

Playing with Risks - Deceptive Design Patterns in Digital Games Popular Among Children and Adolescents

João V Silva
joao.vsilva10@ufrpe.br

Universidade Federal Rural de Pernambuco
Recife, Pernambuco

George Valença
george.valenca@ufrpe.br

Universidade Federal Rural de Pernambuco
Recife, Pernambuco

ABSTRACT

Children are active users of digital platforms, particularly online games, where manipulative design features are often implemented to maximize engagement, retention, and monetization. While many of these mechanisms are considered legitimate game design practices, others may function as unethical design patterns that expose young users to different forms of online risk. In this paper, we investigate deceptive design patterns in digital games popular among young users and examine how these patterns relate to children's online risks. First, we reviewed taxonomies of deceptive and manipulative design in games. Next, we conducted an empirical study with game users who analyzed popular games and identified deceptive patterns based on the Dark Pattern Games taxonomy. Finally, the identified patterns were mapped to the 4Cs framework for children's online risks. Our results reveal 18 deceptive design patterns in 5 widely played games that encompass psychological, monetary, temporal, and social strategies. The findings indicate that these patterns are primarily associated with contract risks, conduct risks, and cross-cutting risks related to health and well-being, while content and contact risks were not directly represented. Hence, this study provides important evidence to promote safer and more ethical digital platforms for children and adolescents.

KEYWORDS

Deceptive Design, Dark Patterns, Children's Rights, Software Requirements

1 INTRODUCTION

According to the TIC Kids Online Brazil 2025 survey, 85% of Brazilian children and adolescents aged 9 to 17 have a profile on at least one social media platform.¹ Social media engagement increases with age, reaching 99% among adolescents aged 15 to 17. Despite their extensive participation in digital environments, many children remain unaware of online risks [24]. A major concern regarding children's digital

rights is the collection and processing of their personal data. Privacy regulations such as the General Data Protection Regulation require parental consent for data processing involving users under 16 [19]. However, children often disclose personal details while using digital platforms, exposing their online behaviors without proper consent, in conflict with the United Nations' (UN) principles on children's privacy rights [2].

Protecting children's well-being in digital platforms requires shielding them from risks such as harmful content, privacy violations, and exploitative commercial practices while also ensuring access to safe and developmentally appropriate online experiences. As children's online presence becomes increasingly valuable from commercial and engagement perspectives, digital platforms have adopted design strategies intended to influence user behavior and maximize participation [9]. Companies across different sectors, including social media and digital games, employ manipulative design strategies, previously termed *dark patterns*, that may pressure users into unintended actions such as making purchases, sharing personal information, or spending additional time on a platform [5]. Digital games constitute a particularly relevant context for studying deceptive and manipulative design. Unlike many online services, games are intentionally designed to sustain engagement through reward systems, progression mechanics, social interactions, and monetization features.

Although many of these mechanisms are legitimate design elements, some features may prioritize commercial goals over player autonomy and informed decision-making. These concerns become especially relevant for children and adolescents, whose online experiences are increasingly shaped by digital games and whose interactions with persuasive design features can expose them to different forms of online risk [12].

Our research investigates deceptive and manipulative design patterns in digital games popular among children and adolescents, as well as the online risks associated with such practices. While previous studies have examined deceptive design in digital platforms and online games, less attention has been given to understanding how these mechanisms relate to established frameworks of children's online risks. In particular, game mechanics designed to maximize engagement, monetization, and social participation may expose young users to several risks.

To address this gap, we first mapped taxonomies of deceptive design from the literature, with particular attention to game-specific patterns. Then, we conducted an empirical study with undergraduate students enrolled in a Digital Games course, who analyzed popular games and identified

¹Research on the use of the Internet by children and adolescents in Brazil - TIC Kids Online Brazil 2025 - <https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2025/>

deceptive patterns based on their previous experience as players. Finally, we mapped the identified patterns to the categories of the 4Cs framework for children's online risks, examining how specific game mechanics may be associated with different forms of risk affecting children and adolescents.

Through these findings, we aim to contribute to ongoing discussions on ethical game design, children's online safety, and the development of digital environments that better respect the rights and wellbeing of young users.

The remainder of this paper is organized as follows. Section 2 presents the conceptual background on deceptive design in games and children's online risks. Section 3 describes the research method. Section 4 presents the deceptive patterns identified in the analyzed games. Section 5 discusses how these patterns relate to children's online risks through the 4Cs framework. Section 6 discusses the implications of the findings for ethical game design, children's protection, and digital regulation. Finally, Section 7 presents concluding remarks, threats to validity, and directions for future research.

2 CONCEPTUAL BACKGROUND

The following sections present the main pillars of this research, which are essential to understand our results.

2.1 Deceptive and Manipulative Design in Games

Digital platforms frequently employ manipulative design strategies to influence user behavior and shape decision-making processes. These practices, often referred to as **deceptive or manipulative design patterns**, may alter how information is presented, create artificial pressures, or steer users toward choices that primarily benefit service providers rather than users themselves [5, 10]. Previous studies have shown that such strategies can affect user autonomy, privacy, and well-being, particularly when they exploit cognitive biases or emotional responses [6, 15].

We consider that digital games constitute a particularly relevant context to study manipulative design. Unlike many online services, games are intentionally designed to maximize engagement, encourage recurring participation, and sustain player investment over time. To achieve these goals, game developers often employ reward systems, progression mechanics, social features, and monetization strategies that shape player behavior [21]. While many of these mechanisms are legitimate game design elements, researchers have argued that some implementations may cross ethical boundaries when they prioritize commercial interests over player wellbeing.

The concept of dark patterns in games was carefully and initially discussed by Zagal, Björk, and Lewis [25], who describe game design practices that create experiences that benefit developers while potentially harming players. Examples include mechanisms that encourage excessive engagement, exploit social pressure, restrict meaningful choices, or incentivize spending through psychological manipulation. More recently, initiatives such as "Dark Pattern Games", which describes

strategies deliberately incorporated into games to create unwanted negative experiences for players while generating positive outcomes for game development companies².

These concerns become particularly relevant when considering children and adolescents. Those young users may face particular challenges in digital platforms characterized by persuasive and commercial design practices, as their capacities for critical evaluation, self-regulation, and decision-making continue to develop [22]. For this reason, child-rights and child-safety frameworks increasingly advocate for age-appropriate design and protections against manipulative digital practices. Hence, understanding how deceptive design patterns are embedded in games and how they relate to children's online risks represents an important step toward developing safer and more ethical digital environments.

2.2 Online Risks

The 4Cs framework is a widely adopted conceptual model for classifying online risks to children and adolescents, proposed by Livingstone and Stoilova [17] within the CO:RE (Children Online: Research and Evidence) project. The framework builds on earlier classifications of online risk and responds to changes in the digital environment by providing a structured and child-centered way to understand how different types of risks emerge through digital technologies.

The model identifies four main categories of online risk based on the child's position within the digital environment. **Content risks** refer to situations in which a child is exposed to potentially harmful or inappropriate material, such as violent, sexual, or hateful content. **Contact risks** occur when a child is targeted by harmful, adult-initiated interactions. These include predatory behaviors such as unwanted communication from strangers, grooming, harassment, or sexual solicitation. **Conduct risks**, in contrast, emerge from interactions among users in which children may be victims, participants, or witnesses of harmful behaviors, including bullying, harassment, or participation in toxic online communities. **Contract risks**, introduced as the fourth dimension, capture risks linked to commercial and contractual relationships between children and digital services, including data exploitation, unfair terms of service, manipulative monetization practices, and insecure platform design. In addition, the framework highlights several **cross-cutting risks** that can manifest across different forms of online activities. These include risks related to *privacy*, *health and wellbeing*, and *inequalities or discrimination*. Such dimensions are particularly relevant in digital environments where commercial, social, and behavioral mechanisms may interact to shape children's experiences and vulnerabilities.

Rather than focusing solely on individual behavior, the 4Cs framework emphasizes that online risks are shaped by platform design, governance structures, and broader digital ecosystems. By offering a clear and flexible classification, the framework supports systematic analysis, comparison, and

²The deceptive patterns and respective examples in several digital games are available at <https://www.darkpattern.games/>

communication of online risks and is widely used in research, policy, and child protection initiatives.

In this study, we adopt the 4Cs framework as analytical lens to interpret deceptive patterns identified in digital games, enabling an examination of how specific game mechanics may be associated with content, contact, conduct, contract, and cross-cutting risks affecting children and adolescents.

2.3 Related Work

We mapped related literature crossing deceptive design with children's protection to understand how we could contribute to the field. The work of Alashwali and Alashwali [1] explored children's privacy when using mobile devices from the perspective of their caregivers. With a rather quantitative approach, the authors adopted survey as a methodology to understand Saudi parents' privacy practices and concerns about their kids' smart device apps. This study analysed several practices that overlap with the list of LR's investigated in our research, such parental control features and privacy setting, but using the lens of parents, not of IT companies responsibilities. In addition, none of the privacy concerns were discussed as negative design features (i.e. deceptive patterns were not embraced by their study).

In their turn, Crepax and Mühlberg [7] investigated what they named as manipulative and addictive strategies in online games for children. Their work provides a rich contribution in terms of legal protections and causes of their failure, also proposing improvements for the current regulatory system in face of risks faced by children as game players (e.g. impacts on their freedom of thought). In addition, there is a discussion about technological approaches for ensuring children's privacy while playing games. Despite the rich contribution to understand manipulative design techniques, this study is centred on games domain. Our work approaches other contexts in which child users are widely present.

Finally, we highlight the investigation performed by Radesky and Hiniker [23]. They studied manipulative design features on apps (such as games) used by preschool-aged children, also obtaining the perspective of parents via a survey. This instrument provided demographic information to be crossed with characteristics of apps and their use by children. This study concluded that manipulative design features aim to fulfill the goals of IT companies, with no respect for children's best interests. Such techniques prolong gameplay or encourage purchases in apps, with clear reduction of autonomy and promotion of consumerism. This scenario calls for attention and regulation, where a possible solution is ethical standards (e.g. bright patterns, as we previously mentioned) and regulation. Hence, none of the papers had established the interplay between those two critical sets: deceptive design patterns and children's rights (here, expressed as legal requirements), which reinforces the originality of our research with respect to the state of the art.

3 RESEARCH METHOD

This study aimed to answer two research questions:

- RQ1 - What deceptive and manipulative design patterns can be identified in popular games among children and adolescents?
- RQ2 - How do the identified deceptive and manipulative design patterns relate to children's online risks?

To address RQ1, the **first phase** of this study consisted of mapping taxonomies of deceptive and manipulative design patterns³ in the Computer Science literature, encompassing contributions from the HCI community. This ad-hoc review considered searches for the terms "dark patterns", "deceptive patterns", and "manipulative patterns" in the titles of papers indexed in the IEEEExplore and Google Scholar databases.

Based on this review, we observed that the categorization proposed by Harry Brignull has been referenced in several studies addressing the topic (e.g. [3], [13], [10], [14], and [11], among others). However, given our focus on the game domain, we decided to consider the research on manipulative game design strategies from Zagal, Björk and Lewis [25]. Their study organizes these practices into *psychological*, *monetary*, *temporal*, and *social* dimensions. This perspective is also reflected in the Dark Pattern Games initiative, as mentioned in Section 2. In particular, we observed these four dimensions enable richer comparisons and discussions, as well as facilitate the replication of our findings through a shared language that supports interdisciplinary research and regulatory action.

Then, in a **second phase**, we obtained the perspective of game users regarding deceptive design in games. Their evaluation was based on a domain-specific taxonomy named "Dark Pattern Games"³, which also builds upon the taxonomy previously described in this paper. This source provides additional strategies deliberately incorporated into games to create unwanted negative experiences for players while generating positive outcomes for game development companies.

During this phase, a total of 15 participants (all students enrolled in Digital Games classes within a Computer Science program) were divided into teams to analyze manipulative strategies employed by technology companies in games, identifying deceptive patterns according to the taxonomy provided. We created a Google Forms questionnaire⁴, in which participants recorded the patterns observed and suggested solutions based on their experiences, as well as guidelines for the development of more ethical features.

After this activity, conducted on campus at the university and lasting approximately 25 minutes, the groups presented their interpretations, highlighting the most relevant points and promoting a collective discussion. This exchange of ideas encouraged critical reflections on the impacts of manipulative design in game development. Finally, we performed a qualitative data analysis on the resulting dataset using Thematic Synthesis [8]. Section 4 presents the outcomes of this phase.

In terms of ethical considerations, we highlight that participation in this study was voluntary and we collected all responses anonymously via a Google Forms questionnaire. In addition, no personally identifiable information was collected,

³Dark Pattern Games - <https://www.darkpattern.games/>

⁴The form is available at <https://forms.gle/azbQhDCsqXagQp716>

and participants could choose not to answer any question or withdraw from the activity at any time without any penalty or impact on course assessment.

Our study followed the ethical principles established by the Brazilian National Health Council Resolution No. 510/2016, which regulates research in the Human and Social Sciences. We consider that the research context involved public opinion and educational activity, with a discussion of a phenomenon in digital environments without the collection of sensitive or personal data or disclosure of the identities of participants. Therefore, our study involved minimal risk, since all participants were only asked to analyze game mechanics and reflect on their potential impacts. Finally, the activity also promoted their critical reflection on ethical design practices in games.

Finally, we conducted a **third phase** to answer RQ2, which aimed at interpreting the identified deceptive patterns through the lens of children's online risks. To achieve this, the deceptive patterns observed in the evaluated games were qualitatively mapped to the categories proposed by the 4Cs framework [17]. Each pattern was examined according to its potential association with content, contact, conduct, contract, and cross-cutting risks, considering the nature of the game mechanic and its possible implications for children and adolescents. Since cross-cutting risks may span multiple categories, particular attention was given to wellbeing-related implications identified across different game mechanics.

This analytical procedure enabled us to move beyond the mere identification of deceptive design strategies and examine the types of risks with which they may be associated in digital gaming environments. Particular attention was given to patterns associated with commercial and monetization mechanisms, social interactions among players, and engagement-oriented features that could affect children's wellbeing. The results of this mapping are presented in Section 5 and discussed in light of the broader literature on children's online safety and digital risks.

4 DECEPTIVE PATTERNS IN GAMES

Our evaluation of deceptive design from the perspective of game users revealed different forms of unethical design, which is the focus of RQ1. In total, study participants analyzed five games widely adopted by young users. After being introduced to the concepts of deceptive patterns and related definitions, the undergraduate students were divided into groups of 3 to 4 people. They selected games with which they were familiar and had previous experience, allowing them to critically examine gameplay mechanics, monetization strategies, social features, and engagement mechanisms that might otherwise require extended periods of interaction to identify. Based on this analysis, the groups identified the following manipulative patterns employed by the games:

- *Temple Run*⁵ is an endless runner game accessible to all ages and quite popular among children due to its simple and intuitive gameplay.

- *Clash Royale*⁶, rated for ages 10 and up, appeals to both children and teenagers, offering real-time strategic battles with a cartoonish visual style.
- *Saint Seiya Awakening*⁷, rated for ages 12 and up, is a mobile RPG that combines elements of nostalgia.
- *League of Legends*⁸, rated 13, has a predominantly teenage player base, influenced by the game's popularity in the competitive scene.
- *Valorant*⁹, rated 16 and up due to its violence and use of firearms, has a more mature target audience, but still attracts younger players, especially those who follow streamers and eSports competitions.

Although the evaluators were adults, the selected games are widely popular among children and adolescents. Therefore, those are all suitable cases to examine manipulative design practices that may affect younger users.

The participants identified multiple deceptive design strategies from four different categories: psychological patterns (PP), monetary patterns (MP), temporal patterns (TP) and social patterns (SP). We explain these categories and the 18 observed strategies in the following paragraphs.

Psychological patterns are strategies that exploit human psychology to encourage engagement and monetization. In this category, 3 patterns were mapped:

- *Badges*: participants found it in other games, such as Valorant. Badges serve as visual rewards that can generate a sense of accomplishment and encourage players to keep playing to get more.
- *Complete the Collection*: this mechanic is adopted by Clash Royale, where players are encouraged to collect all the cards available in the game.
- *Invested/Endowed Value/Progress*: this pattern was identified in League of Legends, for example. Participants pointed out that “*even with money and time, it's still hard to stop playing*”, illustrating how prior investment can hook the player. In Temple Run, the concept of endowed progress is linked to badges, while in Clash Royale it is implemented in achievements and score rankings that allow players to collect more cards.

Monetary patterns, which are deceptive strategies to generate revenue through different monetization mechanisms, were also largely available (6), according to participants:

- *Artificial Scarcity*: this pattern was mentioned in Valorant, where “*weapon skins are available for a specific time before other skins appear*”. This quote denotes a sense of urgency to purchase according to participants.
- *Loot Boxes*: in League of Legends, a participant cited “*new boxes that need to be opened in large quantities to risk winning a specific skin*”, which is a form of gambling.
- *Pay to Skip*: Temple Run allows a player to buy invincible for a finite amount of time when reaching a

⁶ Available at <https://tinyurl.com/mp4c7hzs>

⁷ Available at <https://tinyurl.com/5n8bbjmn>

⁸ Available at <https://tinyurl.com/yc38w7z8>

⁹ Available at <https://tinyurl.com/4529yuse>

⁵ Available at <https://tinyurl.com/b7c54nek>

very difficult stage. In its turn, Saint Seiya Awakening provides an energy system that can be recharged by paying.

- *Pay to Win*: Temple Run, Saint Seiya Awakening and Clash Royale, for example, implement this unethical design. In Saint Seiya Awakening, items purchased with real money give players real advantages, while in Clash Royale “gems” (real money) and season passes give better rewards.
- *Premium Currency*: in Saint Seiya Awakening, this pattern “allows players to pay to have access to premium items”, described a participant.
- *Recurring Fee*: in Valorant, the idea is “the more you play the more items you earn”, suggesting a progressive rewards system, possibly with a paid option to speed up or obtain exclusive rewards.

Some **temporal patterns**, which manipulate the perception of time and availability, could also be identified by participants in a few games. Below, we list the 5 strategies identified by participants.

- *Can't Pause or Save*: online games such as Valorant and League of Legends implement this pattern. For instance, a participant mentioned that “the game (League of Legends) being online does not allow you to disconnect from the match without receiving a penalty (even in casual matches)”.
- *Daily Rewards*: in Saint Seiya Awakening, for example, the daily quest and event system was described by participants as “punishing for not doing it daily”, suggesting that players may feel like they are missing out on something valuable if they don't play every day. In its turn, Clash Royale includes this pattern in “Daily Free Chest” and “Daily Quests that Give Rewards”.
- *Grinding*: participants observed it in Saint Seiya Awakening, which has “resource farming” modes that reward the player for doing it manually without leaving the game instead of automatically, encouraging the repetition of tasks to gain progress.
- *Infinite Treadmill*: in Valorant, this pattern suggests that the game is designed so that there is always something to achieve, keeping players continually engaged.
- *Playing by Appointment*: in a mechanic from Saint Seiya Awakening, a participant noticed that the game modes (e.g. “Galactic Duels”) can only be accessed during certain times of the day.

Finally, a total of 4 **social patterns** were described by study participants. Deceptive patterns from this category exploit social interactions and norms to influence player behavior. We illustrate them as follows.

- *Competition*: games like Valorant and League of Legends create ranks for the user to compete even with their own friends. In Valorant, the “ranked matches that are worth points are constantly reset and there is no maximum point cap”, which foster continuous competition, mentioned a participant.

- *Reciprocity*: in the guilds of Saint Seiya Awakening, this pattern defines a donation mechanic that creates a false sense of responsibility to donate back.
- *Social Obligation/Guilds*: in Saint Seiya Awakening, players have daily responsibilities to improve the guild's performance. In its turn, Clash Royale has guilds and guild matches that give prizes.
- *Social Pyramid Scheme*: this pattern was identified in Saint Seiya Awakening. A participant mentioned the existence of an event to share invitation codes for new players. Hence, the more new players each player brings, the greater the rewards.

In total, 18 specific deceptive and manipulative design patterns were identified in various games, as listed in Table 1. The pattern more widely implemented in games was “Badges” (4/5), when game developers aim to give players a sense of obligation to finish a goal (i.e. such accomplishment will then be represented as a virtual badge).

The game with the highest number of unethical design patterns (10/18) was *Saint Seiya Awakening*, revealing a design strategy focused on maximizing player engagement and monetization. For instance, temporal patterns, such as “Playing by appointment”, “Daily Rewards”, and “Grinding”, are implemented to foster a daily and prolonged gaming habit, creating a sense of obligation and potential loss if the player does not participate regularly.

In their turn, social patterns, including “Social Pyramid Scheme” and “Reciprocity”, exploit interpersonal dynamics to increase loyalty through rewards for invitations and obligations within groups, while monetary patterns, such as “Pay to Skip”, are clearly aimed at offering shortcuts, exclusive items, and competitive advantages in exchange for real money.

In Figure 1, a player can simply pay to obtain benefits and make a character progress more quickly in this game, while others will need to invest time and effort to achieve the same in-game advantages. Finally, the psychological pattern “Invested Value” acts as a retention mechanism, exploiting a player's attachment to the time and resources invested in the game to make it difficult to quit. In essence, the widespread use of these patterns suggests a prioritization of revenue and retention metrics through mechanics that can manipulate players' motivation and behavior.

Finally, some simple strategies were suggested by the participants to promote fair or bright patterns, providing children with a safer digital environment. Initially, for psychological patterns, a suggestion was to bring more casualness and reduce “toxic competitiveness”. In addition, for daily rewards, lower the level of rewards. In terms of monetary deceptive patterns, they reinforced the need to reduce loot boxes and remove penalties for leaving ranked matches. Other idea was to abolish pay-to-win, or as a solution, limit monthly spending per user. Finally, for social obligations, a participant suggested to give more casual guild assignments.

Table 1: Crossing Between Deceptive Patterns and Digital Games.

Deceptive Patterns	Temple Run	Clash Royale	Saint Seiya A.	League of Legends	Valorant
PP1 (Badges)	X	X	X		X
PP2 (Complete the Col.)		X			
PP3 (Invested Value)			X	X	
MP1 (Artificial Sc.)					X
MP2 (Loot Boxes)				X	
MP3 (Pay to Skip)	X		X		
MP4 (Pay to Win)	X	X	X		
MP5 (Premium Cur.)			X		X
MP6 (Recurring Fee)					X
TP1 (Can't Pause)				X	X
TP2 (Daily Rewards)		X	X		X
TP3 (Grinding)			X		
TP4 (Infinite Tr.)					X
TP5 (Playing by Ap.)			X		
SP1 (Competition)				X	X
SP2 (Reciprocity)			X		
SP3 (Social Obl.)		X			
SP4 (Social Pyr.)			X		
Total	3	5	10	4	8

**Figure 1: An example of Pay To Win pattern adopted by Saint Seiya Awakening, when players can use money to gain a competitive edge.**

5 INTERPLAY OF DECEPTIVE PATTERNS AND ONLINE RISKS

To answer RQ2, we mapped the deceptive and manipulative design patterns identified in the five analyzed games to the categories proposed by the 4Cs framework [17]. This analysis enabled us to investigate how specific game mechanics may be related to different forms of online risk affecting children and adolescents. Table 2 presents the resulting mapping.

Our mapping revealed that the deceptive patterns identified in the games are predominantly associated with three dimensions of the 4Cs framework: *Contract Risks*, *Conduct Risks*, and *Cross-cutting Risks*. In contrast, *Content Risks* and *Contact Risks* were not directly represented by the patterns observed in this study. This finding suggests that the primary risks associated with deceptive game design are not

necessarily related to the content consumed by children or to interactions initiated by adults, but rather to the design of engagement, monetization, and social participation mechanisms embedded in the games.

5.1 Contract Risks

Contract risks refer to harms arising from commercial and contractual relationships between users and digital services [17]. This category was strongly represented in the games, particularly through monetary patterns designed to encourage spending or increase the perceived value of purchases.

Patterns such as *Loot Boxes*, *Pay to Win*, *Pay to Skip*, *Premium Currency*, *Recurring Fee*, and *Artificial Scarcity* illustrate how game mechanics can be structured around monetization strategies. In these cases, players are encouraged to spend money to obtain competitive advantages, accelerate progression, unlock exclusive content, or avoid undesirable waiting periods. Hence, artificial scarcity and time-limited offers increase purchasing pressure by creating a perception of urgency and limited opportunity.

From the perspective of children's online risks, these mechanisms may expose young users to commercial exploitation and influence purchasing decisions via manipulative design choices. The prevalence of contract-related patterns across multiple games suggests that monetization is not merely a supplementary feature, but often a central component of contemporary game design.

5.2 Conduct Risks

Conduct risks emerge through interactions among users and may involve social dynamics that encourage potentially harmful behaviors or pressures [17]. In our study, four patterns

Table 2: Mapping Between Deceptive Patterns and Children's Online Risks.

Deceptive Patterns	Content	Contact	Conduct	Contract	Cross-cutting
PP1 (Badges)					X
PP2 (Complete the Col.)				X	X
PP3 (Invested Value)					X
MP1 (Artificial Sc.)				X	X
MP2 (Loot Boxes)				X	X
MP3 (Pay to Skip)				X	
MP4 (Pay to Win)				X	
MP5 (Premium Cur.)				X	
MP6 (Recurring Fee)				X	
TP1 (Can't Pause)					X
TP2 (Daily Rewards)					X
TP3 (Grinding)					X
TP4 (Infinite Tr.)					X
TP5 (Playing by Ap.)					X
SP1 (Competition)			X		X
SP2 (Reciprocity)			X		
SP3 (Social Obl.)			X		
SP4 (Social Pyr.)			X	X	
Total	0	0	4	7	10

were primarily associated with this category: *Competition*, *Reciprocity*, *Social Obligation*, and *Social Pyramid Scheme*.

These mechanics rely on relationships between players to sustain engagement and participation. Competitive ranking systems, guild responsibilities, invitation programs, and reciprocal contribution mechanisms create expectations regarding performance and participation within groups. While social interaction is an important aspect of many games, these patterns may intensify social pressure by linking rewards, progression, or status to continuous participation.

Particularly in games aimed at younger users, such mechanisms may create situations in which they feel obligated to remain active, contribute resources, recruit new users (such as classmates), or maintain their standing within a group. As a result, the associated risks emerge not only from the platform itself but also from the social structures and expectations generated among players.

5.3 Cross-Cutting Risks: Health and Wellbeing

The most prominent cross-cutting dimension identified in the analysis was related to health and wellbeing. According to the 4Cs framework, wellbeing risks may emerge across different online activities and are not restricted to a single risk category [17]. Several psychological and temporal patterns identified by participants were associated with this dimension. Examples include *Badges*, *Invested Value*, *Complete the Collection*, *Daily Rewards*, *Grinding*, *Infinite Treadmill*, *Playing by Appointment*, and *Can't Pause or Save*. Although these mechanics differ in implementation, they share a common characteristic: encouraging recurring participation and sustained engagement.

Daily reward systems encourage players to return frequently to avoid missing benefits. Appointment-based mechanics restrict access to specific activities to predefined periods, while infinite progression systems continuously generate new goals and objectives. Similarly, invested value mechanisms capitalize on the time, effort, and resources already dedicated to a game, making disengagement more difficult.

Our study does not claim that these mechanics directly cause harm. However, their design characteristics may contribute to experiences associated with prolonged engagement, habitual use, fear of missing out, and difficulties disconnecting from the game. Therefore, wellbeing-related risks emerged as a recurrent theme across multiple types of deceptive design.

5.4 Risk Categories Not Represented

None of the identified deceptive patterns were primarily associated with content risks or contact risks. Content risks typically involve exposure to harmful, inappropriate, violent, hateful, or sexual content. While some analyzed games may contain user-generated content or communication features, the deceptive patterns identified by participants were not related to content exposure. Instead, they were linked to engagement, monetization, and progression mechanisms.

Similarly, contact risks generally involve harmful interactions initiated by adults, such as grooming, unwanted communication, or predatory behavior. Although several of the analyzed games support interaction between players, none of the identified deceptive patterns were directly associated with adult-initiated contact risks.

We believe the absence of these two categories suggests that the risks posed by deceptive design in games may differ from those traditionally emphasized in online safety discussions. Rather than emerging primarily through content or contact, the risks identified in our study (despite its limited scope)

arise from the structural design of games that shape player behavior, spending decisions, and patterns of engagement.

6 FINAL CONSIDERATIONS

6.1 Discussion

The previous scenario reinforced the need to establish ethical practices for game development. Our study is part of a growing movement to explore deceptive design across various digital applications, including mobile apps [20], gambling platforms [18] and home robots [4]. Academic research and regulatory reports have focused on identifying and classifying these patterns, which is fundamental since digital vulnerability causes deceptive design to disproportionately affect several groups, particularly for children, making them more susceptible to risks and less resilient to related harms [16].

In this context, Brazil's Law No. 14,852, from May 2024, establishing the National Policy for Digital Rights of Children and Adolescents, aligns with the international landscape, the concerns raised in this study, and the protection of children's rights in digital environments. Even though Brazilian legislation is taking crucial steps in its development, there is a need to identify these patterns within games, where they apply differently than in social media. Phenomena like "cookie fatigue" also complicate effective consent management, for example. This law and other regulatory initiatives, including Brazil's Law 15.211/2025 (Digital Statute of Children and Adolescents - "ECA Digital" in Brazilian Portuguese), which focuses on the protection of children and adolescents in digital environments, offer a legal framework to combat deceptive and manipulative design that impair users' online autonomy and well-being. The "ECA Digital" explicitly addresses manipulative design features in digital environments, such as loot boxes in digital games (mechanisms often used to exploit users via randomized rewards without transparent odds). It also mandates default parental control features and implements purchase limits and alerts. Hence, it fosters greater transparency and fairness for young users.

This paper provides researchers and practitioners (in particular, regulators) with an analysis of how game companies and their platforms impact the protection of children online via deceptive and manipulative design. Our mapping, for example, demonstrates that deceptive design patterns in digital games are closely associated with commercial, social, and wellbeing-related risks. By applying the 4Cs framework, it became possible to move beyond the identification of individual mechanics and understand how these design choices may contribute to broader categories of online risk affecting children and adolescents.

6.2 Threats to Validity

A possible threat to **internal validity** concerns the evidence obtained from participants regarding deceptive design practices in games. Although the evaluators were adults, the selected games are widely popular among children and adolescents, who constitute the target population discussed in our study. Since participants were experienced users of these games,

they were able to provide informed assessments of the identified design practices. Regarding **conclusion validity**, there is a possibility of subjectivity in the identification and interpretation of deceptive patterns, as well as in the mapping of these patterns to children's online risks. To mitigate this threat, the analysis involved two researchers who independently examined the reported examples and subsequently discussed their interpretations. Any discrepancies were resolved via consensus, ensuring a more rigorous classification process.

Finally, participants consisted exclusively of university students, who may hold above-average digital literacy and familiarity with digital games, limiting the representativeness of the findings. Nevertheless, we highlight the qualitative nature of our investigation, when the goal was not to achieve statistical generalization but rather to obtain rich insights into the phenomenon of deceptive design by the digital game industry. Furthermore, the multidisciplinary nature of this study poses interpretative challenges. The absence of legal or psychological specialists on the research team represents a limitation that may affect the interpretation of children's online risks and the broader implications of deceptive design practices. To mitigate this threat, we grounded our analysis in established frameworks from the literature, particularly the 4Cs framework for children's online risks and documented taxonomies of deceptive design patterns.

6.3 Future Work

The upcoming studies will expand this investigation to other digital domains in which children are active users, particularly social robots and social media platforms. We also plan to enrich our analysis by tailoring the risk assessment to different software domains commonly used by children, including games, social robots, and smart toys.

Finally, we intend to discuss our findings with both practitioners, ranging from designers to representatives of game companies, and experts in children's digital rights and protection from organizations such as the Alana Institute (Brazil) and Fairplay (USA). Additional future activities include organizing workshops with parents and caregivers to discuss deceptive patterns in children's digital applications and promote digital literacy and parental mediation.

REFERENCES

- [1] Eman Alashwali and Fatimah Alashwali. 2022. Saudi parents' privacy concerns about their children's smart device applications. *International Journal of Child-Computer Interaction* 33 (2022), 100486.
- [2] UN General Assembly. 1989. Convention on the Rights of the Child. *United Nations, Treaty Series* 1577, 3 (1989), 1–23.
- [3] Pooria Babaei. 2024. *Drivers and Persuasive Strategies to Influence User Intention to Learn About Manipulative Design*. Ph.D. Dissertation. University of Saskatchewan Saskatoon.
- [4] Auxane Boch and Bethany Rhea Thomas. 2025. Human-robot dynamics: a psychological insight into the ethics of social robotics. *International Journal of Ethics and Systems* 41, 1 (2025), 101–141.
- [5] Harry Brignull. 2023. Deceptive patterns: Exposing the tricks tech companies use to control you. (*No Title*) (2023).
- [6] Ishita Chordia, Lena-Phuong Tran, Tala June Tayebi, Emily Parrish, Sheena Erete, Jason Yip, and Alexis Hiniker. 2023. Deceptive design patterns in safety technologies: A case study of the citizen

- app. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–18.
- [7] Tommaso Crepax and Jan Tobias Mühlberg. 2022. Upgrading the protection of children from manipulative and addictive strategies in online games: Legal and technical solutions beyond privacy regulation. *arXiv preprint arXiv:2207.09928* (2022).
 - [8] Daniela S Cruzes and Tore Dyba. 2011. Recommended steps for thematic synthesis in software engineering. In *2011 international symposium on empirical software engineering and measurement*. IEEE, 275–284.
 - [9] Jonathan F Geider. 2021. How to (not) exploit your internet child star: unregulated child labor on YouTube, Instagram and Social Media. (2021).
 - [10] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–14.
 - [11] JOHANNA GUNAWAN, AMOGH PRADEEP, DAVID CHOFFNES, WOODROW HARTZOG, and CHRISTO WILSON. 2021. A Comparative Study of Dark Paterns Across Mobile and Web Modalities. (2021). doi:10.1145/3479521
 - [12] Yujin Jang and Bomin Ko. 2023. Online safety for children and youth under the 4Cs framework—A focus on digital policies in Australia, Canada, and the UK. *Children* 10, 8 (2023), 1415.
 - [13] Dominique Kelly and Jacquelyn Burkell. 2023. Documenting privacy dark patterns: How social networking sites influence users' privacy choices. *FIMS Publications* (2023).
 - [14] Dominique Kelly and Victoria L Rubin. 2022. Dark pattern typology: How do social networking sites deter disabling of user accounts. In *The 12th International Conference on Social Media and Society*. EasyChair.
 - [15] Cherie Lacey and Catherine Caudwell. 2019. Cuteness as a 'dark pattern'in home robots. In *2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*. IEEE, 374–381.
 - [16] Mark Leiser and Cristiana Santos. 2023. Dark patterns, enforcement, and the emerging digital design acquis: Manipulation beneath the interface. (2023).
 - [17] Sonia Livingstone and Mariya Stoilova. 2021. The 4Cs: Classifying online risk to children. (2021).
 - [18] Gabriel Felipe Martins Magalhães. 2026. Casas de Aposta Online (BETS) e as Técnicas Persuasivas Dark Patterns, Dark Nudges e Sludge:: Uma Revisão de Escopo. *Conversas em Psicologia* 7, 1 (2026).
 - [19] Luca Marelli and Giuseppe Testa. 2018. Scrutinizing the EU general data protection regulation. *Science* 360, 6388 (2018), 496–498.
 - [20] Daniel Marques and Thiago Falcão. 2026. Design persuasivo e mediação tecnológica em plataformas digitais de apostas: práticas e dilemas éticos de designers e desenvolvedores. *Arcos Design* 19, 1 (2026).
 - [21] Sam Niknejad, Thomas Mildner, Nima Zargham, Susanne Putze, and Rainer Malaka. 2024. Level up or game over: Exploring how dark patterns shape mobile games. In *Proceedings of the International Conference on Mobile and Ubiquitous Multimedia*. 148–156.
 - [22] Didem Özkul, Steven Vosloo, and Bella Baghdasaryan. 2025. *Best interests of the child in relation to the digital environment*. UNICEF Innocenti–Office of Global Insight and Policy.
 - [23] Jenny Radesky, Alexis Hiniker, Caroline McLaren, Eliz Akgun, Alexandria Schaller, Heidi M Weeks, Scott Campbell, and Ashley N Gearhardt. 2022. Prevalence and characteristics of manipulative design in mobile applications used by children. *JAMA Network Open* 5, 6 (2022), e2217641–e2217641.
 - [24] Elisabeth Staksrud, Kjartan Ólafsson, and Sonia Livingstone. 2013. Does the use of social networking sites increase children's risk of harm? *Computers in human behavior* 29, 1 (2013), 40–50.
 - [25] José P. Zagal, Staffan Björk, and Chris Lewis. 2013. Dark Patterns in the Design of Games. In *Foundations of Digital Games 2013*.