms, direct financial losses, compromised autonomy, and a negative user experience (Aagaard, 2022; Bhatia & Alojail, 2022; Gonzaga, 2023; Gunawan et al., 2021). Companies must weigh these factors carefully, as short-term gains from dark patterns may be outweighed by long-term damage to reputation and user relationships.

### *2.1.8. Ethical implications of dark patterns*

Dark patterns raise significant ethical concerns due to their manipulative nature, which prioritizes business goals over user autonomy and informed consent. These deceptive practices undermine the trust between users and digital platforms, leading to calls for increased regulation and ethical standards in design. Researchers advocate for legal frameworks that address these practices, combining consumer protection and data privacy laws to restrain manipulative designs (Leiser, 2022).

The ethical implications extend to the need for transparency in how digital interfaces are structured, emphasizing user-centric design principles. Companies are encouraged to adopt ethical design practices that prioritize user welfare and long-term trust over short-term gains. Developing and implementing automated tools to detect and flag dark patterns can also play a critical role in protecting users and promoting ethical standards in digital design (Hausner & Gertz, 2021).

Overall, addressing the ethical implications of dark patterns is essential for fostering a more transparent and trustworthy digital environment. By prioritizing ethical considerations, businesses can build stronger, more sustainable relationships with their users, ultimately benefiting both parties in the long term.

## 2.2.Typology and classification of dark patterns

The previous section explored fundamental concepts of dark patterns. This section categorizes and elaborates on different typologies of dark patterns identified in the literature, providing a framework for analyzing these patterns from users' perspectives. Additionally, this section will provide examples of various types of dark patterns that will be the foundation for proposing the new classification in Section 2.2.3.

### *2.2.1. Existing classifications of dark patterns*

Leiser and Yang (2022) identify several taxonomies for dark patterns. A notable classification by Conti and Sobiesk (2010) simplifies Brignull's original typology into 11 groups that are coercion, confusion, distraction, exploiting errors, forced work, interruption, manipulated navigation, obfuscation, restricting functionality, shock, and trickery. These categories capture various ways dark patterns can manipulate users, such as through intimidation, misinformation, and misleading navigation.

Gray et al. (2018) offer another influential taxonomy, categorizing dark patterns into five groups based on designer strategies and motivations. These include nagging (persistent intrusions like pop-ups), obstruction (hindering user actions), sneaking (hiding crucial information), interface interference (manipulating UI to favor certain actions), and forced action (compelling user actions to access features). This classification highlights the diverse tactics used to influence user behavior and preferences.

But for Mathur et al. (2019), the authors provide a taxonomy based on observations of over 10,000 shopping websites, systematically explaining how dark patterns affect decision-making. They define asymmetric designs (imposing unequal choices), restrictive designs (limiting options), covert designs (hiding effects), and deceptive designs (misleading statements). Their seven types of dark patterns include sneaking, urgency, misdirection, social proof, scarcity, obstruction, and forced action.

Finally, Leiser and Yang (2022) also propose a taxonomy focusing on information asymmetry and free choice repression. Concerning information asymmetry, it involves traders holding superior information, leading to power imbalances. This splits into active misleading actions (false information) and passive misleading omissions (withholding information). But for free choice repression, it includes undesirable impositions (pressure through prompts) and restrictions (difficulty in canceling services).

While the existing classifications of dark patterns are extensive according to Leiser and Yang (2022), they have certain limitations. Many current frameworks, as outlined by Leiser and Yang (2022), focus on specific elements like coercion or deception without considering how these elements interact. This can lead to an incomplete understanding of how dark patterns work together to influence user behavior.

Additionally, these classifications often fail to keep up with the fast-paced changes in technology and user interactions. As digital environments evolve, there is a need for a classification system that can adapt and provide insights into new user experiences.

For this, a later proposed classification of dark patterns aims to address these gaps by offering a more comprehensive framework that considers the level of obligation, deception, and visibility of dark patterns. This approach provides a clearer picture of how dark patterns function and helps designers and policymakers create more ethical digital environments. By overcoming the limitations of existing classifications, this new framework adds value to the field by offering a more effective tool for analyzing dark patterns and their effects on users.

### *2.2.2. Dark patterns examples*

This section provides examples of dark patterns identified in the literature, illustrating the diverse tactics companies use to influence user behavior for specific business objectives. The goal is to highlight a few representative examples that demonstrate the strategies behind these manipulative designs. This section will present four specific dark patterns to showcase the variety of tactics employed. However, an exhaustive list of dark patterns, including their definitions, methods used to influence users, objectives, and other details, is provided in Appendix A. These examples help lay the groundwork for understanding the broader scope of dark patterns, which is essential for proposing a new classification framework.

The first example is the "last-minute consent," which requests data collection consent at the final stages of a process, such as during order confirmation, exploiting users' focus on task completion (CNIL, 2019). This tactic often results in frustration and stress.

Second, the "urgency" dark pattern creates artificial deadlines on sales or promotions using countdown timers and limited-time messages (Mathur et al., 2019). It exploits scarcity bias and FOMO, leading to excitement, anxiety, frustration, and mistrust.

Third, the "pay to pass" pattern limits access to features or content unless users pay, commonly seen in mobile games and subscription services (Gray et al., 2018). It targets users at crucial moments, aiming to increase revenue by exploiting their desire for an uninterrupted experience, often resulting in frustration and dissatisfaction.

Lastly, the "just you and me" pattern fabricates a sense of intimacy or exclusivity, commonly found in online dating apps and social media platforms (Gray et al., 2018). This dark pattern creates a perception of personal connection to enhance engagement but can lead to deception and mistrust when the interaction is revealed to be impersonal.

Appendix A provides a detailed explanation of 48[1] dark patterns, outlining their objectives, methods, and user sentiments. Based on the existing literature from well-known academic scholars and authors, these 48 dark patterns constitute an exhaustive list of the existing dark patterns identified in digital interfaces (Bösch et al., 2016; Bringull, 2023; CNIL, 2019; Conti & Sobiesk, 2010; Frobrukerrådet, 2018; Gray et al., 2018; M. Leiser & Yang, 2022; Mathur et al., 2019; Zagal et al., 2013). This ensures that the proposed classification is grounded in a comprehensive analysis of current knowledge.

[1] The 48 dark patterns are: preset & default settings, default sharing, rarity, urgency, social proof, pay to pass, monetized rivalries, last minute consent, security blackmail, ease & manipulation navigation, preventing comparisons and obstructing the comparison, visual interference, diversion of attention and distraction, obscuration, hard to cancel and immortal accounts, difficulties in adjusting confidentiality, obscure and “suckering” privacy settings, frame, confirmshaming and blaming the user, improved experience, just you and me, false rarity, false urgency, fake social proof, false declaration, bait and change, wrong signal, disguised ads and camouflaged advertising, trick, two-sided, misleading wording/trick questions and confusion, chameleon strategy, control and restricted features, forced action and coercion, reward and punishment, impenetrable wall and forced inscription, harassment and repeated incitement, interruption, obstruction, play by appointment, forced labor, automate the user, hidden subscription, false continuity, hidden legal stipulation, hidden costs/nickel and gradation/pre-delivered content/sneakiness, sneak into basket, and trap.

For better understanding, Appendix A includes columns summarizing the proposed classification, each dark pattern's ID, type, explanation, objectives, user sentiments (e.g., how users feel after experiencing the dark pattern), methods used to trick users, and a "blameworthiness" score. The blameworthiness score will further be explained after proposing the new classification in a later section.

### *2.2.3. Proposed classification of dark patterns*

Building on existing literature, this section introduces a new classification framework for dark patterns. By categorizing dark patterns into oriented vs. forced, manipulative vs. deceptive, and hidden vs. visible, this framework aims to capture the complexity and multifaceted nature of these tactics. To note, existing classifications often focus on single dimensions or isolated features, which may overlook the complex ways dark patterns interact and affect user behavior. This new proposed classification will address these gaps by providing a more comprehensive understanding that reflects modern digital contexts and user experiences. This framework allows for a refined analysis of how different dark patterns operate, considering not just their apparent characteristics but also the underlying psychological and ethical implications.

This classification is different from existing ones because it integrates multiple dimensions of dark patterns, offering a holistic view that better captures their impact on users. By combining factors like obligation, deception, and visibility, this new framework offers a structured approach to understanding the mechanisms behind dark patterns and serves as a foundation for developing hypotheses about their influence on users in Section 2.3.

#### *2.2.3.1.Oriented vs forced dark patterns*

In this study, dark patterns are first classified into oriented and forced categories based on how they manipulate user behavior. Oriented dark patterns subtly guide users toward specific decisions, often without their full awareness. They leverage, for example, psychological and emotional biases. Or even asymmetry in the presentation of choices through framing effect to steer users toward actions benefiting the business. Examples include misdirection, which diverts attention from important information, and preselection, where options are pre-ticked to encourage users to make unintended choices (Gray et al., 2018; Mathur et al., 2019).

Conversely, forced dark patterns are tactics that explicitly limit or eliminate users' choices, often compelling them to take specific actions without providing clear alternatives. These patterns interrupt users' tasks, impose coercion, or act without their consent, making them feel trapped or manipulated. An example is forced enrollment, where users are required to sign up or share personal information to access content (Gray et al., 2018).(Gray et al., 2018).

#### *2.2.3.2.Manipulative vs. deceptive dark patterns*

In addition to the first layer of classification discussed above, dark patterns can also be categorized as manipulative or deceptive. Manipulative dark patterns do not deceive the user but exploit various techniques to guide users toward actions benefiting the service provider. These tactics are often subtle, playing on emotions like urgency and scarcity to prompt hasty decisions (Mathur et al., 2019). In the other hand, deceptive dark patterns rely on false or misleading information/elements in the UI or omit crucial details to trick users into making decisions they might not otherwise make. Examples include hidden costs or disguised advertisements (Gray et al., 2018).

Manipulative patterns often leverage influence, while deceptive patterns rely on misinformation or omission of information, leaving the user confused. Understanding this distinction is crucial for identifying unethical design practices in digital interfaces.

#### *2.2.3.3.Hidden vs. visible dark patterns*

Dark patterns are further distinguished as hidden or visible. Hidden patterns operate covertly, influencing users without their explicit awareness. They involve subtle design elements that guide user behavior, such as pre-selected checkboxes or buried information in terms and conditions (Gray et al., 2018). Hidden dark patterns hide the mechanism of influence from the user or hide part of the information needed for decision-making

In the contrary, visible dark patterns, although easily noticed, manipulate behavior through, among others, psychological pressure. Examples include countdown timers that create urgency or recurring pop-ups that prompt subscriptions. These patterns exploit, for example, FOMO or frustration to induce immediate responses (Mathur et al., 2019). They can also imply a coercion or restriction in the choices that is easily visible to the users.

### *2.2.3.4.Proposed classification conceptual framework*

This study proposes a new classification framework for dark patterns based on three layers: oriented vs. forced, manipulative vs. deceptive, and visible vs. hidden. The first layer assesses the degree of obligation, with oriented patterns considered less blameworthy than forced ones. The second layer distinguishes between manipulative and deceptive patterns, with manipulative patterns deemed less blameworthy. Finally, the third layer evaluates visibility, with visible patterns viewed as less blameworthy than hidden ones (Figure 4). The 48 dark patterns in the table (Appendix A) have been inserted into this classification (ID column) according to their attributes.

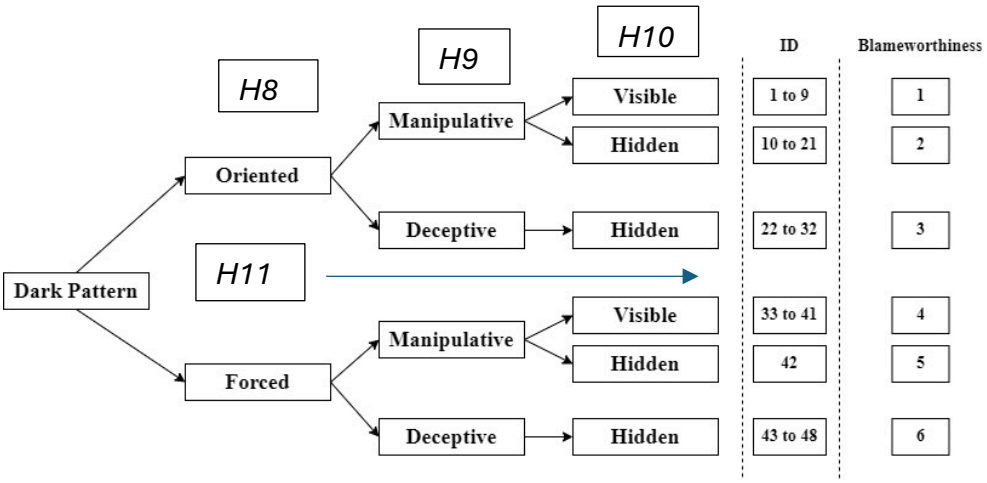



***Figure 4: Proposed classification of dark patterns***

***Source: Composed by the author.***

The blameworthiness score ranges from 1 (least blamable) to 6 (most blamable) and reflects the negative impact of each dark pattern based on its ethical implications (its degree of negative impact on the user, its reprehensibility). This scoring system is structured according to the six main branches of the proposed classification, as depicted in Figure 4. These branches are oriented manipulative visible, oriented manipulative hidden, oriented deceptive hidden, forced manipulative visible, forced manipulative hidden, and forced deceptive hidden.

The rationale for this ranking lies in the nature of each classification level. Patterns are evaluated first by the degree of obligation (forced vs oriented) they impose on users, then by whether they are manipulative or deceptive, and finally by their degree of visibility. For example, "forced-deceptive-hidden" patterns are considered most blameworthy due to their high degree of coercion

and deception, coupled with their lack of transparency, making them difficult for users to identify and avoid. In contrast, "oriented-manipulative-visible" patterns are deemed least blameworthy as they exert less pressure on users and are more straightforward to recognize, allowing users to make informed decisions. This structured approach helps in systematically assessing the ethical implications of different dark patterns, guiding the development of hypotheses in subsequent sections.

It is essential to emphasize that deceptive dark patterns cannot be visible due to their very nature. They must be hidden to the users to be effective, by relying on false information or the omission of information necessary for decision-making. For these tactics to work, it is crucial that users remain unconscious of the “deception” being applied to them.

### 2.3.Hypotheses development

This final section of the literature review develops hypotheses to empirically validate the proposed classification and assess the impact of dark patterns on users' self-reported decision-making, emotions, trust, and loyalty. It also examines how age, confidence in using IT, and awareness of dark patterns influence users' susceptibility to manipulation. These hypotheses are based on the theoretical insights and classifications discussed earlier, aiming to create a structured framework for analyzing the complex effects of dark patterns.

Studies have shown that dark patterns exploit cognitive biases, leading users to make decisions that benefit designers more than users (Mathur et al., 2021). Tactics like countdown timers create a sense of urgency, pushing users to make rushed decisions (Mathur et al., 2019). Similarly, manipulative designs such as pre-selected options or hidden costs can lead users to unknowingly agree to terms they might otherwise reject (Bösch et al., 2016). These tactics exploit psychological vulnerabilities, making it difficult for users to make fully informed decisions (Gray et al., 2021). Therefore, this study hypothesizes:

- **H1: Dark patterns significantly influence users’ self-reported decision-making.**

In addition to that, and as previously mentioned, dark patterns often lead to negative emotional responses. Research shows that exposure to dark patterns can result in frustration, anxiety, and regret (Mathur et al., 2019). Users manipulated into purchases or coerced into subscriptions without clear consent often feel deceived and frustrated. Therefore, it is hypothesized:

- **H2: Dark patterns elicit self-reported negative emotions among users, such as frustration or anger.**

Concerning trust, which is a fundamental component of user interactions with digital platforms, it is very undermined by dark patterns. This is because deceptive tactics like hiding information or providing misleading details breach trust (Gray et al., 2018). For instance, when users realize they have been manipulated or their consent bypassed, they feel betrayed, diminishing their trust in the service. Hence, it is hypothesized:

- **H3: Dark patterns have a significant negative impact on users' self-reported trust in the website/application.**

Concerning loyalty, it is closely tied to trust and satisfaction. When users feel tricked or coerced, their loyalty to the platform is compromised. Studies indicate that users subjected to dark patterns are less likely to return and more likely to share negative experiences (Bösch et al., 2016). This can lead to decreased repeat usage and increased negative word-of-mouth, detrimental to the business. Based on this, this study hypothesizes:

- **H4: Dark patterns have a significant negative impact on users' self-reported loyalty to the website/application.**

It is important to note that in the context of dark patterns, user awareness about them plays a critical role in mitigating their influence on users. Educated users are more vigilant and less likely to be deceived (Gray et al., 2018). However, some scholars argue that this may not hold true in all contexts, such as social media platforms. Since age and confidence in using IT might indirectly increase awareness, it is hypothesized that:

- **H5: Age influences the likelihood of being manipulated by dark patterns.**
- **H6: Confidence in using IT influences the likelihood of being manipulated by dark patterns.**
- **H7: Awareness of dark patterns influences the likelihood of being manipulated by them.**

The remaining hypotheses will investigate the extent to which the proposed classification holds true. For forced dark patterns, they eliminate user choice by compelling actions, infringing on

autonomy, while oriented dark patterns guide users but allow choice. This makes oriented dark patterns seem less intrusive (Gray et al., 2018). Hence, it is hypothesized that:

- **H8: Forced dark patterns are perceived as more blameworthy/reprehensible than oriented dark patterns.**

Similarly, deceptive dark patterns provide false information or hide crucial details, making them perceived as highly unethical. In contrast, manipulative patterns exploit cognitive biases without outright deceit. For this, this study assumes that users view deceptive tactics more negatively, feeling deliberately misled (Mathur et al., 2019). Therefore, it is hypothesized that:

- **H9: Deceptive dark patterns are perceived as more blameworthy/reprehensible than manipulative dark patterns.**

In terms of the last layer of the classification, it is important to note that visible dark patterns are detectable by users, while hidden ones are not. Therefore, this study assumes that hidden patterns have a more negative impact when users later realize they have been deceived, often resulting in greater blameworthiness and perceived unethicality. Hence, this study suggests that:

- **H10: Hidden dark patterns are perceived as more blameworthy/reprehensible than visible dark patterns.**

Finally, the study tests the importance of the order of the three layers of classification, hypothesizing that the degree of obligation is more blameworthy compared to the degree of deception. Additionally, the degree of deception is more blameworthy compared to the degree of visibility. This can be formulated as:

- **H11: The degree of obligation is more blameworthy compared to the degree of deception, and the degree of deception is more blameworthy compared to the degree of visibility.**

This expanded hypothesis framework provides a comprehensive basis for understanding the ethical implications and impacts of dark patterns, contributing to the broader discussion on digital ethics and user protection.

# 3. Methodology

## 3.1.Research design and approach

This study adopts a positivism research philosophy, which asserts that reality can be observed, measured, and analyzed using scientific methods (Bryman, 2016). Positivism emphasizes empirical evidence and statistical methods to identify relationships among variables, aligning with this study's goals to understand how dark patterns affect users' decision-making, emotions, trust, and loyalty in digital interfaces. It also supports validating the classification proposed in the literature review.

This approach aims to produce reliable findings that can be generalized to a broader population.

Additionally, this study employs a quantitative approach, systematically collecting and analyzing numerical data, ideal for testing the study's hypotheses. A structured survey serves as the primary data collection tool, gathering data on users' experiences and perceptions of dark patterns. The survey includes closed-ended questions to measure variables like decision-making, emotions, trust, and loyalty, providing a robust basis for statistical analysis.

Collected data will be analyzed using statistical techniques to identify significant relationships and test the hypotheses. This positivist and quantitative approach will ensure that the findings are based on objective evidence, contributing to a good understanding of dark patterns in digital interfaces.

## 3.2.Sample and sampling method

The current research employs a snowball sampling technique to collect data. This method consists of sharing the survey among authors’ network, which is often used in exploratory research (Naderifar et al., 2017). This approach is effective for rapidly expanding the sample size, mainly through existing social networks.

The survey, initially distributed to individuals in the researcher's network, encourages first respondents to share it with their respective networks, creating a "snowball" effect. This allows the study to reach a broader audience and gather varied experiences and perceptions of dark patterns in digital interfaces.

### 3.3.Survey structure

This study aims to confirm the proposed classification of dark patterns and investigate their influence on variables like self-reported decision-making and emotions. To meet these objectives, a survey was designed to collect primary data from respondents (Appendix B) and analyze it quantitatively for insights.

The survey begins with an introductory paragraph explaining the study's topic, objectives, and data usage, assuring respondents of anonymity and providing the author's contact for inquiries. Respondents must consent to participate before proceeding, and only their responses were included if they agreed.

The first section collects demographic information, including gender, age, internet usage frequency, confidence in using the internet, awareness of dark patterns, and experiences of manipulation by websites or applications.

The second section presents six examples of dark patterns, each representing a branch of the classification in Figure 4. These examples are urgency (oriented manipulative visible dark pattern), confirmshaming (oriented manipulative hidden dark pattern), misleading wording / trick question (oriented deceptive hidden dark pattern), forced Action (forced manipulative visible dark pattern), automate the User (forced manipulative hidden dark pattern), and sneak into basket (forced deceptive hidden dark pattern).

These examples were chosen to ensure survey completion without respondent fatigue. After each example, respondents answer questions about their decision-making, emotions, trust, and loyalty related to the dark pattern.

The final section asks about the perceived blameworthiness of each dark patterns in a ranking and includes questions on respondents' opinions regarding dark patterns in digital interfaces and the need for regulatory protection.

### 3.4.Survey bias

The survey utilized in this study is potentially subject to several biases that could impact the validity and generalizability of the findings. First, there is self-selection bias, which arises when individuals who choose to participate are more interested in or knowledgeable about web design

and online manipulation issues, possibly resulting in a non-representative sample of the broader internet user population (Bethlehem, 2010). Additionally, recall bias may affect the accuracy of participants' responses, as they are not put in a real-life situation and might struggle to accurately remember their past experiences with dark patterns (Coughlin, 1990). This means that users might not assess their emotions accurately and might be imprecise. In other words, participants may not be fully aware of their true emotional responses in a real-life situation, resulting in inaccurate data on emotional reactions (Ekman, 1992). Responses to hypothetical scenarios may not accurately reflect real-world reactions, leading to potential discrepancies between reported and actual behaviors (Kahneman & Tversky, 1979). These are "self-reported" answers.

The sample may also lack representativeness across various age groups, education levels, and computer expertise, limiting the generalizability of the results. This last bias might be the result of the snowball effect. Furthermore, the survey's design, with questions positioned in the same ranking as the study's objectives, might introduce bias by guiding responses towards expected outcomes.

The study's scope is also limited by its context, as only six scenarios were used out of the 48, which might not encompass the full range of dark pattern interactions. Context plays a significant role in user experience, and these scenarios may not cover all possible situations in which dark patterns are encountered. Furthermore, the questionnaire lacks a manipulation check, as no manipulation tool was used to ensure that the 6 examples of dark patterns used in the survey are representative of their respective classification in Figure 4.

By acknowledging these potential biases, the study seeks to provide a nuanced interpretation of the findings and their limitations, recognizing the challenges in capturing the complexity of user interactions with dark patterns.

### 3.5.Link between hypotheses and survey questions

This section links the developed hypotheses to the survey questions, highlighting the measurement units and types of data for each variable.

For hypotheses H1 (“Dark patterns significantly influence users' self-reported decision-making”) the related questions are:

Q9 ("In what way do you think this dark pattern influences or would influence your purchase decision?");

Q14 ("How do you think this dark pattern influences or would influence your decision to unsubscribe?");
Q19 ("In what way do you think this dark pattern impacts or would impact your communication choices?");
Q24 ("How do you think this dark pattern influences or would influence your decision to register on the platform?") and
Q33 ("How do you think this dark pattern impacts or would impact your buying behavior?").

These questions assess the influence of dark patterns on decision-making regarding purchasing, subscribing/unsubscribing, and communication choices using a 5-point Likert scale from 1 (not influenced at all) to 5 (highly influenced).

For hypotheses H2 (“Dark patterns elicit self-reported negative emotions among users, such as frustration or anger”), the related questions are Q10, Q15, Q20, Q25, Q29, and Q34 ("How do you feel, or would you feel about this type of dark pattern?"). Responses are on a 5-point scale: 1 is anger, 2 is frustration, 3 is neutral, 4 is satisfaction, and 5 is joy. An average response below 3 indicates negative emotions.

For hypotheses H3 (“Dark patterns have a significant negative impact on users' self-reported trust in the website/application, the related questions are Q11, Q16, Q21, Q26, Q30, and Q35 ("To what extent do you think this type of dark pattern affects or would affect your trust in the website or app?"). This variable is measured on a 5-point Likert scale from 1 (not affected at all) to 5 (very affected).

For hypotheses H4 (“Dark patterns have a significant negative impact on users' self-reported loyalty to the website/application”), the related questions are Q12, Q17, Q22, Q27, Q31, and Q36 ("Would you revisit a website or application that uses this type of dark pattern?"). Responses are on a 5-point Likert scale from 1 (very unlikely to revisit) to 5 (very likely to revisit).

For hypothesis H5 (“Age influences the likelihood of being manipulated by dark patterns”), the related questions are Q3 ("How old are you?") and Q7 ("Have you ever felt manipulated by the design of a website or application?"). For the Q3, answers are on a 5-point Likert scale to represent the various age groups, while Q7 is a dichotomous variable with a Yes/No answers.

Concerning hypothesis H6 (“Confidence in using IT influences the likelihood of being manipulated by dark patterns”), the related questions are Q7 and Q5 ("How confident are you in your ability to use computer tools and browse the internet?"), where Q5 is a 5-point Likert scale (1 = not at all confident, 5 = very confident) variable.

But for hypothesis H7 (“Awareness of dark patterns influences the likelihood of being manipulated by them”), the related questions are Q7 and Q6 ("Before taking part in this survey, were you aware of the presence of dark patterns on websites and apps?"), where Q6 is also a dichotomous variable with a Yes/No answer.

Finally, hypotheses H8 (“Forced dark patterns are perceived as more blameworthy/reprehensible than oriented dark patterns”), H9 (“Deceptive dark patterns are perceived as more blameworthy/reprehensible than manipulative dark patterns”), H10 (“Hidden dark patterns are perceived as more blameworthy/reprehensible than visible dark patterns”), and H11 (“The degree of obligation is more blameworthy compared to the degree of deception, and the degree of deception is more blameworthy compared to the degree of visibility”) relate to Q37 (“Could you, based on your personal opinion, rank the 6 types of dark patterns seen above according to their 'severity' of use?”). The ordinal variable ranges from 1 (least blameworthy) to 6 (most blameworthy).

### 3.6.Responses collection procedure

This study explores the impact of dark patterns on users' self-reported decision-making, emotions, trust, and loyalty while also aiming to validate the proposed classification of dark patterns. The survey targets an indefinite population of internet users. To distribute the survey, Google Forms was utilized, with all questions set as mandatory to ensure high-quality responses.

The survey was pre-tested by a small group of volunteers to evaluate question clarity and relevance. Feedback from this pre-test helped refine the survey, and these initial responses were excluded from the final analysis to maintain reliability of the final sample

The survey remained open for two weeks, yielding 159 responses. These responses were exported to Excel for coding, where text responses were converted to numerical values, such as "No" to 0 and "Yes" to 1. Age categories were similarly coded, facilitating statistical analysis.

Various ethical considerations have been considered. These ethical considerations are summarized in Appendix D.

### 3.7.Statistical methods

This study employs a survey to examine the impact of dark patterns on internet users and validate the proposed classification. Therefore, the t-test and ANOVA techniques will be used to investigate the hypotheses developed in the literature review. While Appendix E describes the t-test and ANOVA techniques, Appendix F presents the null and alternative hypotheses for each developed hypotheses in the literature review.

## 4. Results and discussion

This section presents the findings on the impact of dark patterns on users' self-reported decision-making, emotions, trust, and loyalty, and examines user perceptions of the blameworthiness of different dark patterns. Results will also highlight the impact of age, IT confidence, and awareness of dark manipulation on the likelihood of their manipulation. The results are structured to reflect statistical analyses conducted through t-tests and ANOVA analysis.

First, Table 1 shows the descriptive statistics that set the stage for analyzing how demographic variables might interact with the effects of dark patterns, providing a foundational context for the more detailed statistical tests that follow.

**Table 1: Survey respondent profile (n=159)**

| Measure | Item | N | (%) |
|---|---|---|---|
| **Gender** | Male | 54 | 33.96% |
| | Female | 104 | 65.41% |
| | Non-binary | 0 | 0.00% |
| | Prefer not to say | 1 | 0.63% |
| **Age** | Less than 25 | 50 | 31.45% |
| | 26-35 | 32 | 20.13% |
| | 36-45 | 19 | 11.95% |
| | 46-55 | 24 | 15.09% |
| | 56 or more | 34 | 21.38% |
| **Internet usage frequency** | Daily | 158 | 99.37% |
| | Many times per week | 1 | 0.63% |
| | Once per week | 0 | 0.00% |

| | | | |
|---|---|---|---|
| | Less than once per week | 0 | 0.00% |
| **Confidence in using internet** | Very low confidence | 1 | 0.63% |
| | Low confidence | 7 | 4.40% |
| | Moderate confidence | 30 | 18.87% |
| | High confidence | 76 | 47.80% |
| | Very high confidence | 45 | 28.30% |
| **Awareness of dark patterns** | Yes | 97 | 61.01% |
| | No | 62 | 38.99% |
| **Experience of being manipulated by a website** | Yes | 137 | 86.16% |
| | No | 22 | 13.84% |

### 4.1.Impact of dark patterns on self-reported decision-making

The analysis of hypothesis H1 was conducted using a t-test to determine if dark patterns significantly influence users' self-reported decision-making. The results, as shown in Table 2, indicate a mean value of 3.02 out of 5 for self-reported decision-making with a t-statistic of 1.65 and a p-value of 0.63, suggesting no statistically significant impact. This finding contradicts previous literature that emphasizes the strong influence of dark patterns on decision-making (Gray et al., 2018; Mathur et al., 2019). One possible explanation for these findings is that users may not always be fully aware of the influence dark patterns have on their behavior, leading them to report that their decisions are unaffected. The disconnect between self-reported data and actual behavior could indicate a bias in how users perceive and rationalize their choices.

**Table 2: t-test results for H1 - Dark patterns significantly influence users' self-reported decision-making**

| Variable | Mean (of 5) | t-statistic | Standard deviation | p-value |
|---|---|---|---|---|
| **Self-reported decision making** | 3.02 | 1.65 | 1.51 | 0.63 |

### 4.2.Impact of dark patterns on self-reported emotions

Hypothesis H2 examined whether dark patterns elicit negative emotions among users. The t-test results, presented in Table 3, show a mean of 1.91 out of 5, with a significant t-statistic of -40.22

and a p-value of 0.00. These results confirm that dark patterns significantly affect users' emotions, eliciting negative feelings such as frustration and anger. This aligns with the study conducted by Mathur et al. (2019), who found similar emotional reactions.

**Table 3: t-test results for H2 - Dark patterns elicit self-reported negative emotions among users, such as frustration or anger**

| Variable | Mean (of 5) | t-statistic | Standard deviation | p-value |
|---|---|---|---|---|
| **Self-reported emotions** | 1.91 | -40.22 | 0.83 | 0.00 |

### 4.3.Impact of dark patterns on self-reported trust on the website/application

For hypothesis H3, the impact of dark patterns on users' trust was analyzed. As illustrated in Table 4, the mean value for self-reported trust was 3.68 out of 5, with a t-statistic of 16.60 and a p-value of 0.00, indicating a significant negative impact on trust. This finding supports the notion that deceptive tactics breach trust, as discussed by Gray et al. (2018).

**Table 4: t-test results for H3 - Dark patterns have a significant negative impact on users' self-reported trust on the website/application**

| Variable | Mean (of 5) | t-statistic | Standard deviation | p-value |
|---|---|---|---|---|
| **Self-reported trust** | 3.68 | 16.60 | 1.26 | 0.00 |

### 4.4.Impact of dark patterns on self-reported loyalty to the website/application

Hypothesis H4 explored the impact of dark patterns on loyalty. The t-test results in Table 5 reveal a mean of 2.20 out of 5, a t-statistic of -19.58, and a p-value of 0.00, confirming the significant negative impact of dark patterns on users' self-reported loyalty. This is consistent with research indicating that manipulative designs lead to decreased user loyalty and increased negative word-of-mouth (Bösch et al., 2016).

**Table 5: t-test results for H4 - Dark patterns have a significant negative impact on users' self-reported loyalty to the website/application**

| Variable | Mean (of 5) | t-statistic | Standard deviation | p-value |
|---|---|---|---|---|
| **Self-reported loyalty** | 2.20 | -19.58 | 1.27 | 0.00 |

### 4.5.Influence of age on the likelihood of being manipulated by dark patterns

The ANOVA analysis for hypothesis H5 was conducted to explore the influence of age on the likelihood of being manipulated by dark patterns. Table 6 shows no significant effect, with an F-value of 0.10 and a p-value of 0.98. This suggests age does not significantly influence susceptibility, aligning with findings that specific knowledge is more crucial (Gray et al., 2018).

**Table 6: ANOVA results for H5 - Age influences the likelihood of being manipulated by dark patterns**

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 0.05 | 4 | 0.01 | 0.10 | 0.98 |
| Within Groups | 18.91 | 154 | 0.12 | | |
| Total | 18.96 | 158 | | | |

### 4.6.Influence of IT confidence on the likelihood of being manipulated by dark patterns

With regards to hypothesis H6, it examined IT confidence's impact on susceptibility to dark patterns. The t-test in Table 7 reveals no significant effect, with a t-statistic of -0.94 and a p-value of 0.35. These results indicate that IT confidence does not significantly reduce the likelihood of being manipulated by dark patterns.

**Table 7: t-test results for H6 - Confidence in using IT influences the likelihood of being manipulated by dark patterns**

| Variable | Mean | Standard deviation | t-statistic (for the difference between the two means) | p-value |
|---|---|---|---|---|
| **Low confidence in IT** | 0.82 | 0.39 | -0.94 | 0.35 |
| **High confidence in IT** | 0.88 | 0.33 | | |

### 4.7.Influence of awareness of dark patterns on their likelihood to manipulate users

For hypothesis H7, empirical findings indicate that awareness of dark patterns significantly influenced their manipulation likelihood, as shown by a t-statistic of -3.10 and a p-value of 0.00 in Table 8. Educated users are less susceptible, supporting the importance of awareness in resisting manipulative tactics (Gray et al., 2018).

**Table 8: t-test results for H7 - Awareness of dark patterns influences the likelihood of being manipulated by them**

| Variable | Mean | Standard deviation | t-statistic (for the difference between the two means) | p-value |
|---|---|---|---|---|
| **No awareness of dark patterns** | 0.76 | 0.43 | -3.10 | 0.00 |
| **Awareness of dark patterns** | 0.93 | 0.26 | | |

### 4.8.Comparison of blameworthiness: visible vs. hidden, manipulative vs. deceptive, and oriented vs. forced dark patterns

The analysis of hypotheses H8, H9, and H10 through t-tests, as shown in Tables 9, 10, and 11, revealed significant differences in the perceived blameworthiness of the different types of dark patterns. The results suggest that users view forced dark patterns as more blameworthy than oriented ones, with a mean score of 4.32 for forced patterns compared to 2.68 for oriented patterns (Table 9). This perception likely stems from the nature of forced patterns, which compel users to take specific actions, often leaving them with little or no choice. This lack of autonomy can lead to feelings of frustration and resentment, as users feel coerced into decisions they might not have made willingly. In contrast, oriented dark patterns, while still manipulative, guide users toward certain choices without completely removing their choice. The ability to make a choice, even if subtly influenced, seems to mitigate the perception of blameworthiness to some extent.

**Table 9: t-test results for H8 - Forced dark patterns are perceived as more blameworthy/reprehensible than oriented dark patterns**

| Variable | Mean | Standard deviation | t-statistic (for the difference between the two means) | p-value |
|---|---|---|---|---|
| **Oriented** | 2.68 | 1.47 | 16.85 | 0.00 |
| **Forced** | 4.32 | 1.53 | | |

Furthermore, deceptive dark patterns were found to be perceived as more blameworthy than manipulative ones, with mean scores of 4.31 and 3.09, respectively (Table 10). Deceptive patterns rely on misinformation or concealment of crucial details, effectively tricking users into making decisions they might not otherwise choose. This intentional complication is seen as a direct violation of trust, making it more reprehensible in the eyes of users. On the other hand, manipulative patterns leverage influence, guiding user behavior through indirect means, such as psychological manipulation or asymmetry in choice. While still ethically questionable, manipulative dark patterns might be viewed as less aggressive compared to deceptive ones.

**Table 10: t-test results for H9 - Deceptive dark patterns are perceived as more blameworthy/reprehensible than manipulative dark patterns**

| Variable | Mean | Standard deviation | t-statistic (for the difference between the two means) | p-value |
|---|---|---|---|---|
| **Manipulative** | 3.09 | 1.65 | 11.00 | 0.00 |
| **Deceptive** | 4.31 | 1.53 | | |

Additionally, hidden dark patterns are perceived as more blameworthy than visible ones, with hidden patterns receiving a mean score of 3.74 compared to 3.02 for visible patterns (Table 11). Hidden dark patterns operate secretly, influencing users without their awareness, which can lead to a greater sense of betrayal once users recognize the manipulation. The hidden nature of these patterns means users often only become aware of the manipulation after the fact, leading to feelings of being deceived and exploited. In contrast, visible patterns, although still manipulative, are more transparent and can be recognized and potentially resisted by users. The ability to identify and understand the manipulation seems to lessen the perceived blameworthiness, as users feel more in control and able to make informed decisions. It's important to note that in both cases, whether visible or hidden, respondents to the questionnaire were aware of the manipulation because they took the time to analyze it. However, the hidden ones were seen as more blameworthy for their lack of transparency.

**Table 11: t-test results for H10 - Hidden dark patterns are perceived as more blameworthy/reprehensible than visible dark patterns**

| Variable | Mean | Standard deviation | t-statistic (for the difference between the two means) | p-value |
|---|---|---|---|---|
| **Hidden** | 3.74 | 1.64 | 6.27 | 0.00 |
| **Visible** | 3.02 | 1.74 | | |

Overall, the findings indicate that the degree of transparency and the method of influence play crucial roles in shaping user perceptions of ethicality. The more overt and coercive the manipulation, the higher the perceived blameworthiness, highlighting the importance of autonomy and informed consent in user interactions with digital interfaces. These insights underscore the need for ethical design practices that prioritize user autonomy and transparency, as well as the potential for regulatory measures to protect users from the most harmful types of dark patterns.

### 4.9.Confirmation of the proposed classification

The ANOVA results for hypothesis H11 confirms the order of importance of the 3 classification layers (horizontally). Indicating that the degree of obligation (forced vs oriented) is more blameworthy compared to the degree of deception (manipulation vs deception) and degree of visibility (hidden vs visible). While the degree of deception is more blameworthy compared to the degree of visibility (F-value: 196.59, p-value: 0.00). This is mainly noticeable as the mean of blameworthiness for the degree of visibility is the lowest compared to the other two layers, followed by the mean of degree of deception, followed by the mean of degree of obligation in an ascending order as shown in Table 13.

**Table 12: ANOVA test results for H11 - The degree of obligation is more blameworthy compared to the degree of deception, and the degree of deception is more blameworthy compared to the degree of visibility**

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| **Between Groups** | 813.89 | 2.00 | 406.95 | 196.59 | 0.00 |
| **Within Groups** | 1968.61 | 951.00 | 2.07 | | |
| **Total** | 2782.50 | 953.00 | | | |

**Table 13: Mean of each layer proposed in this study (visibility, deception, and obligation)**

| Layer | Mean |
|---|---|
| **Visibility** | 2.24 |
| **Deception** | 3.82 |
| **Obligation** | 4.43 |

In addition, the vertical layers of the classification were confirmed in hypotheses 8, 9 and 10. Showing that forced dark patterns are more blameworthy than oriented ones, deceptive ones more blameworthy than manipulative ones, and hidden ones more blameworthy than visible ones. The blameworthiness scores assigned to the 6 layers of the classification in figure 4 are confirmed.

Confirming this classification aids in understanding how users perceive, react to, and experience different types of dark patterns. It emphasizes the importance of designing user interfaces that prioritize user choice and clear communication. By understanding what users find most problematic, designers and policymakers can work toward creating more ethical and user-friendly digital experiences.

## 5. Conclusion

### 5.1.Research summary

In today's digital world, user interface (UI) and user experience (UX) design significantly influence user interactions, raising ethical concerns over the use of dark patterns (Cara, 2019; Hassenzahl, 2018). This research is significant in the field of human-computer interaction as it aims to clarify the understanding of dark patterns and their influence on users. This study aimed to classify dark patterns differently from existing literature by considering their degree of blamability. Additionally, it sought to assess their impact on decision-making, emotions, trust, and loyalty. It also examined the influence of user awareness, age, and IT confidence on susceptibility to these manipulative tactics using t-statistics and ANOVA analysis.

To achieve the research objectives, a hypothetico-deductive approach was employed using a structured survey among 159 participants. The findings reveal a complex picture of how dark patterns affect user behavior. Findings show that dark patterns do not influence users' self-reported decision making, contradicting claims by different authors in the existing literature (Gray et al.,

2018; Mathur et al., 2019). One possible explanation for these findings is that users may not always be fully aware of the influence dark patterns have on their behavior, leading them to report that their decisions are unaffected. The disconnect between self-reported data and actual behavior could indicate a bias in how users perceive and rationalize their choices. The study also revealed that dark patterns significantly elicit negative emotional responses, such as frustration and anger, while they also negatively impact users' trust and loyalty. This aligns with the findings of the literature review (Bösch et al., 2016; Gray et al., 2018; Mathur et al., 2019). These results underscore the potential damage dark patterns can cause to the user experience, emphasizing the need for designers to consider the ethical implications of their work.

With regards to awareness, empirical findings indicate that this variable plays a crucial role in mitigating the effects of dark patterns, as informed users are less likely to feel manipulated. However, age and IT proficiency do not significantly influence the likelihood of being manipulated by dark patterns, suggesting that specific knowledge of dark patterns is more crucial than age and general IT skills. This highlights the importance of educating users about dark patterns, as awareness can serve as a powerful tool in resisting manipulation.

This study revealed notable findings related to the proposed classification of dark patterns. The classification system was confirmed horizontally and vertically. Supporting the hypothesis that the degree of obligation, deception, and visibility influence perceived blameworthiness, each with a different degree of impact. Users perceive the degree of obligation as more blameworthy than the degree of deception, while the degree of deception is considered more blameworthy than the degree of visibility. Furthermore, this study found that within the vertical layers of classification, forced dark patterns are considered more blameworthy than oriented ones. Similarly, deceptive dark patterns are deemed more blameworthy than manipulative ones, and hidden dark patterns are seen as more blameworthy than visible ones. These insights provide an understanding of how users perceive different types of dark patterns, suggesting that transparency and honesty in design can mitigate negative perceptions.

In conclusion, this study enhances the understanding of dark patterns by providing a detailed classification and empirical validation of their effects on user behavior. The findings highlight the importance of ethical design practices that prioritize transparency and user autonomy and underscore the need for regulatory measures to protect users from manipulative tactics. This

research contributes to the ongoing discourse on digital ethics, advocating for efforts to foster a more ethical and user-friendly digital environment.

### 5.2.Theoretical and managerial implications

This study offers valuable theoretical and managerial insights into the use of dark patterns. Theoretically, it enhances understanding by introducing a comprehensive classification system and examining their impact on user behavior. The proposed classification system differentiates dark patterns based on their degree of obligation, deception, and visibility, offering a refined framework for understanding these manipulative tactics. This classification allows for a more refined analysis of how different dark patterns affect users' perceptions and behavior, providing a basis for further research into the cognitive mechanisms that underlie these effects. By highlighting the varying degrees of blameworthiness associated with each type of pattern, the study emphasizes the importance of transparency and user autonomy in digital design.

While the study found that dark patterns don't universally affect self-reported decision-making, this finding implies that users may not be fully aware of how these manipulative designs influence their choices in real-life situations. The lack of impact on self-reported decision-making suggests that dark patterns operate at a subconscious level, subtly guiding user behavior without explicit awareness. This highlights a critical area for further exploration, as understanding the underlying cognitive biases and psychological mechanisms at play can provide deeper insights into how dark patterns exert their influence. It also suggests that enhancing user awareness and education about dark patterns could be an effective strategy to empower users to recognize and resist these manipulative tactics.

From a managerial perspective, the study emphasizes the ethical responsibility of digital platform designers and managers. The adverse effects of dark patterns on emotions, trust, and loyalty suggest they can damage long-term user relationships and brand reputation. With over 82.6% of survey respondents opposing dark patterns and 93.8% advocating for regulations, managers are urged to review design strategies and prioritize ethical practices that build user trust and satisfaction. The classification system provides managers with a tool to assess the ethicality of design practices, enabling them to identify and eliminate the most blameworthy patterns from their interfaces. This approach not only enhances user experience but also aligns with the growing demand for corporate social responsibility and ethical business practices.

In summary, the proposed classification offers a framework for both researchers and practitioners to understand the impact of dark patterns more comprehensively. By addressing the ethical implications of these patterns and promoting transparency in design, the study contributes to the development of more ethical and user-centric digital environments.

### 5.3.Practical recommendations

Several practical recommendations emerge for designers, managers, governments, and policymakers. Designers should avoid manipulative tactics that undermine trust and loyalty, focusing instead on transparent, user-friendly interfaces that respect autonomy. Incorporating principles of ethical design into the early stages of product development can ensure that user needs and rights are prioritized from the beginning. Training programs for design teams can educate them on the ethical implications of dark patterns and the importance of user-centered design. Implementing user feedback mechanisms and regular audits can help identify and eliminate dark patterns. Additionally, developing tools and metrics to measure the impact of design choices on user behavior can provide valuable insights for continuous improvement.

For governments and policymakers, they should take notice of the strong demand for regulation, with 93.8% of respondents supporting measures to protect users. Developing and enforcing guidelines will not only safeguard users but also promote fair competition among digital platforms. Policymakers should consider establishing a framework for assessing and certifying ethical design practices, which could serve as a benchmark for industry standards. Collaborative efforts can foster a more transparent, user-friendly digital environment, ultimately enhancing trust and loyalty. Public awareness campaigns to educate users about dark patterns can empower them to make informed decisions and advocate for their rights, further driving the demand for ethical practices.

### 5.4.Study limitations

This study has several limitations. The reliance on self-reported survey data may lack objectivity, as users are not in real life situations. Responses to hypothetical scenarios may not accurately reflect real-world reactions, leading to potential discrepancies between reported and actual behaviors (Kahneman & Tversky, 1979). Furthermore, it introduces potential biases such as social desirability and recall bias, affecting the accuracy of responses. The use of a snowball sampling method to gather participants may also result in a sample that is not fully representative of the general population, as it depends on the networks of initial respondents. The survey's limited

selection of six examples of dark patterns out of 48 from the table may not capture the full diversity and range of these tactics. Additionally, no manipulation check has been conducted to check if the 6 example of dark patterns used in the survey are representative to their respective classification in Figure 4. In addition, the survey design, i.e. the order of elements and questions, and their formulation might also influence participants' perceptions and responses, potentially skewing the results. Finally, the proposed classification, its categories and the ethical ratings assigned (blameworthiness) may lack objectivity and could have been tested with experts in the field of dark patterns.

Also, a larger sample size would improve generalizability, while more robust statistical methods could provide deeper insights into user interactions with dark patterns.

Despite these limitations, the study offers valuable insights into the impact of dark patterns, highlighting the need for further research with more comprehensive methodologies and diverse samples to better understand their nuanced effects.

### 5.5.Avenues for future research

Future research should incorporate a broader range of explanatory and control variables to better understand how demographic variables, psychological traits, and digital experiences influence susceptibility to dark patterns. Additionally, longitudinal studies could assess the long-term effects of exposure to dark patterns on trust, loyalty, and user experience.

Furthermore, future studies could incorporate real-life methods to mitigate the bias associated with self-reported answers from the respondents.

This research could also be duplicated to industry-specific scenarios, as it could compare dark pattern use and impact across sectors like e-commerce, social media, and gaming, enabling tailored recommendations and regulations. Additionally, exploring AI and machine learning in detecting and mitigating dark patterns offers an innovative research direction, contributing to healthier digital environments.

Finally, the proposed classification can serve as a basis for future studies aimed at measuring the degree of reprehensibility of different types of dark patterns. Such research could explore and test different techniques to mitigate their impact on users. The classification and table of 48 dark

patterns also opens the door for more advanced, extensive research focused on grouping and categorizing the various types of dark patterns found in user interfaces.

## References

Aagaard, J. (2022). A game of dark patterns: Designing healthy, highly-engaging mobile games. *2022 CHI Conference on Human Factors in Computing Systems*, 1–8. https://doi.org/10.1145/3491101.3519837

Bethlehem, J. (2010). Selection bias in web surveys. *International Statistical Review*, *78*(2), 161–188. https://doi.org/10.1111/j.1751-5823.2010.00112.x

Bhatia, S., & Alojail, M. (2022). A novel approach for deciphering big data value using dark data. *Intelligent Automation & Soft Computing*, *33*(2), 1261–1271. https://doi.org/10.32604/iasc.2022.023501

Bogliacino, F., Leonardo, P., Liva, G., & Lupiáñez-Villanueva, F. (2023). *Testing for manipulation: Experimental evidence on dark patterns*. OSF. https://doi.org/10.31235/osf.io/sqt3j

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021). "I am definitely manipulated, even when I am aware of it. It's ridiculous!"—Dark patterns from the end-user perspective. *Proceedings of the 2021 ACM Designing Interactive Systems Conference*, 763–776. https://doi.org/10.1145/3461778.3462086

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*. https://petsymposium.org/popets/2016/popets-2016-0038.php

Bringull, H. (2023). *Deceptive patterns—Types of deceptive pattern*. https://www.deceptive.design/types

Bryman, A. (2016). *Social research methods*. Oxford University Press.

Cara, C. (2019). Dark patterns in the media: A systematic review. *Network Intelligence Studies*, *14*, 105–113.

Chaudhary, A., Saroha, J., Monteiro, K., Forbes, A. G., & Parnami, A. (2022). "Are you still watching?": Exploring unintended user behaviors and dark patterns on video streaming platforms. *Proceedings of the 2022 ACM Designing Interactive Systems Conference*, 776–791. https://doi.org/10.1145/3532106.3533562

Cialdini, R. B. (2006). *Influence: The psychology of persuasion*. Harper Business.

CNIL. (2019). *La forme des choix: Données personnelles, design et frictions désirables* (06; pp. 1–47). Cahiers IP Innovation & Prospective. https://linc.cnil.fr/sites/linc/files/2023-02/cnil_cahiers_ip6.pdf

CNIL. (2019). Shaping Choices in the Digital World. https://www.cnil.fr/sites/cnil/files/2023-06/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

Conti, G., & Sobiesk, E. (2010). Malicious interface design: Exploiting the user. *Proceedings of the 19th International Conference on World Wide Web*, 271–280. https://doi.org/10.1145/1772690.1772719

Coughlin, S. S. (1990). Recall bias in epidemiologic studies. *Journal of Clinical Epidemiology*, *43*(1), 87–91. https://doi.org/10.1016/0895-4356(90)90060-3

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications.

Day, G., & Stemler, A. (2019). *Are dark patterns anticompetitive?* (SSRN Scholarly Paper 3468321). https://doi.org/10.2139/ssrn.3468321

Dula, E., Rosero, A., & Phillips, E. (2023). Identifying dark patterns in social robot behavior. *2023 Systems and Information Engineering Design Symposium (SIEDS)*, 7–12. https://doi.org/10.1109/SIEDS58326.2023.10137912

Ekman, P. (1992). An argument for basic emotions. *Cognition and Emotion*, *6*(3–4), 169–200. https://doi.org/10.1080/02699939208411068

Fansher, M., Chivukula, S. S., & Gray, C. M. (2018). #darkpatterns: UX practitioner conversations about ethical design. *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3170427.3188553

Frobrukerrådet. (2018). *Deceived by design* (pp. 1–44). Frobrukerrådet. https://www.forbrukerradet.no/horinger/2018/

Gonzaga, H. F. (2023). *The legality and regulation of dark patterns* (arXiv:2303.03888). arXiv. https://doi.org/10.48550/arXiv.2303.03888

Graßl, P., Schraffenberger, H., Borgesius, F. Z., & Buijzen, M. (2021). Dark and bright patterns in cookie consent requests. *Journal of Digital Social Research*, *3*(1), Article 1. https://doi.org/10.33621/jdsr.v3i1.54

Gray, C. M., Chen, J., Chivukula, S. S., & Qu, L. (2021). End user accounts of dark patterns as felt manipulation. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 372:1-372:25. https://doi.org/10.1145/3479516

Gray, C. M., Kou, Y., Battles, B., Hoggat, 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

Gray, C. M., Sanchez Chamorro, L., Obi, I., & Duane, J.-N. (2023). Mapping the landscape of dark patterns scholarship: A systematic literature review. *Companion Publication of the 2023 ACM Designing Interactive Systems Conference*, 188–193. https://doi.org/10.1145/3563703.3596635

Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., & Wilson, C. (2021). A comparative study of dark patterns across web and mobile modalities. *Proceedings of the ACM on Human-Computer Interaction*, *5*, 1–29. https://doi.org/10.1145/3479521

Gunawan, J., Santos, C., & Kamara, I. (2022). Redress for dark patterns privacy harms? A case study on consent interactions. *Proceedings of the 2022 Symposium on Computer Science and Law*, 181–194. https://doi.org/10.1145/3511265.3550448

Hassenzahl, M. (2018). The thing and I: Understanding the relationship between user and product. In M. Blythe & A. Monk (Eds.), *Funology 2: From Usability to Enjoyment* (pp. 301–313). Springer International Publishing. https://doi.org/10.1007/978-3-319-68213-6_19

Hassenzahl, M., & Tractinsky, N. (2006). User experience—A research agenda. *Behaviour & Information Technology*, *25*(2), 91–97. https://doi.org/10.1080/01449290500330331

Hausner, P., & Gertz, M. (2021). *Dark patterns in the interaction with cookie banners* (arXiv:2103.14956). arXiv. https://doi.org/10.48550/arXiv.2103.14956

Johnson, E. J., Shu, S. B., Dellaert, B. G. C., Fox, C., Goldstein, D. G., Häubl, G., Larrick, R. P., Payne, J. W., Peters, E., Schkade, D., Wansink, B., & Weber, E. U. (2012). Beyond nudges: Tools of a choice architecture. *Marketing Letters*, *23*(2), 487–504. https://doi.org/10.1007/s11002-012-9186-1

Kitkowska, A. (2023). The hows and whys of dark patterns: Categorizations and privacy. In N. Gerber, A. Stöver, & K. Marky (Eds.), *Human Factors in Privacy Research* (pp. 173–198). Springer International Publishing. https://doi.org/10.1007/978-3-031-28643-8_9

Kollmer, T., & Eckhardt, A. (2023). Dark patterns. *Business & Information Systems Engineering*, *65*(2), 201–208. https://doi.org/10.1007/s12599-022-00783-7

Kühling, J., & Sauerborn, C. (2022). “Dark patterns” under the GDPR and the DSA - New challenge for the digital legal system—Classification and data protection control requirements. *Computer Und Recht*, *38*(4), 226–235. https://doi.org/10.9785/cr-2022-380409

Leiser, M. R. (2022). Dark patterns: The case for regulatory pluralism between the European Unions consumer and data protection regimes. In *Research Handbook on EU Data Protection Law* (pp. 240–269). Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/edcoll/9781800371675/9781800371675.00019.xml

Leiser, M., & Yang, W.-T. (2022). Illuminating manipulative design: From ‘dark patterns’ to information asymmetry and the repression of free choice under the unfair commercial practices directive. *Loyola Consumer Law Review*, *34*(3), 484–528.

Lewis, C. (2014). Temporal dark patterns. In C. Lewis (Ed.), *Irresistible Apps: Motivational Design Patterns for Apps, Games, and Web-based Communities* (pp. 103–110). Apress. https://doi.org/10.1007/978-1-4302-6422-4_9

Lorincz, N. (2024, February 7). *What is A/B Testing? A Complete Guide With Examples*. OptiMonk. https://www.optimonk.com/a-b-testing/

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

Lukoff, K., Hiniker, A., Gray, C. M., Mathur, A., & Chivukula, S. S. (2021). What can CHI do about dark patterns? *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3411763.3441360

Maier, M., & Harr, R. (2020). Dark design patterns: An end-user perspective. *Human Technology*, *16*(2), 170–199. https://doi.org/10.17011/ht/urn.202008245641

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

Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–18. https://doi.org/10.1145/3411764.3445610

Monge Roffarello, A., & De Russis, L. (2022). Towards understanding the dark patterns that steal our attention. *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–7. https://doi.org/10.1145/3491101.3519829

Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball sampling: A purposeful method of sampling in qualitative research. *Strides in Development of Medical Education*, *14*(3). https://doi.org/10.5812/sdme.67670

Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark patterns: Past, present, and future: the evolution of tricky user interfaces. *Queue*, *18*(2), Pages 10:67-Pages 10:92. https://doi.org/10.1145/3400899.3400901

Neuman, W. L. (2013). *Social research methods: Qualitative and quantitative approaches*. Pearson Education.

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

Obi, I., Gray, C. M., Chivukula, S. S., Duane, J.-N., Johns, J., Will, M., Li, Z., & Carlock, T. (2022). *Let's Talk About Socio-Technical Angst: Tracing the History and Evolution of Dark Patterns on Twitter from 2010-2021* (arXiv:2207.10563). arXiv. http://arxiv.org/abs/2207.10563

OECD. (2022). *Dark commercial patterns*. OECD. https://doi.org/10.1787/44f5e846-en

Raju, S. H., Waris, S. F., Adinarayna, S., Jadala, V. C., & Rao, G. S. (2022). Smart dark pattern detection: Making aware of misleading patterns through the intended app. In S. Shakya, V. E. Balas, S. Kamolphiwong, & K.-L. Du (Eds.), *Sentimental Analysis and Deep Learning* (pp. 933–947). Springer. https://doi.org/10.1007/978-981-16-5157-1_72

Runge, J., Wentzel, D., Huh, J. Y., & Chaney, A. (2023). "Dark patterns" in online services: A motivating study and agenda for future research. *Marketing Letters*, *34*(1), 155–160. https://doi.org/10.1007/s11002-022-09629-4

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). *Research methods for business students*. Pearson Education.

Schneider, C., Weinmann, M., & vom Brocke, J. (2018). Digital nudging: Guiding online user choices through interface design. *Communications of the ACM*, *61*(7), 67–73. https://doi.org/10.1145/3213765

Sin, R., Harris, T., Nilsson, S., & Beck, T. (2022). Dark patterns in online shopping: Do they work and can nudges help mitigate impulse buying? *Behavioural Public Policy*, 1–27. https://doi.org/10.1017/bpp.2022.11

Singh, D., Yadav, B., & Singh, S. (2023). Who is responsible for the prolonged use of dark patterns? *SCRS Proceedings of International Conference of Undergraduate Students*, 185–192.

Sunstein, C. R. (2015). The ethics of nudging. *Yale Journal on Regulation*, *32*, 413.

Sunstein, C. R. (2019). *On Freedom*. Princeton University Press. https://press.princeton.edu/books/hardcover/9780691191157/on-freedom

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness* (pp. x, 293). Yale University Press.

Troisi, O., Maione, G., Grimaldi, M., & Loia, F. (2020). Growth hacking: Insights on data-driven decision-making from three firms. *Industrial Marketing Management*, *90*, 538–557. https://doi.org/10.1016/j.indmarman.2019.08.005

Vanderdonckt, J., Zen, M., & Vatavu, R.-D. (2019). AB4Web: An on-line A/B tester for comparing user interface design alternatives. *Proceedings of the ACM on Human-Computer Interaction*, *3*, 1–28. https://doi.org/10.1145/3331160

Voigt, C., Schlögl, S., & Groth, A. (2021). Dark patterns in online shopping: Of sneaky tricks, perceived annoyance and respective brand trust. In F. F.-H. Nah & K. Siau (Eds.), *HCI in Business, Government and Organizations* (pp. 143–155). Springer International Publishing. https://doi.org/10.1007/978-3-030-77750-0_10

Weinmann, M., Schneider, C., & Brocke, J. vom. (2016). Digital nudging. *Business & Information Systems Engineering*, *58*(6), 433–436. https://doi.org/10.1007/s12599-016-0453-1

Wolfgang, S. (2023, January 20). Dark patterns examples: Recognizing manipulative marketing and design. *Raidboxes*. https://raidboxes.io/en/blog/security/dark-patterns/

Yada, Y., Feng, J., Matsumoto, T., Fukushima, N., Kido, F., & Yamana, H. (2022). Dark patterns in e-commerce: A dataset and its baseline evaluations. *2022 IEEE International Conference on Big Data (Big Data)*, 3015–3022. https://doi.org/10.1109/BigData55660.2022.10020800

Young-gug, Y. (2022). A review of the regulatory direction of dark patterns in online transactions. *Koreanstudies Information Service System*, *30*(3), 79–104.

Zagal, J. P., Björk, S., & Lewis, C. (2013). *Dark patterns in the design of games*. Foundations of Digital Games 2013. https://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-24252

Zhao, M. (2018). Choice architecture in consumer financial decisions. *Review of Behavioral Economics*, *5*(3–4), 417–437. https://doi.org/10.1561/105.00000088

**Appendix A: Proposed classification of dark patterns with their definitions, objectives, sentiments, methods, and hypothesized ethical impact – Source: Composed by the author.**

| Category | | | ID | Type | Explanation | Source | Objectives | Sentiments | Methods | Blameworthiness (out of 6) |
|---|---|---|---|---|---|---|---|---|---|---|
| **Oriented** | **Manipulative** | **Visible** | 1 | Preset & Default Settings | These dark patterns exploit the tendency of users to accept default settings without scrutinizing them, presenting pre-selected options or pre-accepted conditions that influence their decision-making. Bottom of the form | (Bringull, 2023; Frobrukerrådet, 2018) | Any action that benefits the company | Resignation, irritation | UI manipulation in the UI, asymmetry, default effect, status quo bias | 1 |
| | | | 2 | Default sharing | Pre-check information sharing options, which won't always be unchecked when logging in. | (CNIL, 2019) | Incentive for data collection and sharing | Mistrust, frustration, resignation | UI manipulation, asymmetry, default effect, status quo bias | 1 |
| | | | 3 | Rarity | Merchant services and sites play with the scarcity effect by signaling, for example, limited availability or high demand for an offer. Low-stock and high-demand messages are used. | (Mathur et al., 2019) | Incentive to engage or purchase | Excitement, anxiety, frustration, mistrust | Psychological manipulation, scarcity bias, FOMO | 1 |
| | | | 4 | Urgency | Imposes a deadline on a sale or promotion, thus speeding up the purchase and decision-making process more broadly (FOMO). Limited-time countdowns and messages are used. | (Mathur et al., 2019) | Incentive to engage or purchase | Excitement, anxiety, frustration, mistrust | Psychological manipulation, scarcity bias, FOMO | 1 |
| | | | 5 | Social Proof | The principle of the group effect, which states that an individual constructs his or her choices by examining those of others. Social proof messages typically indicate other users' product shopping activities and experiences | (Mathur et al., 2019) | Incentive to engage or purchase | Trust, mistrust, satisfaction | Psychological manipulation, bandwagon effect | 1 |
| | | | 6 | Pay to pass | The player is presented with the possibility of paying in order to pass a level that is too difficult or simply to advance faster in the game. | (Zagal et al., 2013) | Incentive to buy | Frustration, powerlessness, reluctance | Psychological manipulation, hyperbolic discounting, positive reinforcement | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 7 | Monetized rivalries | Players are encouraged to spend money that they would not have otherwise spent in order to gain status and a competitive advantage over other players through in-game purchases. This model is colloquially known as "Pay to Win". | (Zagal et al., 2013) | Incentive to buy | Frustration, injustice, disappointment | Psychological manipulation, hyperbolic discounting, social influence | 1 |
| | | | 8 | Last-minute consent | Exploits the user's moments of vulnerability by asking them to consent to data collection at a late stage of the process, such as the integration of a prospecting opt-in during the final stages of order confirmation. | (CNIL, 2019) | Incentive for data collection and sharing | Frustration, irritation, stress | Psychological manipulation, opportunism | 1 |
| | | | 9 | Security blackmail | When logging in, ask for additional information in addition to that strictly necessary for the service in situations where the user is under pressure (when he has just changed his password or placed an order, for example). | (CNIL, 2019) | Incentive for data collection and sharing | Anxiety, frustration, vulnerability | Psychological manipulation, opportunism | 1 |
| | | **Hidden** | 10 | Ease & Manipulative Navigation | Facilitate access to the choices desired by the designer (through design, colors) while making alternatives difficult to find. For example, by making the free version of an app harder to find than the commercial version on a seller's site. | (Conti & Sobiesk, 2010; Frobrukerrådet, 2018) | Any action that benefits the company | Distrust, resignation, confusion, irritation | Hidden, UI manipulation, framing effect, asymmetry | 2 |
| | | | 11 | Preventing comparisons and obscuring the comparison | Make comparisons between different services, between different products, or between different parameters difficult. For example, by making features and prices more complex or by hiding information. | (Bringull, 2023; CNIL, 2019) | Maximizing profits and business objectives | Frustration, confusion, agacement | Hidden, UI manipulation, asymmetry | 2 |
| | | | 12 | Visual interference | The user expects to see the information presented in a clear and predictable manner on the page, but it is hidden, obscured, or disguised. | (Bringull, 2023) | Any action that benefits the company | Frustration, confusion, irritation | Hidden, UI manipulation, asymmetry | 2 |
| | | | 13 | Diversion of attention & distraction | Draw the user's attention away from their current task by exploiting perception, especially pre-attentive processing. For example, working on the color of a "continue" button while leaving the "learn more" or "configure" button smaller or gray. | (CNIL, 2019; Conti & Sobiesk, 2010) | Deter any action that is not beneficial to the company | Confusion, annoyance, mistrust | Hidden, UI manipulation, framing effect, asymmetry, pre-attentive processing | 2 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 14 | Obscuration | Hide the desired information and interface elements. For example, by reducing the contrast of a close button on an advertisement. | (Conti & Sobiesk, 2010) | Deter any action that is not beneficial to the company | Confusion, frustration, irritation | Hidden, UI manipulation asymmetry, pre-attentive processing | 2 |
| | | | 15 | Hard to cancel & immortal accounts | These dark patterns simplify sign-up or subscription for users while making it difficult to unsubscribe or cancel, creating "immortal accounts." | (Bösch et al., 2016; Bringull, 2023) | Maximize user retention | Frustration, irritation, disappointment | Hidden, UI manipulation, asymmetry, framing effect | 2 |
| | | | 16 | Difficulties in adjusting confidentiality | Facilitate consent with a simple action ("continue" button) and make the data protection process longer and more complicated ("learn more" and scroll bars). | (CNIL, 2019) | Maximizing data collection and sharing | Frustration, confusion, irritation | Hidden, UI manipulation, asymmetry, framing effect | 2 |
| | | | 17 | Obscure & "Zuckering" Privacy Settings | These dark patterns deliberately make privacy settings either excessively long and complex, or so fine and complicated that they cause users to abandon or unintentionally change their privacy preferences. | (Bösch et al., 2016; CNIL, 2019) | Maximizing data collection and sharing | Frustration, confusion, helplessness | Hidden, UI manipulation, asymmetry, framing effect | 2 |
| | | | 18 | Frame | Manipulate the user through the formulation of the different options by focusing on the positive aspects of a choice, while ignoring the potentially negative aspects. | (Frobrukerrådet, 2018) | Any action that benefits the company | Distrust, trust, satisfaction | Hidden, manipulation through formulation, framing effect, asymmetry | 2 |
| | | | 19 | Confirmshaming & Blaming the user | The user is emotionally manipulated through words by making them feel guilty or ashamed of their choices. For example, when they opt out of ad tracking or use an ad blocker. | (Bringull, 2023; CNIL, 2019) | Deter any action that is not beneficial to the company | Guilt, shame, frustration | Hidden, psychological manipulation, framing effect, asymmetry | 2 |
| | | | 20 | Improved experience | Use the argument of personalization and improved user experience to encourage the user to share more data. | (CNIL, 2019) | Incentive for data collection and sharing | Trust, satisfaction, mistrust | Hidden, manipulation through formulation, framing effect | 2 |
| | | | 21 | Just you and me | Request additional data that is not strictly necessary for the performance of the service with the promise that this data will remain "invisible" and under the control of the user. | (CNIL, 2019) | Incentive for data collection and sharing | Confidence, mistrust, disappointment | Hidden, manipulation through formulation, framing effect | 2 |
| **Forced** | **Deceptive** | **Hidden** | 22 | False rarity | The user is tricked into taking an action because they are presented with a false | (Bringull, 2023) | Incentive to engage or purchase | Excitement, anxiety, | Hidden, misleading, scarcity bias, | 3 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | indication of limited supply or popularity. | | | frustration, mistrust | FOMO, false information | |
| | | | 23 | False urgency | The user is pressured to perform an action because they are presented with a false time limit. | (Bringull, 2023) | Incentive to engage or purchase | Excitement, anxiety, frustration, mistrust | Hidden, misleading, scarcity bias, FOMO, false information | 3 |
| | | | 24 | Fake social proof | The user is led to believe that a product is more popular or credible than it actually is, because they have been shown fake reviews, testimonials, or fake activity messages. | (Bringull, 2023) | Incentive to engage or purchase | Confidence, distrust, disappointment, irritation | Hidden, misleading, bandwagon effect, false information | 3 |
| | | | 25 | False declaration | Misleads users by providing them with ambiguous and incorrect information, thus encouraging them to take actions in the interest of the shareholder, in a direct and explicit way. | (Gray et al., 2018) | Any action that benefits the company | Frustration, mistrust, anger | Hidden, misleading, false information | 3 |
| | | | 26 | Bait and change | An adjustment or choice made by the individual produces a different result than the one desired. For example, giving an acceptance value to a button with a cross, which in the minds of users is synonymous with "close and continue". | (CNIL, 2019) | Any action that benefits the company | Frustration, confusion, anger, mistrust | Hidden, misleading in the UI | 3 |
| | | | 27 | Wrong signal | Using a "universally" understood graphic code to mean the opposite, thus creating confusion among the user about the choice he or she is making. For example, adding a padlock to an interface that is not particularly secure. | (CNIL, 2019) | Incentive to engage or purchase | Confusion, mistrust, irritation | Hidden, misleading in the UI | 3 |
| | | | 28 | Disguised Ads & Camouflaged Advertising | The user mistakenly believes that they are clicking on an interface element or native content, when in fact it is a disguised advertisement. | (Bringull, 2023; CNIL, 2019) | Maximizing Ad Revenue | Frustration, confusion, anger, mistrust | Hidden, misleading in the UI | 3 |
| | | | 29 | Trick | Deceiving the user or other attempts at deception, such as spoofing content or interface elements. For example, installing additional software without the user's knowledge or consent. | (Conti & Sobiesk, 2010) | Any action that benefits the company | Frustration, confusion, anger, mistrust | Hidden, misleading in the UI | 3 |
| | | | 30 | Two-sided | Two-faced dark patterns present conflicting information to the user, prompting them to follow a predetermined path. Like an ad blocker | (Gray et al., 2018) | Incentive to engage or purchase | Confusion, frustration, irritation | Hidden, misleading in the UI | 3 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | app with the words "Contains ads" written in small letters. | | | | | |
| | | | 31 | Misleading Wording, Trick Question & Confusion | These dark patterns mislead the user with ambiguous or confusing language, such as a question formulated with a double negative that can lead to an unintended answer, thus creating a deliberately confusing experience. | (Bringull, 2023; CNIL, 2019; Conti & Sobiesk, 2010) | Any action that benefits the company | Confusion, frustration, bewilderment | Hidden, misleading, ambiguous and misleading language | 3 |
| | | | 32 | Chameleon strategy | Adopts the appearance of an existing website to integrate a third-party service into the browsing process, thus encouraging the user to take unintended actions, such as installing software or subscribing to additional services. | (CNIL, 2019) | Incentive to engage or purchase | Confusion, mistrust, disappointment | Hidden, misleading in the UI | 3 |
| | **Manipulative** | **Visible** | 33 | Control & Restricted Features | Explicitly directs the user's workflow by limiting or omitting necessary controls, such as deselect options in pre-checked mailing lists, or by using non-skippable pop-ups. | (Conti & Sobiesk, 2010; Gray et al., 2018) | Deter any action that is not beneficial to the company | Frustration, irritation, helplessness | UI manipulation, restriction, asymmetry | 4 |
| | | | 34 | Forced action and coercion | The user is forced to take unwanted actions or comply with rules if they want to continue their task, such as the need to fill in mandatory fields in a form. | (Bringull, 2023; Conti & Sobiesk, 2010; Mathur et al., 2019) | Any action that benefits the company | Frustration, irritation, injustice | Coercive manipulation, restriction, asymmetry | 4 |
| | | | 35 | Reward and punishment | Use incentives to reward the "right" choice and punish choices that the service provider deems undesirable. This use of ultimatums is sometimes referred to as a "take it or leave it" situation. | (Frobrukerrådet, 2018) | Any action that benefits the company | Frustration, injustice, irritation | Coercive manipulation, restriction, asymmetry | 4 |
| | | | 36 | Impenetrable Wall & Forced Inscription | Blocking access to a service by creating an account or a cookie wall when it is not necessary to use the service as such. A "take it or leave it" situation. | (Bösch et al., 2016; CNIL, 2019) | Incentive for data collection and sharing | Frustration, irritation, helplessness | Coercive manipulation, restriction, asymmetry | 4 |
| | | | 37 | Harassment & repeated incitement | Confusing the user with requests or inducements to do something else, even if it is not in their best interest, such as repeated pop-ups asking for data sharing while browsing a website. | (Bringull, 2023; CNIL, 2019; Gray et al., 2018) | Incentive for engagement and data collection | Irritation, fatigue, frustration | UI manipulation, interruption | 4 |
| | | | 38 | Interruption | Interrupt the flow of the user's task by covering it with ads for example. | (Conti & Sobiesk, 2010) | Maximizing Ad Revenue | Irritation, fatigue, annoyance | UI manipulation, interruption | 4 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 39 | Obstruction | Hindering the flow of a task, making an interaction more difficult than it should be in order to deter an action. For example, ads blocking access to information, or disabling features in pop-ups. | (Bringull, 2023; Gray et al., 2018; Mathur et al., 2019) | Deter any action that is not beneficial to the company | Frustration, irritation, resignation | UI manipulation, restriction | 4 |
| | | | 40 | Play by appointment | The player must play at certain times of the day or week so as not to lose their progress in the game. | (Zagal et al., 2013) | Engagement Incentive and Retention | Satisfaction, frustration, irritation, disappointment | Coercive manipulation, restriction, FOMO, positive renforcement | 4 |
| | | | 41 | Forced labor | Deliberately increasing the user's workload, such as by making it difficult to uninstall software or making the user wait with countdowns. | (Conti & Sobiesk, 2010) | Deter any action that is not beneficial to the company | Frustration, irritation, resignation | UI manipulation, restriction | 4 |
| | | **Hidden** | 42 | Automate the user | Designers who automate the user automate the process of performing tasks without the user's consent or confirmation, redirecting the agency to partially or fully collaborate with the system to perform a particular action. | (Gray et al., 2018) | Any action that benefits the company | Surprise, powerlessness, anger | Hidden, manipulation in the system, restriction | 5 |
| | **Deceptive** | **Hidden** | 43 | Hidden subscription | The user is unknowingly enrolled in a recurring subscription or payment plan without being clearly informed or having given their explicit consent. | (Bringull, 2023) | Incentive to engage or purchase | Surprise, frustration, mistrust, anger | Hidden, misleading, lack of consent | 6 |
| | | | 44 | False continuity | Asking the user to give their address to read the article without warning clearly enough that it is in fact a subscription to a newsletter. | (CNIL, 2019) | Incentive to engage or purchase | Frustration, disappointment, mistrust, irritation | Hidden, misleading, lack of consent | 6 |
| | | | 45 | Hidden legal stipulation | Terms and conditions, often ignored by users due to their length and complexity, can be used to conceal clauses impacting the user's privacy, such as data collection clauses, without the user being aware of it. | (Bösch et al., 2016) | Incentive for data collection and sharing, minimizing legal liabilities | Frustration, anger, helplessness | Hidden, misleading, lack of consent | 6 |
| | | | 46 | Hidden costs, nickel & gradation, pre-delivered content, sneakiness | These dark patterns lure users in with low upfront prices and then impose hidden fees or require additional purchases, misleading about the total cost or included features. | (Bringull, 2023; Gray et al., 2018; Zagal et al., 2013) | Maximizing Profits | Surprise, disappointment, frustration, resignation | Hidden, misleading, coercion, anchoring bias, foot-in-the-door technique, sunk cost | 6 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | 47 | Sneak into basket | Automatic addition of items to the shopping cart without the user's explicit consent, often done by pre-checking options or hiding add actions. | (Mathur et al., 2019) | Incentive to engage or purchase | Surprise, frustration, mistrust, irritation | Hidden, misleading, lack of consent | 6 |
| | | | 48 | Trap | The user is incentivized to perform actions that benefit the shareholder, often by trapping them in choices that are difficult to avoid or correct, such as choosing between paying or watching ads to unlock content with time limitations. | (Gray et al., 2018) | Incentive to engage or purchase | Frustration, anger, disappointment | Hidden, misleading, coercion | 6 |

## Appendix B: Survey - Study on the impact of “Dark patterns” on website and application users.

### B.1. Introductory paragraph

Hello everyone,

Thank you for your interest in this study, which is part of my thesis in management sciences at UCLouvain. This survey focuses, more specifically, on the impact of “dark patterns” on website and application users. Your participation in this, on a voluntary basis, should not take more than 10 minutes of your time and is a valuable and essential aid to the success of my university course.

A dark pattern is a user interface designed to deceive or influence users to take actions or decisions that they did not initially intend to take. A well-known and often experienced example on the web is the difficulty in adjusting privacy, where consent to cookies is facilitated by a simple action (“continue” button) while the data protection process is made longer and tedious (button “learn more” and scrollbars). Another example is default pre-selection, where certain options like subscribing to newsletters or agreeing to additional terms are automatically checked, forcing the user to uncheck them if they don't want them.

- There are no specific conditions for participation, simply being an internet user.
- There is no right or wrong answer, it is all about expressing your personal opinion.
- Responses are confidential and anonymous and will be used for educational purposes only.

I am available at this address for any questions, comments or discussions on the subject: roman.vandenschrick@student.uclouvain.be

Many thanks in advance for your time and attention!

Romain Vandenschrick

***Consent statement to be filled by respondents:***

I freely and knowingly consent to participate in this study, understanding that my responses will be used for research purposes only and will remain confidential.

- o I would like to participate in this study
- o I do not wish to participate in this study

**B.2. Section I: Demographic & general questions**

What is your gender?

- Male
- Female
- Non-binary
- Prefer not to say

What is your age?

- 25 years old or less
- Between 26 and 35 years old
- Between 36 and 45 years old
- Between 46 and 55 years old
- 55 years old or older

How often do you use the internet?

- Daily
- Many times per week
- Once per week
- Less than once per week

How confident are you in your ability to use computer tools and navigate the internet?

- 1 (Very low confidence)
- 2 (Low confidence)
- 3 (Moderate confidence)
- 4 (High confidence)
- 5 (Very high confidence)

Before taking part in this survey, were you aware of the presence of dark patterns on websites and applications?

- Yes
- No

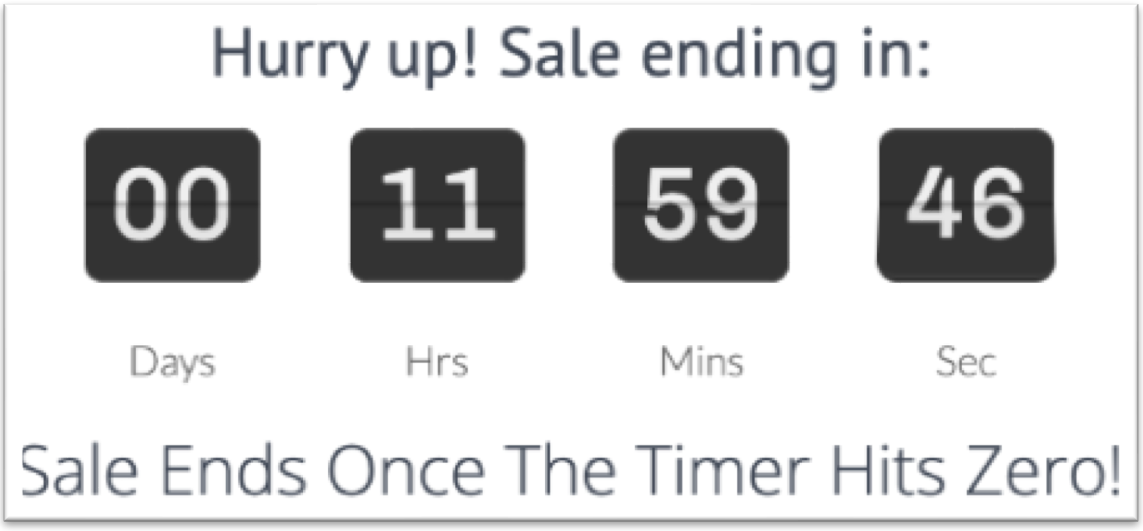
Have you ever felt manipulated by the design of a website or application?

- Yes
- No

### B.3. Section II: Questions related to dark patterns

#### *B.3.1. Urgency dark pattern*

This type of dark pattern displays a delay on sales or promotions, thus speeding up the purchasing and decision-making process. Countdowns are generally used.




This example illustrates a dark pattern of this type, have you already encountered it?

- Yes
- No

How do you think this dark pattern impacts or would impact your purchasing behavior?

- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

How do you feel, or would you feel about this type of dark pattern?

- Angry
- Frustrated
- Neutral
- Satisfied
- Joy

To what extent do you think this type of dark pattern affects or would affect your trust on the website or application?

- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

Would you revisit a website or application that uses this type of dark pattern?

- 1 (Highly unlikely)
- 2
- 3 (Neutral)
- 4
- 5 (Highly likely)

### *B.3.2. Confirmshaming dark pattern*

This type of dark pattern manipulates the user emotionally through words by making them feel shame or guilt about their choices.


This example illustrates a dark pattern of this type, have you already encountered it?

- Yes
- No

In what way do you think this dark pattern influences or would influence your decision to unsubscribe?

- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

How do you feel, or would you feel about this type of dark pattern?

- Angry
- Frustrated
- Neutral
- Satisfied
- Joy

To what extent do you think this type of dark pattern affects or would affect your trust on the website or application?

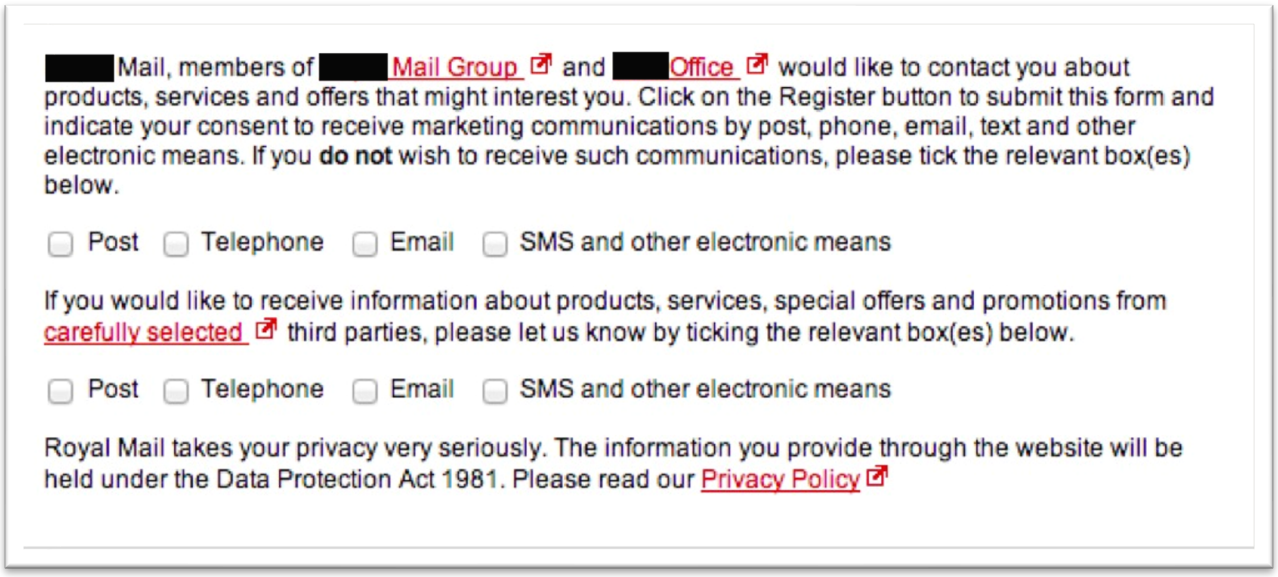
- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

Would you revisit a website or application that uses this type of dark pattern?

- 1 (Highly unlikely)
- 2
- 3 (Neutral)
- 4
- 5 (Highly likely)

### *B.3.3. Misleading Wording / Trick Question dark pattern*

This type of dark pattern misleads the user through ambiguous language or confusing questions. Like a question phrased with a double negative which can lead to an unintended answer, thus creating confusion.




This example illustrates a dark pattern of this type, have you already encountered it?

- Yes
- No

How do you think this dark pattern impacts or would impact your communication choices?

- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

How do you feel, or would you feel about this type of dark pattern?

- Angry
- Frustrated
- Neutral
- Satisfied
- Joy

To what extent do you think this type of dark pattern affects or would affect your trust on the website or application?

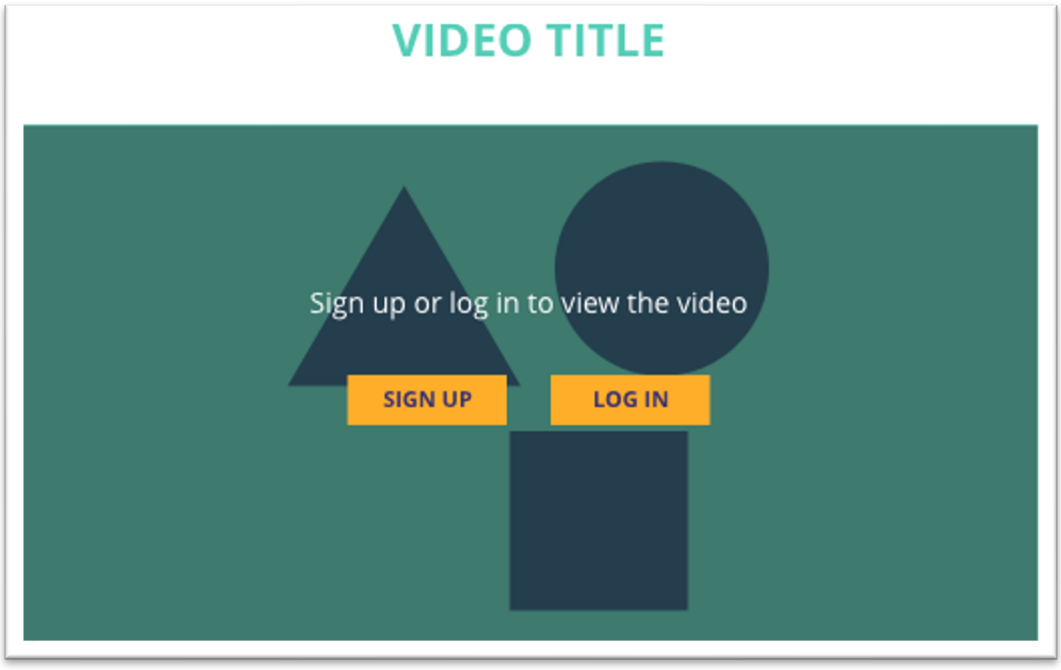
- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

Would you revisit a website or application that uses this type of dark pattern?

- 1 (Highly unlikely)
- 2
- 3 (Neutral)
- 4
- 5 (Highly likely)

***B.3.4. Forced action dark pattern***

This type of dark pattern forces the user to take unwanted actions or comply with rules if they want to continue their task, such as the need to fill out required fields in a form.




This example illustrates a dark pattern of this type, have you already encountered it?

- Yes
- No

In what way do you think this dark pattern influences or would influence your decision to register on the platform?

- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

How do you feel, or would you feel about this type of dark pattern?

- Angry
- Frustrated
- Neutral
- Satisfied
- Joy

To what extent do you think this type of dark pattern affects or would affect your trust on the website or application?

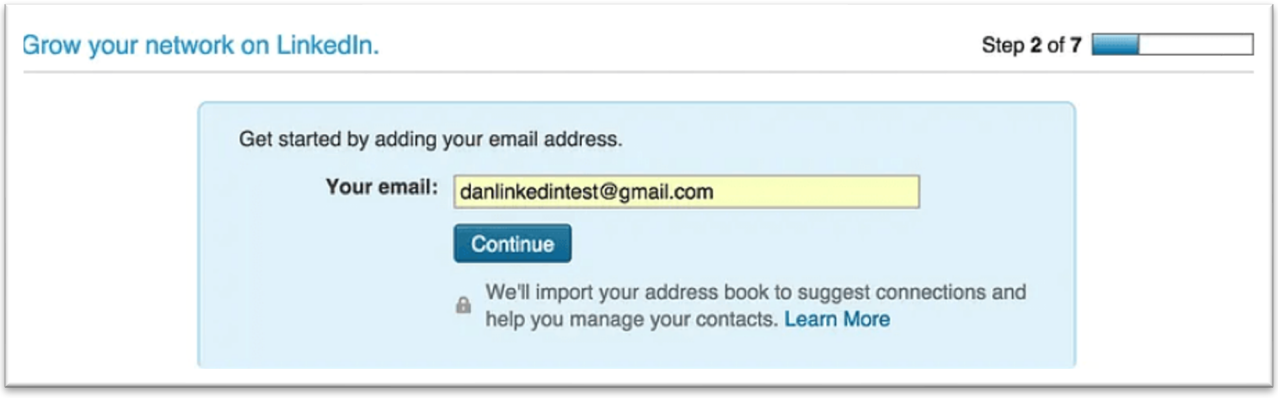
- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

Would you revisit a website or application that uses this type of dark pattern?

- 1 (Highly unlikely)
- 2
- 3 (Neutral)
- 4
- 5 (Highly likely)

#### *B.3.5. Automate the user dark pattern*

This type of dark pattern automates the task execution process, usually without user consent or confirmation.




This example illustrates a dark pattern of this type, have you already encountered it?

- Yes
- No

How do you feel, or would you feel about this type of dark pattern?

- Angry
- Frustrated
- Neutral
- Satisfied
- Joy

To what extent do you think this type of dark pattern affects or would affect your trust on the website or application?

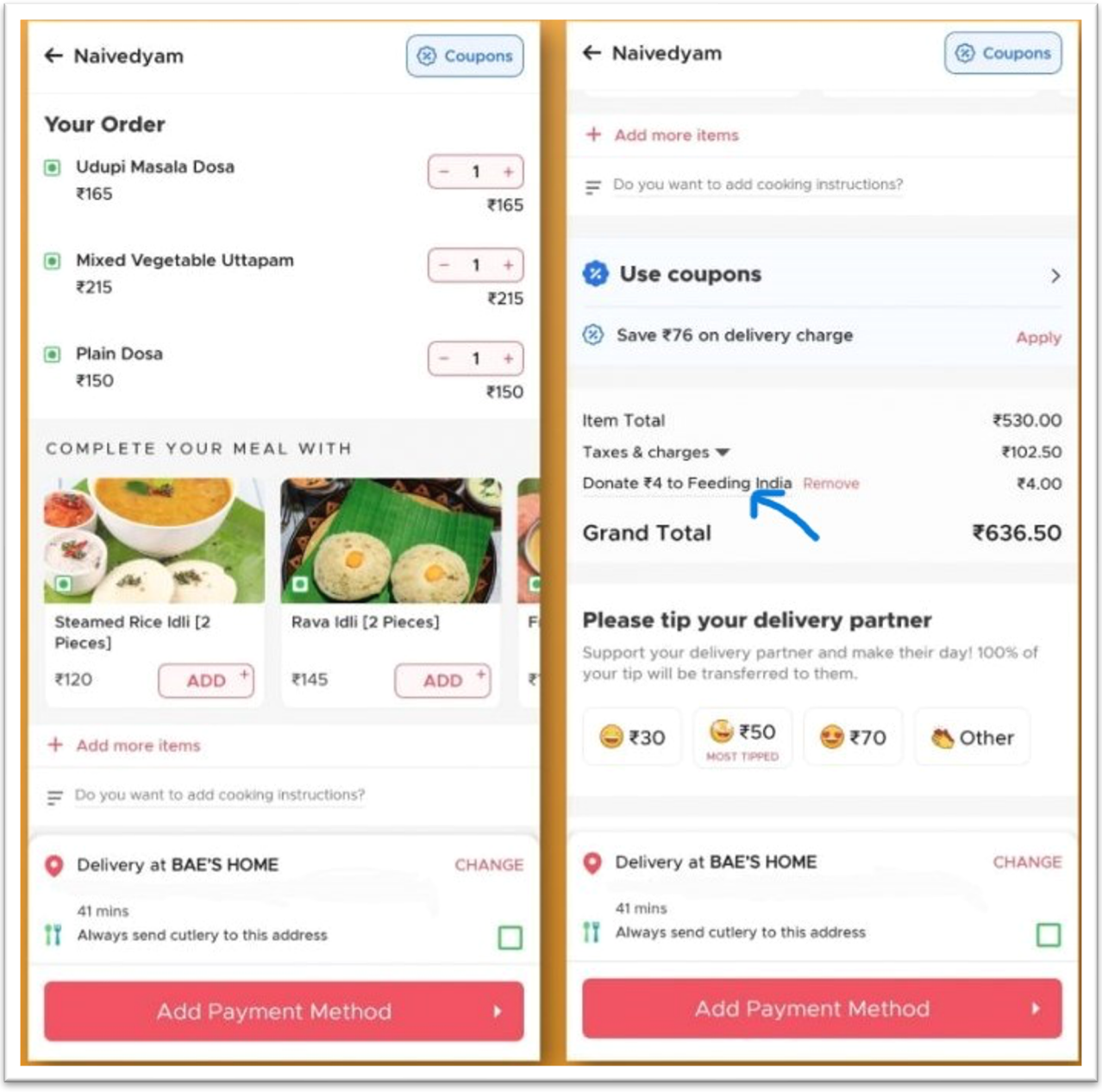
- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

Would you revisit a website or application that uses this type of dark pattern?

- 1 (Highly unlikely)
- 2
- 3 (Neutral)
- 4
- 5 (Highly likely)

### *B.3.6. Sneak into basket dark pattern*

This type of dark pattern refers to the automatic addition of items or charges to the shopping cart without the user's explicit consent, often by pre-checking options or hiding the addition process.




This example illustrates a dark pattern of this type, have you already encountered it?

- Yes
- No

How do you think this dark pattern impacts or would impact your purchasing behavior?

- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

How do you feel, or would you feel about this type of dark pattern?

- Angry
- Frustrated
- Neutral
- Satisfied
- Joy

To what extent do you think this type of dark pattern affects or would affect your trust on the website or application?

- 1 (Not impacted at all)
- 2
- 3
- 4
- 5 (Very impacted)

Would you revisit a website or application that uses this type of dark pattern?

- 1 (Highly unlikely)
- 2
- 3 (Neutral)
- 4
- 5 (Highly likely)

### B.4. Section III: Dark patterns classification

Evaluation and perception of “Dark patterns”.

Reminder of the 6 types of dark patterns seen previously:

- **Urgency:** imposes a delay on sales or promotions, thereby speeding up the purchasing and decision-making process.
- **Confirmshaming:** manipulates the user emotionally through words by making them feel shame or guilt about their choices.
- **Misleading Wording & Trick Question:** Misleads the user through ambiguous language or confusing questions, thereby creating confusion.
- **Forced action:** forces the user to take unwanted actions or comply with rules if they want to continue their task.
- **User Automation:** Automates the process of performing tasks, usually without user consent or confirmation.
- **Sneak into basket:** Automatically adding items or charges to the shopping cart without the user's explicit consent.

Could you, based on your personal opinion, classify the 6 types of dark patterns seen previously according to their “severity” of use (impact on the user, ethical and moral)?

Where 1 would designate the least blameworthy/criticisable and 6 the most blameworthy/criticisable (one box per row and per column).

Note: On smartphone, please scroll the table to the left to see its entirety.

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Urgency | ○ | ○ | ○ | ○ | ○ | ○ |
| Confirmshaming | ○ | ○ | ○ | ○ | ○ | ○ |
| Misleading wording & trick question | ○ | ○ | ○ | ○ | ○ | ○ |
| Forced action | ○ | ○ | ○ | ○ | ○ | ○ |
| Automating the user | ○ | ○ | ○ | ○ | ○ | ○ |
| Sneak into basket | ○ | ○ | ○ | ○ | ○ | ○ |

What do you think about using dark patterns in the user interface?

- ○ 1 (completely disagree)
- ○ 2 (Somehow disagree)
- ○ 3 (Neutral)
- ○ 4 (Somehow agree)
- ○ 5 (Completely agree)

Do you think more regulations should be implemented to protect users from dark patterns?

- Yes
- No
- Uncertain

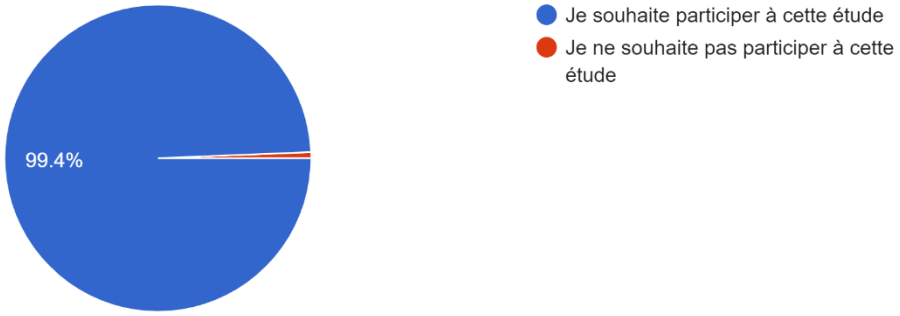
**B.5. Thank you note**

Your responses have been recorded. Thank you for taking the time to participate in this survey!

## Appendix C: Summary of survey answers

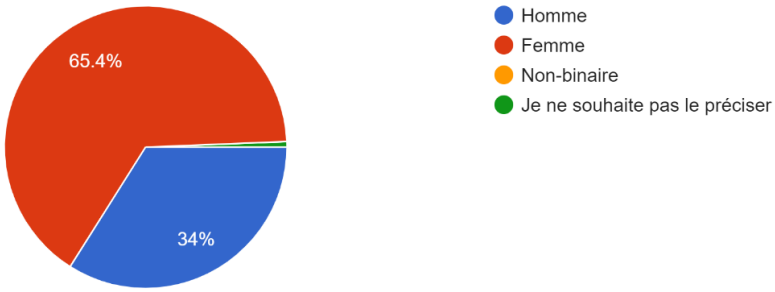
Je consens librement et en toute connaissance de cause à participer à cette étude, comprenant que mes réponses seront utilisées uniquement à des fins de recherche et resteront confidentielles.

159 responses



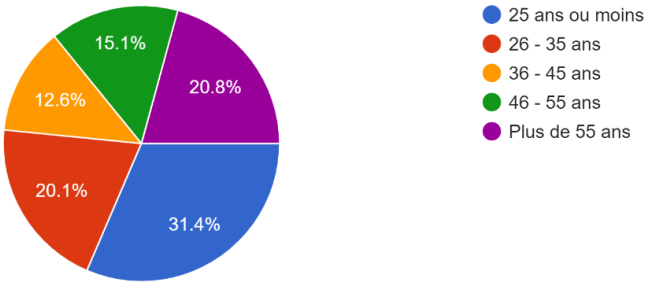

Quel est votre genre ?

159 responses



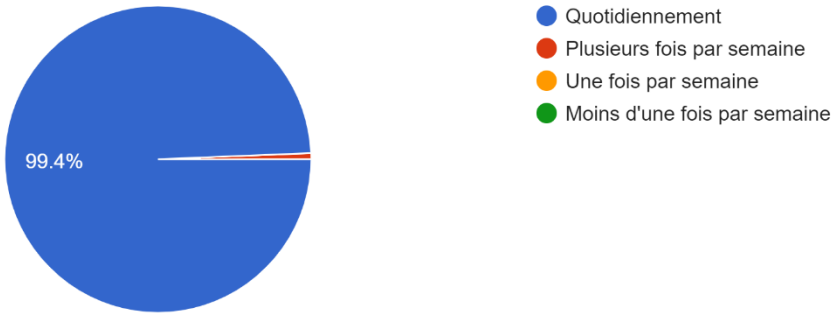

Quel est votre âge ?

159 responses



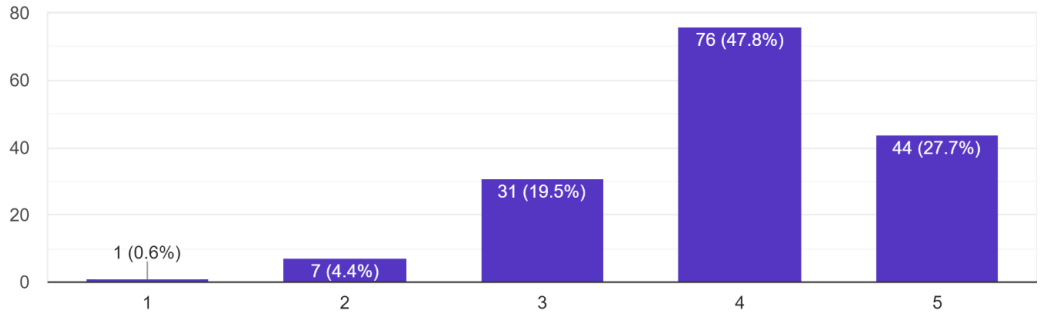
A quelle fréquence utilisez-vous internet ?

159 responses



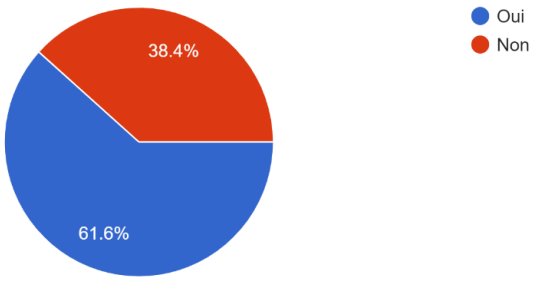

Dans quelle mesure êtes-vous confiant(e) dans votre capacité à utiliser des outils informatiques et naviguer sur internet ?

159 responses



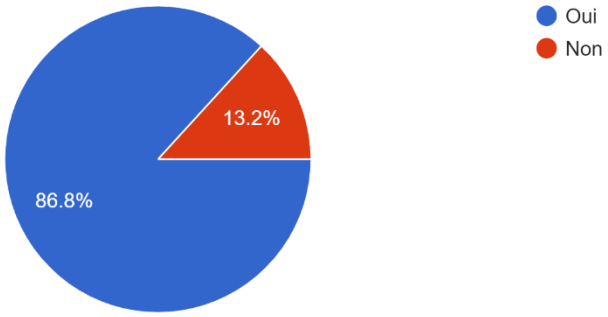

Avant de prendre part à cette enquête, aviez-vous connaissance de la présence des dark patterns sur les sites web et applications ?

159 responses



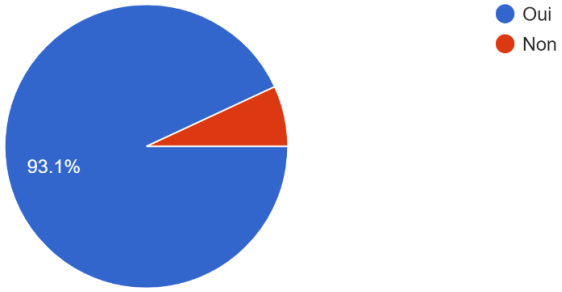
Vous êtes-vous déjà senti manipulé(e) par le design d'un site web ou d'une application ?

159 responses



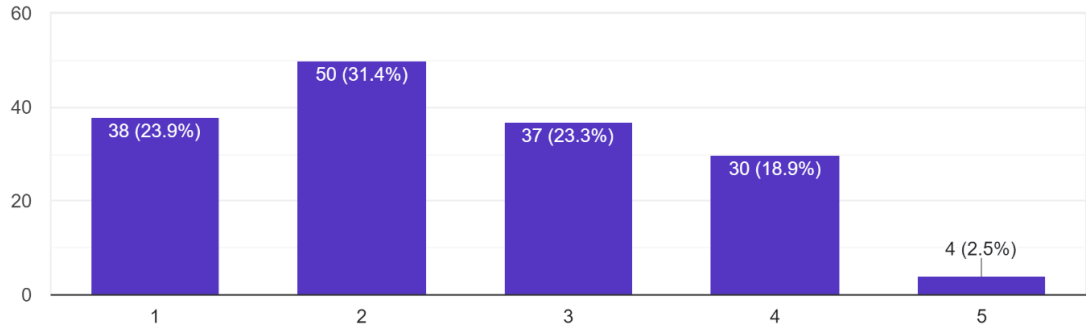

Cet exemple illustre un dark pattern de type "Urgence", l'avez-vous déjà rencontré ?

159 responses

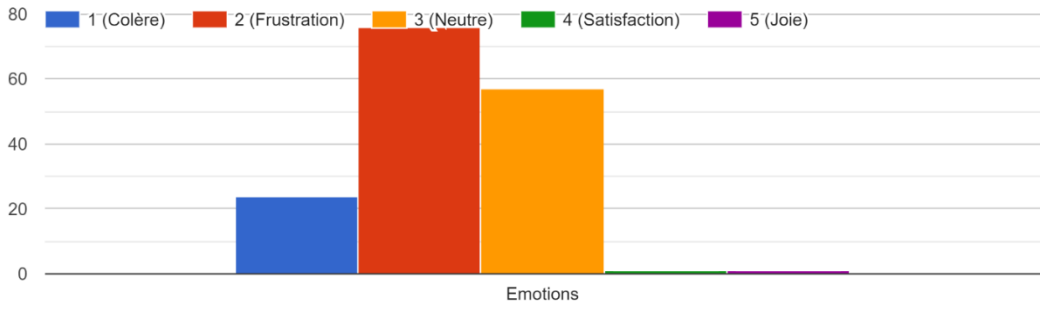



De quelle manière pensez-vous que ce dark pattern influence ou influencerait votre décision d'achat ?

159 responses

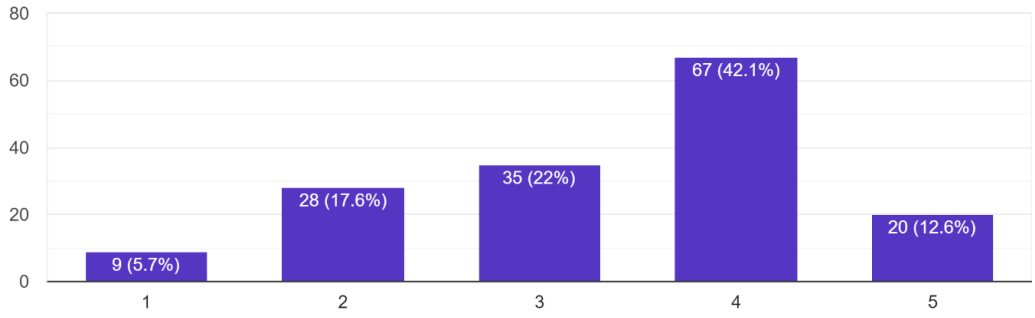


Que ressentez ou ressentiriez-vous face à ce type de dark pattern ?



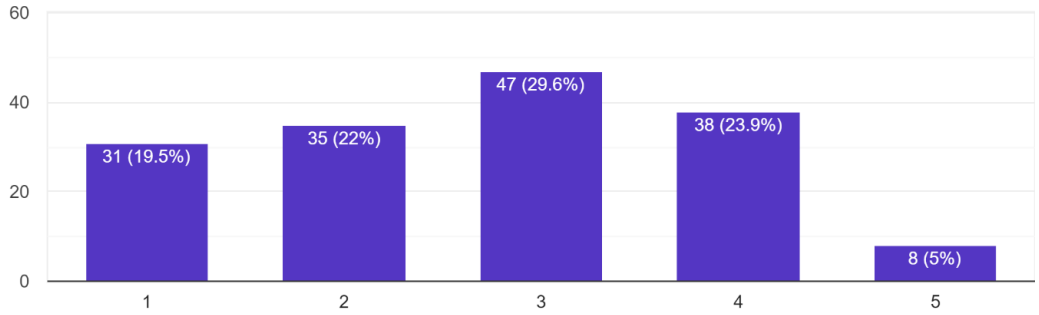

Dans quelle mesure pensez-vous que ce type de dark pattern affecte ou affecterait votre confiance envers le site web ou l'application ?

159 responses



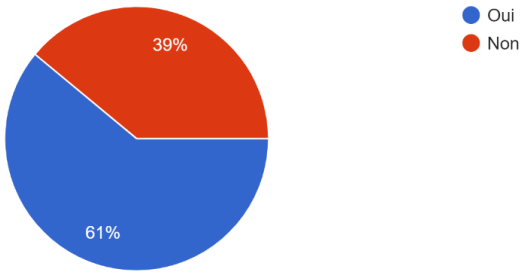

Revisiteriez-vous un site web ou une application faisant usage de ce type de dark pattern ?

159 responses



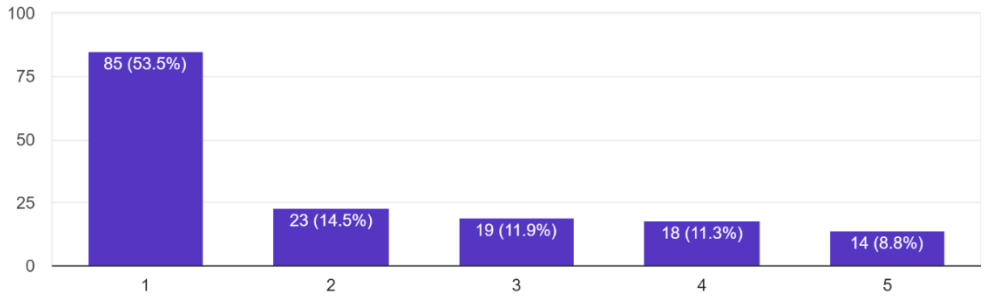
Cet exemple illustre un dark pattern de type "Confirmshaming", l'avez-vous déjà rencontré ?

159 responses

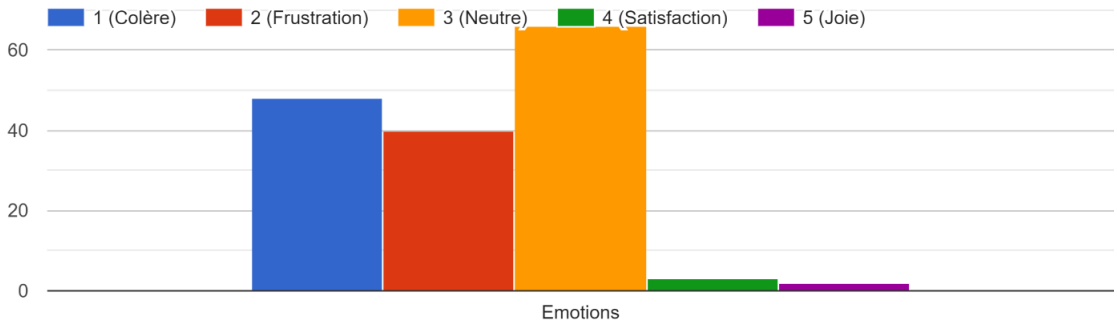



De quelle manière pensez-vous que ce dark pattern influence ou influencerait votre décision de vous désabonner ?

159 responses

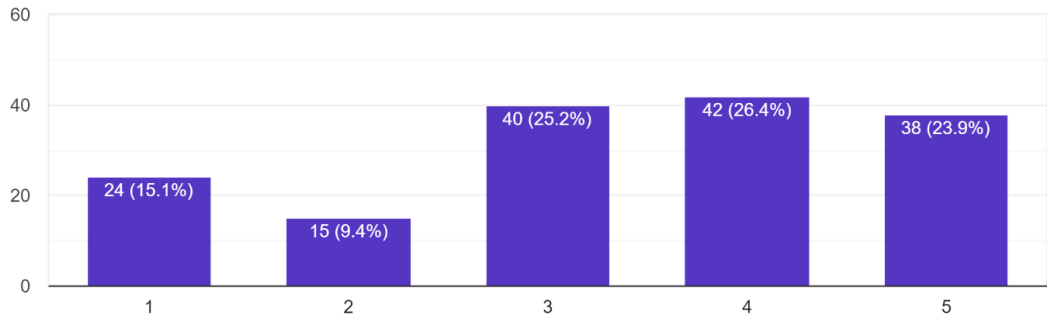



Que ressentez ou ressentiriez-vous face à ce type de dark pattern ?



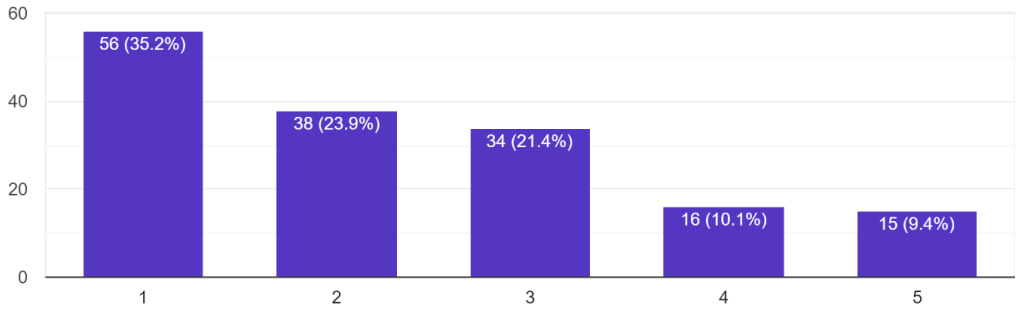
Dans quelle mesure pensez-vous que ce type de dark pattern affecte ou affecterait votre confiance envers le site web ou l'application ?

159 responses



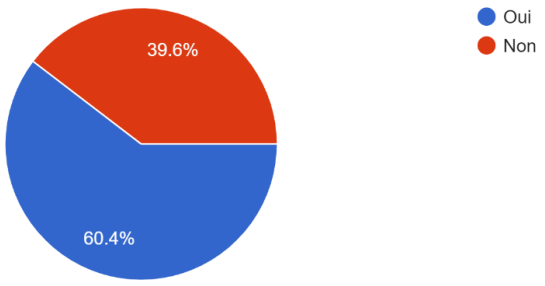

Revisiteriez-vous un site web ou une application faisant usage de ce type de dark pattern ?

159 responses



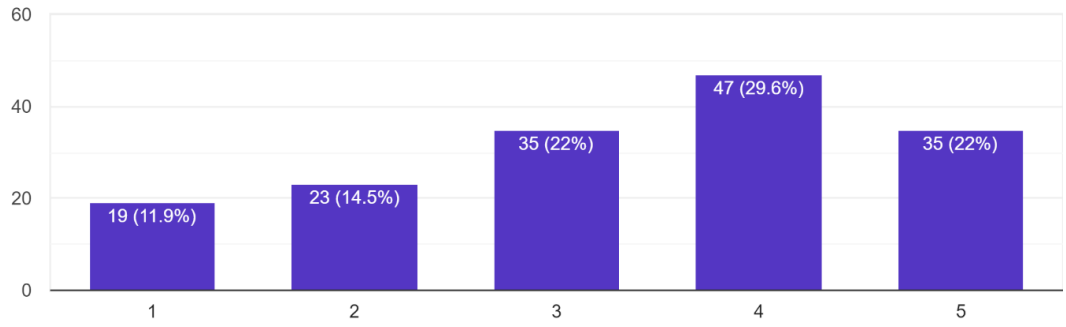

Cet exemple illustre un dark pattern de ce type, l'avez-vous déjà rencontré ?

159 responses

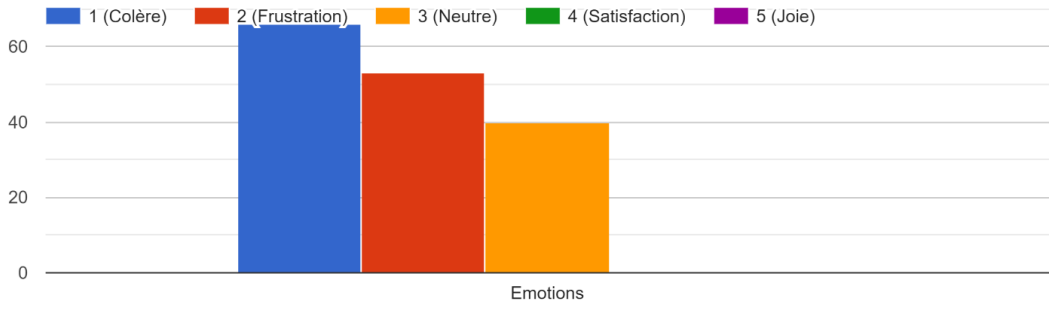


De quelle manière pensez-vous que ce dark pattern impacte ou impacterait vos choix de communication ?

159 responses

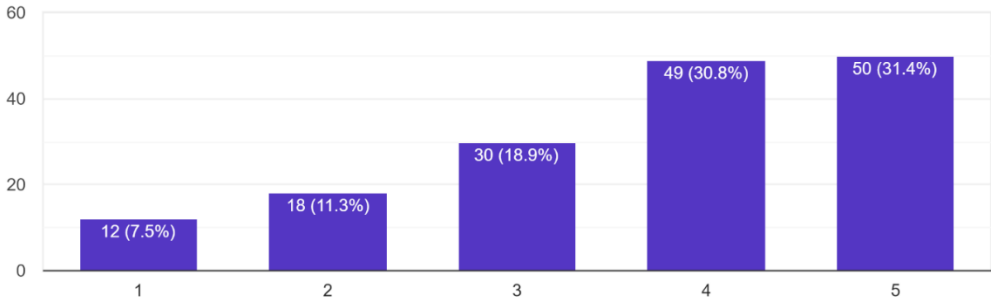



Que ressentez ou ressentiriez-vous face à ce type de dark pattern ?



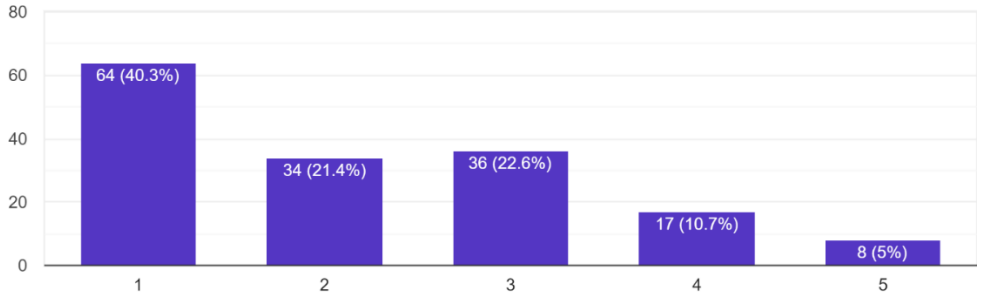

Dans quelle mesure pensez-vous que ce type de dark pattern affecte ou affecterait votre confiance envers le site web ou l'application ?

159 responses



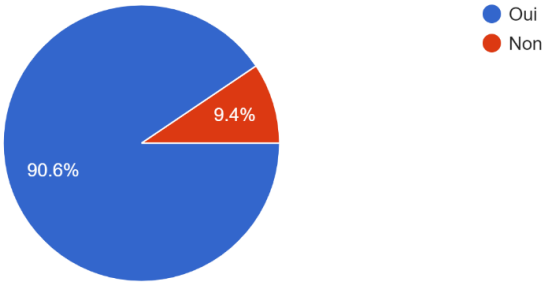
Revisiteriez-vous un site web ou une application faisant usage de ce type de dark pattern ?

159 responses



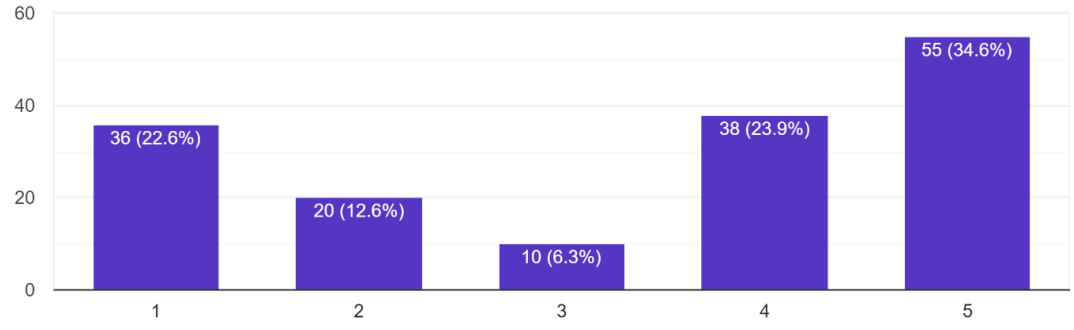

Cet exemple illustre un dark pattern de type "Action forcée", l'avez-vous déjà rencontré ?

159 responses

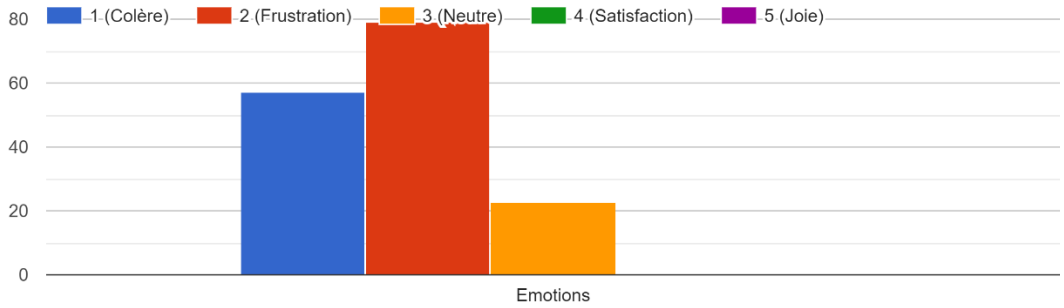



De quelle manière pensez-vous que ce dark pattern influence ou influencerait votre décision de vous inscrire sur la plateforme ?

159 responses

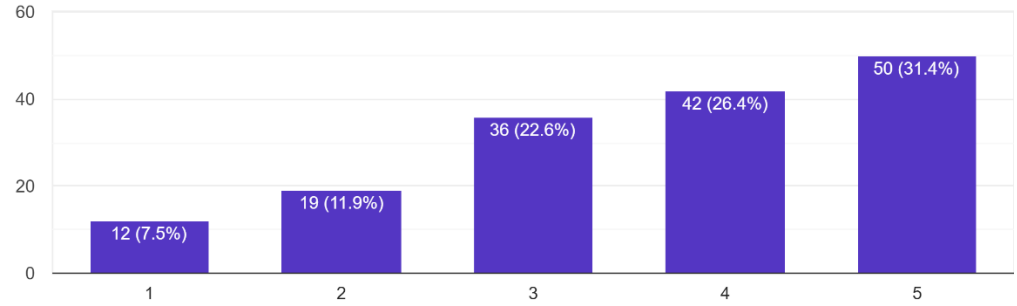


Que ressentez ou ressentiriez-vous face à ce type de dark pattern ?



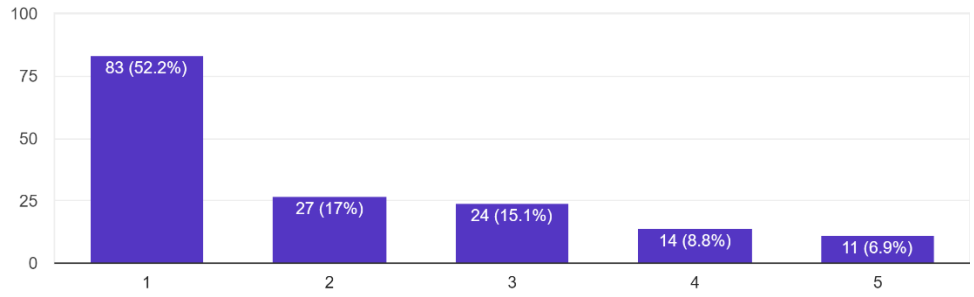

Dans quelle mesure pensez-vous que ce type de dark pattern affecte ou affecterait votre confiance envers le site web ou l'application ?

159 responses



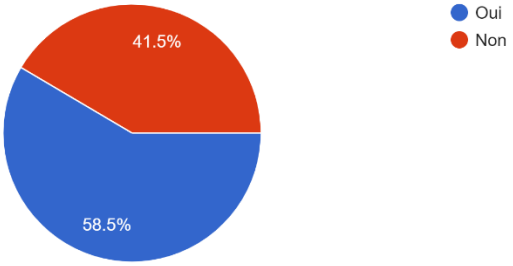

Revisiteriez-vous un site web ou une application faisant usage de ce type de dark pattern ?

159 responses

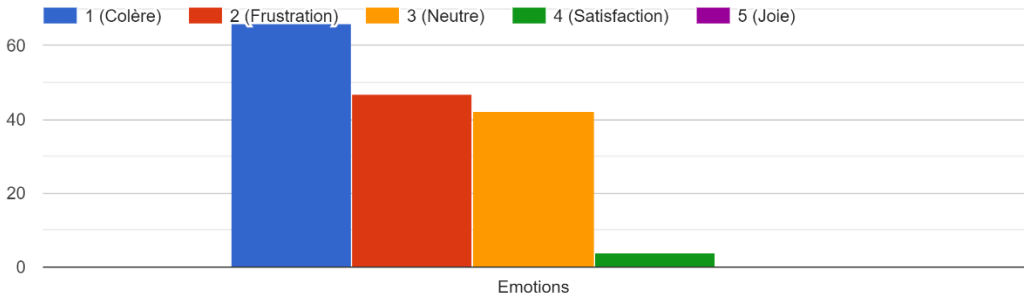


Cet exemple illustre un dark pattern de ce type, l'avez-vous déjà rencontré ?

159 responses

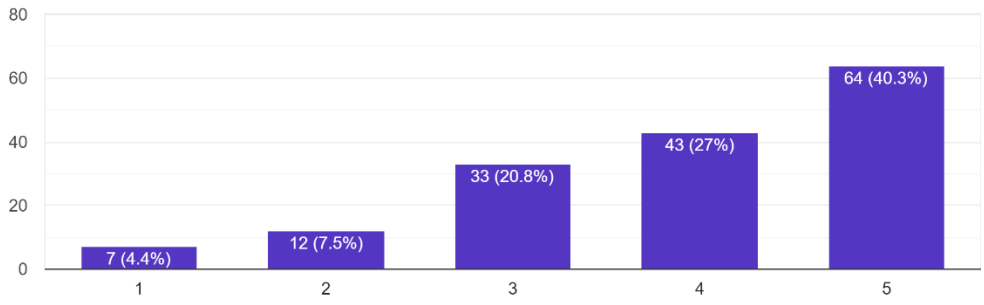



Que ressentez ou ressentiriez-vous face à ce type de dark pattern ?



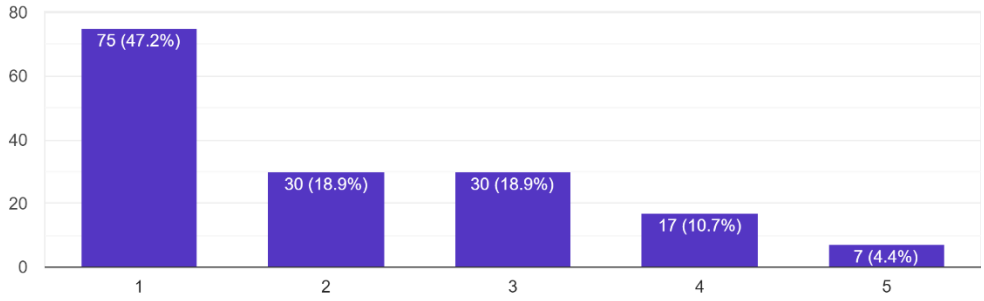

Dans quelle mesure pensez-vous que ce type de dark pattern affecte ou affecterait votre confiance envers le site web ou l'application ?

159 responses



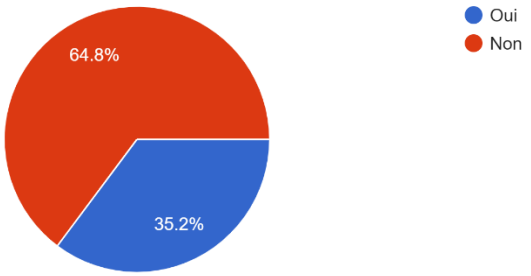
Revisiteriez-vous un site web ou une application faisant usage de ce type de dark pattern ?

159 responses



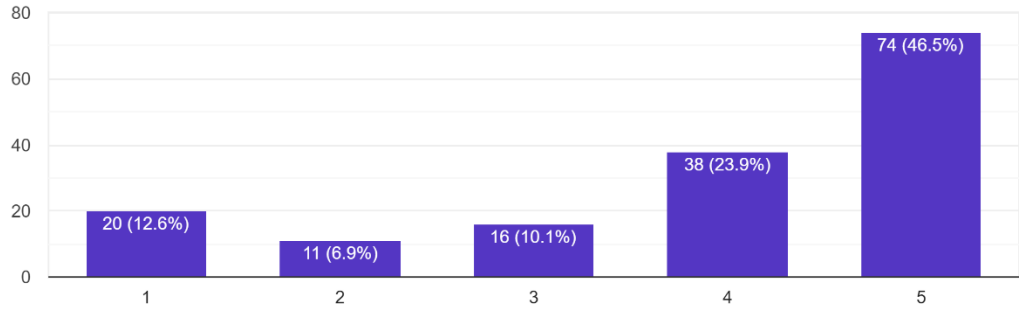

Cet exemple illustre un dark pattern de ce type, l'avez-vous déjà rencontré ?

159 responses

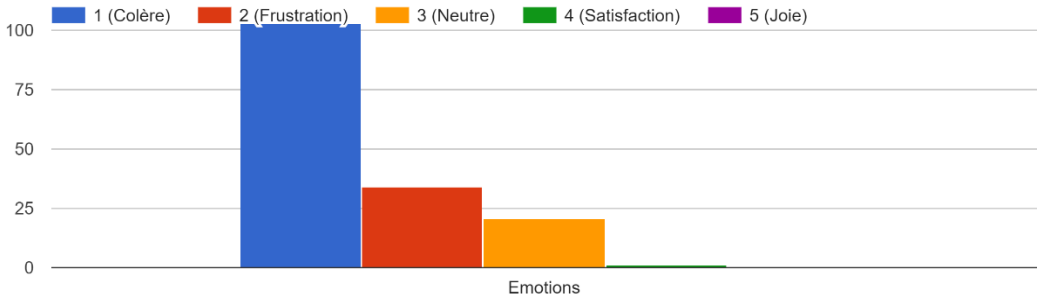



De quelle manière pensez-vous que ce dark pattern impacte ou impacterait votre comportement d'achat ?

159 responses

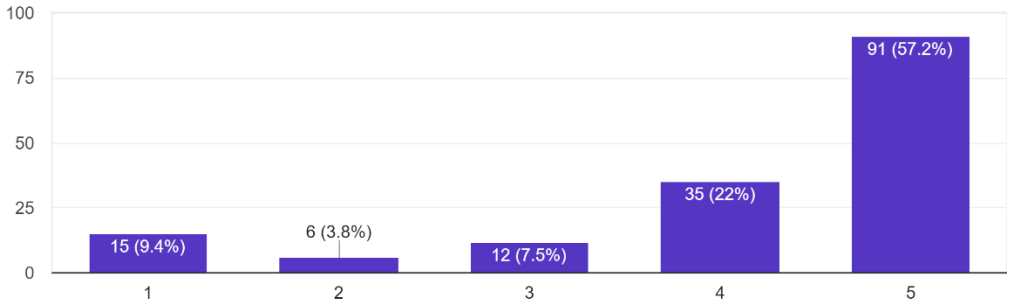


Que ressentez ou ressentiriez-vous face à ce type de dark pattern ?



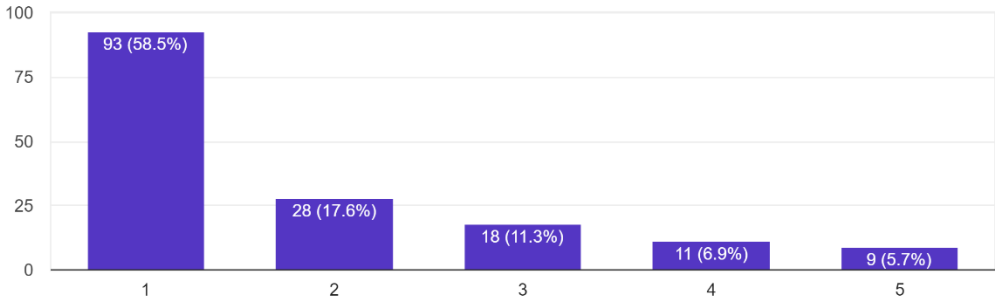

Dans quelle mesure pensez-vous que ce type de dark pattern affecte ou affecterait votre confiance envers le site web ou l'application ?

159 responses

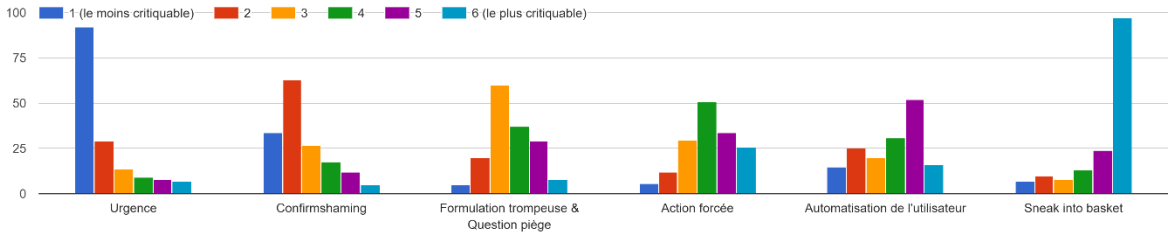



Revisiteriez-vous un site web ou une application faisant usage de ce type de dark pattern ?

159 responses

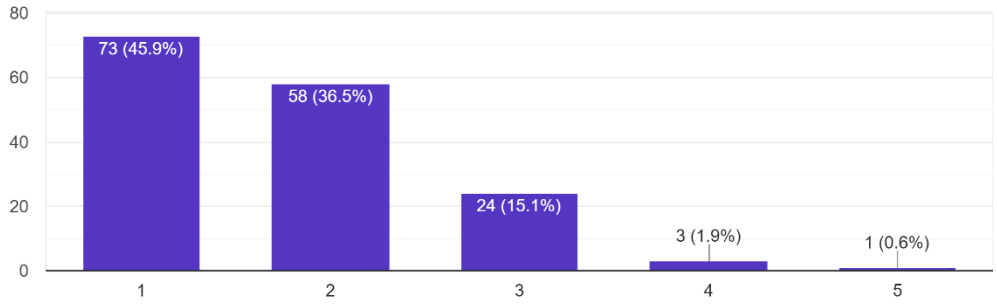


Pourriez-vous, sur base de votre opinion personnelle, classer les 6 types de dark patterns vu précédemment d'après leur « gravité » d'utilisation (impact sur l'utilisateur, éthique et moral) ?  Où 1 désignerait le moins blâmable/critiquable ...artphone, veuillez faire défiler le tableau vers la gauche pour voir son entièreté.



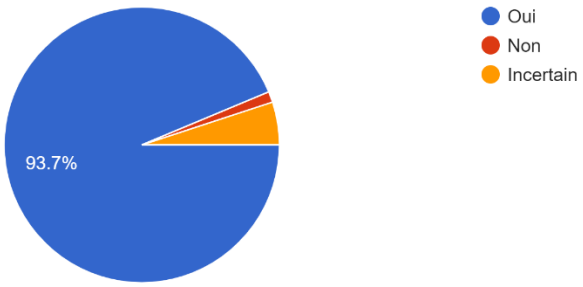

Que pensez-vous de l'utilisation des dark patterns dans l'interface utilisateur ?

159 responses




Pensez-vous que davantage de réglementations devraient être mises en œuvre pour protéger les utilisateurs contre les dark patterns ?

159 responses



## Appendix D: Survey collection ethical considerations

Ethical considerations are crucial in research involving human participants. This study adheres to strict ethical guidelines to protect participants' rights and well-being.

### D.1. Informed consent

Informed consent is vital for this research. Participants receive detailed information about the study's objectives, their involvement, and any potential risks and benefits before participating. Participation is voluntary, with the right to withdraw at any time without consequences. Consent is given through the completion and submission of the survey (Bryman, 2016).

### D.2. Confidentiality, anonymity, and data protection

Confidentiality and anonymity are essential for protecting participants' privacy. No personal identifiers are collected, and data is anonymized and securely stored to prevent unauthorized access. Digital data is safeguarded, stored in a secure Google Drive folder, and protected against third-party access (Creswell & Creswell, 2017).

### D.3. Minimizing harm

The study is also designed to minimize potential harm to participants. Survey questions are crafted to avoid distress or discomfort, with risks no greater than those encountered in daily life. Participants can discontinue their involvement at any time if they experience discomfort (Saunders et al., 2019).

### D.4. Transparency and Integrity

The study is conducted with transparency and integrity. Participants are fully informed about the study’s aims, methods, and potential impacts. Conflicts of interest are disclosed to maintain trust and objectivity. Procedures are carried out impartially, and findings are reported honestly (Neuman, 2013).

By adhering to these ethical guidelines, this study ensures participant protection and respects their rights, enhancing the credibility and integrity of the research.

## Appendix E: T-test and ANOVA techniques

### E.1. T-test analysis

The t-test analysis enables comparing between a mean and a variable, and between two means using the following formula:

$$t = \frac{\bar{X} - \mu}{s/\sqrt{n}}$$

Where $\bar{X}$ is the sample mean, μ is the hypothesized mean or the mean of the other group, $s$ is the standard deviation, and n is the sample size. Using the resulted t-value, the p-value is derived. If the p-value is less than the significance level ($\alpha$ = 0.05), the null hypothesis is rejected, otherwise we fail to reject the null hypothesis.

### E.2. ANOVA analysis

The ANOVA (Analysis of Variance) test enables to compare the difference between two or more groups using the following formula

:

$$F = \frac{Between\ group\ variability}{Within\ group\ variability} = \frac{MS_{between}}{MS_{within}}$$

Where $MS_{between}$ is the mean square between the groups and $MS_{within}$ is the mean square within the groups.

In this case, a p-value is derived from the resulted F-statistic, and if it is less than 5%, the null hypothesis is rejected, else, we fail to reject the null hypothesis.

## Appendix F: Null and alternative hypotheses development for H1 to H11

For each of the developed hypotheses in the literature review (H1 to H11), this section presents the null and alternative hypotheses corresponding to each one of them. For H1, H2, H3, H4, H6, H7, H8, H9, and H10, the analysis will consist of the comparison between two means using the t-test. However, for H5, and H3, the analysis will consist of the comparison between three or more means using the ANOVA analysis.

### F.1. Hypothesis H1: Influence on self-reported decision making

For H1, this study aims to investigate if the mean response for self-reported decision making is significantly higher than 3. In this context, the response scale ranges from 1 to 5, where 1 indicates no influence, 3 indicates neutrality, and 5 indicates a significant influence. Therefore, the null and alternative hypotheses for H1 are:

- **Null hypothesis ($H_0$):** Dark patterns do not significantly influence users' self-reported decision making ($\mu \leq 3$)
- **Alternative hypothesis ($H_a$):** Dark patterns significantly influence users' self-reported decision making ($\mu > 3$)

### F.2. Hypothesis H2: Influence on self-reported emotions

For H2, which measures the influence of dark patterns on users' emotions, a neutral value is 3. Values less than 3 indicate negative emotions (such as frustration or anger), and values greater than 3 indicate positive emotions. Since this study aims to investigate the negative influence, the hypotheses are:

- **Null hypothesis ($H_0$):** Dark patterns do not significantly influence users' self-reported emotions ($\mu \geq 3$)
- **Alternative hypothesis ($H_a$):** Dark patterns significantly and negatively influence users' self-reported emotions ($\mu < 3$)

### F.3. Hypothesis H3: Influence on self-reported trust

H3 investigates the impact of dark patterns on users' trust. Similar to H1, a mean value of 3 or less indicates no influence, while a value higher than 3 indicates a significant influence. The hypotheses are:

- **Null hypothesis ($H_0$):** Dark patterns do not significantly influence users' self-reported trust on the website/platform ($\mu \leq 3$)
- **Alternative hypothesis ($H_a$):** Dark patterns significantly influence users' self-reported trust on the website/platform ($\mu > 3$)

### F.4. Hypothesis H4: Influence on self-reported loyalty

H4 examines the influence of dark patterns on users' loyalty. Again, a mean value of 3 or less indicates no influence, while a value higher than 3 indicates significant influence. The hypotheses are:

- **Null hypothesis ($H_0$):** Dark patterns do not significantly influence users' self-reported loyalty towards the website/platform ($\mu \leq 3$)
- **Alternative hypothesis ($H_a$):** Dark patterns significantly influence users' self-reported loyalty towards the website/platform ($\mu > 3$)

### F.5. Hypothesis H5: Influence of age on the likelihood of being manipulated by dark patterns

For H5, the analysis examines whether age influences the likelihood of being manipulated by dark patterns. This involves comparing mean susceptibility scores across different age groups using ANOVA analysis. The hypotheses are:

- **Null hypothesis ($H_0$):** Age does not influence the likelihood of being manipulated by dark patterns ($\mu_{Less25} \geq \mu_{25\text{-}34} \geq \mu_{35\text{-}46} \geq \mu_{45\text{-}55} \geq \mu_{More55}$).
- **Alternative hypothesis ($H_a$):** Age influences the likelihood of being manipulated by dark patterns ($\mu_{Less25} < \mu_{25\text{-}34} < \mu_{35\text{-}46} < \mu_{45\text{-}55} < \mu_{More55}$).

### F.6. Hypothesis H6: Influence of IT confidence on the likelihood of being manipulated by dark patterns

Concerning H6, the focus is on determining if confidence in using IT affects the likelihood of being manipulated by dark patterns. The comparison between the means of being manipulated by dark patterns of people with high IT confidence (respondents with scores of 4 or 5) and people with less IT confidence (respondents with scores 3, 2, and 1) will be conducted using the t-test analysis. The null and alternative hypotheses for H6 are:

- **Null hypothesis ($H_0$):** Confidence in using IT does not influence the likelihood of being manipulated by dark patterns ($\mu_{Confident} \geq \mu_{NOTconfident}$).
- **Alternative hypothesis ($H_a$):** Confidence in using IT influences the likelihood of being manipulated by dark patterns ($\mu_{Confident} < \mu_{NOTconfident}$).

### F.7. Hypothesis H7: Influence of awareness on the likelihood of being manipulated by dark patterns

H7 explores whether awareness of dark patterns affects susceptibility to manipulation. The t-test analysis compares the mean of the group aware of dark patterns against the group not aware of dark patterns. This is to identify if the group aware of dark patterns is less likely manipulated by them or not. The hypotheses are:

- **Null hypothesis ($H_0$):** Awareness of dark patterns does not influence the likelihood of being manipulated by them ($\mu_{aware} \geq \mu_{NOTaware}$).
- **Alternative hypothesis ($H_a$):** Awareness of dark patterns decreases users' influence of dark patterns ($\mu_{aware} < \mu_{NOTaware}$).

### F.8. Hypothesis H8: Forced dark patterns are perceived as more blameworthy/reprehensible than oriented dark patterns

H8 evaluates whether forced dark patterns are perceived as more blameworthy than oriented ones. A t-test will compare the mean blameworthiness scores between these two categories. Therefore, it can be hypothesized that:

- **Null hypothesis ($H_0$):** Forced dark patterns are not perceived as more blameworthy than oriented dark patterns ($\mu_{Forced} \leq \mu_{Oriented}$).
- **Alternative hypothesis ($H_a$):** Forced dark patterns are perceived as more blameworthy than oriented dark patterns ($\mu_{Forced} > \mu_{Oriented}$).

### F.9. Hypothesis H9: Deceptive dark patterns are perceived as more blameworthy/reprehensible than manipulative dark patterns

For H9, the study investigates whether deceptive dark patterns are perceived as more blameworthy than manipulative ones. A t-test will be used to compare their mean blameworthiness scores. Hence:

- **Null hypothesis ($H_0$):** Deceptive dark patterns are not perceived as more blameworthy than manipulative dark patterns ($\mu_{Deceptive} \leq \mu_{Manipulative}$).
- **Alternative hypothesis ($H_a$):** Deceptive dark patterns are perceived as more blameworthy than manipulative dark patterns ($\mu_{Deceptive} > \mu_{Manipulative}$).

### F.10. Hypothesis H10: Hidden dark patterns are perceived as more blameworthy/reprehensible than visible dark patterns.

H10 assesses whether hidden dark patterns are perceived as more blameworthy than visible ones. A t-test will compare the mean blameworthiness scores for these categories. The hypotheses are:

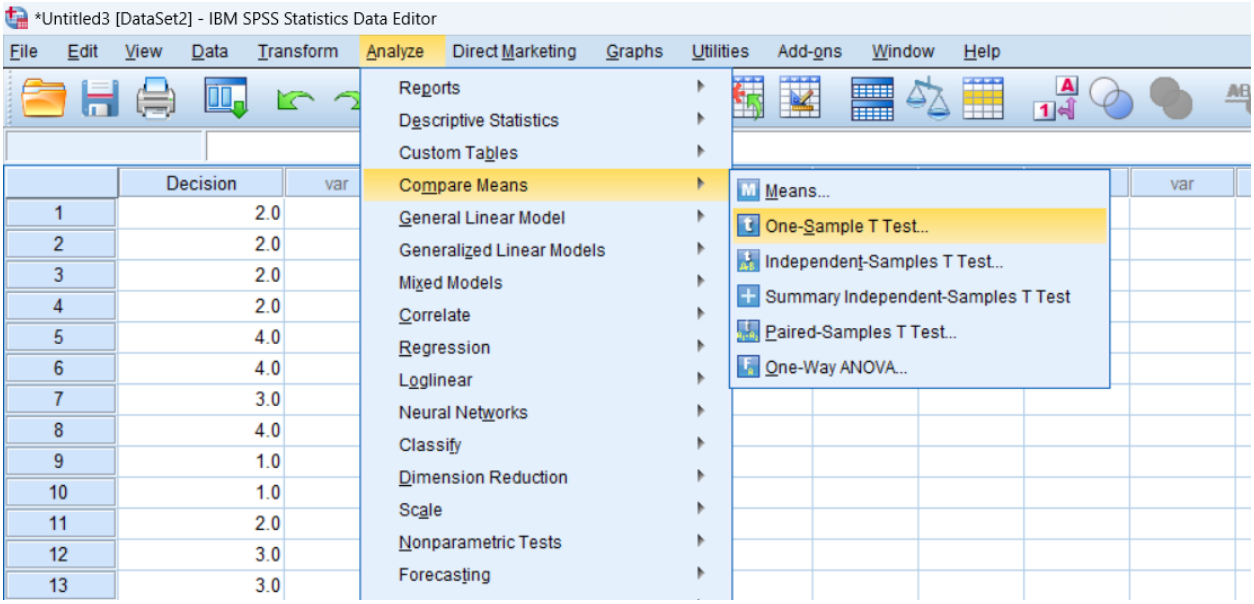
- **Null hypothesis ($H_0$):** Hidden dark patterns are not perceived as more blameworthy than visible dark patterns ($\mu_{Hidden} \leq \mu_{Visible}$).
- **Alternative hypothesis ($H_a$):** Hidden dark patterns are perceived as more blameworthy than visible dark patterns ($\mu_{Hidden} > \mu_{Visible}$).

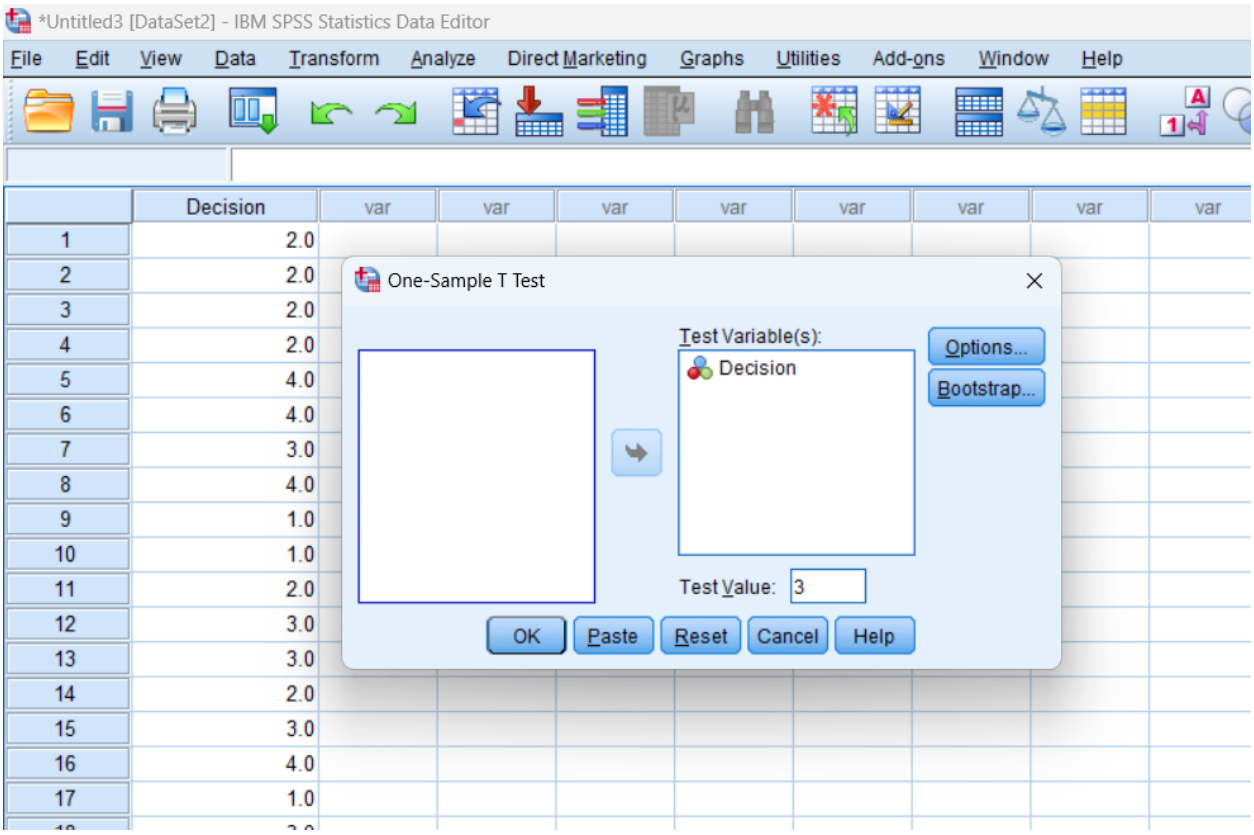
### F.11. Hypothesis H11: The degree of obligation is more blameworthy compared to the degree of deception, and the degree of deception is more blameworthy compared to the degree of visibility

With regards to H11, it tests the importance of the classification order, specifically whether the degree of obligation is perceived as more blameworthy than the degree of deception, and the degree of deception is perceived as more blameworthy than the degree of visibility. Therefore, this study hypotheses the following:

- **Null hypothesis ($H_0$):** There is no difference between the different layers of the proposed classification ($\mu_{Obligation} \leq \mu_{Deception} \leq \mu_{Visibility}$).
- **Alternative hypothesis ($H_a$):** The degree of obligation is more blameworthy than the degree of deception, and the degree of deception is more blameworthy than the degree of visibility ($\mu_{Obligation} > \mu_{Deception} > \mu_{Visibility}$).

# Appendix G: Steps to conducting t-test on SPSS



# T-Test

[DataSet2]

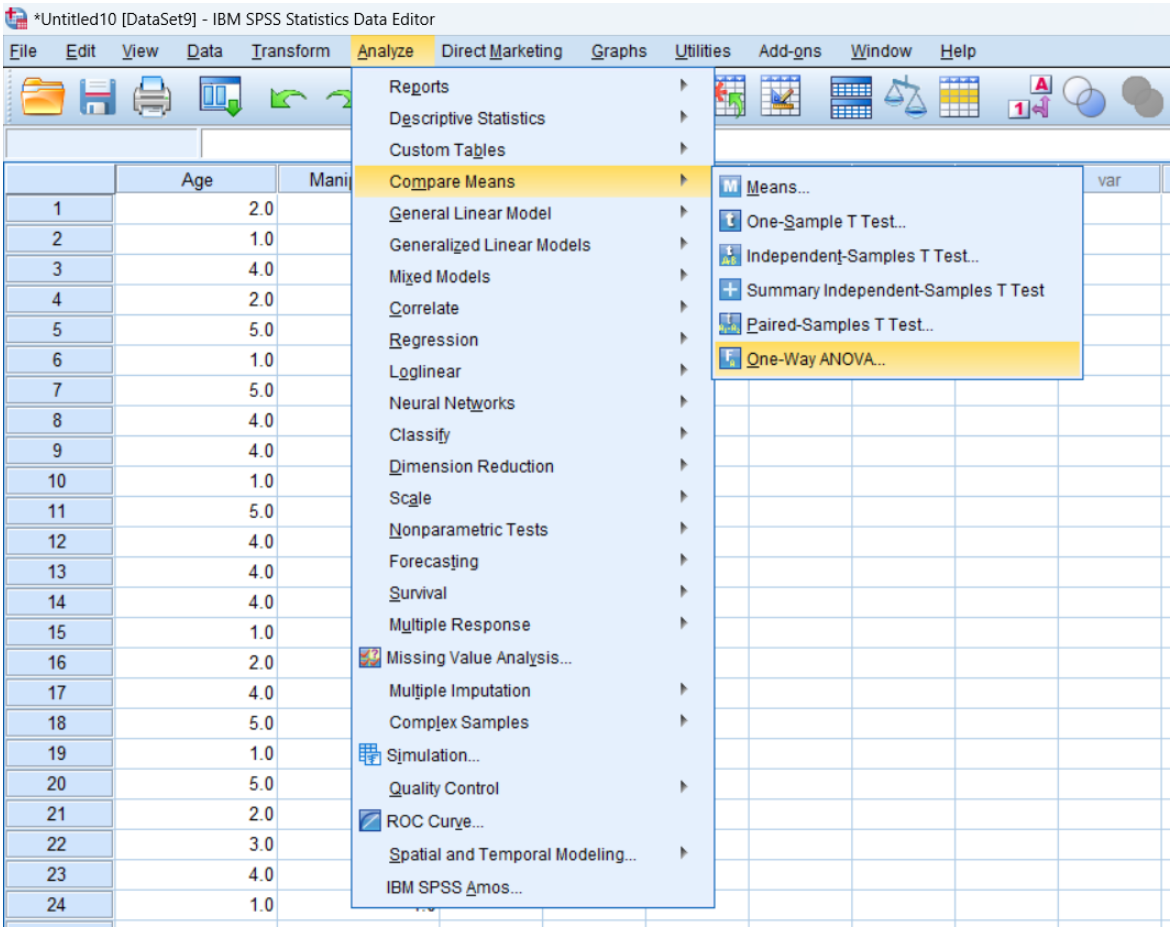
**One-Sample Statistics**

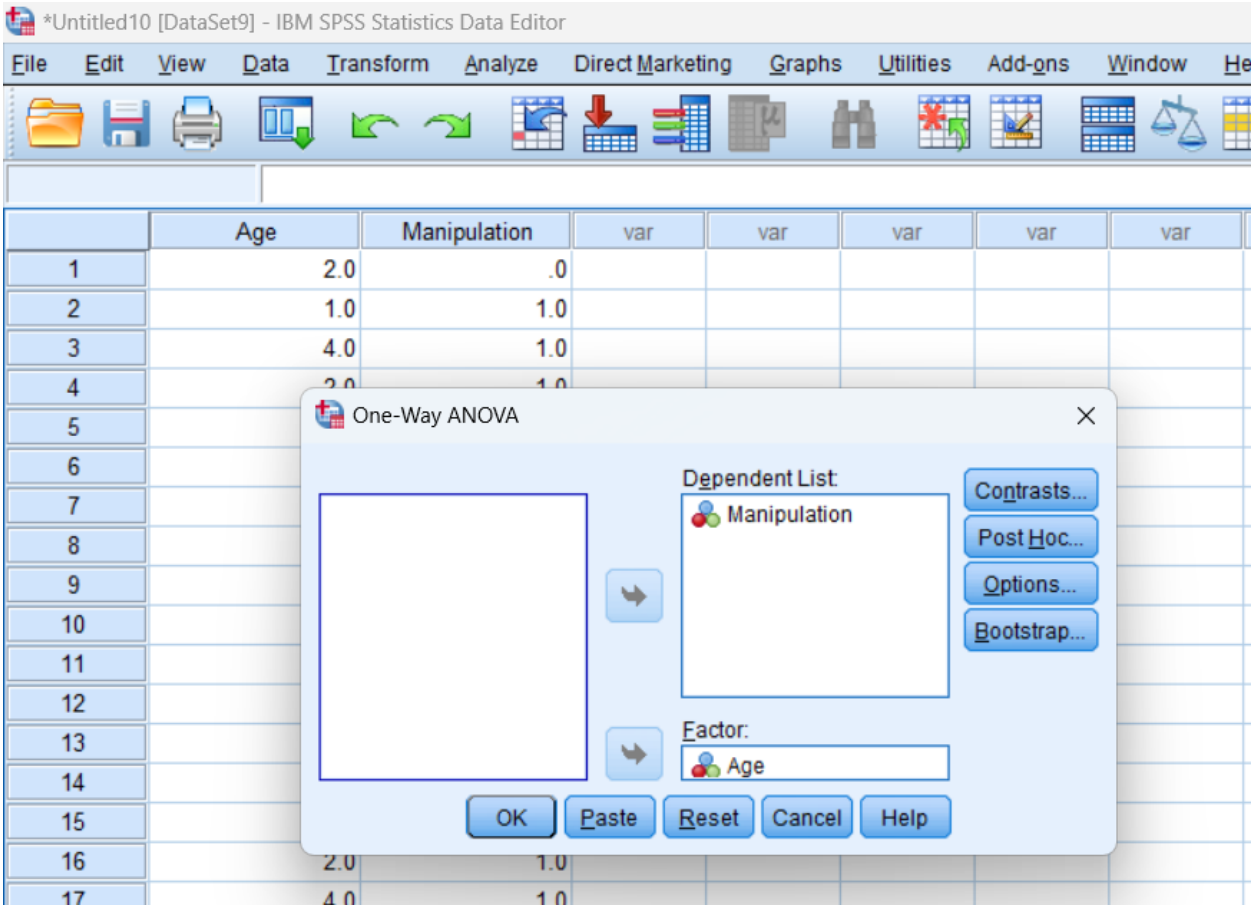
| | N | Mean | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|
| Decision | 795 | 3.018 | 1.5089 | .0535 |

**One-Sample Test**

| | Test Value = 3 | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 95% Confidence Interval of the Difference | |
| | t | df | Sig. (2-tailed) | Mean Difference | Lower | Upper |
| Decision | .329 | 794 | .742 | .0176 | -.087 | .123 |

# Appendix H: Steps to conduct ANOVA in SPSS






## Oneway

[DataSet9]

**ANOVA**

Manipulation

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | .047 | 4 | .012 | .096 | .984 |
| Within Groups | 18.909 | 154 | .123 | | |
| Total | 18.956 | 158 | | | |