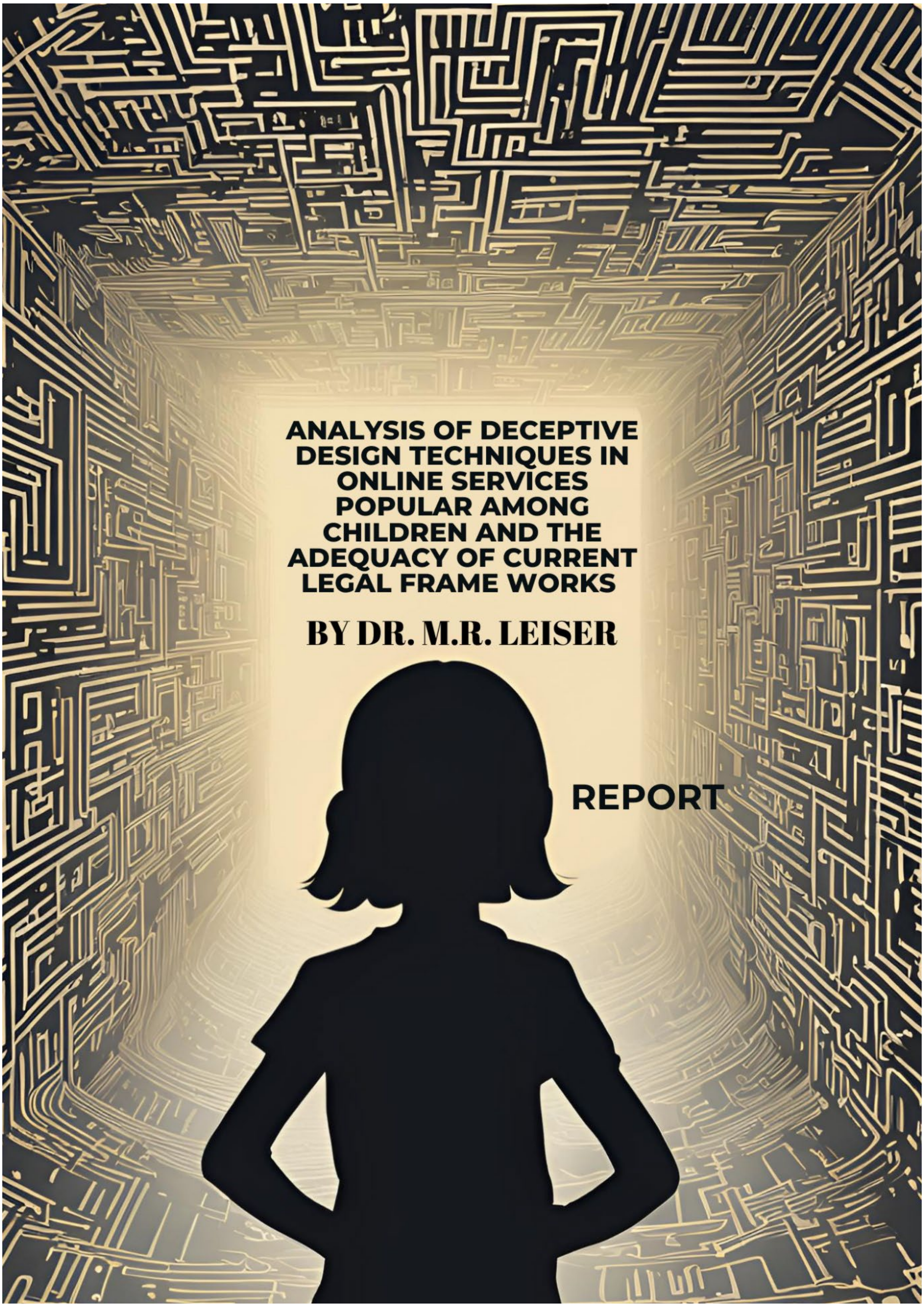


ANALYSIS OF DECEPTIVE DESIGN TECHNIQUES IN ONLINE SERVICES POPULAR AMONG CHILDREN AND THE ADEQUACY OF CURRENT LEGAL FRAME WORKS

BY DR. M.R. LEISER

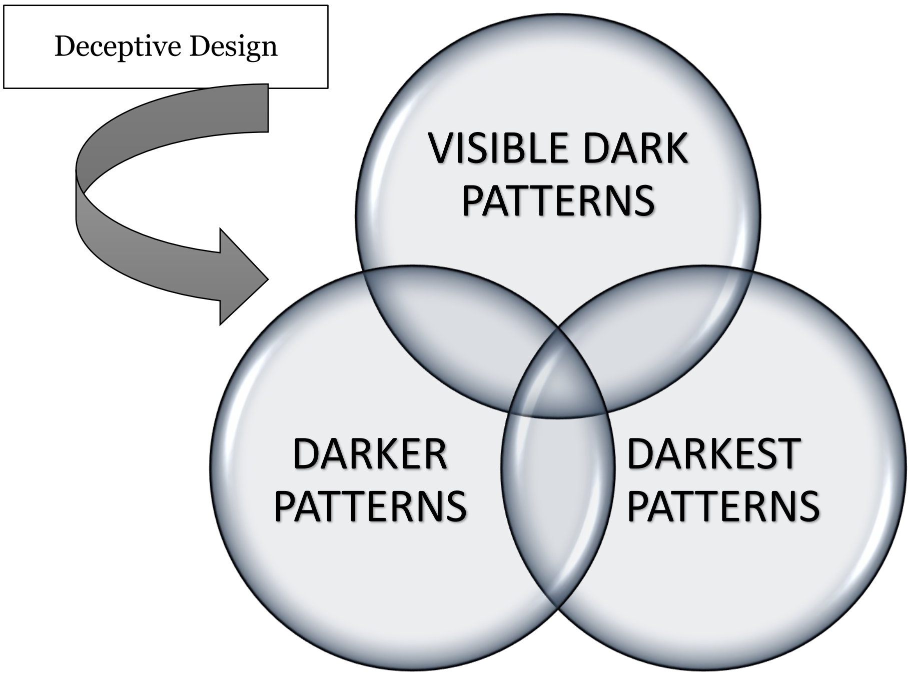
REPORT

List of Tables and Diagrams

DARK PATTERNS VS DECEPTIVE DESIGN TERMINOLOGY EXPLAINED

In 2010, Dr Harry Brignull coined the term **"Dark Patterns"** to describe a "*user interface that has been carefully crafted to trick users into doing things, such as buying overpriced insurance with their purchase or signing up for recurring bills*".[i] After registering darkpatterns.org, he created a "pattern library with the specific goal of naming and shaming deceptive user interfaces."[ii] **Based on Brignull's work on user interface designs, visible dark patterns** represent open and overt manipulative tactics that directly influence user decision-making. Thus, these patterns are quickly identified, such as when designers deliberately obscure or hide an unsubscribe button. In contrast, **darker patterns** are more subtle and elusive. These patterns employ persuasive design techniques to exploit user vulnerabilities or biases, leading to outcomes like hidden fees or misleading advertising. Users often realise the consequences of these patterns only after the fact. The **darkest patterns** involve more complex tactics.

Introductory Diagram #1: Terminology Visualised



They are either deterministic, relying on advanced coding or architecture to produce specific outcomes, or stochastic (non-deterministic), where the system behaves like a black box, and no one can explain precisely why it outputs specific results. These systems may produce different outputs for the same inputs, such as in machine learning or other statistical models. Unlike visible and darker patterns, these more intricate techniques do not lend themselves to straightforward interpretation from a flowchart. Deceptive design covers the full spectrum of manipulative tactics, from the easily identifiable to the deeply embedded and obscure. It includes visible, darker, and darkest patterns, illustrating how designers shape user experiences at various interface and system architecture levels. However, it is essential to note that not all deceptive design strategies fall under the legal definition of dark patterns, as regulated in frameworks like the GDPR and DSA. These legal frameworks focus on more visible and explicit manipulative techniques. Still, many other forms of deceptive design operate beyond these regulations, often embedded in complex algorithms or subtle user interfaces. This broader concept acknowledges that manipulative design is not limited to what users can immediately see or easily detect but extends to subtle psychological nudges and highly complex algorithmic mechanisms. Deceptive design operates across user interfaces, back-end architectures, and machine learning systems, systematically exploiting user vulnerabilities to achieve specific outcomes, often undermining transparency, autonomy, and fairness. By encompassing all these categories, deceptive design highlights the evolving nature of manipulative practices in digital environments. It underscores the urgent need for regulatory frameworks, ethical design principles, and technological scrutiny to protect user rights and prevent exploitation, particularly for vulnerable groups like children. Recognising deceptive design in its entirety enables a comprehensive approach to tackling manipulation in modern digital ecosystems.

EMPTY ON PURPOSE

EXECUTIVE SUMMARY

AI-driven systems rapidly shape the digital world by employing sophisticated techniques to manipulate user behaviour, particularly among vulnerable groups such as children. These systems offer remarkable capabilities in personalisation and decision-making, autonomously adapting to user data and behaviours in real-time. While this can improve user experience, it also gives rise to manipulative practices that exploit children's developmental vulnerabilities. This report addresses the growing concern around AI-driven deceptive design practices, highlighting their disproportionate impact on minors. It explores the adequacies of current regulatory frameworks such as the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA) and advocates for the introduction of a more comprehensive regulatory framework through the forthcoming Digital Fairness Act (DFA). However, the precise form of the DFA—whether it will be a patchwork addition to existing laws or a wholly new regulation- is still unknown. This report presents solutions that can be applied regardless of their final shape, ensuring robust protections for children in digital environments.

The Need for Enhanced Protection for Children

Children are uniquely vulnerable to digital manipulation due to their limited ability to assess online content critically and their heightened susceptibility to emotional cues. AI systems exploit these vulnerabilities by tailoring content, advertisements, and engagements to foster dependence and increase profitability. Techniques like dynamic personalisation, real-time behavioural nudging, and emotionally charged gamification can erode children's autonomy and privacy, often without their awareness. While valuable, the GDPR and DSA primarily focus on user consent and transparency, which fail to adequately address the deeper manipulations driven by AI, particularly those that operate beneath the surface of user interfaces. A new DFA could catalyse substantial regulatory change. However, the specific nature of this act remains uncertain. It may either build upon existing frameworks like the GDPR or introduce entirely new measures tailored to the challenges posed by modern AI systems. Regardless of its exact form, it must address the systemic manipulations embedded in AI algorithms, specifically those that exploit children's cognitive vulnerabilities. The need for reform is critical, particularly as technologies like Large Action Models (LAMs) continue to evolve.[iii]

Manipulative Design and Vulnerable Minors: Digital platforms exploit minors' cognitive vulnerabilities using AI-driven deceptive designs, such as engagement loops, gamification, and personalized nudges, to maximize engagement and profit.

Psychological and Ethical Concerns: These tactics undermine autonomy, mental health, and privacy, fostering dependency and exploiting developmental limitations like impulse control and social validation.

Regulatory Gaps in Existing Frameworks: Current laws, including the GDPR, UCPD, DSA and AI Act inadequately address system-level manipulations and AI-driven personalisation, relying too heavily on transparency and consent mechanisms unsuited for minors.

Opportunities for Reform: The Digital Fitness Check and the potential to legislate for digital fairness offer pathways to regulate manipulative designs with targeted measures like algorithmic audits, child-specific design mandates, and stricter AI limits.

Call for Adaptive Protections: Regulatory frameworks must evolve to proactively address emerging manipulative tactics, focusing on child-centred protections that balance innovation with ethical standards.

Current Regulations and the EU AI Act

While the EU has made significant strides in regulating AI through the EU AI Act, the framework's application to the unique challenges posed by AI-driven deceptive design remains a critical concern. Articles 5(1)(a) and (b) of the EU AI Act, which addresses psychological manipulation and harm to vulnerable groups, set very high thresholds for intervention. These high thresholds may limit the effectiveness of the regulation in providing adequate protection against the subtle, systemic manipulations enabled by AI. Specifically, AI systems like LAMs can influence users through complex, real-time adaptations based on a vast range of data points, making it difficult to demonstrate clear harm or manipulation under these criteria. The result is that the thresholds for intervention in the AI Act might be too high to address the nuanced, dynamic manipulations targeting minors, especially in personalised content and behavioural nudging. In addition, the rapid development of Large Action Models (LAMs) introduces a new layer of complexity. LAMs take manipulative practices to a previously unattainable level by integrating real-time decision-making with predictive analytics. These models predict user preferences and act autonomously on that data, influencing decisions through personalised prompts, urgency cues, and microtransactions that target users' emotional states. The opacity of these systems further complicates efforts to regulate them effectively, as the adaptive nature of LAMs makes them challenging to scrutinise or audit. A warning is necessary: the rapid rise of LAMs might outpace existing regulatory efforts, including the EU AI Act, presenting a significant challenge for regulators.

Key Recommendations for Reform

1. **Establish Child-Centred Design Standards**: Implement mandatory age-appropriate, ethical design standards for digital platforms that prioritise children's welfare over engagement metrics. These standards should address AI-driven personalisation and prohibit harmful design tactics, including countdown timers, loot boxes, and in-app purchase nudges.
2. **Introduce Mandatory Algorithmic Audits**: Platforms must regularly audit their AI algorithms to assess compliance with child protection standards. These audits should focus on identifying manipulative techniques and ensuring platforms are not exploiting children's vulnerabilities through AI-driven personalisation and nudging.
3. **Ban Harmful Manipulative Practices**: Prohibit the deployment of dynamic pricing, personalised urgency cues, and behavioural nudging that exploit cognitive biases and encourage addictive behaviours, particularly in children.
4. **Harmonise EU and National Frameworks**: Ensure the new regulations are harmonised across the EU, addressing the regulatory gaps left by current frameworks. This approach should establish consistent protection for minors and ensure that platforms operate under clear, child-centric standards.
5. **Foster Global Collaboration**: The EU should collaborate with international regulators to develop global standards for protecting children from deceptive digital design. This collaboration should be informed by lessons from jurisdictions like South Korea and Australia, adopting global best practices for a European context.
6. **Strengthen Enforcement Mechanisms**: Enhance enforcement measures to ensure compliance with new regulations. Regulators should be empowered to monitor, audit, and act against platforms that employ manipulative AI techniques. These measures should include developing tools to detect hidden manipulations within system architectures, often overlooked in traditional regulatory approaches.

Conclusion

The EU's regulatory frameworks must evolve to keep pace with the rapid advancements in AI, particularly concerning its use in exploiting children's vulnerabilities. There is a pressing need to close the regulatory gaps left by the GDPR, the UCPD, and the DSA, ensuring more robust protections for minors. Whether through amendments to existing laws or the introduction of new, targeted regulations, any reform must address the systemic manipulations enabled by AI systems such as LAMs, which present significant regulatory challenges. The high thresholds set by the EU AI Act, particularly in Articles 5(1)(a) and (b), may prove inadequate in the face of the complex, real-time manipulations that LAMs can perform. A comprehensive approach to AI regulation, incorporating the key recommendations in this report, would help ensure that digital environments remain safe, fair, and transparent for children, preventing the exploitation of vulnerable users through AI-powered deceptive design. However, as AI-driven manipulation becomes increasingly sophisticated, a fundamental question arises: can the EU's *Digital Design Acquis* (GDPR, ePrivacy Directive, UCPD, DSA, DMA, Data Act, and AI Act) effectively capture all forms of manipulation enabled by AI? Additionally, the limits of recognising children as consumers across the broad range of digital environments they engage with challenge the adequacy of current EU protections. The existing legal framework may struggle to provide sufficient safeguards in spaces where children are not consistently classified as consumers. How far policymakers can extend protections within these environments remains an open question that requires urgent attention.

CONTENTS

PROTECTING CHILDREN FROM DECEPTIVE DESIGN: AN INTERNATIONAL PERSPECTIVE

As the digital landscape evolves, protecting minors from economic exploitation remains a critical obligation under international frameworks such as the United Nations Convention on the Rights of the Child (UNCRC). Article 32 UNCRC explicitly calls on states to protect children from economic exploitation and hazardous work, while Article 17 emphasises safeguarding children from harmful material in the media. In digital environments, these obligations require proactive measures to mitigate deceptive design practices and ensure children's rights to well-being, autonomy, and informed decision-making. The UNCRC obligates signatories to take legislative, administrative, and other measures to protect children from exploitation, including economic manipulation. Dark patterns, manipulative consent banners, and gamified monetisation tactics directly contradict these principles in digital spaces. These practices exploit children's developmental vulnerabilities, such as their heightened impulsivity and limited ability to critically evaluate persuasive techniques critically, thus violating their rights to protection from economic exploitation.

In the United States, regulatory approaches to deceptive design targeting minors have been piecemeal. The Federal Trade Commission (FTC) has taken enforcement actions against companies employing dark patterns, particularly in cases involving children. For example, the FTC's settlement with Epic Games addressed deceptive practices in Fortnite, including exploitative monetisation mechanisms encouraging children to make unintended purchases. However, broader legislative efforts, such as the Kids Online Safety Act (KOSA), remain in development and face significant political hurdles. Moreover, the Children's Online Privacy Protection Act (COPPA) aims to protect children under 13 by requiring verifiable parental consent before collecting their data. While COPPA provides a foundation for protecting minors, it does not adequately address dark patterns that exploit children's attention or incentivise excessive spending.

The EU has taken a more systemic approach to addressing deceptive design through broader regulatory frameworks like the GDPR and the DSA. The GDPR emphasises fairness and transparency in data practices, indirectly targeting dark patterns by requiring transparent and informed consent mechanisms. The DSA builds on these principles by imposing accountability measures for platforms accessible to minors. The EU also recognises the unique vulnerabilities of children in its Audiovisual Media Services Directive, which prohibits commercial practices that directly exploit children's inexperience or credulity. However, enforcement challenges remain, particularly in ensuring compliance across member states and addressing less visible manipulative techniques embedded in system architectures. South Korea has emerged as a leader in addressing manipulative design in gaming, a sector that disproportionately targets minors. The Game Rating and Administration Committee enforces strict limits on practices like loot boxes, mandating clear disclosures of probability rates to prevent exploitative monetisation. These measures reflect a broader commitment to protecting children from addictive and financially manipulative game mechanics. Australia has adopted a consumer protection lens to tackle deceptive design. The Australian Competition and Consumer Commission (ACCC) has actively pursued cases involving dark patterns, emphasising transparency and fairness in digital interactions. While not child-specific, the ACCC's focus on manipulative practices in digital platforms has led to increased scrutiny of features like gamified consent mechanisms and algorithmic nudges that disproportionately impact minors.

While global efforts to regulate deceptive design provide critical insights, their successful adaptation requires understanding jurisdictional constraints, regulatory capacity, and cultural attitudes toward digital consumer protection. The political will to enforce child-specific protections varies widely; for instance, while the EU has pursued systemic regulatory approaches, enforcement remains uneven across Member States due to national priorities and resources. Similarly, while South Korea has implemented strict gaming regulations, this approach may face resistance in markets where commercial interests, such as the United States, wield significant influence over digital policy. Additionally, cultural attitudes toward digital autonomy and parental responsibility play a role in shaping regulatory responses; for example, Australia's consumer protection approach focuses on transparency and fairness, whereas the U.S. regulatory model emphasises parental consent under COPPA, placing the burden on guardians rather than digital service providers. To create compelling and enforceable standards, regulators must consider these structural differences, ensuring that protective measures are robust and adaptable to each jurisdiction's sociopolitical and economic conditions. Several key lessons emerge from global efforts to address deceptive design targeting minors:

1. **Transparency Requirements**: South Korea's strict disclosure mandates for gaming mechanics provide a model for ensuring children and their guardians have the information needed to make informed decisions.

2. **Harmonized Enforcement**: The EU's systemic frameworks highlight the importance of harmonising regulations to prevent cross-border exploitation, though stronger enforcement mechanisms are needed.
3. **Child-Specific Protections**: The U.S., COPPA, and Australian consumer protection initiatives underscore the need for targeted measures to address the unique vulnerabilities of minors.
4. **Proactive Oversight**: International efforts reveal the value of proactive regulatory oversight, as demonstrated by South Korea's gaming regulations, which directly pre-empt exploitative practices rather than relying solely on after-the-fact enforcement.
5. **Context-Sensitive Implementation:** While regulatory models such as South Korea's gaming restrictions and the EU's harmonised frameworks offer valuable blueprints, successful implementation depends on adapting these measures to different political, legal, and cultural contexts. For example, enforcement strategies must account for the decentralised regulatory structures in the US, the jurisdictional complexities within the EU, and varying levels of institutional capacity across global markets.

Operationalising a Unified Framework

Given the inherently cross-border nature of digital platforms, ensuring effective protections for minors against deceptive design requires coordinated international enforcement mechanisms. One approach is the development of a global registry of deceptive design practices, a shared database maintained by a coalition of consumer protection agencies, regulators, and civil society organisations. Some private initiatives already exist, such as the deceptive.design enforcement database, which tracks regulatory actions against manipulative digital practices, and research-driven projects like Fair Patterns, which use neuroscience and behavioural insights to assess how design influences decision-making—these efforts remain fragmented. Additionally, Bright Patterns exemplifies an emerging counter-movement that nudges users toward better, more autonomous decision-making rather than exploiting cognitive biases. A unified, publicly accessible registry could integrate these insights, serving as a repository of known manipulative techniques—such as coercive consent flows, algorithmic reinforcement loops, and exploitative monetisation strategies—allowing regulators to track emerging trends and identify repeat offenders. Such a system would enhance regulatory agility by enabling real-time data sharing, allowing authorities to act pre-emptively rather than relying solely on post-hoc enforcement. Furthermore, a global registry would provide a valuable resource for industry actors seeking to comply with best practices, ensuring that platform design aligns with internationally recognised standards of fairness and transparency.

To complement such a registry, cross-border enforcement agreements should be established to facilitate coordinated action against deceptive design practices that impact minors across multiple jurisdictions. Existing frameworks such as the Consumer Protection Cooperation (CPC) Network in the EU or the International Consumer Protection and Enforcement Network (ICPEN) could serve as models for broader international cooperation. These agreements should include provisions for joint investigations, mutual recognition of enforcement actions, and streamlined complaint mechanisms that allow affected users—particularly children and their guardians—to report violations across jurisdictions. By integrating enforcement mechanisms across regulatory bodies, policymakers can prevent platforms from exploiting jurisdictional loopholes, ensuring that digital protections remain robust and enforceable regardless of where a company is headquartered. Such cooperation would enhance regulatory effectiveness and signal a global commitment to upholding children's rights.

METHODOLOGY

This research takes a multidisciplinary approach to address the evolving challenges of deceptive design practices targeting minors. By integrating perspectives from law, cognitive science, behavioural psychology, and technology studies, the study examines how manipulative design operates across user interfaces, system architectures, and AI-driven platforms. The research aims to provide evidence-based recommendations for improving child-centric regulatory frameworks within the European Union (EU) and beyond.

Research Objectives and Scope

The study aims to:

1. Develop a comprehensive taxonomy of deceptive design practices, distinguishing between visible manipulations, subtle persuasive techniques, and sophisticated AI-driven tactics.

2. Assess these practices' psychological, emotional, and developmental impacts on minors.

3. Evaluate the adequacy of existing Dutch and EU legal frameworks in addressing deceptive design and propose actionable reforms to strengthen child protection.

Methodological Framework

The methodology employs three core analytical approaches:

1. Data Collection and Case Study Analysis

- **Data Sources**: The study relies on a systematic review of primary and secondary sources, including:
    - Regulatory texts include the General Data Protection Regulation (GDPR), Digital Services Act (DSA), and AI Act.
    - Academic literature on manipulative design, child psychology, digital ethics and regulation.
    - Platform-specific case studies that focus on systems frequently used by minors.
- **Case Study Selection Criteria**: The study selects platforms based on their prevalence among minors and documented use of manipulative tactics. Key examples include:
    - **Gaming environments**: Exploring loot boxes and randomised rewards.
    - **Social media platforms**: Analysing infinite scrolling and personalised recommendations.
    - **Short-form video platforms**: Investigating AI-driven nudges and emotional triggers.
- **Analysis Approach**: The research examines each case study to identify the mechanisms of manipulation, their impact on user behaviour, and gaps in regulatory oversight.

2. Comparative Legal and Policy Analysis

- **Framework Evaluation**: The study critically evaluates the effectiveness of Dutch and EU regulations in addressing manipulative design practices. The analysis focuses on:
    - Examining GDPR's emphasis on transparency and consent and identifying its limitations in addressing system-level manipulations.
    - Assessing the DSA's provisions on systemic risk assessments and the role of algorithmic audits in ensuring compliance.
- **Best Practices**: The study incorporates international regulatory benchmarks to identify effective strategies for addressing deceptive design.

3. Interdisciplinary Integration

- **Developmental Psychology and Behavioural Science**: The study uses insights from these fields to understand minors' cognitive vulnerabilities, such as impulsivity, sensitivity to social validation, and limited comprehension of digital systems.

- **Technology Studies**: The study analyses how AI and machine learning amplify manipulative tactics, focusing on the ethical implications of algorithmic opacity and non-deterministic outcomes.

Assumptions and Constraints

The research operates under the following assumptions:

1. Minors are particularly vulnerable to manipulative design due to developmental immaturity.

2. Existing regulatory frameworks must evolve beyond transparency and consent models to effectively address system-level manipulations.

3. AI-driven techniques require targeted interventions to mitigate their impact on vulnerable groups.

Key constraints include:

- The reliance on case studies may not fully capture algorithmic manipulations' dynamic and opaque nature.

- The challenge of accounting for jurisdictional differences within a unified EU framework.

Expected Contributions

The research aims to:

1. Propose a robust regulatory framework that prioritises child-centred protections based on fairness-by-design principles.

2. Bridge gaps between legal, cognitive, and technological disciplines to provide a holistic understanding of deceptive design practices.

3. Inform Dutch and EU policymakers about actionable reforms to harmonise child protection standards and enforce compliance with ethical digital design practices.

This refined methodology articulates the research methods clearly and focuses on delivering practical insights for addressing the systemic and nuanced challenges of deceptive design.

SECTION 1: INTRODUCTION

1.1 PURPOSE, SCOPE, AND OBJECTIVES

In the evolving digital landscape, digital platforms increasingly expose children and adolescents to sophisticated design techniques that subtly manipulate user behaviour.[iv] These platforms, including social media, gaming environments, and streaming services, are designed for engagement and to increase profitability. However, the strategies employed to achieve these aims often exploit minors' developmental vulnerabilities, making children particularly susceptible to manipulative tactics that steer their choices and impact their well-being. Known as “dark patterns" and “deceptive design,” these carefully crafted techniques are designed to influence user behaviour in ways that benefit the platform, often at the expense of the user's autonomy and agency.[v] Such tactics pose unique risks for young users who lack the cognitive maturity to identify or resist these manipulations, underscoring the need for robust regulatory measures specifically designed to protect minors in digital spaces.

Purpose, Scope, and Objectives

Minors are increasingly exposed to manipulative design techniques in digital platforms.

AI and machine learning enhance these manipulations, exploiting children’s cognitive vulnerabilities.

Current regulatory frameworks (GDPR, DSA, AI Act, EU Consumer Law (Primarily, the UCPD) inadequately address manipulative system-level tactics.

The mechanisms underlying deceptive design have become increasingly sophisticated with the integration of artificial intelligence (AI) and machine learning. Platforms can construct highly individualised profiles by analysing user data, predicting responses, and tailoring interactions to maximise engagement.[vi] Such AI-enhanced tactics leverage vast datasets to create an environment where design choices—such as gamified notifications, reward systems, or nudges highlighting specific actions—are personalised to influence young users' behaviours.[vii] For instance, a platform may gamify interactions by offering points or rewards for repetitive engagement, encouraging minors to return to the platform frequently[viii], often leading to dependency or even addiction. Similarly, AI-driven content recommendations and targeted advertisements guide minors towards certain content or products based on data collected from their online behaviour.[ix] This process creates a feedback loop reinforcing certain. Behaviours gradually shape young users' choices without full awareness or consent.

The impact of these techniques on children's mental health, autonomy, and privacy is particularly concerning.[x] Unlike adults, minors are in crucial cognitive and social development stages and are less equipped to understand or manage the psychological effects of these engagements. The fear of missing out (FOMO) or peer comparisons are often embedded in these platforms, exacerbating social pressures and influencing children's sense of identity and self-worth.[xi] Furthermore, collecting personal data—often for profiling and behaviour prediction—raises serious privacy concerns. Children's lack of comprehension about data sharing and how companies influence their decisions raises ethical issues about informed consent and autonomy, which are fundamental to child rights in digital contexts.[xii]

> *“Deceptive design techniques exploit minors' developmental vulnerabilities, steering their choices and eroding autonomy”*

The EU has made significant progress in acknowledging and addressing the risks posed by manipulative digital practices through legislative measures such as the GDPR[xiii] and the DSA[xiv]. The GDPR, for example, established a foundational framework for data protection and user consent, providing essential safeguards for privacy. Similarly, the DSA introduced transparency obligations and systemic risk assessments, marking a significant step toward holding platforms accountable for harmful digital practices. However, these frameworks exhibit critical limitations in regulating manipulative tactics embedded within system architectures or algorithms, which often operate beyond the reach of transparency and consent-based measures. The European Commission has announced its intention to propose a Digital Fairness Act (DFA)[xv] to tackle unethical techniques and commercial practices, such as dark patterns, marketing by social media influencers, the addictive design of digital products, and online profiling, mainly when businesses exploit consumer vulnerabilities for commercial purposes. However, it is essential to note that the Commission has not yet put forward this legislation. The drafting of the DFA has not yet started, and its future form remains uncertain. Addressing covert manipulations, especially those targeting minors, will require regulatory approaches that go beyond surface-level interventions.

Additionally, the AI Act includes provisions such as Article 5(1)(b), which aims to prevent the psychological manipulation of vulnerable groups, including children. While this provision represents a promising step, its application remains constrained by high evidentiary thresholds and a lack of specificity regarding children's unique vulnerabilities in digital environments. A more unified and forward-looking regulatory approach is required to address these gaps effectively. Such an approach should combine existing frameworks' strengths while directly targeting system-level manipulations that disproportionately impact minors. The EU must prioritise a comprehensive strategy to ensure robust protection for vulnerable users in digital spaces, whether through the eventual DFA or targeted amendments to existing legislation.

The problem, therefore, is twofold: sophisticated, manipulative digital environments increasingly target children while existing regulatory frameworks need help to provide the necessary protections. Currently, most regulations focus on transparency and consent, which may fail to address the deeper issues regarding AI-enhanced manipulative design. For example, the GDPR's emphasis on informed consent is less effective when users are children who may need help understanding it.

The challenge is multifaceted: increasingly sophisticated digital environments target children with manipulative practices while existing regulatory frameworks face significant limitations in providing adequate protection. While the GDPR, DSA, consumer protection directives, and the AI Act collectively address a broad spectrum of regulatory concerns, their applicability to covert, adaptive manipulative design remains incomplete. The GDPR, for instance, establishes robust principles of data protection, fairness, and accountability, emphasising informed consent and transparency. These provisions are critical but often insufficient in the context of children, who may lack the capacity to understand the implications of their consent. Similarly, transparency obligations, while essential, do not inherently dissuade platforms from deploying sophisticated AI-driven tactics that operate beyond the immediate visibility of users or regulators. Such practices dynamically adapt to individual behaviours, creating a significant enforcement challenge.

The DSA builds on the GDPR by introducing systemic risk assessments, mandatory algorithmic audits, and accountability mechanisms for online platforms. However, its focus on transparency and interface-level manipulations does not extend to system-level manipulations embedded within algorithms or platform architecture. The limitations of the DSA's definition of online platforms make these gaps especially evident in environments such as standalone apps, smart toys, and educational tools, which are increasingly part of children's digital experiences.

Consumer protection legislation, such as the UCPD, provides additional safeguards by prohibiting misleading and aggressive practices. However, its focus on overt commercial tactics leaves subtle, algorithmic manipulations—such as urgency prompts or dynamic pricing—largely unregulated. Similarly, while the AI Act's Article 5(1)(b) addresses the exploitation of vulnerabilities, its high evidentiary thresholds and limited specificity regarding children's unique needs constrain its applicability.

Collectively, these frameworks address far more than transparency and consent alone. However, their limitations in confronting AI-enhanced manipulative practices' covert and adaptive nature underscore the need for targeted reforms. Policymakers must address these gaps by bolstering existing legislation and ensuring a coordinated and comprehensive approach that reflects the evolving risks children face in digital spaces. [xvi] Such tactics are particularly problematic in AI-driven design choices that dynamically adapt to individual users' behaviours, making it challenging for regulators to establish clear accountability for manipulative outcomes.

In response to these challenges, this research critically examines how deceptive design techniques operate within Dutch and EU regulatory frameworks, focusing on identifying regulatory gaps and proposing comprehensive measures to protect minors. The primary objective is to assess the effectiveness of existing EU laws, such as the GDPR, DSA, and AI Act, and determine how these frameworks can adopt more robust measures to address manipulative techniques comprehensively. Where existing frameworks prove insufficient, complementary measures, such as those potentially introduced through the proposed DFA, could be envisaged to close the regulatory gaps. This analysis will evaluate the systemic nature of deceptive design, recognising that manipulative practices often extend beyond visible user interfaces to the underlying system architectures that shape user experiences. Key areas of improvement include stricter rules on data use for personalisation, enhanced restrictions on AI-driven content recommendations that exploit minors' vulnerabilities, and more robust oversight of engagement-boosting features such as reward systems and notification loops. By focusing on these issues, the research aims to propose a balanced approach that strengthens protections for children while fostering a digital ecosystem that aligns with EU values of fairness, transparency, and accountability.

Building on the foundational work of the European Commission's Digital Fitness Check on Consumer Law and other legislative initiatives, this study recognises the need for regulatory frameworks to evolve in tandem with technological advancements. The research will assess whether existing enforcement mechanisms in the Netherlands are sufficient to counteract manipulative designs effectively or require recalibration to address the systemic risks posed by AI-enhanced deceptive design techniques. Ultimately, the study will provide actionable policy recommendations that bridge existing gaps and deliver meaningful protections for minors in a rapidly changing digital landscape.

Creating a comprehensive regulatory framework that addresses the specific vulnerabilities of minors is of utmost importance. Children are less equipped to identify manipulative tactics and more likely to be influenced by social pressures and the persuasive design elements embedded within digital platforms. Therefore, this research will adopt a child-centred approach, acknowledging how digital manipulation can impact young users' decision-making, privacy, and well-being. By aligning with recent legislative reforms, the research will provide a framework to anticipate better and mitigate the evolving risks posed by AI and machine learning in digital spaces. Accordingly, this research seeks to bridge the gap between the current regulatory landscape and the sophisticated, often subtle, manipulative techniques employed by digital platforms targeting minors. Through a detailed analysis of deceptive design techniques and their implications within the Dutch and EU regulatory contexts, this study will propose recommendations that underscore the importance of adaptive, enforceable protections for young users. Doing so aims to contribute to a safer, fairer digital landscape for minors, ultimately fostering an environment where digital platforms prioritise ethical standards over engagement metrics and profit.

1.2 RATIONALE AND RESEARCH SIGNIFICANCE

The digital landscape has become an intrinsic part of children's lives, shaping their daily interactions, entertainment, and learning experiences. As these platforms become increasingly sophisticated, they often employ design techniques to attract and retain user engagement through persuasive, algorithmically driven tactics. While the benefits of technology for education and socialisation are clear, the intentional use of design choices that exploit minors' cognitive and emotional vulnerabilities raises significant ethical and legal concerns. This study emerges in response to these pressing issues, as digital manipulative practices—often termed deceptive design or "dark patterns"—are particularly effective on minors who lack the cognitive maturity to identify or resist these strategies. This research examines these manipulative strategies' impact on young users, who are particularly vulnerable due to their limited ability to understand and resist digital manipulation.

Rationale and Research Significance

Minors lack the cognitive maturity to recognise manipulative design.

Existing EU legislation, while progressive, fails to target nuanced AI-enhanced manipulative practices.

GDPR's reliance on consent and transparency is ineffective for protecting children.

Rapid advancements in AI and machine learning have enabled a new class of personalised and responsive engagement tactics that dynamically adapt to each user, creating carefully tuned experiences to influence behaviour. For minors, this presents a unique challenge: they are less likely to recognise subtle manipulative cues, such as fear-of-missing-out (FOMO) prompts, social validation nudges, or gamified reward systems. Additionally, the data-driven nature of these techniques often implicates children's privacy rights, as personal data is continually collected and analysed to optimise platform interactions. This interplay of user engagement, data privacy, and child protection has become a focal point for digital rights advocates and regulatory bodies alike, particularly within the EU.

> *"Minors lack the cognitive tools to identify or resist manipulative digital practices, raising significant ethical concerns."*

The urgency of addressing these challenges has spurred legislative action within the EU, including the introduction of the GDPR, which focuses on user consent and data protection, and the DSA, which enhances transparency and accountability requirements for platforms. However, gaps remain in ensuring fairness in digital design practices, necessitating further regulatory developments to address emerging risks in the digital environment. However, while these laws lay the necessary groundwork, they often need more specificity to address the ways AI and machine learning can amplify manipulative design effects, especially when targeting minors. Article 5(1)(b) of the AI Act, for example, prohibits the psychological manipulation of vulnerable groups. Nevertheless, it does not go far enough to address the nuanced ways in which digital platforms leverage AI to create addictive or coercive experiences for children. Therefore, this research aims to build upon these legislative developments by exploring the cognitive and developmental risks posed by AI-driven manipulative design techniques, focusing on identifying regulatory gaps and proposing child-centred reforms.

The GDPR has become a foundational regulation in data protection and user rights, setting a global standard for consent and transparency. Nevertheless, its reliance on informed consent as a mechanism for safeguarding users is less effective for children, who may need help understanding the implications of consent or the complexities of data sharing. For instance, platforms often use language that obscures the extent of data processing, limiting minors' ability to make fully informed decisions. The challenge intensifies as many design choices, though technically compliant with GDPR standards, still exploit cognitive biases through complex opt-out processes, default settings that favour data collection, and strategically placed nudges to encourage tracking or sharing practices.[xvii] Thus, while GDPR addresses privacy rights, it does not adequately address the subtle, behaviour-influencing tactics that AI makes possible, creating a gap in protective measures for minors.

The DSA represents another significant step forward, aiming to bring transparency to large platforms' operations and set accountability standards. However, because it primarily focuses on illegal content, misinformation, and systemic risks, it does not directly address manipulative design strategies.[xviii] This focus creates a regulatory vacuum where deceptive design targeting young users remains legally permissible if it does not involve overtly harmful content or misinformation. The AI Act attempts to address some of these concerns by targeting practices that psychologically manipulate vulnerable groups, including children. Nevertheless, its scope and enforcement mechanisms need more specificity to cover nuanced, system-level manipulations embedded within AI architectures.

For instance, regulations do not explicitly prohibit AI-enabled engagement tactics that create compulsive usage loops, allowing platforms to exploit minors' attention spans and developmental vulnerabilities without meaningful consequences. In this regulatory context, the new DFA emerges as a promising instrument with the potential to directly address manipulative design by establishing more precise standards for fairness and transparency in digital interfaces. However, the law must incorporate adaptive, child-specific protections to be genuinely effective. For example, while prohibitions on FOMO-driven prompts, gamified notifications, or personalised nudges would be beneficial, they must be part of a broader regulatory strategy that limits how AI can influence minors' behaviour opaquely. This research will contribute to shaping the regulatory understanding by highlighting the specific design techniques that disproportionately affect young users and suggesting enforcement mechanisms to ensure compliance.

Protective legislation is essential due to the significant long-term impacts of manipulative design on children's cognitive development, mental health, and autonomy. Digital environments that repeatedly trigger reward-seeking behaviour can shape minors' neural pathways, conditioning them to seek validation from digital interactions and diminishing impulse control.[xix] These patterns may result in heightened screen dependency, reduced personal agency, and difficulties forming balanced relationships with technology. The risks extend beyond behavioural concerns to include substantial privacy issues. Platforms often collect and process minors' data to enhance engagement, steering choices, predicting preferences, and delivering targeted advertising. While the GDPR offers foundational protections, such as its emphasis on consent, its broad language and reliance on transparency mechanisms may not adequately mitigate risks inherent in platforms designed to maximise data extraction and user engagement. This research critically examines whether existing frameworks sufficiently protect children or leave them vulnerable to AI-driven manipulative practices and data exploitation. This research responds to the pressing need for stronger child-specific protections within EU digital regulations, recognising the profound risks posed by AI-driven manipulative design. A nuanced understanding of how these techniques impact minors is essential, as they often operate beneath the surface of user interfaces, dynamically adjusting to exploit individual preferences and vulnerabilities. By examining the intersection of cognitive science, data privacy, and regulatory theory, this study aims to evaluate the effectiveness of current frameworks and determine whether they adequately address these risks or require significant enhancements.

The analysis will investigate how behavioural psychology and developmental neuroscience principles can inform regulatory strategies, particularly in anticipating and mitigating the influence of AI on young users. Evidence-based recommendations will ensure that designers create digital environments frequented by children to prioritise their well-being, autonomy, and privacy rather than exploiting their developmental vulnerabilities. This comprehensive approach seeks to provide a robust foundation for advancing child-centred protections in the evolving digital landscape.

Ultimately, this research seeks to guide EU and Dutch regulators by identifying shortcomings in existing frameworks and offering precise recommendations for a more dynamic, child-focused approach to digital regulation. While recognising the foundational value of existing measures such as the GDPR, DSA, and UCPD, this study underscores that their scope and enforcement often fall short of addressing the covert, systemic nature of AI-driven manipulative practices targeting minors. These gaps demand not only incremental improvements but also a more nuanced approach to regulation, which reflects the complexities of modern digital environments and the specific vulnerabilities of young users. By drawing on the principles outlined in the Digital Fitness Check on Consumer Law, this study advocates for an evolved regulatory approach that accounts for the limitations of existing frameworks. Although transparency and consent mechanisms remain vital consumer protection components, their application alone does not sufficiently counteract the sophisticated behavioural tactics embedded in system architecture and algorithmic decision-making. The research will demonstrate how adaptive protections, aligned with cognitive science and developmental psychology insights, can address these gaps more effectively, providing protection that anticipates rather than reacts to manipulative practices. The findings will also emphasise the necessity of continuous regulatory monitoring to remain responsive to emerging manipulative techniques enabled by AI and machine learning advancements. This approach aims to close the gap between theoretical protections codified in existing legislation and the practical safeguards necessary to ensure the well-being of minors. This research contributes to a regulatory vision that balances technological innovation with a resolute commitment to ethical standards and child protection by addressing the interaction between AI-driven design strategies and children's cognitive development. It aspires to foster a safer, more equitable digital environment that prioritises minors as users and individuals whose rights and development take precedence.

1.3 AI-ENHANCED MANIPULATION OF CHILDREN

AI-driven "engagement loops" exploit children's cognitive vulnerabilities.

Gamification reinforces addictive behaviours through rewards and social validation.

Continuous AI adaptations erode minors' Autonomy.

AI has revolutionised the digital landscape, enabling highly personalised experiences that can captivate and retain users in unprecedented ways. While offering numerous benefits, this technological advancement also introduces complex ethical and regulatory challenges, mainly when applied to minors. AI's ability to personalise content, predict behaviours, and adapt interfaces in real-time has led to the development of intricate manipulative tactics, such as gamification and personalised engagement loops, which can significantly influence young users.[xx] Unlike traditional design techniques, which often rely on generic or one-size-fits-all approaches, AI-fuelled manipulations operate dynamically and individually, rendering them incredibly potent and potentially harmful for minors, who are less equipped to recognise and resist these tactics. At the heart of AI-enabled manipulative design lies the creation of "engagement loops." These loops are feedback-driven systems that encourage repetitive user behaviours by continually adapting to individual responses. Rossi et al. discuss the micro, meso, and macro vulnerability factors in digital settings, mainly focusing on how AI systems exploit data to personalise user experiences.[xxi] Persuasive design strategies, including reward loops and nudging enabled by big data, have been highlighted as significant concerns in digital environments.[xxii]

AI algorithms can observe and learn from users' online behaviour through complex data processing, identifying patterns, preferences, and vulnerabilities. Platforms then use this data to predict the types of content, notifications, or incentives most likely to elicit continued interaction. For minors, such adaptive mechanisms can lead to significant behavioural impacts.[xxiii] Tailored notifications or gamified rewards often draw children into cycles of repetitive engagement that exploit cognitive tendencies like reward-seeking behaviour, fear of missing out (FOMO), and social validation.[xxiv] AI's role in shaping these interactions thus extends beyond mere content recommendation to create a deeply personalised, responsive environment engineered to maximise engagement.[xxv]

Gamification is a prevalent AI-driven manipulative tactic. By embedding gaming elements, such as point scoring, rewards, and social competition, into non-gaming environments, platforms can tap into minors' inherent desire for achievement and social belonging. For instance, AI may assess a child's response to specific rewards, adjusting subsequent challenges or notifications to maintain engagement that sustains interest. These gamified systems, powered by real-time data analysis, operate on an understanding of minors' developmental stages, often exaggerating emotional responses.[xxvi] The resulting cycles of achievement, gratification, and social reinforcement can trap young users in prolonged engagement, with some platforms strategically exploiting these cognitive vulnerabilities to foster dependency. For young users, who may struggle with impulse control and are particularly susceptible to peer influence, such gamified loops become challenging to disengage from, raising concerns about their effects on mental health, self-regulation, and autonomy.

AI's capacity for dynamic adaptation amplifies the efficacy of these personalised engagement loops. Unlike static or predetermined user experiences, AI-driven systems continuously evolve in response to user behaviour, creating an environment where the experience is never truly complete. This "infinite scroll" effect, fuelled by algorithms that predict optimal engagement points, leads minors into a seemingly endless interaction. AI can modify interfaces in real-time by analysing individual engagement patterns, such as response times, content preferences, and usage frequency, to align with each user's vulnerabilities. For example, a platform may increase the frequency of notifications if it detects a minor's tendency to respond to social prompts, creating a tailored feedback loop that heightens perceived social pressures or stimulates compulsive usage. The personalised nature of these loops ensures that the platform experience feels intuitive. Nevertheless, it subtly erodes the user's agency, directing behaviour in ways that are difficult to detect or resist, particularly for minors who lack the cognitive maturity to question these nudges.

The ethical concerns arising from these tactics are profound, as they exploit the developmental vulnerabilities of young users in ways that transcend traditional advertising or persuasive design. AI-fuelled manipulations create environments that encourage prolonged engagement, often leading to dependency or unhealthy attachment to digital platforms. For minors in critical stages of cognitive and emotional development, the potential impacts of these interactions are deeply concerning. Without adequate regulation, AI-driven manipulative tactics represent a unique and evolving challenge to protecting young users, calling for a robust, adaptive regulatory framework that can anticipate and mitigate the long-term effects of personalised engagement strategies on minors.

1.4 EXTENDING THE DIGITAL FITNESS CHECK: UNCOVERING DECEPTIVE DESIGN'S EFFECTS ON MINORS

This research builds upon the foundational work of the European Commission's Digital Fitness Check on Consumer Law by concentrating specifically on minors, a uniquely vulnerable group within the digital economy. While the Digital Fitness Check assessed the adequacy of current consumer protection laws and identified gaps in a technologically advancing landscape, it addressed consumer protections in general terms. Focusing on the risks minors face from manipulative digital practices, this study addresses an essential dimension not fully explored in the original Fitness Check, offering targeted insights into how AI-driven systems can impact young users.

One of the core contributions of this research lies in its detailed analysis of how AI and machine learning (ML) intensify the effects of deceptive design on minors. AI and ML are not simply tools that enhance user experience but have evolved into complex systems that can predict and influence user behaviour. These adaptive systems present unique challenges for minors in crucial cognitive and social development stages. Unlike adults, minors have far fewer tools to recognise or resist manipulative design elements, leaving them particularly susceptible to features like fear-of-missing-out prompts or personalised nudges that encourage prolonged engagement. By examining these adaptive design tactics in-depth, this research contributes to a more nuanced understanding of the ethical and regulatory issues that arise when such technologies interact with minors' cognitive limitations.

An essential aspect of this study is its empirical approach, which provides concrete, data-driven insights into how manipulative digital practices operate on platforms commonly used by children and adolescents. This research catalogues various deceptive design tactics and assesses their impact on young users by drawing on real-world examples and case studies from digital platforms. Through this systematic approach, the study builds an evidence base beyond theoretical analysis, shedding light on how AI-driven systems manipulate young users' behaviours. These findings not only substantiate the need for stricter regulations but also highlight gaps in existing frameworks that currently fail to address the unique risks minors face in digital spaces.

"The DFA offers a promising pathway for regulating manipulative AI-driven tactics targeting minors."

This study's comparative aspect further enhances its contributions, examining how digital manipulative practices affect minors in the Netherlands and across broader European regulatory contexts.

"Harmonised EU policies can bridge gaps in child protection standards."

By analysing national and EU-level regulatory frameworks, this research identifies disparities in enforcement and protection standards that may lead to inconsistent safeguards for young users across the EU. Such a comparative approach allows this study to provide EU policymakers with insights into where harmonisation efforts could be intensified, particularly in areas where national policies diverge from the overarching principles of EU consumer protection laws. This dual focus on Dutch and EU regulatory contexts offers a comprehensive understanding of how different legislative landscapes impact minors and where coordinated efforts could lead to more consistent protections for children across member states. In advancing the insights of the Digital Fitness Check, this study also addresses the inadequacies of traditional consumer protection frameworks when applied to minors who need more cognitive maturity to understand or opt out of complex data practices. While transparency and informed consent are core principles of EU consumer protection laws, they may need to catch up in safeguarding minors, who often need to fully comprehend what they consent to or the implications of sharing personal data. This research, therefore, advocates for regulatory adjustments that move beyond transparency and consent, proposing targeted interventions to restrict the use of AI-driven design techniques specifically for platforms frequented by young users. Such child-focused adjustments would provide a stronger foundation for legal frameworks, ensuring that they align with minors' developmental needs and address the specific vulnerabilities of young users.

Additionally, this study builds on existing literature by examining the ethical dimensions of AI-powered deceptive design, integrating previous findings with empirical insights into how these techniques influence minors. Researchers analyse digital tactics like gamified rewards, adaptive nudges, and social comparison prompts to understand their effects on children's self-regulation and impulse control, which are fundamental to mental and emotional development. By exploring how these practices affect children's well-being over time, this research provides evidence for the need to include protective mechanisms within digital frameworks that account for children's mental health and autonomy. The research's interdisciplinary approach also enriches its contributions by combining insights from developmental psychology, cognitive science, and regulatory studies to uncover why children are especially susceptible to manipulative digital practices. This interdisciplinary framework demonstrates that protective measures for minors cannot solely focus on privacy or transparency but must address the behavioural and psychological effects of digital interactions. By presenting a deeper understanding of the ways that children's developmental characteristics, such as reduced impulse control and increased sensitivity to social validation, make them more vulnerable to AI-driven design manipulations, this study offers a solid foundation for regulatory strategies that actively safeguard children's rights and promote their healthy development within digital spaces. Moreover, this study's contributions extend beyond current research by proposing evidence-based policy considerations to inform the development of EU and Dutch regulations. In anticipation of the Digital Fitness Check's focus on consumer protection improvements, this research outlines practical suggestions for shaping future regulatory developments within the EU, emphasising the importance of integrating protections that address the unique needs of minors. However, the scope and direction of these regulatory efforts remain uncertain, leaving room for further refinement and stakeholder input. Recommendations include implementing regular audits of AI-driven systems to assess compliance with child protection standards, mandating transparency around the algorithms influencing children's online behaviours, and establishing restrictions on using engagement-boosting tactics on platforms accessible to minors. These proposals aim to translate research findings into actionable policies, equipping the EU with adaptive regulatory tools that evolve alongside technological advances to protect young users. Finally, this study offers a rigorous, child-centred framework that advances the European Commission's initial consumer protection efforts by addressing gaps in safeguarding minors. By focusing on the complex relationship between AI-enhanced manipulative design and children's developmental vulnerabilities, this research aligns with the EU's commitment to creating a safe digital environment for all users. It emphasises the importance of harmonised, cross-national protections that account for visible and hidden digital manipulations, establishing a cohesive regulatory structure that prioritises the rights and autonomy of young users.

> *"Child-first design mandates can safeguard minors from engagement-driven exploitation".**

Therefore, this research not only builds on the foundational work of the Digital Fitness Check but also enriches it by introducing an empirical, child-centred approach to understanding deceptive design's impact on minors. This research provides EU and Dutch policymakers with a comprehensive view of minors' risks in digital environments through a unique blend of theoretical insights, interdisciplinary analysis, and comparative study. It underscores the urgency of developing regulations that go beyond traditional consumer protections. The study advocates for an EU-wide regulatory approach that is forward-thinking and responsive to technological advancements, thereby creating a safer, more ethical digital landscape for young users.

1.5 ADDRESSING IMPACTS OF DECEPTIVE DESIGN ON MINORS

In concluding this section, it is essential to underscore the profound implications of deceptive design techniques on minors' autonomy, mental well-being, and privacy in digital spaces. The research has elucidated how these strategies systematically exploit cognitive vulnerabilities unique to children and adolescents through a detailed examination of AI-enhanced manipulative tactics' psychological and behavioural impacts.

> AI-driven manipulations prioritise engagement over autonomy.
>
> Existing regulations inadequately address nuanced threats to minors' well-being.

As platforms increasingly leverage data-driven, adaptive algorithms, young users find themselves in environments that encourage continuous engagement, often at the expense of their autonomy and informed decision-making. The analysis highlights the pressing need for regulatory frameworks that extend beyond traditional transparency and consent models, addressing the subtle yet impactful ways AI systems influence minors' choices and online behaviours.

*Child-first design is a user-centred approach to creating digital environments that prioritise children's rights, developmental needs, and well-being over business objectives such as engagement, data collection, or monetisation. Child-first design, rooted in fairness, transparency, and autonomy principles, tailors interfaces, system architectures, and algorithms to align with minors' cognitive, emotional, and social capacities. This approach avoids exploitative tactics like dark patterns and persuasive nudges while promoting age-appropriate experiences that support healthy development. Child-first design aligns with international child rights standards, such as the United Nations Convention on the Rights of the Child (UNCRC), ensuring that digital platforms respect and uphold children's best interests.

"Adaptive regulatory approach is necessary to safeguard minors in evolving digital landscapes."

Current European and Dutch regulatory frameworks provide a foundational level of consumer protection, with provisions in the GDPR and the DSA targeting transparency and accountability. However, these frameworks must improve their ability to counter manipulative design practices tailored to engage young users. The analysis of these gaps reveals that while existing legislation addresses privacy and data protection concerns, it falls short in curbing more sophisticated, system-level manipulations that leverage AI to create dependency and encourage impulsive behaviours. As a result, there is an evident need for a more nuanced regulatory approach that can adapt to the rapidly evolving landscape of AI-driven personalisation and engagement tactics. The following section will build upon these insights, focusing on the study's research objectives: First, it will ***identify and categorise deceptive design techniques*** targeting minors, establish a typology of manipulative strategies, and examine the psychological mechanisms underpinning each tactic. This categorisation will provide a structured framework for understanding the unique challenges posed by dark patterns in digital environments frequented by children. Second, the research will ***analyse the adequacy of current EU and Dutch legal frameworks*** in addressing these manipulative tactics, emphasising AI-driven deceptive practices. By examining the efficacy of existing legislation and identifying enforcement gaps, the study aims to assess the regulatory landscape comprehensively. Lastly, this research will ***propose targeted policy recommendations*** for enhanced minor protections. These recommendations will advocate for updates to the relevant regulatory instruments, encouraging policymakers to adopt proactive, child-centred regulations that can respond to the challenges posed by emerging digital technologies. The research intends to advance these objectives by offering actionable insights for policymakers and regulatory bodies safeguarding young users. The following sections will contribute to a more resilient, adaptive regulatory framework for minors through a systematic approach that combines empirical analysis, legal evaluation, and policy recommendations. This framework ensures that digital environments respect and protect children's rights, prioritising their developmental needs over commercial imperatives in a rapidly advancing digital age.

1.6 CONCLUSION

The digital world is increasingly shaping children's and young people's lives, but it often does so in ways that exploit their vulnerabilities. Sophisticated design techniques, enhanced by artificial intelligence, influence behaviour, encourage prolonged engagement and collect personal data. These strategies, often referred to as dark patterns or deceptive designs, pose severe risks to children's mental health, privacy, and autonomy. Existing regulations, including the GDPR and the DSA, provide essential protections for data and transparency. However, they do not sufficiently address manipulative practices embedded in digital platforms, particularly those targeting children. Techniques such as personalised engagement loops, gamification, and fear-of-missing-out prompts remain largely unregulated. This report highlights the urgent need for a regulatory framework prioritising children's rights in the digital space. It identifies current weaknesses in European and Dutch legislation and offers clear recommendations for improvement. These include stricter controls on how platforms use data to personalise content, requirements for algorithmic audits, and mandatory age-appropriate design standards. By adopting a child-focused approach to digital regulation, policymakers can ensure that platforms respect children's developmental needs and rights. The goal is to create a safer, more ethical digital environment that aligns innovation and profitability with the well-being of young users. By implementing robust legal protections and proactive oversight, this research seeks to contribute to a digital landscape prioritising trust, fairness, and respect for children across Europe.

SECTION 2: PROTECTING CHILDREN ACROSS THEIR DIGITAL WORLDS: ADDRESSING MANIPULATIVE DESIGN

2.1 INTRODUCTION

This section provides a foundational overview of critical issues affecting child protection in digital environments, establishing the basis for the broader analysis. It introduces the central challenges that policymakers and stakeholders must tackle to create a safer digital space for minors. The discussion explores key aspects of the problem, focusing on the prevalence of manipulative design practices, shortcomings in existing regulatory frameworks, and the heightened vulnerability of young users to digital exploitation. First, the section reviews children's unique online risks, focusing on how deceptive design tactics exploit their cognitive and emotional vulnerabilities. It then explores the limitations of current regulatory instruments, highlighting issues of enforcement complexity and the gaps in existing laws that allow harmful practices to persist. Ultimately, this section aims to inform the Ministry's role in shaping the law by outlining the key areas where targeted intervention could mitigate harm and foster a safer digital landscape for children.

2.2 VULNERABILITY OF CHILDREN IN DIGITAL ENVIRONMENTS

Children warrant special protection in the digital environment due to their unique vulnerabilities and the increasingly sophisticated commercial practices designed to exploit these vulnerabilities.[xxvii] As they grow up in a digital world, children regularly encounter manipulative tactics known as 'dark patterns'[xxviii], as well as aggressive advertising methods that target their cognitive and emotional immaturity.[xxix] The Fitness Check on EU Consumer Law highlights this issue, noting that children's limited understanding of digital ecosystems and commercial strategies makes them less likely to identify or resist manipulative practices.[xxx] Unlike adults, children are still developing the cognitive skills required to interpret advertising, identify marketing intent, and evaluate the potential consequences of their online interactions.[xxxi] This fundamental developmental gap justifies the need for special protective measures tailored to children's needs in digital environments, ensuring that commercial practices respect their rights, safety, and welfare.[xxxii]

> *Children's developmental stages make them particularly vulnerable to digital tactics such as dark patterns and personalised nudges that exploit their cognitive and emotional immaturity."*
> *- European Commission Fitness Check on EU Consumer Law*

Digital platforms frequently employ deceptive design strategies, such as in-app purchases, loot boxes, and gamification elements, to actively engage users and often provoke impulsive actions.[xxxiii] These features can mimic gambling mechanics, encouraging children to engage repeatedly through rewards, randomised outcomes, or competitive elements.[xxxiv] The allure of these features taps into children's natural impulsivity and susceptibility to immediate gratification while exploiting their limited capacity to understand the long-term implications of such purchases.[xxxv] Particularly concerning is the use of virtual currencies in games, which obscures the real-world financial cost of purchases. This added abstraction layer makes it harder for children to recognise the monetary impact of their decisions[xxxvi] , leading to repeated transactions without a clear understanding of their consequences. Such practices exemplify how deceptive design techniques exploit developmental vulnerabilities, imposing unintended financial burdens on families.[xxxvii] These predatory tactics underscore the urgency for child-centred protections that explicitly limit the use of exploitative mechanisms in digital environments frequented by minors.[xxxviii]

The pervasive use of data-driven algorithms and AI further compounds these risks, as platforms increasingly employ personalisation strategies to tailor content and advertisements to individual children.[xxxix] For children, these personalised engagement loops can foster dependency, as platforms continually present them with content that reinforces their existing behaviours and preferences.[xl] Children are less likely to recognise that algorithms carefully craft such recommendations to maximise engagement than adults.[xli] Instead, they often perceive personalised content as an authentic reflection of their interests, unaware that systems strategically generate these suggestions to promote products or behaviours to keep them engaged.[xlii] This lack of transparency about how algorithms function in the background raises serious ethical questions, as children unwittingly enter cycles of consumption and engagement without the complete understanding or consent necessary to make informed choices.[xliii]

> *"Dark patterns manipulate user behaviour through interfaces designed to maximise engagement and profitability. When directed at children, such designs raise ethical and regulatory issues." - (Norwegian Consumer Council, Deceived by Design Report)*

Adding to these concerns is the issue of consent, particularly concerning data collection and privacy. Digital platforms frequently collect extensive behavioural data from minors, building detailed profiles that they then use to inform targeted advertising and personalised content strategies.[xliv] While adults may better understand the implications of data sharing, children often need more awareness to grasp what it means to provide personal information or to appreciate the privacy risks associated with their online activities entirely.[xlv] The consent mechanisms that platforms design exacerbate this issue, as they often encourage agreement rather than informed decision-making. Simplified or overly generalised consent options can mislead children into sharing data without understanding its potential use. This practice undermines children's privacy rights and exposes them to potential exploitation, as platforms use their data to manipulate their engagement and drive consumption without respecting their autonomy.[xlvi] The prevalence of dark patterns, which are manipulative design techniques embedded within user interfaces to influence behaviour, further underscores the need for special protections for children.[xlvii] These dark patterns are crafted to guide users toward actions that benefit the platform, often at the expense of the user's interests. Children are particularly vulnerable, given their limited capacity to recognise and resist such designs. For example, dark patterns can include endless scroll and countdown timers that create a false sense of urgency, nudges to make in-app purchases, or deceptive options that make it challenging to opt out of certain data-sharing practices.[xlviii] These design choices exploit children's susceptibility to social validation and fear of missing out (FOMO), encouraging impulsive actions that can have financial and emotional repercussions. For regulators and consumers alike, addressing these dark patterns is crucial, as they disproportionately affect minors and risk normalising manipulative engagement strategies that can harm children's well-being and autonomy.[xlix]

2.3 DECEPTIVE DESIGN

The digital landscape increasingly incorporates sophisticated design strategies, often called "dark patterns," that subtly manipulate user behaviour to maximise engagement and profitability. These deceptive tactics are of particular concern when directed at children and adolescents at critical stages of cognitive and emotional development, and they are especially susceptible to these influences. For minors, dark patterns leverage their limited understanding and impulse control, raising significant ethical and regulatory issues within the EU.

Dark patterns encompass a variety of methods that capture attention, drive impulsive actions and foster dependency. Standard techniques include frequent notifications, variable rewards, misleading visual prompts, and complex subscription mechanisms. These design elements often exploit specific developmental vulnerabilities in children, such as a strong desire for social validation or sensitivity to peer influence. For example, loot boxes and randomised rewards in gaming mimic gambling mechanics, encouraging repetitive play and in-game spending. This design exploits children's impulsivity and limited financial literacy, leading to unintended economic consequences and fostering addictive behaviours—risks that children may not fully comprehend. These manipulative design elements embed commercial pressures into young users' digital interactions, exposing them to monetisation strategies prioritising profit over well-being. Studies, such as the Norwegian Consumer Council's *Deceived by Design* report, document the harm caused by nudging users toward privacy-intrusive or behaviourally exploitative choices.

These reports underscore the pressing need for enhanced EU consumer protection frameworks to address critical gaps. While regulations such as the GDPR provide a foundational basis for data protection, they frequently fail to adequately address the sophisticated, AI-driven manipulative techniques that target minors. These techniques often exploit personalised content recommendations to influence children's engagement in digital environments. Addressing these challenges requires a regulatory approach that centres on the developmental needs and rights of minors. Introducing fairness-by-design principles and age-appropriate consent mechanisms into EU laws would hold platforms to standards prioritising child welfare over engagement. Platforms could be required to use age-appropriate language when communicating data practices, with strict limitations on personalisation that targets young users. Implementing such safeguards could help reduce the impact of manipulative features like autoplay and "freemium" models, which encourage prolonged screen time and impulsive spending.

In social media, dark patterns often appear as frequent notifications, social validation cycles, and algorithmically tailored content that creates feedback loops of dependency. Features such as "likes" and instant alerts can intensify young users' need for social validation, embedding these motives into platform design and contributing to anxiety and diminished self-esteem. Regulatory measures within the EU could be critical in establishing safeguards addressing these developmental risks. Studies like the European Commission's *Digital Fitness Check* underscore the importance of enhancing EU frameworks to counter these advanced manipulative strategies. As the EU continues to evaluate and improve its consumer protection standards, establishing child-specific guidelines within existing and forthcoming regulations would be a crucial step in creating a digital environment that respects the developmental needs of minors. This research aims to support these regulatory efforts by identifying critical dark patterns that impact children, highlighting regulatory gaps, and providing recommendations to foster a fairer and safer digital environment for Europe's youngest users.

The following table provides a non-exhaustive list of deceptive design tactics minors commonly encounter in digital environments and descriptions of each technique. While existing EU legislation could regulate each of these tactics, the current regulatory framework faces significant challenges. These include a) ineffective enforcement mechanisms that limit the reach of laws, b) the difficulty of investigating these tactics due to the need for specialised expertise, and c) gaps in regulatory scope, allowing many manipulative practices to escape scrutiny. These challenges enable the persistence of deceptive design tactics that continue to exploit the developmental vulnerabilities of minors.

Table 2.3 Deceptive Design Tactics Explained

Deceptive Design Tactic	Description
Push Notifications and Instant Alerts	Platforms use frequent notifications to draw children back into apps or games, tapping into their need for instant updates and creating a fear of missing out (FOMO). This tactic disrupts focus and encourages frequent re-engagement, contributing to prolonged screen time and dependency.[l]
Variable Rewards and Loot Boxes	Games often incorporate loot boxes or randomised rewards that mimic gambling mechanics, appealing to children's desire for unexpected rewards. This design encourages compulsive behaviours and can lead to excessive spending, as children may not understand the real-world costs involved.[li]
Misleading Visual Cues and Interface Manipulations	Platforms employ brightly coloured visuals, animations, and misleading navigation paths to divert attention and lead children toward specific actions, such as making in-app purchases or sharing data. These cues manipulate children's sensitivity to visual stimuli, making it difficult to differentiate between genuine choices and manipulative prompts.[lii]
Subscription Traps and Obstructive Cancellations	Platforms frequently use "subscription traps" that lure children into free trials that auto-renew into paid services. They complicate cancellations by requiring phone cancellations or directing users to retention-focused pages, trapping minors in financial commitments they may need help understanding.[liii]
Addictive Design in Gaming and Social Media	Social media and gaming platforms use addictive design elements like autoplay, infinite scrolling, and gamified rewards to keep children engaged. These tactics exploit psychological vulnerabilities, leading to excessive screen time, reduced self-regulation, and potential mental health issues, such as anxiety and poor self-control.[liv]
Gambling-like Features and In-Game Purchases	Many games incorporate gambling-like features, such as loot boxes and virtual currencies for in-game purchases. These elements exploit minors' need for financial literacy, encouraging them to spend impulsively without realising the actual costs.[lv]
Algorithmic Personalisation and AI-Driven Targeting	Platforms increasingly use AI-driven personalisation to tailor content and advertisements, adapting based on children's behavioural data. This creates a feedback loop that encourages compulsive engagement, often without children's informed consent. EU regulations currently lack specific protections against these AI-driven manipulative tactics.[lvi]
Social Validation and Peer Comparison	Social media platforms use likes, shares, and follower counts to encourage children's engagement and dependency on social approval. This fosters a validation-driven usage cycle that can negatively impact self-worth and mental health, promoting anxiety and low self-esteem among young users.[lvii]
Photo Editing and Filters for Social Approval	Platforms offer editing tools and filters that align with social trends, subtly encouraging children to alter their appearance to meet perceived standards.

	This tactic can distort self-image, exacerbating body image issues and promoting unrealistic social comparisons.[lviii]
Artificial Scarcity and Urgency Prompts	Techniques like countdown timers and limited-time offers create a false sense of urgency, pressuring children into making immediate decisions. This often results in impulsive purchases or actions, preying on children's fear of missing out.[lix]
Dopamine Hits from 'Likes' and Notifications	Social interactions, such as likes and comments, create dopamine-driven feedback loops that foster dependency on platform engagement. These cycles encourage children to seek continuous social approval, leading to potential anxiety and a reliance on external validation.[lx]
In-App Purchases and "Freemium" Traps	Many free apps entice children to make in-app purchases to enhance their experience or advance in games. Children often need to realise the financial implications, as these purchases exploit their limited understanding of digital economies.[lxi]
Constant Distractions through Multi-Tasking Encouragement	Platforms keep children engaged in a constant loop by sending notifications, messages, and alerts across multiple apps. This disrupts focus, fragmenting attention, and encourages prolonged screen time, impacting productivity and well-being.[lxii]
Autoplay and Infinite Scrolling	Features like autoplay and endless scrolling reduce natural stopping points, making it challenging for children to disengage. This design encourages extended use, which impacts sleep and overall mental health.[lxiii]
Data Collection and Profiling	Platforms collect extensive data on children's interactions, creating detailed profiles that inform targeted engagement and advertising. Children unknowingly contribute personal data, which may be sold to third parties or used to manipulate their behaviours further.[lxiv]
Inadequate Transparency and Consent Mechanisms	Consent prompts are often simplified to expedite agreement, encouraging children to share data without fully understanding its implications. These mechanisms conflict with children's best interests by prioritising ease of consent over informed choice.[lxv]

2.4 INSIGHTS FROM THE DIGITAL FITNESS CHECK

European consumer protection frameworks, such as the Unfair Commercial Practices Directive (UCPD)[lxvi] and the Consumer Rights Directive (CRD)[lxvii], already address some aspects of unfair and aggressive commercial practices. However, these frameworks must catch up regarding the digital-specific manipulations that target children. The UCPD prohibits misleading advertising and certain aggressive practices· Nevertheless, it needs provisions tailored to digital platforms' unique challenges, especially concerning personalisation algorithms and AI-driven content targeting. Similarly, the CRD mandates transparency[lxviii] and informed consent[lxix] but does not address how digital platforms can exploit children's cognitive vulnerabilities. Recognising these gaps, there is an opportunity to enhance children's protection by implementing stricter standards that account for their vulnerabilities in the digital environment.[lxx]

A regulatory framework could play a pivotal role in bridging these gaps by introducing child-specific standards for data collection, consent, and algorithmic transparency. For example, platforms could be required to implement age-appropriate consent mechanisms that provide clear and understandable information about data collection practices.[lxxi] Such mechanisms would empower children and their guardians to make informed choices about data sharing, ensuring that children are not unknowingly surrendering their personal information. Additionally, as will be discussed throughout this report, regulatory measures could establish better prohibitions on deceptive design targeting children, banning the use of manipulative design elements like countdown timers and loot boxes that exploit impulsive decision-making.[lxxii]

Integrating fairness-by-design principles into platform architecture is key to enhancing child protection. Fairness-by-design mandates that platforms prioritise ethical considerations, particularly when engaging with vulnerable groups like children.[lxxiii] Applying these principles involves designing user interfaces that respect children's autonomy, avoiding choices that promote addictive behaviours, and ensuring transparency around algorithmic decisions.[lxxiv] Algorithmic transparency is essential in this context, as it would enable children, parents, and regulators to understand how personalisation strategies influence user behaviour.[lxxv] Platforms could be required to conduct regular algorithmic audits, verifying that their AI systems do not foster dependency or manipulate young users through targeted engagement tactics.[lxxvi] This approach would enhance accountability and consumer trust, addressing the ethical concerns associated with algorithmic targeting while ensuring that children's interactions with digital platforms are safe and supportive of their developmental needs.[lxxvii]

The demand for such protections aligns with the broader objectives of EU policy frameworks, which prioritise consumer welfare and data protection. In addition to the UCPD and CRD, the GDPR provides a foundation for privacy rights. Still, it lacks child-specific provisions for transparency and consent that address the intricacies of digital engagement. Law reform could complement these existing laws by establishing age-appropriate design codes and adaptive review mechanisms that monitor platforms' compliance with child-centric standards. For instance, algorithmic audits and disclosures about how platforms use nudges, gamification, and personalisation could provide an added layer of oversight, ensuring that digital environments remain fair and conducive to children's well-being.[lxxviii]

The prevalence of addictive design elements in digital platforms also highlights the necessity for a robust regulatory framework. Social media and gaming platforms often use features like autoplay, infinite scrolling, and reward-based systems to increase engagement. These tactics tap into children's psychological vulnerabilities, encouraging prolonged screen time and fostering patterns of dependency. Such practices can lead to adverse mental health outcomes, including anxiety, reduced self-regulation, and impaired social interactions. The law should directly address these concerns by prohibiting addictive design features that disproportionately impact minors, thereby promoting healthier engagement habits and reducing the risk of digital addiction.[lxxix]

Children's unique vulnerabilities and lack of digital literacy make them particularly susceptible to exploitation in digital environments. Aggressive marketing tactics, personalised targeting, and dark patterns used by platforms expose minors to financial, emotional, and privacy-related risks. As the digital landscape continues to expand, it is essential to implement child-specific protections that prevent the commercial exploitation of minors while promoting safe and ethical digital engagement. By incorporating fairness-by-design principles, mandating transparency in personalisation algorithms, and enforcing stricter data handling standards, the law can safeguard children's rights and developmental needs, thereby fostering a digital environment that respects the autonomy and welfare of Europe's youngest consumers.[lxxx]

Presenting a list of the sixteen deceptive design techniques sets the foundation for an urgent need for child-specific protections within digital environments. This builds on the insights of the Digital Fitness Check and empirical evidence of AI-driven manipulative practices that disproportionately target young users. Children's developmental stages make them particularly vulnerable to sophisticated digital tactics, such as dark patterns and personalised nudges, that exploit their cognitive and emotional immaturity. Additionally, this section highlights the influence of AI techniques, such as dopamine-triggering notifications and peer validation prompts, that manipulate children's desire for social connection and instant rewards.

2.6 CONCLUSION

The analysis in this section underscores the necessity of expanding the regulatory scope to encompass both the overt and latent mechanisms of digital influence, ensuring a more comprehensive approach to safeguarding children's rights in online spaces.

To this end, targeted reforms are necessary to mitigate the risks posed by algorithmic personalisation and engagement techniques that exploit behavioural insights. Implementing age-appropriate disclosures would empower minors and their guardians to make more informed decisions regarding digital consumption. Simultaneously, imposing restrictions on personalisation algorithms targeting children—especially those engineered to create dependency-inducing feedback loops—would help prevent exploitative engagement tactics. Additionally, mandating transparency obligations requiring platforms to disclose the operational mechanisms underlying recommendation systems and AI-driven design strategies would enhance regulatory oversight and accountability. These measures should form part of a layered regulatory approach that balances transparency with preventative restrictions. The categorisation and limitation of exploitative techniques—such as gamification, variable rewards, and social comparison mechanisms—would constitute a crucial pillar of child-specific protections, ensuring that digital platforms do not capitalise on minors' cognitive and emotional vulnerabilities. Furthermore, introducing compliance audits and reporting obligations would reinforce the accountability of digital service providers, compelling them to demonstrate that their systems align with ethical and developmental considerations.

A recalibrated regulatory framework incorporating child-centric standards can bridge these gaps, fostering coherence across EU legislation and advancing a holistic model of digital fairness. Such an approach would reinforce protections for young users and position the EU as a global leader in safeguarding child welfare in an increasingly complex digital landscape. The following sections will build upon these insights, delineating specific policy recommendations to embed robust child-focused regulatory safeguards within the evolving EU digital governance framework. The following section builds on this by looking closely at the tactics children routinely encounter online. These serve as the basis for later analysis of EU and national regulatory approaches across Sections 4-6, identifying gaps and inconsistencies that create a fragmented landscape of child protection standards. Harmonising these protections across EU member states would not only develop uniform standards for child safety online but also allow for adaptive frameworks that can respond to emerging manipulative techniques.   This study extends the Digital Fitness Check's objectives by offering evidence-based recommendations that align regulatory measures with the specific risks AI-enhanced manipulations pose to children.   Through these efforts, the EU can establish a unified digital environment that upholds Europe's youngest users' rights and developmental needs.

SECTION 3: DECEPTIVE DESIGN TACTICS

3.1 INTRODUCTION TO CASE STUDIES

The Internet offers both opportunities and risks in children's increasingly digital lives. Among the latter, deceptive design tactics—called dark patterns—pose significant threats. These tactics exploit children's cognitive vulnerabilities, leading them to decisions that often prioritise corporate profits over their welfare. Understanding these manipulative designs is essential to developing effective regulatory and ethical countermeasures. Deceptive design refers to intentional user interface (UI) and experience (UX) choices crafted to mislead users into behaviours they might not otherwise choose. Unlike ethical design practices, which guide users toward beneficial outcomes, deceptive patterns exploit psychological principles such as scarcity, urgency, and social proof.[lxxxi] These tactics are particularly egregious in children's contexts as they capitalise on developmental limitations, such as reduced critical reasoning and heightened suggestibility.[lxxxii] A prominent example is the gamification of financial transactions in online games. Design strategies entice children to make repeated purchases without fully understanding the economic implications, often framing these transactions as unlocking rewards or progressing in gameplay.[lxxxiii] Critics have condemned these mechanics for fostering addictive behaviours and creating pathways for exploitative monetisation.[lxxxiv]

Social media platforms also employ manipulative tactics, such as infinite scrolling and algorithmically personalised content. These designs trap children in cycles of prolonged engagement, distorting their perception of time and fostering dependency. Personalised nudges, tailored using behavioural data, exacerbate this issue by presenting emotionally charged content that aligns with children's vulnerabilities.[lxxxv] Moreover, digital ecosystems frequently deploy deceptive consent mechanisms. Cookie banners and privacy settings often obscure user-friendly choices, coercing children into sharing personal data through tactics such as pre-selected options, misleading phrasing, and obfuscation of data-sharing implications.[lxxxvi] Such practices undermine the principles of informed consent enshrined in data protection laws like the GDPR.[lxxxvii] Critically, the impact of these designs is not limited to immediate harms like financial loss or data misuse. They also contribute to long-term psychological effects, including increased anxiety, reduced autonomy, and diminished trust in digital environments.[lxxxviii] Children, being less equipped to discern manipulative intent, are disproportionately affected, making them a priority demographic for intervention.

Addressing these challenges requires a multifaceted approach. Case studies of manipulative design in games, social media, and consent architectures provide crucial insights into how these tactics function and impact children. By analysing these examples, policymakers, designers, and advocates can craft targeted solutions to safeguard children's digital rights.[lxxxix] Deceptive design tactics represent a pervasive and evolving threat in children's digital lives. Case studies illuminate the mechanisms behind these manipulations and underscore the urgent need for UX and regulatory framework reforms. Only by understanding the nuances of these designs can we ensure a safer, more equitable digital environment for children.

3.2 THE PSYCHOLOGICAL AND EMOTIONAL VULNERABILITIES OF MINORS

The digital environment poses a unique and profound challenge to children's psychological and emotional well-being. The intersection of their developmental stage with the sophisticated manipulative tactics of digital platforms creates vulnerabilities that require urgent attention from policymakers and scholars. Children, as "digital natives," navigate these online spaces with enthusiasm but lack the cognitive maturity to recognise or resist manipulative designs.[xc]

3.2.1 COGNITIVE IMMATURITY AND SUSCEPTIBILITY

Children's developmental limitations make them particularly susceptible to deceptive design tactics. Lacking fully developed executive functions, they need help with impulse control, risk assessment, and distinguishing persuasive intent.[xci] Design elements like infinite scrolling, loot boxes, and misleading consent mechanisms exploit this susceptibility. These tactics create addictive behaviours and encourage excessive data sharing or financial expenditure.[xcii]

3.2.2 MANIPULATION THROUGH PERSONALISATION

The personalisation of online content exacerbates this vulnerability. Algorithms leverage data collected from children's online behaviour to present targeted content to maximise engagement. These algorithms often use emotionally charged nudges or addictive features that exploit children's inexperience and desire for social validation. For instance, platforms use gamified interfaces that reward continued interaction, embedding psychological hooks into seemingly innocuous activities.

3.2.3 HIDDEN COMMERCIAL INTERESTS

The commodification of children's digital experiences adds another layer of vulnerability. Platforms often obscure the commercial nature of their operations, presenting games and educational tools that subtly integrate advertising or require in-app purchases to progress.[xciii] These tactics exploit children's lack of understanding about financial transactions, leading to overspending and economic exploitation.[xciv]

3.2.4 EMOTIONAL HARM AND MENTAL HEALTH

The consequences of these manipulations extend beyond financial harm. Continuous exposure to manipulative designs has been linked to increased anxiety, reduced self-esteem, and behavioural issues. Children often internalise the pressures created by social media algorithms, leading to a cycle of dependency and dissatisfaction.[xcv] Moreover, using dark patterns in consent mechanisms infringes on their autonomy, fostering a sense of helplessness and distrust in digital environments.[xcvi]

3.2.5 REGULATORY AND ETHICAL CHALLENGES

Current regulatory frameworks often fail to adequately protect children from these harms. While laws like the GDPR provide some safeguards, enforcement still needs consistency, and the designs evolve rapidly to circumvent legal constraints.[xcvii] Ethical considerations also lag behind technological advancements, leaving children exposed to increasingly sophisticated manipulative tactics.[xcviii]

3.2.6 TOWARD PROTECTIVE INTERVENTIONS

Addressing these challenges requires a multifaceted approach. Design frameworks should prioritise transparency and fairness, ensuring platforms cater to children's developmental needs rather than exploiting their vulnerabilities. Educational initiatives for children and parents can also be critical in building resilience against manipulative designs.[xcix] Policymakers must implement stricter regulations and robust enforcement mechanisms to deter unethical practices and hold platforms accountable.[c]

The psychological and emotional vulnerabilities of minors in digital spaces are a pressing issue that demands immediate action. The interplay between developmental immaturity and advanced digital manipulation creates a perfect storm of exploitation and harm. By understanding these vulnerabilities, stakeholders can develop targeted interventions to safeguard children's rights and foster healthier digital environments.

3.3 THE ROLE OF GAMIFICATION IN EXPLOITING COGNITIVE BIASES

Gamification, using game-like elements in non-game contexts, is a dominant feature of digital platforms targeting children. While it can enhance engagement and learning, it also manipulates cognitive biases to influence behaviour in ways that benefit commercial interests, often at the expense of children's well-being.[ci]

3.3.1 EXPLOITING COGNITIVE BIASES THROUGH GAMIFIED MECHANICS

Children are particularly vulnerable to gamification because their cognitive abilities, such as impulse control and decision-making, are still developing.[cii] Gamified elements like rewards, points, and leaderboards exploit biases like **hyperbolic discounting**, where immediate rewards overshadow long-term consequences. For example, game loot boxes use randomised rewards to create anticipation, encouraging children to spend money impulsively without grasping the financial implications.[ciii] Another prevalent tactic is loss aversion, which motivates children to act to avoid perceived losses in virtual environments. For instance, platforms implement mechanisms that penalise players for inactivity, pressuring children to engage to avoid losing progress continually.[civ] These designs capitalise on children's emotional investment, creating dependencies that extend engagement time and increase revenue streams for companies.

3.3.2. MANIPULATION THROUGH PERSONALISATION

Gamification becomes even more manipulative when coupled with personalisation. Algorithms analyse children's interactions to tailor challenges and rewards that maximise engagement. This optimisation often leads children into addictive cycles of play, where the platform continually reinforces specific behaviours. For example, social media platforms gamify interactions with features like "streaks" and badges, compelling children to prioritise online activity over offline responsibilities.[cv]

3.3.3 PSYCHOLOGICAL IMPACT AND BEHAVIOURAL CONDITIONING

The psychological effects of gamification are significant. By constantly rewarding specific actions, platforms condition children to associate engagement with pleasure, creating addictive behaviours akin to those seen in gambling.[cvi] This conditioning exploits **confirmation bias**, where children seek affirming experiences within the gamified system, reinforcing their dependency on the platform. Furthermore, the constant feedback loop of rewards can erode intrinsic motivation. Children become reliant on external validation, leading to issues like reduced self-esteem and heightened anxiety when platforms withhold rewards.[cvii] Social comparison compounds the emotional toll, as leaderboards and rankings foster feelings of inadequacy among less successful participants.

3.3.4 COMMERCIALISATION OF GAMIFIED EXPERIENCES

Gamification is rarely neutral; its primary goal is to drive commercial gain. Platforms embed monetisation strategies within game mechanics, encouraging in-app purchases through tactics like "pay-to-win" models.[cviii] These practices exploit **anchoring bias**, where initial free rewards set a precedent for later purchases, luring children into spending money on upgrades or features.[cix]

3.3.5 THE NEED FOR REGULATION AND ETHICAL DESIGN

Addressing these manipulations requires robust regulatory intervention. Policies like the EU's Digital Services Act and proposed guidelines under the AI Act aim to curtail exploitative practices in gamified environments.[cx] However, regulators must strengthen enforcement mechanisms to ensure compliance, particularly safeguarding children's rights. Fair design principles should also play a pivotal role. Developers must prioritise transparency and accountability, creating gamified systems that enhance learning and creativity without exploiting cognitive biases.[cxi] Additionally, educating parents and children about the risks of gamification can build resilience against manipulative tactics.[cxii] While gamification can potentially enrich children's digital experiences, its misuse in exploiting cognitive biases poses significant risks. By understanding these tactics, policymakers, designers, and educators can work together to create a safer and more equitable digital landscape.

3.4 CASE STUDY 1: LOOT BOXES IN GAMING – A GATEWAY TO GAMBLING?

Loot boxes epitomise the intersection of gaming and gambling, exploiting children's cognitive vulnerabilities and causing financial, psychological, and social harm. A robust, unified regulatory framework across jurisdictions is essential to mitigate these risks. Additionally, educational initiatives for children and parents can raise awareness about the dangers of loot boxes, promoting safer gaming environments.

Background

A popular multiplayer online game introduces loot boxes containing rare in-game assets. To increase sales, the game advertises limited-time offers and creates scarcity by restricting item availability.

Mechanisms of Exploitation

Randomised Rewards: Each loot box contains items of varying rarity, with the odds of obtaining high-value rewards deliberately undisclosed.

Social Reinforcement: Players often showcase rare items on leaderboards or social media, encouraging peers to purchase loot boxes.

Emotional Triggers: Bright animations and celebratory sounds accompany every loot box opening, creating a sense of achievement regardless of the outcome.

Impacts on Children

Behavioural Patterns: Frequent purchases to "chase the reward" mirror gambling behaviours

Financial Strain: One child reportedly spent €2,000 on loot boxes within a year, using a parent's credit card without permission.

Normalisation of Gambling: The randomised nature of rewards fosters a tolerance for risk-taking and gambling-like decisions

Regulatory Intervention

Following public outcry, authorities in Belgium launched an investigation. The game was eventually banned from sale until the loot box system was removed. This set a critical precedent for recognising the risks loot boxes pose to children.

3.5 CASE STUDY 2: INFINITE SCROLLING ON SOCIAL MEDIA – CAPTURING ATTENTION LOOPS

Background

A global video-sharing platform employs infinite scrolling to display short, engaging videos tailored to users' preferences. The platform's user base includes a significant percentage of children.

Mechanisms of Exploitation

Algorithmic Personalization: The platform's AI continuously adapts video recommendations based on user behaviour, ensuring that content remains relevant and engaging.

Variable Rewards: The unpredictability of discovering popular or unique videos creates a cycle of continuous interaction

Social Validation: Features like comments, likes, and shares encourage children to remain active to gain peer approval and maintain social status

Impacts

Behavioural Changes: Children spend an average of three hours daily on the platform, reducing time for homework, sleep, and physical activity.

Psychological Harm: Many report feelings of inadequacy when comparing themselves to influencers or peers on the platform.

Data Exploitation: The platform monetises behavioural data, raising ethical concerns about child-targeted advertising and privacy

Regulatory and Ethical Implications

Despite growing awareness of these harms, regulation of infinite scrolling remains limited. Existing EU frameworks, such as the DSA, aim to increase platform accountability but fall short of addressing children's specific vulnerabilities. Ethical guidelines like fairness-by-design and transparency principles are vital but require robust enforcement mechanisms to ensure compliance.

Infinite scrolling, a design feature that allows users to consume content without manual navigation endlessly, exemplifies addictive design practices in the digital environment. Its psychological allure, particularly for children, is rooted in its capacity to exploit attention loops, creating sustained engagement at the expense of mental health and well-being.[cxiii] Infinite scrolling capitalises on psychological mechanisms such as variable reward schedules, where the unpredictability of new content mirrors the engagement patterns found in gambling.[cxiv] For children, this unpredictability triggers dopamine release, fostering an addictive cycle of anticipation and reward. Furthermore, children's underdeveloped impulse control exacerbates their susceptibility to prolonged screen time.[cxv] This mechanism is amplified by algorithms that personalise feeds, ensuring that the content presented aligns with children's preferences and emotional triggers.[cxvi] For example, a child interested in specific genres of videos or images will find their feed continuously updated with similar, engaging material, reducing the likelihood of disengagement.[cxvii]

Social media platforms that employ infinite scrolling also create social validation loops. Children are motivated to remain online to maintain visibility, interact with peers, and respond to content engagement metrics such as likes or comments.[cxviii] The constant need for validation heightens anxiety and fosters a fear of missing out (FOMO), which further entraps children in these digital spaces.[cxix] The emotional toll of these dynamics includes decreased self-esteem, increased anxiety, and, in extreme cases, a detachment from offline social relationships. Reports show that children experiencing these pressures may exhibit behavioural changes, including irritability and reduced academic performance.[cxx] Infinite scrolling intricately connects to commercial interests, extending beyond mere behavioural concerns. Prolonged engagement increases ad impressions and facilitates the collection of granular user data, which platforms use to refine content recommendations and monetise user activity.[cxxi] For children, this constitutes dual harm: companies compromise their data and privacy while manipulating their behavioural patterns to maximise corporate profits.[cxxii]

3.6 HOW AI-POWERED ALGORITHMS PERSONALISE MANIPULATION

AI-powered algorithms have transformed how digital platforms interact with users, particularly children, by tailoring content and experiences to individual preferences and vulnerabilities. This personalisation relies on vast data collection and advanced predictive analytics, creating a double-edged sword. While it can enhance user experience, it also enables subtle manipulations that exploit cognitive biases and psychological tendencies.

Children are especially susceptible to such manipulations due to their underdeveloped critical thinking and impulse control. To build detailed user profiles, AI systems analyse vast amounts of data, such as browsing history, social interactions, and in-game behaviour. These profiles allow algorithms to predict and influence a child's actions, from recommending specific content to encouraging extended screen time. For example, a recommendation engine might amplify emotionally charged content to capture a child's attention, creating a feedback loop that increases engagement while potentially exacerbating anxiety or other emotional vulnerabilities.

Personalised manipulations often manifest through digital interfaces that exploit behavioural patterns. For instance, AI can adaptively display options to maximise click-through rates or purchases. In children's cases, such manipulations may leverage their susceptibility to rewards or social validation. Platforms might gamify interactions, rewarding children with badges or tokens for actions that align with business objectives, thus fostering dependency on the platform's ecosystem. The opacity of AI-driven systems exacerbates these risks. Many algorithms operate as "black boxes," making it difficult for users, regulators, and developers to understand how they make decisions. This complexity allows platforms to deploy manipulative strategies that evade detection and accountability. For example, dynamic pricing models might adjust in real-time based on perceived willingness to pay, subtly encouraging children to make in-app purchases or subscribe to premium services. Regulatory frameworks such as the EU's GDPR and the AI Act address these challenges by emphasising transparency, consent, and protection against subliminal manipulation. Article 5(1)(a) of the AI Act, for instance, prohibits AI systems from exploiting psychological vulnerabilities to distort behaviour. However, these frameworks often fail to address the cumulative effects of subtle manipulations, leaving gaps where harm can occur undetected.

The ethical implications of such manipulations are profound. When platforms use AI to exploit children's psychological profiles for profit, they erode trust and autonomy while amplifying inequalities. Children from vulnerable socio-economic backgrounds may face heightened risks due to increased reliance on digital services for education and entertainment.[cxxiii] Moreover, normalising manipulative practices in childhood could have long-term impacts, conditioning future generations to accept reduced agency in digital interactions.

Mitigating these harms requires a multi-pronged approach. Regulatory bodies must enforce stricter oversight of algorithmic transparency and hold platforms accountable for outcomes that harm children. Educational initiatives should empower children and parents to recognise and resist manipulative tactics. Ethical AI design principles must guide future developments, prioritising fairness and user welfare over profit maximisation. While AI-powered personalisation offers remarkable potential for enhancing user experiences, it also introduces significant risks, especially for children. Addressing these challenges necessitates robust legal frameworks, proactive regulatory measures, and a societal commitment to ethical technology use.

3.7 CASE STUDY 3: TIKTOK'S ALGORITHM – DRIVING ENGAGEMENT THROUGH EMOTIONAL NUDGES

TikTok, one of the most popular social media platforms globally, provides a striking example of how AI-powered algorithms manipulate user engagement through emotionally charged content. The platform's "For You" page, a personalised feed powered by AI, demonstrates how algorithms exploit children's cognitive and emotional vulnerabilities, raising significant concerns about such practices' ethical and psychological impacts. At the core of TikTok's success lies its recommendation engine, which collects and analyses massive amounts of user data, including video views, likes, comments, watch time, and interaction patterns. This data-driven approach enables the platform to create a highly personalised and engaging feed for each user. This personalisation becomes a tool for manipulation rather than mere entertainment for children, who are more emotionally impressionable and less adept at critical reasoning. The algorithm identifies and amplifies emotionally provocative content that resonates with users' preferences and vulnerabilities. Design practices can actively exploit preferences and vulnerabilities. For example, a child engaging with content focused on challenges or trends may experience a feedback loop where their feed becomes increasingly dominated by similar videos. This dynamic drives prolonged engagement by leveraging emotional responses like excitement, curiosity, or fear of missing out (FOMO). The platform effectively nudges users to spend more time interacting with the app by leveraging the dopamine release associated with viewing content that aligns with their interests.

One of the most controversial aspects of TikTok's algorithm is its ability to exploit social validation loops. Children are particularly susceptible to social approval, and TikTok capitalises on this by prominently displaying likes, comments, and follower counts. The algorithm further reinforces this dynamic by favouring content that garners high engagement, thereby encouraging children to participate in trends or challenges for the prospect of viral fame. This prioritisation of high-engagement content increases time spent on the platform and pressures children to seek validation through the app's metrics. The platform's seamless design and infinite scrolling functionality exacerbate these effects. Videos autoplay as users scroll, creating a near-effortless consumption cycle. This removes natural stopping points for children, making it difficult to disengage. The algorithm's ability to prioritise content that elicits solid emotional reactions ensures that each swipe delivers a new stimulus, keeping the user hooked. This exploitation of variable reward schedules, akin to gambling mechanics, underscores the addictive nature of TikTok's design.[cxxiv] Critics argue that TikTok's practices blur the line between entertainment and manipulation. Children lack the cognitive maturity to recognise when an algorithm influences their behaviour, leaving them vulnerable to long-term psychological effects. Studies suggest that prolonged exposure to emotionally charged content can contribute to anxiety, reduced self-esteem, and compulsive usage patterns, particularly in younger users.

Regulatory bodies, including the European Union, have begun scrutinising such platforms for their manipulative design practices. The AI Act specifically targets algorithms that exploit psychological vulnerabilities, and consumer protection laws like the DSA aim to enhance transparency and accountability. However, enforcement remains a challenge due to the opacity of algorithmic operations and the global nature of platforms like TikTok.[cxxv] TikTok's algorithm demonstrates the powerful yet concerning potential of AI-driven personalisation. While the platform's success stems from its ability to deliver highly engaging content, its reliance on emotional nudges raises ethical questions about exploiting children's vulnerabilities. Addressing these issues requires a combination of regulatory oversight, ethical AI development, and digital literacy initiatives to empower children and their guardians to navigate such environments responsibly.

Case Study: TikTok's Algorithm – Driving Engagement Through Emotional Nudges

Mechanisms of Exploitation

Data Collection and Personalisation TikTok collects extensive behavioural data from users, including viewing habits, time spent on videos, interactions, and content preferences. The algorithm uses this information to refine recommendations and present increasingly tailored content. For children, this targeted personalisation amplifies specific interests and behaviours, reducing exposure to diverse content and creating a narrowed focus on emotionally stimulating material.

Emotionally Charged Content The algorithm prioritises videos that evoke strong emotional reactions, such as excitement, humour, or curiosity. By leveraging dopamine-driven feedback loops, the platform keeps children watching videos that resonate emotionally. The constant delivery of engaging content fosters dependency on the platform, encouraging prolonged usage without conscious decision-making.

Social Validation and Peer Influence TikTok prominently displays metrics like likes, comments, and follower counts, which act as social validation triggers. Children often measure their self-worth and social standing by these metrics, driving them to participate in trending challenges or mimic popular content. The algorithm amplifies highly engaged posts, increasing peer pressure to conform and participate, which reinforces reliance on external validation for self-esteem.

Infinite Scrolling The platform employs infinite scrolling, allowing users to consume content without interruptions. This design eliminates natural stopping points, making it difficult for children to break away from the app. TikTok further reinforces user engagement by deploying variable reward schedules, where the unpredictable nature of the next video encourages continuous interaction.

Impacts on Children

Behavioural Changes Many children develop compulsive usage patterns due to the algorithm's reinforcement of engagement loops. These behaviours disrupt critical aspects of daily life, including sleep schedules, academic performance, and offline relationships.

Psychological Harm Personalised content and constant exposure to trending videos create unrealistic social expectations and foster negative self-comparisons. Children who fail to meet perceived online standards often experience anxiety, reduced self-confidence, and social withdrawal.

Loss of Autonomy The algorithm manipulates children's decision-making by subtly steering their actions toward platform goals. As a result, many children struggle to recognise the extent of external influence on their behaviours, which diminishes their ability to make independent choices.

Regulatory and Ethical Considerations

Governments and regulatory bodies increasingly scrutinise platforms like TikTok for employing manipulative tactics. The European Union's AI Act and Digital Services Act aim to improve transparency in algorithmic systems and reduce exploitative practices. Despite these efforts, platforms frequently evade detection by using complex, evolving algorithms. Parents, educators, and policymakers must push for stricter enforcement mechanisms to protect children from manipulative designs.

3.8 THE IMPACT OF FAKE URGENCY AND COUNTDOWN TIMERS

Fake urgency and countdown timers represent pervasive examples of dark patterns designed to exploit users' decision-making vulnerabilities, particularly those of children. These design tactics are strategically deployed in online environments to create a sense of time pressure, compelling users to make hasty decisions. The impact can be incredibly manipulative and harmful for children who lack the cognitive maturity to evaluate such prompts critically. Countdown timers often appear during online shopping, gaming, or promotional events, displaying messages such as "Hurry! Only 10 minutes left!" or "Sale ends soon." These timers rarely reflect genuine scarcity or urgency. Instead, they exploit the psychological phenomenon of temporal urgency, pressuring users to act quickly out of fear of missing out on perceived opportunities. For children, the immediacy created by such timers can override their ability to pause and assess whether a decision aligns with their actual needs or desires.

This manipulation becomes particularly concerning when integrated with gamified elements in digital platforms. Countdown timers may prompt children to purchase in-game items or extend gameplay sessions to secure bonuses or rewards in many gaming applications or platforms targeted at children. These tactics capitalise on children's impulsivity and intertwine emotional appeals with artificial scarcity. As a result, children may feel compelled to make decisions that lead to financial expenditures or prolonged screen time, often without parental oversight.[cxxvi]

The commercial incentives behind these tactics are clear. Countdown timers significantly increase the likelihood of impulsive purchases or engagement, driving business profits. However, their implications for children extend beyond immediate financial harm. Repetitive exposure to such manipulative prompts normalises high-pressure decision-making environments, which could adversely shape their long-term cognitive and behavioural patterns. Children might grow to associate decision-making with anxiety and urgency rather than rational deliberation.

Moreover, these practices frequently intersect with data collection efforts. As children interact with timed offers, their behavioural responses are logged and analysed to refine future manipulative tactics. Platforms often use the extracted data to personalise subsequent nudges, making the patterns even harder to resist. This practice deepens concerns over children's privacy and autonomy in digital environments.[cxxvii]

Advocates argue for stricter oversight of companies' use of countdown timers and similar tactics, emphasising the need for transparency and genuine disclosures regarding their purpose.[cxxviii] The implications of deploying fake urgency mechanisms on platforms accessed by children are profound and demand careful consideration. By prioritising short-term engagement and profits, companies risk long-term harm to a generation of digital users. Addressing this issue requires a concerted effort from regulators, industry stakeholders, and educators to promote ethical design principles, enhance digital literacy, and ensure robust protections for children in online spaces.

3.9 DARK PATTERNS IN SUBSCRIPTION MODELS – OBSTRUCTING CANCELLATION

Dark patterns embedded within subscription models obstruct the cancellation process, a tactic that poses unique risks to children navigating digital environments. These manipulative designs, referred to as "roach motel" patterns, make it significantly easier for users, including children, to subscribe to a service than to cancel it. For children who need more cognitive maturity to navigate complex or obfuscated processes, these designs can lead to unintentional financial commitments and sustained engagement with services they no longer wish to use.

Subscription models targeting children deploy enticing entry points, such as free trials or one-time offers, which require minimal activation effort. However, designers intentionally make cancellation mechanisms counterintuitive or difficult to access. Because children may be unfamiliar with procedural requirements or lack the attention to detail required to locate and follow hidden cancellation steps, these tactics place them at a distinct disadvantage. For instance, subscription platforms may bury the cancellation option in deep layers of menus or require interaction with multiple confirmation screens, a process that is particularly challenging for younger users.[cxxix]

Furthermore, these designs leverage psychological barriers to cancellation. Subtle language cues may invoke feelings of loss or guilt, such as messages warning users of the "benefits they will miss out on" or suggesting that cancelling would lead to losing progress in games or achievements in educational apps. Such messaging exploits children's susceptibility to emotional manipulation, prompting hesitation or outright abandonment of the cancellation process.[cxxx]

A critical concern lies in the use of automated billing mechanisms. Subscription models rely on recurring payments tied to a parent's credit card, initiated through seemingly harmless one-click signups. Children, lacking awareness of financial consequences, may inadvertently allow charges to accumulate over time. These charges can go unnoticed until they become substantial, causing stress for families and eroding trust in digital services.[cxxxi]

The interplay between dark patterns and algorithmic personalisation exacerbates the issue. Platforms use data-driven insights to place nudges that dissuade cancellation strategically. For instance, after users initiate a cancellation request, some platforms might present personalised offers or highlight features aligned with a child's past usage patterns. These targeted interventions can confuse or distract children, discouraging them from completing the process. Such tactics exploit children's cognitive vulnerabilities, making it nearly impossible for them to exit subscriptions independently.[cxxxii]

Regulatory efforts to address these practices have focused on transparency and simplicity. Proposals like the EU's DSA and enhancements to the UCPD emphasise the need for streamlined cancellation processes that are as simple as signing up. However, enforcement remains inconsistent, and children remain an afterthought in policy considerations. Advocates stress that companies must proactively design cancellation mechanisms that account for children's cognitive abilities and ensure minimal friction.[cxxxiii]

The implications of obstructive cancellation processes are profound. These practices exploit the inherent power imbalance between platforms and children, prioritising profit over user autonomy and well-being. Beyond financial harm, such experiences can undermine children's confidence in digital interactions, leaving lasting psychological and emotional impacts. Efforts to mitigate these harms require a multifaceted approach, including stricter regulatory oversight, child-centric design standards, and education initiatives that equip children and their families with the tools to navigate digital environments safely. By addressing the structural challenges posed by these dark patterns, stakeholders can help create a more equitable and child-friendly digital ecosystem.

3.10 CASE STUDY 4: DUTCH PLATFORMS – LOCALISED EXPLOITATIVE DESIGNS

In the Netherlands, digital platforms catering to local audiences, such as educational apps, gaming platforms, or regional e-commerce websites, frequently employ dark patterns tailored to cultural and regional contexts. These designs exploit users' vulnerabilities to achieve commercial objectives, with children being a particularly susceptible demographic. For instance, platforms like Coolblue, Dutch-language gaming interfaces, or localised streaming services may utilise manipulative techniques that resonate more effectively with users familiar with the Netherlands' language, norms, and specific online habits. These techniques often align with behavioural patterns observed within the Dutch population, creating a nuanced challenge for regulatory oversight.

Mechanisms of Exploitation

Language-Specific Manipulation: Many Dutch platforms exploit the subtleties of language to manipulate users. For instance, subscription models on children-focused educational platforms or gaming sites use language that normalises urgency, scarcity, or guilt. These platforms might include prompts such as “Je wilt dit toch niet missen?” (“You don’t want to miss this, do you?”) to pressure children into purchasing in-game items or upgrading to premium tiers.

Gamified Loyalty Systems: Dutch platforms frequently incorporate gamified elements that reward continued interaction. For example, some apps aimed at Dutch children integrate loyalty points or badges into their interfaces, incentivising frequent use and penalising inactivity. These systems often tie rewards to purchasing behaviours, encouraging children to spend money to maintain their digital status or avoid losing accrued rewards.

Parental Involvement Loopholes: Many local platforms claim to offer safeguards, such as parental controls or clear consent mechanisms, but these features often lack genuine effectiveness. For instance, platforms may allow children to bypass spending limits by exploiting ambiguous consent flows or simplified authentication mechanisms. This results in children making purchases without meaningful parental oversight, exposing families to unintentional financial harm.

Impacts on Children

Behavioural Conditioning: Platforms condition children to associate spending with rewards, creating compulsive behaviours. For instance, children who regularly receive badges for completing tasks or purchasing items may internalise a connection between spending and success, reinforcing the likelihood of future transactions.

Financial Strain on Families: Dutch platforms that target children often rely on low-cost entry points followed by microtransaction-heavy models. Families may notice the financial impact of these incremental charges once they accumulate over time. Such models exploit children’s inability to understand the full financial implications of their decisions.

Psychological Impact: The manipulative designs of Dutch platforms contribute to stress and anxiety among children. A child who fails to achieve a gamified goal due to financial limitations may experience feelings of inadequacy, while frequent exposure to scarcity messages fosters a fear of missing out. These impacts are amplified in children who already face socio-economic vulnerabilities.

Regulatory and Ethical Response

In the Netherlands, the Dutch Authority for Consumers and Markets (ACM) has increasingly scrutinised dark patterns in digital services, with a specific focus on platforms targeting children. While enforcement actions have targeted high-profile cases of deceptive consent mechanisms and unfair pricing practices, regulatory efforts remain limited by the fast-evolving nature of digital manipulation. Current legal frameworks, such as the GDPR and the UCPD, provide a foundation for addressing these practices, but enforcement requires a more granular understanding of localised designs. Dutch platforms exemplify the nuanced ways in which cultural and regulatory contexts influence the deployment of dark patterns. By tailoring manipulative designs to local norms and behaviours, these platforms exacerbate the vulnerabilities of children, leading to financial, psychological, and behavioural harm. Addressing these challenges requires stronger enforcement of existing laws, greater transparency in platform design, and education initiatives aimed at children and their families. These measures, combined with stricter oversight of regional platforms, can help mitigate the impact of exploitative designs on Dutch children.

3.11 BEHAVIOURAL DATA COLLECTION: BUILDING PROFILES TO AMPLIFY MANIPULATION

Behavioural data collection drives digital platforms' operations, enabling highly personalised and manipulative user experiences. These systems collect extensive information about children's online behaviours and leverage it to create detailed profiles. Platforms gather data through interactions with apps, games, and educational tools. This data includes activity patterns, clickstreams, and even biometric information. Often unaware of these processes, children are particularly vulnerable to such practices due to their limited understanding of data privacy.[cxxxiv]

The profiling process involves analysing behavioural data to predict and influence future actions. For instance, platforms use algorithms to identify children's preferences, habits, and emotional states. These profiles drive personalisation strategies, which optimise recommendations for maximum engagement. Platforms present content, advertisements, or gamified experiences tailored to a child's data-driven profile, which deepens their engagement while subtly manipulating their decisions.[cxxxv]

Data collection extends beyond explicit interactions. Technologies like cookies, device fingerprinting, and web beacons monitor browsing habits and device usage, often without users' awareness. These passive collection techniques are insidious, as children are less likely to recognise or understand the implications. The accumulation of such data enables platforms to refine manipulative tactics, such as micro-targeted ads or nudges designed to elicit specific responses.[cxxxvi]

Platforms' commercial incentives shape how they leverage this data. Detailed profiles allow businesses to increase advertising revenue by targeting children with personalised ads or offers. These ads exploit psychological and emotional vulnerabilities, such as a fear of missing out or the appeal of immediate rewards. Children who lack the cognitive skills to evaluate these tactics critically are likelier to act impulsively, contributing to the platforms' profit motives while compromising their autonomy.[cxxxvii]

The ethical implications of these practices are profound. Manipulative environments condition children to accept them as usual, shaping their online behaviours and decision-making processes. These experiences may undermine their ability to distinguish between authentic and manipulative interactions, potentially leaving them susceptible to exploitation in other areas of life. Moreover, the extensive surveillance required for profiling raises significant concerns about children's right to privacy and the long-term implications of these invasive practices.[cxxxviii]

Legal frameworks like GDPR aim to address these challenges by promoting transparency and accountability in data practices. GDPR mandates principles like data minimisation and privacy by design, which require platforms to limit data collection and implement safeguards. However, enforcement needs to be more consistent, and platforms often find ways to bypass these regulations. This results in a limited real-world impact on protecting children from data-driven exploitation.[cxxxix]

Addressing the issue requires a multifaceted approach. Regulators must ensure strict compliance with data protection laws, while educators and parents should empower children to understand and navigate these dynamics critically. Developers should adopt ethical design principles to prioritise users' rights and well-being over profit-driven motives. Collaboration among stakeholders can help create a safer, more equitable digital environment for children, mitigating the risks posed by behavioural data collection and manipulative profiling.[cxl]

3.12 AI-POWERED EMOTIONAL TRIGGERS: NUDGING CHILDREN'S DECISIONS

AI-powered emotional triggers have emerged as sophisticated tools for influencing children's decisions in the digital space. These mechanisms utilise artificial intelligence to exploit children's developmental vulnerabilities, leveraging emotional responses to drive engagement and specific behaviours. Due to their limited ability to critically assess persuasive designs, children are particularly susceptible to manipulative tactics that prioritise profit over their well-being.

Digital platforms frequently deploy AI to tailor content and interactions to the emotional states of young users. For example, algorithms analyse children's reactions to specific stimuli—such as images, music, or themes—and use this data to predict and amplify responses. By presenting emotionally charged content, platforms create heightened levels of engagement, reinforcing cycles of interaction that are difficult for children to break. The dopamine-driven feedback loop, where the anticipation of rewards fuels continuous use, is particularly effective in holding a child's attention.

Personalised nudges, another feature of AI systems, often exploit children's desire for validation and inclusion. Social media platforms, for instance, use AI to recommend content or connections based on perceived interests. These recommendations frequently exploit social dynamics, encouraging behaviours to gain likes, comments, or followers. Children's inherent need for peer approval exacerbates the influence of such triggers, as they may prioritise online validation over other activities, potentially leading to diminished self-esteem and increased anxiety .[cxli]

Emotional triggers also manifest in urgency mechanisms, which compel children to make rapid decisions. For instance, amplified by AI, limited-time offers in games or shopping platforms prey on a child's fear of missing out (FOMO). These mechanisms use real-time data to personalise urgency, aligning the timing of offers or prompts with a child's online behaviour. The result is an environment that fosters impulsive decision-making, often with financial or emotional consequences.[cxlii]

AI-powered systems also create parasocial relationships, where children develop emotional connections with virtual characters or influencers. Virtual assistants, chatbots, or AI-driven avatars simulate empathy and understanding, creating the illusion of genuine relationships. For children who must develop the ability to differentiate between simulated and authentic interactions, these experiences can distort perceptions of relationships and encourage dependency on digital environments.[cxliii]

The ethical implications of these practices are significant. By using AI to manipulate emotional responses, platforms risk undermining children's autonomy and long-term mental health. These triggers influence immediate decisions and shape behavioural patterns, conditioning children to respond to external stimuli rather than exercising independent thought. Such conditioning can have lasting effects, affecting how they interact with technology and make decisions in adulthood.[cxliv]

Regulatory frameworks like GDPR have introduced safeguards aimed at curbing manipulative data practices. Provisions for transparency and fairness in AI systems aim to protect vulnerable groups, including children. However, enforcement remains inconsistent, and the rapid evolution of AI technologies often outpaces regulatory measures. Strengthening these frameworks and prioritising children's rights within AI design is essential for mitigating the risks associated with emotional manipulation.[cxlv]

Addressing the influence of AI-powered emotional triggers requires a multifaceted approach. Policymakers must implement stricter enforcement of existing regulations, while developers should adopt child-centric design principles that minimise manipulative practices. Educators and parents also play a crucial role in fostering digital literacy, empowering children to navigate online environments critically. By prioritising ethical considerations and collective responsibility, stakeholders can create safer digital spaces that respect and protect children's developmental needs.

3.13 CASE STUDY 5: INSTAGRAM'S SOCIAL VALIDATION LOOPS

A leading social media platform, Instagram relies heavily on social validation mechanics to drive user engagement. These mechanisms include visible likes, comments, shares, and follower counts, reinforcing a user's sense of acceptance and popularity. For children who are particularly sensitive to peer validation and social feedback, Instagram's design creates a compelling yet manipulative environment. Social validation loops exploit their developmental vulnerabilities, encouraging behaviours prioritising online approval over genuine self-expression or well-being.

Instagram's social validation loops exemplify how digital platforms exploit psychological vulnerabilities to maximise engagement. The interplay between algorithmic amplification, peer influence, and visible metrics creates a powerful yet harmful environment for children. Addressing these issues requires regulatory intervention, promoting digital literacy, and ethical platform design. By fostering a healthier relationship between children and social media, stakeholders can mitigate the risks associated with validation-driven digital experiences.

Case Study: Instagram's Social Validation Loops

Mechanisms of Exploitation

Engagement Metrics as Rewards: Instagram prominently displays metrics such as likes and follower counts on posts, which act as quantifiable indicators of social approval. For children, these metrics serve as psychological rewards, reinforcing their behaviour. A post that garners significant engagement encourages them to replicate similar content, perpetuating a cycle of dependency on external validation.

Algorithmic Amplification: The platform's algorithm favours posts that generate high engagement, prioritising such content in feeds and explore pages. Children who receive lower engagement may feel compelled to adapt their behaviour or appearance to align with trending norms or themes. This amplification mechanism creates a disparity in perceived popularity, leading to increased social comparison and pressure to conform.

Temporary Content Features: Instagram's temporary content options, such as Stories, heighten the urgency of social interaction. Stories disappear after 24 hours, encouraging children to check the app frequently to view and respond to peers' updates. The platform leverages this transient nature to create a fear of missing out (FOMO), ensuring consistent interaction with its features.

Peer Influence and Trends: Instagram amplifies peer dynamics by promoting trends and challenges. Children often engage with these trends to gain social acceptance or visibility within their peer group. This behaviour not only deepens their reliance on the platform but also exposes them to potential risks, such as sharing personal information or engaging in activities they would typically avoid.

Impacts on Children

Psychological Effects: Relying on social validation can lead to heightened anxiety and reduced self-esteem, particularly when engagement metrics do not meet a child's expectations. Constant comparison with more "successful" peers fosters feelings of inadequacy and dissatisfaction with one's own achievements or appearance.

Behavioural Conditioning: Instagram conditions children to prioritise online interactions over offline activities. This behaviour often manifests in compulsive posting or checking of engagement metrics, diverting attention from other aspects of life, such as academics or personal relationships.

Distorted Self-Perception: Exposure to highly curated and often unrealistic portrayals of life on Instagram can distort children's understanding of authenticity and self-worth. Many children equate their value with the level of engagement they receive, leading to a fragile sense of identity that hinges on external feedback.

Regulatory and Ethical Considerations

Regulatory bodies have scrutinised Instagram's practices, particularly regarding its impact on children's mental health and well-being. Proposed measures include limiting the visibility of engagement metrics and enhancing transparency in algorithmic content promotion. While Instagram has trialled features such as hiding likes, critics argue that such efforts often fall short of addressing the root causes of manipulation.

3.14 VIRTUAL CURRENCIES AND OBFUSCATION OF REAL-WORLD COSTS

Virtual currencies are pervasive in many online platforms, particularly games targeting children. They often obscure real-world costs, creating an environment that disconnects spending decisions from tangible financial considerations. This disconnect allows platforms to exploit cognitive and emotional vulnerabilities in children, leading to increased spending and engagement.

The two-stage purchasing mechanism, where users first buy virtual currency with real money and then use it for in-app purchases, complicates children's understanding of monetary value. This design leverages the concept of money illusion, wherein children perceive the virtual currency as less valuable than its real-world equivalent. The lack of precise conversion rates between virtual and real currencies further obscures costs, making it challenging for young users to grasp the financial implications of their purchases.[cxlvi]

Game developers often integrate multiple layers of virtual currencies to increase complexity. For example, some games require users to earn one type of currency through gameplay and purchase a different kind with real money. This layered approach fragments the connection between spending and value, encouraging children to spend impulsively without considering the real-world impact. Additionally, many platforms offer virtual currency in predefined bundles, often exceeding the amount needed for a particular purchase. This bundling tactic encourages users to spend more than necessary, creating a surplus currency that nudges them toward further transactions.[cxlvii]

Platforms also deploy dark patterns to amplify the manipulative potential of virtual currencies. These include frequent promotions, limited-time offers, and artificial scarcity cues, heightening the urgency of spending. The fear of missing out (FOMO) induced by these tactics can lead to impulsive decisions for children. Additionally, the gamification of the expenditure—where purchases unlock new features or rewards—further normalises the act of spending, embedding it as a routine behaviour within the game.[cxlviii]

The psychological impact of these mechanisms on children is profound. They condition children to prioritise instant gratification over delayed rewards, undermining their impulse control. Over time, this can lead to unhealthy spending habits and a distorted understanding of financial responsibility. Moreover, the emotional rewards tied to virtual purchases, such as unlocking exclusive content or improving social status within the game, exploit children's developmental vulnerabilities, reinforcing a cycle of spending and engagement.[cxlix]

While regulatory frameworks like GDPR provide some protections, such as transparency requirements and limits on data collection, they do not adequately address the manipulative nature of virtual currencies. Current laws focus more on privacy and less on the economic and psychological exploitation facilitated by these systems. There is a growing call for stricter regulations, including mandatory disclosure of real-world costs alongside virtual prices and prohibitions on bundling strategies that lead to unnecessary spending.[cl]

Mitigating the harm caused by virtual currencies requires a multifaceted approach. Developers must design systems prioritising transparency and fairness, providing clear information about costs and value. Regulators should enforce stricter standards on pricing disclosures and limit the use of manipulative tactics in games targeting children. Furthermore, educational initiatives can equip children and their families with the tools to critically evaluate and resist these manipulative designs, fostering healthier digital behaviours.

3.15 EXPLORING HIDDEN DECISION-MAKING ARCHITECTURES IN ONLINE SERVICES

Hidden decision-making architectures in online services have emerged as potent mechanisms to influence children's behaviour, exploiting their cognitive limitations and emotional vulnerabilities. These systems, powered by algorithmic decision-making, operate covertly, tailoring experiences that nudge children towards specific actions, often without their awareness. These architectures rely on data collection and predictive modelling to shape interactions that maximise engagement and monetisation, often at the expense of the child's autonomy.

Platforms deploy algorithms that analyse a child's digital footprint, including preferences, browsing history, and engagement patterns. This data forms the foundation of decision-making systems, enabling platforms to personalise content and interactions. For instance, a platform may identify a child's interest in specific themes and use this insight to curate feeds that are both compelling and hard to resist. The result is an environment that traps users in feedback loops, amplifying their reliance on the platform and limiting their capacity to disengage.[cli]

Decision-making architectures often incorporate dark patterns that exploit psychological biases. These patterns can be particularly effective for children still developing critical thinking skills. Elements such as urgency cues, scarcity tactics, and social validation triggers are embedded within user interfaces to manipulate decision-making. These tactics reduce the ability of young users to make informed choices, steering them towards actions aligned with the platform's objectives, such as in-app purchases or extended screen time.[clii] The lack of transparency surrounding these architectures further exacerbates their impact. Children and their guardians rarely receive information about how decisions occur or the factors influencing their interactions. This opacity allows platforms to operate without scrutiny, embedding manipulative strategies into their systems. Even when platforms disclose information, they often present it in dense, technical language, rendering it inaccessible to the average user.

Regulatory frameworks like GDPR impose obligations on platforms to ensure transparency and fairness in automated decision-making. For instance, GDPR mandates that platforms provide users with meaningful information about the logic behind such processing. However, the enforcement of these provisions needs to be more consistent, and platforms continue to find ways to bypass compliance. This regulatory gap exposes children to the unchecked influence of hidden decision-making systems.[cliii] The ethical implications of these architectures are profound. By shaping behaviours without explicit consent, platforms infringe on children's autonomy and developmental rights. These systems influence immediate choices and condition long-term behaviours, normalising manipulative digital environments. This conditioning raises concerns about the broader societal impact as children grow accustomed to opaque and exploitative interactions in their digital lives.[cliv]

Addressing the challenges posed by hidden decision-making architectures requires a holistic approach. Policymakers must strengthen regulatory enforcement to ensure platforms adhere to transparency and fairness standards. Developers need to prioritise ethical design principles that safeguard user autonomy. Educational initiatives should equip children and their guardians with the knowledge to recognise and resist manipulative tactics. By fostering greater accountability and awareness, stakeholders can mitigate the risks associated with these covert systems, creating a safer and more equitable digital landscape for young users.

3.16 MANIPULATIVE CONSENT MECHANISMS: FORCING AGREEMENT

Manipulative consent mechanisms are increasingly prevalent in online environments. These mechanisms often use deceptive design tactics to coerce users—particularly children—into agreeing to data collection or other actions without genuine choice. These mechanisms are typically embedded within user interfaces and leverage children's cognitive and emotional vulnerabilities, exploiting their limited ability to evaluate terms and conditions critically. Under GDPR, consent must be freely given, informed, specific, and unambiguous, yet online platforms routinely subvert these requirements.[clv]

One common technique involves using dark patterns that obscure or de-emphasise the option to refuse consent. For instance, refusal buttons may be hidden in hard-to-locate menus or appear in less visually prominent forms, such as smaller font sizes or less vibrant colours. These design choices create an implicit hierarchy of options, steering children towards the path of least resistance—often the "accept" button.[clvi] Pop-ups demanding consent appear so usually that they interrupt the user experience, creating frustration that prompts hasty agreement. This interruption tactic is particularly effective for children, as it exploits their impulsivity and desire to return to engaging content. The language in these pop-ups often employs urgency or emotional appeals, framing consent as necessary for an enhanced experience or access to specific features. These manipulations directly contradict the principle of freely given consent under GDPR.[clvii]

Another widespread tactic is bundling consent for multiple purposes into a single agreement. Children may not realise they consent to more than the immediate action, such as enabling a game or app feature. This strategy exploits the general need for more comprehension among younger users regarding the broader implications of their agreement. GDPR requires granular consent for distinct purposes, yet platforms often circumvent this by presenting vague, overarching terms.[clviii] The practice of pre-ticking consent boxes further undermines the integrity of the process. While GDPR explicitly prohibits this practice, it remains a covert method to default users into agreeing. Children may overlook such settings, assuming the default configurations are necessary and harmless. These tactics condition users to view data-sharing agreements as minor, routine decisions, diluting the importance of informed consent.[clix]

The implications are significant. Manipulative consent mechanisms erode trust in digital platforms and condition children to accept exploitative practices as standard. They also compromise the autonomy of young users, shaping behaviours that prioritise compliance over critical engagement. This conditioning extends into adulthood, fostering a generation of users more susceptible to manipulative digital practices.[clx] Addressing this issue requires vigorous regulatory enforcement and greater emphasis on child-centred design principles. GDPR provisions, such as those mandating transparency and accessibility, must be rigorously applied to interfaces targeting children. Developers should design consent mechanisms that are straightforward, visually neutral, and age-appropriate, enabling children to make genuinely informed decisions. Furthermore, educational initiatives should equip young users with the skills to recognise and resist manipulative practices, fostering a more equitable digital environment.[clxi]

3.17 QUANTIFYING THE IMPACTS: BEHAVIOURAL, EMOTIONAL, AND FINANCIAL HARM

The practices of data collection, algorithmic profiling, and deceptive interface designs deeply intertwine with the behavioural, emotional, and financial harm inflicted on children by manipulative digital environments. Often invisible to users, these mechanisms systematically erode autonomy and well-being, leveraging cognitive vulnerabilities unique to children. Quantifying these harms necessitates an analysis of their specific manifestations across behavioural patterns, emotional stability, and financial outcomes.

Behaviourally, platforms condition children to engage in ways prioritising corporate objectives over their developmental needs. Algorithmically driven recommendations, coupled with endless scrolling features, trap children in feedback loops that reinforce addictive behaviours. These systems exploit underdeveloped impulse control, making disengagement difficult and leading to excessive screen time at the expense of other critical developmental activities like education, social interaction, and creative play. Persistent and push notifications amplify this behavioural conditioning by capitalising on children's need for immediate gratification.[clxii] Emotionally, the impact of manipulative designs on children is profound. Social validation mechanisms such as likes and comments foster an environment where self-worth becomes tied to online recognition. Children exposed to curated and often unrealistic depictions of life online experience heightened feelings of inadequacy and exclusion. The normalisation of social comparison exacerbates this emotional toll, which research links to increased anxiety, depression, and low self-esteem. The introduction of parasocial relationships with influencers or avatars further complicates children's emotional landscapes, as they form attachments to entities designed to manipulate their preferences and behaviours.[clxiii]

The financial harms children face are equally significant, often stemming from exploitative in-app purchase mechanisms and the obfuscation of real-world costs. Many platforms employ virtual currencies to mask actual expenses, encouraging children to spend impulsively without clearly understanding the financial implications. Limited-time offers and dynamic pricing further exacerbate this issue, preying on children's fear of missing out to drive unnecessary purchases. Parents frequently bear the financial burden of these practices, resulting in disputes and unintended expenses. The cumulative effect of these harms underscores the broader systemic issue of prioritising profit over child welfare. Regulatory frameworks such as GDPR aim to protect children by enforcing transparency and fairness, yet enforcement gaps persist. Platforms continue to employ designs that obscure data collection practices, condition children into exploitative behaviours, and fail to provide accessible mechanisms for withdrawal or informed refusal of consent.

Addressing these harms requires robust interventions that go beyond regulatory compliance. Designers must incorporate child-centred principles that prioritise developmental needs over engagement metrics. Educational initiatives are also critical, equipping children and their caregivers with the knowledge to navigate digital spaces critically. By fostering accountability among stakeholders, it is possible to mitigate the adverse impacts of these exploitative practices and create a digital environment that upholds the rights and well-being of children.[clxiv]

3.18 CONCLUSION

The analysis of deceptive design practices across digital environments has demonstrated the extensive and multi-layered vulnerabilities children face. This section has highlighted how manipulative design tactics, rooted in behavioural economics and advanced technologies like AI, exploit children's developmental immaturity and emotional susceptibilities. Through examples spanning various sectors—gaming, social media, educational tools, and consent mechanisms—it becomes evident that these designs prioritise corporate interests over children's well-being, often at the cost of their autonomy, privacy, and mental health.

Children are particularly susceptible to dark patterns due to their limited impulse control, underdeveloped critical reasoning skills, and heightened susceptibility to social validation. Features such as loot boxes, infinite scrolling, and emotionally charged content amplify these vulnerabilities, creating addictive cycles of engagement and fostering dependency. Moreover, the normalisation of these manipulative tactics conditions children to accept exploitative digital environments as standard, raising concerns about their long-term behavioural and psychological development. The economic exploitation facilitated by virtual currencies, dynamic pricing, and obstructive subscription models further compounds the harm. By obfuscating real-world costs and leveraging time-sensitive offers, platforms exploit children's lack of financial literacy, leading to unintentional spending and undue economic pressure on families. Such practices underscore the need for transparency and fairness in digital design, particularly in systems targeting young users. Consent mechanisms add another layer of complexity. While frameworks like GDPR emphasise the importance of informed, freely given consent, manipulative designs often obscure these processes, forcing children into agreements without meaningful understanding. These practices highlight a significant enforcement gap in existing regulations, allowing platforms to prioritise profit over ethical considerations.

The findings in this section serve as a foundation for transitioning into a comparative legal analysis in Section 4. By identifying the harms caused by deceptive designs and examining the regulatory challenges, this section establishes the urgency for robust legal frameworks tailored to children's digital experiences. Comparative analysis will explore how jurisdictions address these challenges, offering insights into best practices and potential gaps in enforcement. As we move forward, the focus will shift to examining how legal systems across different jurisdictions regulate manipulative digital practices targeting children. By comparing approaches, we aim to identify strengths and weaknesses in current frameworks, assess their alignment with international standards, and propose actionable recommendations for enhancing legal protections. This transition marks a crucial step in bridging the insights gained from behavioural analysis with the legal mechanisms necessary to safeguard children's rights in the digital age.

SECTION 4: COMPARATIVE LEGAL AND POLICY ANALYSIS

4.0 INTRODUCTION

In the evolving digital landscape, ensuring robust protections for children and other vulnerable groups necessitates a nuanced interplay between national regulatory frameworks and overarching EU directives. Section 4 explores this intersection by examining how the Netherlands navigates these dynamics as a regulatory leader while striving to harmonise its approaches with EU goals. It explores the challenges and opportunities in addressing manipulative design practices, algorithmic exploitation, and the rapidly advancing technologies shaping consumer interactions. This section critically analyses the tensions between local cultural and legal specificities and the EU's ambition for harmonisation. It highlights the Netherlands' unique contributions, such as leveraging behavioural insights and embedding fairness-by-design principles, while addressing the limitations of broader EU frameworks in adequately protecting vulnerable groups.

National vs EU Frameworks: The section explores the interplay between national regulations, particularly in the Netherlands, and broader EU frameworks like GDPR and DSA. It highlights the strengths of localised protections, such as age-appropriate content laws, and the challenges of harmonising these with EU-wide standards.

Regulatory Tensions and Gaps: It examines the tension between culturally specific regulatory approaches in the Member States and the EU's ambition for uniformity. The fragmented enforcement of GDPR and jurisdictional overlaps leave critical gaps that platforms exploit, particularly to the detriment of children.

Innovative Approaches in the Netherlands: Dutch regulators leverage behavioural insights, fairness-by-design principles, and AI-driven tools to address manipulative digital practices targeting children. These strategies offer potential models for scalable solutions across the EU.

Algorithmic Opacity and Child-Centric Design: The section underscores the challenges of addressing opaque algorithmic processes and manipulative decision-making architectures. It highlights Dutch efforts to enforce transparency and prioritise protections tailored to children's cognitive and emotional needs.

Pathways to Harmonisation: The section concludes by advocating for a collaborative governance approach, where national initiatives inform and enhance EU-wide policies. This reciprocal innovation ensures that regulatory frameworks are both locally relevant and effective

Furthermore, it investigates the regulatory challenges of cross-border digital services and the necessity of scalable compliance mechanisms that align with national priorities and EU standards. Through a series of focused discussions, Section 4 evaluates Dutch and EU approaches to digital fairness, the role of transparency and accountability in overseeing AI-driven personalisation, and the importance of adaptive frameworks to future-proof regulations. By critically analysing jurisdictional overlaps, enforcement mechanisms, and proactive design interventions, this section underscores the need for collaborative, innovative, and anticipatory strategies. Section 4 aims to provide actionable insights and recommendations for harmonising Dutch and EU regulatory efforts. It envisions a cohesive digital governance framework that balances innovation with fairness, ensuring consistent and effective protections for children across jurisdictions while maintaining the Netherlands' position as a thought leader in digital regulation.

4.1 JURISDICTIONAL OVERLAPS IN CROSS-BORDER DIGITAL REGULATION

The intersection of national sovereignty and EU-level frameworks presents a complex challenge in enforcing digital regulations that protect children. EU regulations like the GDPR, DSA, and AI Act aim for harmonisation, yet jurisdictional overlaps and inconsistencies remain endemic. National enforcement bodies often grapple with discrepancies in legal interpretations, operational capacities, and prioritisation of children's digital rights. These divergences exacerbate inconsistencies in addressing cross-border violations, particularly manipulative design practices targeting minors.[clxv]

The GDPR's one-stop-shop mechanism attempts to streamline data protection enforcement but has practical limitations. Issues arise in cases where national supervisory authorities disagree over the impacts of cross-border practices on vulnerable groups like children. Similarly, while the DSA enhances transparency obligations for very large online platforms (VLOPs), enforcement gaps persist in regulating subtle manipulative practices embedded in system architectures, often bypassing interface-level scrutiny. [clxvi]

The principle of country-of-origin further compounds jurisdictional ambiguities under directives like the AVMSD. This principle limits the ability of host countries to enforce stricter regulations on foreign providers targeting local audiences, creating loopholes that platforms exploit. For instance, algorithmic systems that amplify harmful content for children are often designed in jurisdictions with weaker enforcement mechanisms, circumventing stringent protections elsewhere.[clxvii]

The fragmented approach to implementing the Representative Actions Directive (RAD)[clxviii] highlights another dimension of enforcement complexity. While the directive encourages collective redress mechanisms, discrepancies in funding, procedural frameworks, and access to legal resources among Member States hinder unified enforcement. This uneven landscape often leaves child-specific harms, such as financial exploitation through in-app purchases, under-addressed.[clxix] Furthermore, digital sovereignty debates, underscored by the rise of localisation requirements, reveal tensions between EU-wide principles and national prerogatives. Some Member States advocate for stricter data residency rules to enhance enforcement capacities, but these clash with the borderless nature of digital services and the EU's Single Market principles.[clxx] The disconnection between digital governance's territoriality and the inherently global digital ecosystem complicates coherent policy application. Harmonisation efforts must also contend with cultural and legal diversity across Member States. Differences in societal norms, regulatory priorities, and interpretations of fairness impede the consistent application of child-centric protections. For example, approaches to gamification's addictive features vary widely, undermining collective efforts to mitigate their psychological impacts on children.[clxxi]

Technological advancements like AI-driven personalisation outpaces regulatory frameworks, exposing enforcement gaps in addressing opaque algorithms and backend manipulations. The AI Act's risk-based approach introduces mitigation measures but remains limited by a lack of precise enforcement tools for child-specific vulnerabilities.[clxxii]

4.2 RECONCILING DUTCH AND EU APPROACHES TO DIGITAL FAIRNESS

The Dutch Mediawet[clxxiii] exemplifies a comprehensive, culturally embedded approach to consumer protection, particularly in safeguarding children in digital environments. Its emphasis on transparent advertising, age-appropriate content, and minimal exploitation contrasts with EU law's overarching but often abstract frameworks. Reconciling these approaches reveals both synergies and critical gaps. At the EU level, regulations like the DSA and DMA focus on harmonisation and interoperability but fall short of addressing cultural nuances, particularly in their application to children. For instance, while the DSA mandates transparency for content moderation and algorithmic operations, it lacks specificity in curbing manipulative designs targeting minors. In this area, Mediawet excels by directly imposing content and advertisement restrictions tailored to youth audiences.[clxxiv]

However, this dual structure creates enforcement ambiguities. The EU's emphasis on harmonisation, as seen in directives like the UCPD, often limits Member States' ability to enforce stricter, locally adapted measures. For example, Dutch regulators seeking to impose stringent rules on addictive app features may face legal pushback if these measures conflict with the principle of maximum harmonisation under EU law.[clxxv] This clash is particularly evident in practices like loot boxes or in-app purchases, where the Mediawet advocates outright bans or strict controls, contrasting with EU frameworks' more lenient positions.[clxxvi]

Synergies exist in the shared prioritisation of vulnerable populations. The Mediawet's alignment with principles in the GDPR, particularly around consent and transparency for minors, showcases compelling interplay. Both frameworks aim to ensure that children can navigate digital spaces without undue manipulation, reinforcing the necessity of accessible and understandable consent mechanisms.[clxxvii]

However, the evolving nature of digital fairness demands a more integrated approach. This issue underscores the need to extend protections against dark patterns and emotional manipulation, areas that remain under-addressed in the *Mediawet*. Dutch experiences could provide valuable insights for legal reform, particularly in embedding fairness-by-design principles.[clxxviii] However, the lack of reciprocity—where EU laws often dictate but do not absorb best practices from Member States—remains a structural flaw.

The integration of child rights frameworks, such as those suggested by the UK's Age-Appropriate Design Code, offers a model for mutual reinforcement. While the Mediawet incorporates aspects of child-centric design, the EU could elevate these protections by mandating a baseline standard that adapts to local legal traditions, ensuring cohesive but context-sensitive protections.[clxxix] Finally, enforcement discrepancies exacerbate these issues. The fragmented oversight by the Dutch ACM and EU CPC network illustrates the need for more precise jurisdictional boundaries. Shared accountability mechanisms could reduce duplication while leveraging national expertise, particularly in culturally sensitive areas like child-targeted advertising. [clxxx]

4.3 INNOVATIVE POLICY INSTRUMENTS FOR DUTCH REGULATORY LEADERSHIP

The Netherlands has established itself as a regulatory leader, particularly in safeguarding children in digital environments. With a new Digital Fairness Act, Dutch policymakers have a unique opportunity to align their nationally recognised practices with emerging EU standards, addressing critical gaps in consumer protection while fostering innovation. This alignment positions the Netherlands as a pioneer in harmonising local expertise with broader European goals.

> *"Fragmented enforcement of GDPR and DSA creates opportunities for platforms to exploit regulatory gaps, undermining the consistency of children's digital protections."*

A significant pathway for Dutch leadership lies in embedding fairness-by-design principles into system architectures. Leveraging successes such as the Mediawet, these principles could mandate transparent, user-friendly interfaces designed to prevent manipulation at the source. Algorithmic auditing, a shared concern for Dutch and EU regulators, could be formalised as a compliance requirement, ensuring digital systems operate transparently and fairly for children. Extending this approach to include design standards would create a more resilient digital ecosystem bolstered by accountability mechanisms tailored to address the opacity of personalisation systems. [clxxxi] The push to combat dark patterns complements Dutch efforts to regulate manipulative interfaces. Dutch regulators could refine enforcement strategies by introducing innovative oversight mechanisms like behavioural analysis tools and AI-driven detection systems. These tools would enable the identification of deceptive nudges and manipulative interface designs, ensuring timely interventions. Advanced detection systems could strengthen the Netherlands' role in protecting children's digital rights while promoting compliance with EU-wide objectives.[clxxxii]

Adaptive governance models offer another avenue for leadership. Dutch regulators could champion a co-regulatory approach involving industry stakeholders, advocacy groups, and policymakers. Such a model would enable flexible and responsive frameworks, fostering collaboration on measures like loot box bans and stricter controls on in-app purchases. Rooted in Dutch expertise, these efforts could shape broader EU policies to address digital risks.[clxxxiii]

Addressing the fragmented enforcement landscape is critical to harmonisation. Dutch regulators could advocate for creating a centralised EU oversight body focused on child protection, which would synchronise regulatory efforts and reduce inconsistencies. Dutch authorities could use their expertise in investigating algorithmic exploitation and manipulative practices to guide the methodologies of this body, ensuring consistent and effective enforcement across Member States.[clxxxiv]

Another innovative path is integrating child rights frameworks, such as UNICEF's guidelines,[clxxxv] into EU regulatory strategies. Dutch regulators could establish regulatory sandboxes to test child-friendly technologies, aligning with human rights principles while fostering innovation. Coupling these initiatives with financial incentives for ethical innovation, such as grants or tax benefits, would attract developers committed to prioritising children's digital rights.[clxxxvi]

Finally, cross-border enforcement could benefit from Dutch-led initiatives in data sharing. By spearheading secure and interoperable data-sharing mechanisms for investigating manipulative practices, the Netherlands could enhance the enforceability of EU rules. This collaborative model would underscore the Netherlands' ability to harmonise local expertise with EU priorities, ensuring high accountability and transparency across digital platforms. [clxxxvii] Through these multifaceted approaches, the Netherlands can solidify its position as a thought leader, influencing the evolution of digital fairness at both national and EU levels.

4.4 ALGORITHMIC TRANSPARENCY & SYSTEM ACCOUNTABILITY IN DUTCH LAW

The increasing sophistication of AI-driven personalisation poses significant regulatory challenges, particularly in safeguarding vulnerable groups like children. Dutch regulatory frameworks, renowned for their consumer-centric focus, are uniquely positioned to adapt and lead in overseeing algorithmic transparency and systemic accountability. Leveraging existing laws, the Netherlands can innovate enforcement mechanisms and align with EU-wide efforts to address the risks inherent in these technologies.

Dutch regulators can expand the principles embedded in the Mediawet to ensure algorithmic transparency in AI-driven personalisation. The Mediawet's focus on transparency in advertising and age-appropriate content provides a strong foundation for extending similar requirements to personalisation algorithms. For instance, regulators could mandate platforms targeting Dutch audiences to disclose the parameters influencing algorithmic decisions, such as ranking or recommendation criteria. This transparency would empower consumers, particularly children and guardians, to understand and challenge manipulative practices.[clxxxviii]

To ensure systemic accountability, the Netherlands could introduce mandatory algorithmic auditing frameworks. These audits would evaluate AI systems' fairness, safety, and compliance with national and EU regulations. Dutch regulators could draw on methodologies developed for financial and data protection audits, ensuring that AI audits are robust and impartial. This approach would align with broader EU initiatives under regulations like the AI Act, creating a harmonised framework for oversight.[clxxxix]

AI-driven personalisation often exploits behavioural data, amplifying vulnerabilities, particularly among children. Dutch law can adapt by instituting stricter data collection and usage controls in personalisation systems. Provisions from the GDPR, as implemented in the Netherlands, already impose data minimisation and purpose limitation requirements. Dutch lawmakers could extend these provisions to prohibit using sensitive behavioural data in personalisation targeting minors, ensuring that AI systems prioritise user welfare over engagement metrics.[cxc]

Enforcement remains a critical challenge in overseeing complex algorithmic systems. The Netherlands could pioneer the use of AI tools to monitor compliance dynamically. Dutch regulators could enhance their enforcement capabilities by deploying AI systems to analyse and flag potential instances of bias, discrimination, or manipulation in real-time. This proactive approach would ensure that regulators can respond swiftly to violations, preventing harm before it occurs.[cxci]

Collaborative governance offers another avenue for advancing accountability. Dutch regulators could establish multi-stakeholder forums to bring together industry leaders, consumer advocates, and academic experts to co-develop guidelines and best practices for algorithmic transparency. These forums could serve as innovation hubs, enabling the Netherlands to influence EU-level discussions while ensuring that national standards remain adaptable and forward-looking.[cxcii]

Finally, integrating a child rights framework into AI oversight could enhance protections for young users. Drawing on principles from UNICEF's AI policy guidelines[cxciii], Dutch regulators could require platforms to demonstrate how their personalisation systems adhere to child-centric design principles. Such requirements would ensure that algorithms operate in ways that respect children's autonomy and developmental needs. Through these measures, the Netherlands can adapt its regulatory frameworks to oversee AI-driven personalisation effectively, ensuring transparency and accountability while protecting the most vulnerable. This approach reinforces Dutch leadership and sets a benchmark for regulatory innovation at the EU level.

4.5 CHALLENGES IN HARMONISING DEFINITIONS OF MANIPULATIVE DESIGN

The effort to harmonise manipulative design definitions between Dutch and EU legal frameworks reveals significant challenges stemming from divergent terminologies, interpretations, and enforcement mechanisms. These discrepancies not only create legal ambiguities but also hinder effective regulation, particularly when addressing manipulative practices targeting children.

> *"A reciprocal flow of innovation between national and EU frameworks is essential to address the complexities of manipulative digital practices"*

In The Netherlands, regulations like the Mediawet[cxciv] provide a culturally embedded perspective on manipulative practices, focusing on age-appropriate content and transparent advertising standards. This culturally specific approach contrasts with EU-level frameworks, such as the DSA and the UCPD, which adopt broader, technology-neutral definitions. While the EU's approach aims for uniformity across Member States, it often lacks the specificity needed to address local regulatory priorities, such as protections tailored for children in the Dutch context.

One key area of divergence lies in the definition of dark patterns. Dutch law often references manipulative design as actions that exploit user vulnerabilities, such as misleading interface designs or coercive subscription traps. EU texts, however, lean on general terms like "unfair commercial practices" or "materially distorting consumer behaviour." These broader categories risk omitting subtler manipulative tactics, such as emotional manipulation through colour schemes or gamified features targeting minors. The absence of uniform definitions leads to inconsistent enforcement as regulators struggle to apply abstract EU standards to specific Dutch cases.[cxcv]

The "average consumer" versus "vulnerable groups" further complicates harmonisation. EU regulations frequently rely on the concept of the average consumer, presumed to possess a basic level of digital literacy. Dutch laws, by contrast, emphasise the protection of vulnerable users, including children, reflecting cultural and policy priorities. This misalignment makes it difficult to reconcile enforcement actions under both frameworks, particularly in cases involving exploitative designs aimed at children.[cxcvi]

Moreover, a unified glossary for manipulative design practices exacerbates legal ambiguities. Terms like "nudge," "coercion," and "dark pattern" often lack standardised definitions across Dutch and EU legal texts. For instance, while Dutch regulators might categorise loot boxes as manipulative, EU laws usually view them through the lens of transparency and disclosure obligations, leading to differing enforcement outcomes.[cxcvii]

Enforcement frameworks also reveal disparities. The Netherlands' strong emphasis on behavioural insights allows regulators to identify subtle manipulative tactics, whereas EU-level enforcement often relies on prescriptive measures like transparency requirements. This divergence risks creating loopholes that manipulative designs can exploit, as platforms operating across borders may adhere to minimal EU requirements while avoiding stricter Dutch standards.[cxcviii]

The Netherlands could propose an EU-wide taxonomy for manipulative design to address these challenges. This taxonomy would integrate Dutch specificity with EU uniformity, covering a spectrum of manipulative practices from overt coercion to subtle emotional manipulation. Furthermore, Dutch regulators could advocate for an expanded definition of "vulnerable groups" in EU laws to explicitly include children, ensuring protections align with national priorities.[cxcix] Harmonisation efforts can bridge these gaps and create a more consistent and effective regulatory landscape, safeguarding consumers across jurisdictions while respecting national priorities.

4.6 EMPOWERING DUTCH REGULATORS IN TACKLING DARK PATTERNS

Strengthening Dutch regulators' enforcement mechanisms to combat dark patterns requires addressing the systemic challenges of manipulative digital designs. These practices, which exploit cognitive biases and behavioural vulnerabilities, disproportionately impact children and undermine consumer trust. Enhancing cross-agency coordination within the Netherlands offers a strategic path forward.

Dutch regulators like the Authority for Consumers and Markets have historically prioritised consumer protection through behavioural insights and proactive oversight. To combat dark patterns effectively, regulators must develop more sophisticated detection tools. AI-powered systems identifying manipulative design elements in real-time, such as hidden costs or default opt-ins, could augment their enforcement capabilities. Deploying these tools would not only increase efficiency but also ensure timely interventions.[cc]

Creating a specialised task force dedicated to digital fairness within existing regulatory bodies is crucial to improving enforcement. This task force could pool expertise from behavioural science, law, and technology to assess complex dark pattern cases. Its remit would include scrutinising interfaces for deceptive practices, evaluating systemic risks posed by manipulative design, and recommending legal action against non-compliant entities. Establishing such a unit aligns with EU-level priorities under the Digital Services Act while ensuring national contexts are addressed.[cci]

Cross-agency collaboration is essential to addressing dark patterns' multifaceted nature. By fostering partnerships with agencies overseeing data protection, media regulation, and consumer rights, the Netherlands can develop a cohesive approach to tackling digital manipulation. Collaborative frameworks could integrate insights from GDPR enforcement, leveraging data privacy violations as a complementary avenue to combat dark patterns targeting children.[ccii]

Empowering regulators also necessitates legislative support. The Netherlands could advocate for a robust EU-wide anti-circumvention clause in consumer law, explicitly targeting dark patterns. This clause would close legal loopholes companies exploit to avoid compliance, such as rebranding manipulative tactics under new guises. At the national level, incorporating detailed definitions of manipulative practices into existing laws like the Mediawet would provide regulators with more explicit enforcement guidelines.[cciii]

Consumer education initiatives must complement enforcement efforts. Informing parents and guardians about the risks associated with dark patterns in children's apps and online games can mitigate harm while increasing public support for regulatory actions. Dutch regulators could collaborate with educational institutions to integrate digital literacy programmes into school curricula, teaching children to recognise and resist manipulative designs.[cciv]

Finally, fostering international cooperation is critical to addressing cross-border challenges. The Netherlands could lead in EU forums, advocating for harmonised standards and shared enforcement tools to tackle dark patterns. Establishing joint investigations with other Member States and sharing best practices would enhance collective capabilities while ensuring a unified approach across the Single Market.[ccv] By strengthening enforcement mechanisms, enhancing cross-agency collaboration, and promoting consumer education, Dutch regulators can effectively address the challenges posed by dark patterns. These measures would reinforce The Netherlands' position as a leader in digital fairness, safeguarding its citizens while contributing to broader EU regulatory goals.

4.7 ADAPTIVE COMPLIANCE MECHANISMS FOR THE DUTCH MARKET

Scalable enforcement mechanisms are critical for aligning Dutch regulatory frameworks with evolving EU standards, particularly in the context of adaptive compliance. With its reputation for regulatory leadership, the Netherlands can pioneer innovative approaches to enhance enforcement capabilities while maintaining alignment with the broader objectives of EU law.

One approach is implementing a tiered compliance system, which prioritises resource allocation based on risk assessment. High-risk sectors, such as those involving AI-driven personalisation or targeting vulnerable groups, can be subject to intensified scrutiny and periodic audits. This method ensures efficient use of regulatory resources while addressing areas with the highest potential for harm, particularly to children and other vulnerable populations.[ccvi]

Data-sharing mechanisms between Dutch regulators and their EU counterparts offer another solution to streamline enforcement. By creating interoperable data platforms, Dutch authorities could access shared databases to track compliance trends and flag violations. Such mechanisms would enable real-time monitoring and foster cross-border collaboration, reducing redundancies and enhancing the overall effectiveness of enforcement across jurisdictions.[ccvii]

The integration of AI-driven tools for compliance monitoring further strengthens enforcement capacities. Automated systems that analyse large datasets can identify patterns indicative of non-compliance, such as deploying dark patterns or algorithmic discrimination. These tools can supplement human oversight, ensuring faster and more accurate responses to emerging issues in digital markets.[ccviii]

Cross-agency collaboration within the Netherlands is essential for adaptive compliance. Regulatory bodies such as the Authority for Consumers and Markets and the Dutch Data Protection Authority must coordinate efforts to address multifaceted challenges. Joint task forces or inter-agency agreements could harmonise enforcement actions and reduce jurisdictional overlaps, thereby enhancing the coherence of the Dutch regulatory approach.[ccix]

Legislative adaptations are also necessary. Dutch lawmakers could advocate for incorporating adaptive compliance clauses into EU directives, allowing Member States to implement context-specific measures without deviating from overarching EU standards. This flexibility would empower Dutch regulators to address unique market dynamics while remaining aligned with EU objectives.[ccx]

> "The tension between national specificities and the EU's technology-neutral approach highlights the need for harmonised yet adaptable regulatory frameworks to protect children in the digital age."

Consumer education initiatives play a complementary role in adaptive compliance. Informing businesses about regulatory expectations and consumers' rights helps build a culture of compliance and accountability. Dutch regulators could develop digital platforms or interactive tools to disseminate this information effectively, promoting voluntary compliance and reducing the enforcement burden.[ccxi]

Finally, the Netherlands could lead efforts to establish EU-wide benchmarks for compliance assessment. These benchmarks would standardise expectations across Member States while allowing for local variations in enforcement strategies. Such an approach ensures consistency in protecting consumers and maintaining market integrity, aligning Dutch efforts with EU-wide goals.[ccxii] Through these strategies, the Netherlands can enhance its enforcement mechanisms to align with EU standards, ensuring scalable and adaptive compliance that addresses the complexities of modern digital markets.

4.8 CULTURAL AND LEGAL DIVERGENCES IN CONSUMER PROTECTION

Implementing child-specific consumer protections across EU Member States highlights critical cultural and legal divergences that challenge harmonisation efforts. While the EU mandates overarching frameworks like the UCPD, Member States interpret and enforce these rules through local cultural norms and legal traditions. This divergence complicates the consistent application of child-specific protections, as regional variations in values and priorities influence enforcement.[ccxiii]

The Netherlands, for instance, integrates vital behavioural insights into its regulatory approach, focusing on nudges and manipulative designs targeting children. By leveraging behavioural economics, Dutch law prioritises protections against exploitative commercial practices, such as deceptive in-app purchases. This focus on specificity contrasts with broader EU directives, which tend to employ generalised language and assume a uniform consumer profile, thereby overlooking the specific needs of vulnerable groups like children.[ccxiv] Differences also emerge in the interpretation of key terms. For example, the term "dark patterns" lacks a universally accepted definition across Member States, leading to varied enforcement. In countries like The Netherlands, regulators view dark patterns as systemic manipulations requiring robust oversight. At the same time, authorities in other jurisdictions might categorise such practices under broader notions of unfair commercial behaviour, diluting their specific impact on children.[ccxv]

> "The Netherlands' integration of behavioural insights into regulatory tools demonstrates how localised approaches can drive effective protections against algorithmic manipulation."

Enforcement mechanisms further illustrate these disparities. The EU promotes cooperation through instruments like the Consumer Protection Cooperation Network, but national authorities often apply these tools unevenly. In the Netherlands, proactive investigations and public awareness campaigns underpin enforcement, yet neighbouring countries may lack the institutional capacity or cultural prioritisation to replicate these measures effectively. This uneven enforcement undermines the EU's objective of creating a consistent regulatory environment.[ccxvi]

Cultural attitudes towards consumer agencies also play a significant role. In some Member States, individual responsibility is emphasised, with protections focusing on enhancing transparency and consumer education. Conversely, the Dutch approach leans towards pre-emptive intervention, where regulators enforce strict design standards to shield children from exposure to harmful digital environments. Such differences underscore the challenges of aligning regulatory philosophies under a single EU framework.[ccxvii]

The rise of cross-border digital services exacerbates these inconsistencies. Platforms operating in multiple jurisdictions often exploit regulatory gaps, adhering only to the minimum standards of less stringent Member States. This problem is especially pronounced in child-targeted sectors like gaming and social media, where companies can evade stricter Dutch regulations by basing operations in countries with weaker enforcement frameworks.[ccxviii]

Addressing these divergences requires an EU-wide commitment to refining and harmonising definitions, enforcement strategies, and compliance mechanisms. The Netherlands could advocate for a child-centric regulatory taxonomy that bridges cultural differences while respecting national priorities. Moreover, leveraging technological solutions, such as AI-driven compliance tools, can help standardise enforcement across Member States, ensuring consistent protections for children regardless of jurisdiction.[ccxix] Addressing these cultural and legal discrepancies can strengthen the EU's regulatory framework, ensuring that child-specific protections are uniformly implemented and enforced across its Member States.

4.9 BEST PRACTICES IN PROACTIVE DESIGN INTERVENTIONS

Introducing fairness-by-design principles into Dutch law offers an opportunity to align with EU standards while enhancing protections in the digital environment. This approach mitigates manipulative practices and empowers consumers, particularly vulnerable groups like children, as opaque algorithms and personalised choice architectures increasingly influence digital interactions.

Fairness-by-design entails embedding proactive safeguards to prevent manipulative and harmful user interfaces in digital systems. Drawing on successful practices, such as the UK's Age-Appropriate Design Code[ccxx], Dutch regulators could enforce mandatory child-focused design standards. These include transparent interfaces and opt-out mechanisms for data collection, ensuring digital services prioritise children's best interests from the outset.[ccxxi] The EU's ongoing emphasis on combating dark patterns complements this approach. Dark patterns, ranging from misleading consent flows to coercive subscription models, significantly impact consumer autonomy. The Netherlands could mandate that platforms incorporate intuitive navigation paths and explicitly disclose the consequences of user actions. Such measures would align with EU directives like the UCPD, reinforcing consumer rights in digital interactions.[ccxxii]

Enforcement is crucial for operationalising fairness by design. Dutch regulators like the Authority for Consumers and Markets could adopt behavioural testing to identify non-compliant interfaces. Incorporating AI-driven audits would enhance the detection of subtle manipulative practices embedded in design elements. These audits could focus on misleading default settings or forced continuity mechanisms disproportionately affecting children.[ccxxiii] Cross-agency collaboration is vital to implement and enforce these principles effectively. Establishing partnerships between data protection authorities and consumer agencies would allow holistic compliance oversight. Leveraging insights from cases like TikTok, where privacy violations in design were flagged, could inform better enforcement strategies and deter similar practices.[ccxxiv] Policy integration is another avenue for fostering fairness. The Netherlands could advocate for specific legislative amendments at the EU level, such as requiring platforms to demonstrate compliance with fairness principles through design certifications. These certifications would evaluate interfaces for transparency, accessibility, and user-friendliness, focusing on protecting vulnerable users like children.[ccxxv] Consumer education also plays a critical role. Dutch authorities could launch public awareness campaigns highlighting manipulative digital practices and equipping users to navigate digital services safely. These initiatives would enhance digital literacy among parents and children, fostering resilience against exploitative designs.[ccxxvi]

"Dutch regulators' focus on fairness-by-design and algorithmic transparency could set a benchmark for child-centric digital governance across Europe."

To ensure scalability, the Netherlands could propose EU-wide harmonisation of fairness-by-design frameworks. Such harmonisation would include aligning definitions and enforcement mechanisms, allowing for consistent application across Member States. The Netherlands' leadership in integrating these standards could set a benchmark for others, promoting a unified digital fairness landscape across the EU.[ccxxvii] By adopting and refining fairness-by-design principles, the Netherlands can strengthen its regulatory framework, safeguarding consumers and fostering trust in digital systems. This proactive stance would enhance national protections and contribute to shaping a resilient, fair, and inclusive digital environment across the EU.

4.10 FUTURE-PROOFING DUTCH REGULATIONS IN A DIGITAL ECOSYSTEM

Future-proofing Dutch regulations in the rapidly evolving digital ecosystem requires an anticipatory legal framework that balances innovation with robust consumer protections, particularly for vulnerable groups like children. Emerging technologies, such as generative AI and immersive platforms, demand forward-looking strategies to align national law with EU objectives while addressing the unique characteristics of the Dutch digital market.[ccxxviii]

The Netherlands can lead by adopting a regulatory approach rooted in adaptability and principles of fairness by design. Anticipatory frameworks should embed safeguards at the design stage of digital systems, ensuring they operate transparently and ethically. For example, mandating proactive risk assessments for emerging technologies, such as AI-driven personalisation and automated decision-making, would ensure systems comply with GDPR and upcoming EU-level regulations like the AI Act.[ccxxix]

The key to this adaptability is integrating mechanisms that evolve with technological advances. Periodic legislative reviews, informed by cross-sectoral research, would allow Dutch regulations to pre-emptively address novel risks, such as deepfake misuse or algorithmic discrimination. Collaborations with academic and industry stakeholders could foster innovation while ensuring emerging technologies respect consumer rights and data protection.[ccxxx]

Interoperability and harmonisation with EU legal frameworks are vital. Dutch policymakers must align national initiatives, such as Mediawet protections against manipulative advertising, with broader EU objectives under directives like the Digital Services Act. Ensuring mutual reinforcement between these frameworks would streamline platform compliance while bolstering protections for Dutch consumers.[ccxxxi] Enforcement mechanisms must also evolve to accommodate the complexities of the digital ecosystem. Dutch regulators could leverage AI and big data analytics to monitor compliance dynamically, enabling real-time interventions against harmful practices. Tools such as automated detection of dark patterns or transparency audits for algorithmic processes would strengthen enforcement capacities, particularly in cross-border contexts.[ccxxxii]

Future-proofing also demands a child-centric perspective. As digital environments become increasingly immersive, the Netherlands should champion EU-level child rights provisions tailored to emerging technologies. Measures like mandatory default privacy settings, content moderation designed for minors, and restrictions on algorithmic profiling of children would ensure regulatory frameworks remain relevant and protective.[ccxxxiii] Consumer empowerment must accompany regulatory enforcement. Digital literacy programmes targeting parents and children would equip users with the tools to navigate complex digital interfaces. Such initiatives would complement regulatory efforts, fostering a digitally resilient society capable of identifying and resisting manipulative practices.[ccxxxiv]

Finally, fostering cross-border cooperation and alignment within the EU is critical. By advocating for a unified regulatory approach, the Netherlands can ensure that its anticipatory frameworks address domestic challenges and contribute to a coherent and comprehensive EU digital strategy. This dual focus strengthens national protections and the EU's collective capacity to govern the digital ecosystem.[ccxxxv] The Netherlands can position itself at the forefront of digital governance through an anticipatory, adaptive, and collaborative regulatory approach. This high-level strategy ensures a resilient and fair digital environment that protects its citizens while supporting innovation.

4.11 CONCLUSION

Section 4 has illuminated the intricate interplay between national and EU-level regulations in addressing the challenges posed by digital manipulation, particularly concerning protecting children. The Netherlands' proactive approach, grounded in its robust legal frameworks like the Mediawet and its alignment with EU directives, showcases its capacity to advance consumer protections. However, the analyses reveal persistent gaps that hinder harmonisation, such as divergent definitions, enforcement disparities, and the lack of unified compliance mechanisms across Member States. The discussion has underscored the importance of adaptive governance and fairness-by-design principles, highlighting how Dutch initiatives can guide EU-level strategies in combating manipulative design, algorithmic exploitation, and systemic opacity. Moreover, integrating child rights frameworks and leveraging technological tools like AI audits emerge as critical strategies for addressing future challenges. These measures, coupled with enhanced cross-border collaboration and a unified regulatory taxonomy, can ensure consistent protections for vulnerable groups while fostering innovation.

As the digital ecosystem evolves, the Netherlands stands at a crossroads: it must navigate the tension between maintaining its leadership in child-specific protection and adapting to broader EU objectives. Dutch regulators can influence a cohesive, forward-looking digital governance framework that aligns national priorities with EU ambitions by prioritising scalability, transparency, and systemic accountability.

Building on this comparative analysis, Section 5 focuses on the Dutch legal framework's operationalisation of these principles. It delves into how national laws, enforcement bodies, and judicial interpretations address deceptive design, with a particular emphasis on protecting minors in AI-driven environments. By examining practical measures such as consumer protection laws, GDPR enforcement, and advertising regulations, Section 5 provides a granular perspective on the Netherlands' capacity to translate policy ambitions into actionable safeguards, ensuring a safer digital space for children.

SECTION 5: THE NETHERLANDS

5.0 INTRODUCTION

Section 5 examines the Netherlands' contributions to regulating manipulative and deceptive digital practices, particularly those targeting vulnerable groups such as children. It explores the interplay between Dutch regulatory initiatives and broader EU frameworks, highlighting alignment and divergence. Dutch authorities, including the ACM and AP, have adopted enforcement measures that address systemic risks and align with EU directives such as the GDPR, UCPD, and the evolving AI Act while also addressing gaps in these frameworks. Dutch regulatory efforts often focus on reactive enforcement, responding to manipulative practices such as dark patterns, algorithmic profiling, and gamified interfaces that exploit cognitive vulnerabilities. These approaches underscore the challenges posed by system-level manipulations embedded in digital architectures. While reactive measures have been central to Dutch enforcement, there is increasing recognition of the need for proactive mechanisms, such as algorithmic audits and fairness-by-design principles, to anticipate and mitigate harm, particularly for children.

The section also addresses the enforcement challenges arising from jurisdictional and procedural complexities, particularly in the context of cross-border platforms. Mechanisms like the GDPR's one-stop-shop system often impede timely interventions, prompting Dutch regulators to advocate for decentralised enforcement powers and enhanced coordination among national authorities. These efforts highlight the tension between national innovation and the procedural constraints of EU harmonisation. Section 5 critically assesses Dutch regulatory strategies and their interaction with EU instruments. It provides a detailed perspective on the challenges and opportunities in addressing manipulative practices in digital systems. It underscores the importance of balancing immediate enforcement with long-term systemic reform to ensure robust protections for vulnerable users in a digitalised society.

5.1 OVERVIEW OF DUTCH LEGAL FRAMEWORKS ON DECEPTIVE DESIGN

The Dutch approach to addressing deceptive design targeting children demonstrates a nuanced interplay between national enforcement mechanisms and EU-level consumer protection laws. Key actors, including the ACM and the Autoriteit Persoonsgegevens (AP), operate within the constraints of overlapping regulatory frameworks, such as the UCPD[ccxxxvi], GDPR[ccxxxvii], and sector-specific directives like the DSA[ccxxxviii] and DMA[ccxxxix]. However, enforcement complexities arise from divergent interpretations and inconsistent application of these laws across jurisdictions, often leaving vulnerable groups, particularly children, inadequately protected.[ccxl]

The ACM, empowered by the Wet handhaving consumentenbescherming, enforces compliance with EU principles that aim to curb manipulative practices targeting children. Nevertheless, the UCPD's principle-based approach struggles to effectively address advanced algorithmic personalisation and dark patterns. Algorithmically driven nudges, for example, reveal gaps in the law's application, requiring the ACM to navigate these uncertainties within Dutch consumer markets. The emergence of immersive technologies further exacerbates these gaps, challenging traditional consumer protection models.[ccxli]

The ACM's regulatory efforts focus on children's heightened vulnerability to manipulative practices such as gamification, reward mechanisms, and exploitative marketing. Practices like loot boxes and in-app purchases exploit children's cognitive immaturity, leading to compulsive behaviours. The ACM and the SDT advocate embedding protections into digital design, stressing that transparency alone is insufficient. Their position underscores the importance of robust, harmonised EU-level standards to address systemic risks effectively.[ccxlii]

The GDPR introduces significant safeguards by mandating transparency and accountability in data processing, particularly for children. However, enforcement challenges persist in addressing nuanced manipulations within system architecture, such as covert tracking or predictive profiling. For instance, the AP's investigation into TikTok highlighted a failure to provide child-accessible information about data usage, resulting in a €750,000 fine. However, TikTok's subsequent relocation to Ireland transferred jurisdiction to the DPC, illustrating procedural inefficiencies under GDPR's one-stop-shop mechanism and raising concerns about effective cross-border enforcement.[ccxliii]

The DSA further complements the GDPR by establishing stricter obligations for platforms to ensure safer digital environments for minors. These include provisions to combat manipulative interfaces and behavioural targeting—however, resource constraints at the national level limit enforcement bodies like the AP in overseeing compliance. Meanwhile, the ACM's advocacy for prohibitions on in-game currencies and addictive game mechanics, particularly those targeting children, reflects a proactive stance in addressing harmful commercial practices.[ccxliv]

Advertising codes within the Mediawet also provide specific protections for children, such as prohibitions on product placement in children's content. Nevertheless, the rapid development of AI-driven personalised content challenges the applicability of these frameworks. Generative AI technologies and algorithmic curation systems introduce dynamic risks that traditional laws are ill-equipped to address. Dutch regulators have called for updating these provisions to safeguard minors effectively.[ccxlv]

The upcoming AI Act introduces new oversight layers, particularly for high-risk AI systems. However, concerns persist about the extended transition periods and the lack of child-specific standards in the interim. Dutch regulators, including the ACM and AP, emphasise the urgent need for robust AI product standards and algorithmic transparency measures to address inherent biases and discriminatory profiling in systems affecting children. The AI Act's implementation within the Dutch regulatory framework underscores the need for accelerated timelines and practical enforcement mechanisms.[ccxlvi]

Although these frameworks provide a comprehensive basis for addressing deceptive design targeting children, enforcement still needs to be more cohesive due to jurisdictional and resource-related challenges. Initiatives such as algorithm registration and investments in AI literacy aim to enhance transparency and accountability. These measures are critical for ensuring that public and private sector stakeholders uphold protections for minors in an evolving digital landscape.[ccxlvii]

5.2 CONSUMER PROTECTION AND VULNERABLE USERS

Dutch consumer protection laws protect vulnerable users, particularly minors, against misleading practices and exploitative tactics in an increasingly digitalised marketplace. At the core of this framework lies the UCPD, as implemented in Dutch law, which prohibits misleading and aggressive commercial practices. The prohibition on directly pressuring children to make purchases serves as a critical safeguard, particularly in contexts such as online gaming and targeted advertising, where minors are highly susceptible to manipulation. Dutch regulators emphasise that practices like embedding purchase prompts in games exploit children's inability to understand the financial implications of their actions thoroughly. This legal framework aligns with the GDPR, which restricts the processing of children's data for targeted marketing purposes without demonstrable safeguards that prioritise the child's best interests.[ccxlviii]

The AP plays a significant role in ensuring compliance with data protection laws, particularly concerning minors' data. The AP has highlighted instances where platforms like TikTok failed to present age-appropriate privacy policies, leading to fines and regulatory scrutiny.[ccxlix] These enforcement actions underline the need for clear, accessible information to enable children and their guardians to make informed data-sharing choices. Dutch law extends beyond the GDPR by incorporating provisions explicitly addressing children's vulnerabilities. For instance, profiling minors for behavioural advertising is generally deemed incompatible with the GDPR's requirements and Dutch implementations of consumer law principles. However, enforcement gaps persist, particularly in cases involving cross-border platforms where jurisdictional complexities arise.[ccl]

The ACM also actively targets manipulative practices through its authority under the Wet handhaving consumentenbescherming, including efforts to address dark patterns in user interfaces. These practices involve default settings that encourage unnecessary spending or data sharing. The ACM's approach integrates behavioural insights, recognising that children are particularly vulnerable to these subtle forms of manipulation. For example, platforms often use mechanisms like countdown timers and rewards for in-app purchases to exploit children's psychological need for inclusion and immediate gratification. The ACM has developed guidelines for digital services, advising companies to eliminate these exploitative tactics and design interfaces that promote informed decision-making.[ccli] Despite this, the rapid evolution of AI-driven personalisation challenges the applicability of existing legal frameworks, necessitating continual updates to guidance and enforcement priorities.[cclii]

Advertising codes under the Mediawet further bolster protections for children. These include prohibitions on product placement and aggressive marketing tactics in content aimed at minors. However, the rise of user-generated content and influencer marketing complicates enforcement. Platforms often fail to adequately label sponsored content, exposing children to covert advertising that exploits their limited ability to distinguish between genuine endorsements and commercial interests. The Samenwerkingsplatform Digitale Toezichthouders (SDT), comprising the AP, ACM, and other regulatory bodies, collaborates to address these issues by issuing joint guidelines and promoting proactive compliance within the advertising and tech industries.[ccliii]

Efforts to enhance consumer protection extend to legislative proposals, which should harmonise child-focused safeguards across the EU. Dutch regulators advocate incorporating behavioural testing requirements and ensuring algorithmic transparency to mitigate manipulative tactics targeting minors. While these proposals represent a significant step forward, their effectiveness will depend on resolving jurisdictional challenges and providing adequate resources for enforcement. Regulatory bodies like the ACM and AP consistently stress the importance of integrating children's rights into the design and governance of digital services, underscoring the need for a holistic approach to consumer protection that bridges existing gaps (9, 10).

5.3 DATA PROTECTION AND AI REGULATION

The evolving Dutch framework for data protection reflects the growing tension between rapid technological advancements and the existing regulatory mechanisms. At the core of this framework is the AP, which leverages the GDPR to address manipulative practices targeting children. Article 12 of the GDPR demands transparency in providing information about data processing, particularly in child-accessible language. However, transparency alone is insufficient when AI systems exploit children's vulnerabilities through predictive profiling or behavioural nudging. Dutch regulators recognise these limitations, emphasising the need for systems that pre-emptively embed safeguards against exploitation rather than relying solely on after-the-fact enforcement.[ccliv]

AI-driven manipulative practices have brought new complexities to regulatory enforcement. The AP has identified specific instances where AI systems use extensive behavioural profiling, capturing sensitive data from minors to predict and influence their actions. For example, algorithms within educational apps often collect granular data to personalise learning but simultaneously create risks of profiling that could negatively shape a child's educational opportunities. Such systems challenge the traditional principles of fairness and non-discrimination enshrined in GDPR Article 5(1). The AP's recent guidelines urge the development of algorithmic impact assessments tailored to minors, highlighting the need to assess risks before deploying these systems.[cclv]

Implementing AI systems in children-focused sectors such as education, gaming, and social platforms has exposed gaps in current protections. Profiling under GDPR Article 22, while heavily restricted, is often circumvented through consent mechanisms that fail to reflect the cognitive capabilities of children. Dutch regulators have advocated for stricter interpretations of what constitutes valid consent, particularly in contexts where manipulative interfaces pressure minors into data-sharing agreements. Initiatives like algorithm registration—where organisations document and justify their use of AI systems—have been proposed as a critical step towards enhancing accountability and transparency.[cclvi]

The AI Act introduces additional safeguards by categorising high-risk systems and imposing obligations on developers to ensure compliance with ethical and legal standards. However, Dutch regulators have voiced concerns about the extended transition periods, which leave children exposed to high-risk AI systems with minimal oversight. The AP has pushed for expedited enforcement timelines and the inclusion of child-specific safeguards to address issues such as covert tracking and discriminatory algorithmic outputs. Current examples highlight how gaps in oversight can allow systemic risks to proliferate, particularly in cross-border applications of AI technologies.[cclvii]

Coordination between Dutch regulators is central to addressing these challenges. The Samenwerkingsplatform Digitale Toezichthouders, encompassing the AP, ACM, and others, provides a unified approach to regulating AI and data-driven manipulative practices. Their collaborative guidelines stress the importance of designing child-centric AI systems that actively mitigate risks such as excessive data collection and nudging behaviours. For instance, regulators have instructed game developers to avoid techniques that exploit children's desires for social inclusion or achievements, often implemented through in-app purchases or gamification tactics.[cclviii]

Despite robust theoretical protections, the AP consistently highlights the challenges of operationalising these frameworks. The regulatory landscape in the Netherlands requires more significant investment in enforcement capacity, particularly as AI systems become more sophisticated and integrated across sectors. These efforts include expanding the scope of mandatory algorithm registration to include semi-public organisations and implementing AI-specific literacy programs to raise awareness among developers, educators, and parents alike. As the digital ecosystem grows more complex, Dutch regulators stress the urgency of embedding child protections into the very foundations of AI governance frameworks.[cclix]

5.4 MEDIA AND ADVERTISING STANDARDS FOR MINORS

The Media Act (Mediawet) and the Code for Advertising Targeting Children[cclx] collectively serve as a robust framework for protecting minors from manipulative advertising practices in the Netherlands. The Media Act establishes a foundational legal basis for audiovisual content regulation, while the Advertising Code provides industry-specific guidelines tailored to children's vulnerabilities in digital environments. Together, they represent a concerted effort to address traditional and emerging advertising forms that exploit children's limited cognitive and emotional maturity.

The Media Act is integral to regulating the broadcasting and digital content accessible to minors. Article 3 mandates that audiovisual content targeting children should not include explicit product placement, surreptitious advertising, or any form of embedded marketing likely to mislead. Additionally, it requires broadcasters to maintain a clear demarcation between content and advertising, thereby ensuring children can differentiate promotional content from entertainment or educational material.[cclxi] Platforms operating in the Netherlands must comply with these stipulations to avoid embedding deceptive elements into their media offerings. The Act also addresses the digital transformation of media consumption. With the rise of streaming platforms and on-demand content, the Media Authority has interpreted these provisions to include digital content services accessible to children. Provisions such as mandatory sponsor disclosures aim to curtail the covert promotion of goods and services in children's programming. However, enforcing these rules in online contexts, especially on global platforms, remains a significant challenge due to jurisdictional and technical complexities.[cclxii]

The Code for Advertising Targeting Children builds upon the Media Act's principles by explicitly targeting manipulative digital marketing practices. One of its cornerstones is the prohibition against behavioural targeting and profiling of children. AI-driven personalised advertising, which exploits minors' browsing habits and inferred preferences, is deemed incompatible with the ethical guidelines under the code. Advertisements cannot leverage psychological tactics that exploit insecurities or social desirability biases, such as portraying a product as essential for peer acceptance.[cclxiii] Interactive advertising, such as gamified ads within apps or digital games, is another focal point. The code stipulates that these ads must communicate their commercial intent and avoid exploiting children's impulsive decision-making tendencies. Regulators scrutinise practices like bundling in-game rewards with real-world purchases for their manipulative potential.

The convergence of traditional and digital advertising presents enforcement hurdles. Influencer marketing, for instance, often blurs the lines between personal endorsement and commercial promotion. While the code requires influencers to disclose paid partnerships conspicuously, variability in enforcement across platforms and regions complicates regulatory efforts. These challenges underscore the need for harmonised EU standards that align with the Media Act's objectives while addressing the unique issues posed by digital platforms. As digital technologies evolve, the Media Act and the Advertising Code will need periodic updates to address new forms of media manipulation. For example, Generative AI and augmented reality introduce unprecedented risks of creating hyper-targeted content that children may not recognise as advertising. The SDT has advocated for anticipatory regulation, urging the integration of child-centric ethical principles into the design and deployment of new media technologies. These measures are crucial to safeguarding minors in an increasingly immersive and algorithmically mediated MEDIA LANDSCAPE.[cclxiv]

5.5 ALGORITHMIC TRANSPARENCY AND ENFORCEMENT GAPS

Algorithmic transparency has emerged as a cornerstone of efforts to regulate AI systems, particularly those that influence minors' behaviour. However, enforcing transparency remains challenging due to the inherently opaque nature of many AI systems and the rapid pace of technological innovation. Using complex algorithms to personalise content, predict behaviours, and drive engagement introduces risks often challenging to identify and mitigate. As a result, enforcement gaps emerge, leaving minors vulnerable to exploitation and manipulation.

One major challenge is the opacity of algorithmic decision-making processes. Many AI systems, especially those used in digital platforms, rely on machine learning models that operate as "black boxes." These systems often make decisions—such as recommending content or targeting advertisements—without transparent or explainable logic. This lack of transparency can result in exposure to content or advertisements that exploit developmental vulnerabilities for minors. Dutch regulators, including the AP and ACM, have highlighted the risks of behavioural nudging, where algorithms subtly manipulate user choices, making it imperative that companies ensure their systems are comprehensible and auditable.

Another enforcement gap lies in the limited visibility regulators have in algorithmic operations. Platforms often claim proprietary rights or technical limitations to avoid disclosing details about their algorithms. As a result, authorities struggle to assess compliance with legal requirements such as those under the GDPR and the DSA. For example, Dutch regulators have emphasised the need for algorithmic impact assessments that account for the specific risks posed to children. These assessments must include details about how algorithms influence user behaviour and whether they perpetuate harmful biases or exploit psychological vulnerabilities. Nevertheless, enforcing such requirements needs to be more consistent across jurisdictions.[cclxv]

Algorithmic profiling further exacerbates these transparency issues. AI systems frequently create detailed profiles of minors based on their online activities and subsequently leverage them to deliver personalised content and advertisements. While GDPR provisions such as Articles 12 and 22 place strict limits on automated decision-making and profiling, the practical application of these rules requires improvement due to the difficulty of auditing complex algorithms. Profiling practices often evade detection, particularly when embedded in digital environments like games or social media platforms, where minors are encouraged to engage in activities that generate more data for these systems.[cclxvi]

Cross-border enforcement also presents significant challenges. Many platforms operate internationally, complicating jurisdictional oversight. While designed to streamline enforcement, the one-stop-shop mechanism under the GDPR has proven slow and inefficient in algorithmic transparency cases. Dutch regulators have called for more decentralised enforcement powers, enabling national authorities to address violations more directly. Such measures are necessary for platforms to avoid exploiting jurisdictional gaps to delay compliance or dilute regulatory obligations.[cclxvii]

Regulating opaque AI systems also requires balancing transparency with innovation. Dutch authorities have proposed the mandatory registration of algorithms used in high-risk sectors, including those affecting children. Such registries would enable regulators to monitor algorithmic operations more effectively and hold platforms accountable for harmful outcomes. However, achieving this balance is challenging, as platforms often resist such requirements, citing competitive disadvantages or technical infeasibility. To address these enforcement gaps, regulators emphasise the importance of proactive measures such as fairness testing and robust documentation of algorithmic systems. These measures aim to make AI systems more interpretable while ensuring they align with ethical and legal standards. As AI systems evolve, bridging the gap between technical opacity and regulatory oversight will be crucial to protecting minors from manipulative influences.

5.6 ROLE OF THE DUTCH ACM IN COMBATING DARK PATTERNS

The ACM is pivotal in addressing dark patterns, leveraging its enforcement powers under Dutch consumer law and EU frameworks like the UCPD and GDPR. Its primary focus is on manipulative practices that exploit cognitive biases, particularly in children. Through enforcement and guidelines, the ACM targets deceptive designs such as misleading subscription processes and gamified monetisation models that encourage compulsive behaviours in minors. These practices often violate fundamental principles of fairness and transparency embedded in regulatory frameworks.[cclxviii]

One key area of intervention has been prohibiting tactics such as countdown timers, which artificially create urgency, and loot boxes designed to obscure the costs of in-game purchases. These measures align with broader efforts to ensure transparency in digital environments frequented by minors. The ACM has emphasised that transparency alone is insufficient, advocating for more robust preventative measures to address systemic manipulation, including bans on personalised advertising and pricing strategies that exploit children's emotional vulnerabilities.[cclxix] Despite these advances, enforcement challenges persist. Platforms frequently exploit jurisdictional gaps and the complexity of algorithmic systems to evade compliance. The ACM has called for enhanced cross-border cooperation through the CPC network, stressing the need for harmonised standards to address digital manipulation effectively. The global nature of platforms amplifies the challenges, requiring regulators to navigate conflicts between national mandates and EU-wide frameworks.[cclxx] (5, 6).

Algorithmic transparency remains central to ACM's efforts. It advocates for mandatory audits and registries for high-risk systems, particularly those that shape user behaviour through profiling and nudging. Such measures are essential for ensuring algorithms operate within the bounds of fairness and accountability. By pushing for these measures, the ACM aims to proactively address risks rather than relying on reactive enforcement, especially in cases involving children, who are less equipped to navigate complex digital systems.[cclxxi]

Joint initiatives focus on embedding safeguards directly into the design of digital products, targeting practices like opaque pricing and personalised ads. These efforts align with broader EU initiatives, including the AI Act and guidelines from the EDPB.[cclxxii] However, gaps still need to be in translating these high-level principles into enforceable measures, particularly in rapidly evolving digital markets. As digital manipulation techniques become increasingly sophisticated, the ACM's role becomes increasingly critical. Its focus on systemic protections, cross-border cooperation, and proactive regulation highlights the evolving complexity of enforcing consumer protections in a digital landscape increasingly shaped by opaque AI systems.

5.7 GAPS IN CURRENT REGULATORY MECHANISMS

Gaps in current regulatory mechanisms addressing system-level manipulations reveal significant challenges, particularly in protecting children. While frameworks such as the GDPR, UCPD, and the AI Act establish broad protections, the complexity of digital ecosystems often renders enforcement inadequate. System-level manipulations, which integrate exploitative techniques into the architecture of platforms and services, remain a critical blind spot for regulators. These manipulations inherently embed themselves in the functionality and design of digital systems rather than manifesting as overt, rule-breaking behaviours, making them more complex to detect and regulate.

A critical gap lies in the limited scope of existing transparency requirements. While laws like the GDPR mandate clear and accessible information about data processing, they do not account for manipulative design choices that influence user behaviour before users explicitly consent. For instance, dark patterns in account registration processes may nudge children to share excessive personal data or subscribe to unwanted services. These subtle manipulations often operate below the threshold of current legal definitions of unfair practices, leaving children exposed to risks such as data exploitation and financial harm. The lack of regulatory clarity on manipulative architecture exacerbates enforcement challenges, allowing platforms to exploit these grey areas.

Another issue arises from the need for harmonised standards for algorithmic design and oversight. Algorithms that underpin system-level manipulations frequently operate without scrutiny, exploiting behavioural data to personalise content and optimise engagement. The AI Act seeks to address this by imposing obligations on high-risk systems, but its scope needs to encompass the nuanced risks posed to minors entirely. Furthermore, the long transition periods for implementing AI-specific regulations leave significant temporal gaps where children remain vulnerable. The ACM and other Dutch regulators have called for expedited timelines and more comprehensive requirements to address the specific risks of predictive profiling and behavioural nudging in children-focused services.

Cross-border enforcement poses another significant challenge. Platforms often exploit jurisdictional gaps to delay compliance or dilute regulatory obligations. While intended to streamline enforcement, the one-stop-shop mechanism under the GDPR has proven ineffective in cases involving cross-border system-level manipulations. This inefficiency is particularly problematic for global platforms that design systems that influence user behaviour across multiple jurisdictions. Dutch regulators have advocated for reforms that decentralise enforcement capabilities, enabling national authorities to act more decisively against harmful practices targeting children.

The lack of pre-emptive regulation further exacerbates vulnerabilities. Most existing frameworks rely on reactive enforcement, addressing harm only after it has occurred. Such reliance proves insufficient in the face of rapidly evolving technologies that enable system-level manipulations. Dutch regulators have proposed mandatory algorithm registration and behavioural impact assessments as tools to identify and mitigate risks pre-emptively. These measures would allow for better oversight of how algorithms influence behaviour, particularly in contexts like gaming and social media, where companies aim disproportionate targeting efforts at minors.

Addressing these regulatory gaps requires a shift toward anticipatory and systemic approaches. Strengthening collaboration between regulators, introducing child-centric design principles into platform architecture, and expanding the scope of existing laws are critical steps. These measures are necessary because the inherent opacity of system-level manipulations continues to outpace regulatory efforts, leaving children exposed to digital harms that current frameworks are unprepared to address.

5.8 COMPARATIVE APPROACHES: DUTCH AND EU INTERPLAY

The interplay between Dutch regulatory initiatives and broader EU frameworks reveals alignment and divergence, particularly in regulating manipulative practices and safeguarding vulnerable groups such as children. Dutch regulators, notably the ACM and the AP, frequently align their enforcement strategies with EU directives like the UCPD and GDPR. However, they also implement distinct, context-sensitive measures that extend beyond EU-level requirements, showcasing both the strengths and limitations of harmonisation efforts. Dutch enforcement efforts often exceed the foundational protections set out in EU frameworks. For example, the ACM has taken a proactive stance against dark patterns by targeting specific manipulative practices like loot boxes and gamified monetisation strategies, which are prevalent in digital gaming environments targeting minors. These practices exploit psychological vulnerabilities, such as the impulse for reward-seeking behaviour, and EU-level consumer protection laws do not explicitly address them. In contrast, the UCPD's principle-based prohibitions against unfair commercial practices lack the specificity to address such design-focused manipulations comprehensively.[cclxxiii]

The GDPR provides harmonised rules on data protection, yet Dutch regulators have interpreted its provisions expansively, particularly concerning minors' rights. The AP has taken significant action to penalise platforms that fail to provide privacy information in age-appropriate formats. This enforcement demonstrates a solid commitment to child-centric protections and highlights gaps in broader EU-level approaches, which often overlook the specific needs of minors in rapidly evolving digital contexts.[cclxxiv] The AI Act complements these efforts by proposing harmonised rules for high-risk AI systems, particularly those with significant societal impacts. However, Dutch regulators have expressed concerns over its implementation timelines and limited focus on child-specific risks. The ACM has called for immediate measures to regulate algorithms in education and social media sectors, where children are disproportionately affected by behavioural nudging and predictive profiling. This divergence illustrates the tension between the EU's broader legislative timelines and the urgency of Dutch enforcement priorities.

Cross-border enforcement further complicates this regulatory interplay. Mechanisms like the GDPR's one-stop-shop aim to streamline oversight but often result in procedural delays, particularly in cases involving multinational platforms. These delays frustrate Dutch regulators, who have advocated for decentralised enforcement powers to address violations more efficiently. This tension underscores the need for a regulatory framework that balances harmonised EU standards with localised enforcement to ensure timely and effective interventions.[cclxxv]

Despite these challenges, Dutch authorities actively contribute to shaping EU policy. During the EU's Digital Fairness Fitness Check, the ACM's input reflects the Netherlands' commitment to aligning national efforts with broader EU objectives while advocating for stricter consumer protections. Such contributions underscore the dynamic interplay between national innovation and EU harmonisation, ensuring that both levels of governance address shared challenges effectively and adapt to the complexities of digital markets.

5.9 TOWARDS A CHILD-CENTRIC DIGITAL FAIRNESS FRAMEWORK

The Netherlands has emerged as a frontrunner in integrating behavioural science into digital regulatory frameworks, leveraging empirical insights into human cognition to counteract digital manipulation, particularly where vulnerable groups such as children are concerned. Dutch regulatory authorities—most notably the Authority for Consumers and Markets (ACM) and the Autoriteit Persoonsgegevens (AP)—have pioneered an approach that extends beyond traditional enforcement mechanisms, embedding fairness-by-design principles directly into the architecture of digital systems. This anticipatory model seeks to pre-empt manipulative design tactics before they materialise, ensuring that digital environments are structured to protect rather than exploit users' cognitive vulnerabilities.

At the core of this regulatory strategy is a behaviourally informed approach to deceptive design, acknowledging that dark patterns and related manipulative practices disproportionately affect users with heightened psychological susceptibility, such as children. Dutch regulators have focused on the cognitive and developmental characteristics that render minors particularly vulnerable—including their susceptibility to social proof, preference for immediate gratification, and tendency to defer to perceived authority—and have used these insights to craft regulatory interventions that directly address these exploitative mechanisms. For instance, ACM's prohibition of loot boxes in gaming and its advocacy for eliminating misleading countdown timers reflects a broader commitment to aligning platform design with consumer welfare rather than commercial exploitation.

A critical distinction between conventional consumer protection measures and the Dutch approach is the recognition that fairness-by-design must extend beyond banning overtly manipulative practices to address more insidious, system-level forms of influence. Many deceptive techniques operate below the user interface, embedded within algorithmic decision-making processes and system architectures that dynamically manipulate user behaviour at an imperceptible level. Dutch regulators have therefore emphasised the need for substantive, rather than procedural, transparency obligations, particularly in child-facing digital environments. This entails moving beyond superficial compliance mechanisms, such as lengthy and legally dense privacy notices, towards age-appropriate, cognitively accessible disclosures that enhance user understanding. The AP's enforcement actions against platforms failing to present information in a child-comprehensible manner exemplify this commitment to substantive, rather than performative, transparency.

In addition to ex post enforcement measures, the Dutch model significantly emphasises ex ante regulatory interventions, ensuring that digital services undergo robust scrutiny before deployment. This includes mandatory algorithmic audits and behavioural impact assessments, particularly for platforms that systematically target minors. Algorithmic audits assess whether platform architectures align with legal principles of fairness, transparency, and accountability, while behavioural impact assessments evaluate the psychological consequences of digital design choices. These measures represent a paradigm shift in digital governance, moving away from the reactive enforcement models that prevail in many jurisdictions toward a proactive regulatory strategy that mitigates harm before it occurs. Dutch regulators have further advocated for introducing algorithmic registries, requiring platforms to document, disclose, and justify high-risk digital systems, particularly those that shape children's online experiences through personalisation, predictive analytics, and engagement-maximisation techniques.

The Netherlands' behaviourally informed regulatory model provides a scalable and pragmatic blueprint for embedding fairness-by-design principles into EU-wide digital governance frameworks. By integrating cognitive science into regulatory decision-making, Dutch regulators are not merely responding to the immediate harms of manipulative design. Still, they are fundamentally reshaping the trajectory of digital governance to prioritise user autonomy, particularly for vulnerable demographics. This approach underscores the necessity of aligning digital regulation with empirical research on human decision-making, ensuring that consumer protection frameworks do not merely address exploitative tactics retrospectively but proactively mitigate their emergence.

However, achieving a harmonised, behaviourally informed approach at the EU level presents considerable challenges, particularly cross-border enforcement and regulatory harmonisation. Platforms across multiple jurisdictions frequently exploit regulatory asymmetries, leveraging inconsistent enforcement regimes to delay compliance or dilute obligations. Dutch regulators have, therefore, consistently advocated for stronger cooperation mechanisms between national enforcement bodies and EU-level regulatory authorities, ensuring that deceptive practices do not persist in regulatory blind spots. Notably, the Dutch push for decentralised but interoperable enforcement powers reflects an understanding that localised regulatory expertise must be preserved while ensuring cohesive cross-border coordination to prevent regulatory arbitrage.

The Netherlands is at the forefront of developing a regulatory paradigm that moves beyond traditional consumer protection toward anticipatory, architecture-focused governance by embedding behavioural insights into platform oversight, algorithmic accountability, and child-specific safeguards. This model offers a scalable, evidence-based framework for mitigating digital manipulation, ensuring that fairness-by-design becomes a foundational principle of future digital regulatory strategies. As deceptive design techniques become increasingly sophisticated, integrating behavioural science into regulatory decision-making will ensure that digital platforms foster autonomy rather than systematically undermining it, particularly for vulnerable groups such as children.

5.10 CONCLUSION

The Netherlands has demonstrated a robust yet complex approach to regulating manipulative and deceptive digital practices, balancing national innovation with EU-wide harmonisation efforts. While Dutch regulators, such as the ACM and AP, have made significant strides in addressing dark patterns and system-level manipulations, the emphasis has predominantly been reactive, addressing harm post-occurrence rather than pre-emptively embedding fairness into system design. This reactive approach underscores the limitations of existing frameworks like the GDPR, UCPD, and Media Act, which, despite their strengths, struggle to contend with the rapid evolution of AI-driven manipulations and system architecture complexities. Dutch authorities have frequently exceeded EU-level requirements by targeting specific manipulative practices, such as loot boxes and covert profiling in children's digital environments. However, systemic challenges remain, including jurisdictional hurdles, resource constraints, and procedural inefficiencies under mechanisms like the GDPR's one-stop-shop. These challenges highlight a critical need for more agile, child-centred regulatory measures anticipating emerging threats rather than merely responding to existing harms.

The interplay between Dutch innovation and EU harmonisation exemplifies the opportunities and constraints of multi-level governance in digital regulation. As the EU moves forward with initiatives like the AI Act, there is a compelling opportunity to integrate Dutch insights into broader frameworks. This integration could amplify protections for vulnerable users, particularly children while fostering a regulatory environment prioritising transparency, accountability, and fairness. Section 6 transitions from the Netherlands' national context to a broader examination of systemic regulatory challenges at the EU level. It explores the inadequacies in current frameworks, the enforcement complexities of cross-border digital ecosystems, and practical recommendations for embedding child-specific protections into EU legislation. by addressing these structural gaps, Section 6 proposes a cohesive vision for protecting minors across increasingly interconnected and algorithmically governed digital landscapes.

SECTION 6: FINDINGS

6.0 INTRODUCTION

Children are among the most vulnerable users in an increasingly complex digital environment, navigating platforms and services predominantly designed with adult consumers in mind. The rapid integration of artificial intelligence, personalised content, and engagement-maximisation techniques into digital systems has introduced unprecedented risks to minors, who often lack the cognitive maturity or digital literacy necessary to recognise manipulative online practices. Deceptive design tactics, commonly called "dark patterns," exploit children's inherent curiosity, trust, and limited decision-making capacity, creating digital environments that subtly coerce or influence their behaviour to serve commercial rather than user-centric interests. Addressing these challenges necessitates a forward-thinking regulatory approach that explicitly acknowledges the distinct vulnerabilities of young users and the broader societal implications of an evolving digital landscape. This section outlines targeted, evidence-based interventions designed to protect minors from manipulative design strategies, ensuring that digital spaces are structured in a manner that prioritises their well-being rather than their exploitation. Drawing on insights from the EU's Digital Fitness Check, these recommendations address gaps in the existing consumer protection framework, highlighting areas where legal reform is urgently required. As children engage with digital platforms at increasingly younger ages, the regulatory environment must evolve in parallel, ensuring that legislative protections remain robust, enforceable, and adaptable to emerging threats. The development of stronger, child-centric regulatory safeguards represents a crucial opportunity to establish protections that are not only comprehensive but also sufficiently flexible to account for the dynamic nature of digital manipulation, reflecting a deeper understanding of how digital platforms shape and, in many cases, systematically influence user behaviour.

Protecting Children in the Digital Age

☐ Analyses regulatory shortcomings in protecting children from manipulative digital practices, including deceptive system architecture, AI-driven personalisation, and engagement-maximisation techniques.

☐ Identifies key enforcement challenges across EU Member States, highlighting gaps in existing frameworks such as the GDPR, DSA, and DMA, particularly in addressing system-level manipulation and covert algorithmic influence.

☐ Examines deficiencies in current protections for children, emphasising the need for stronger legal safeguards against AI-driven persuasion, dark patterns, and exploitative engagement tactics.

☐ Proposes targeted regulatory interventions, including banning addictive design features, mandating algorithmic transparency, imposing fairness-by-design obligations, and strengthening cross-border enforcement mechanisms.

☐ Outlines a structured roadmap for integrating child-specific protections into EU digital legislation, ensuring that platforms are legally obligated to prioritise children's rights, autonomy, and digital well-being over commercial incentives.

A significant focus of this section lies in translating the findings of the Digital Fitness Check into actionable strategies that align with the specific needs of young users. While existing consumer protection regulations provide a foundational layer of safeguards, they were developed in a different regulatory era and fail to account for the complexities of today's AI-driven, hyper-personalised online experiences. This section explores the most effective mechanisms for bridging these gaps, drawing on established best practices from other jurisdictions and innovative regulatory approaches that reflect the EU's broader commitment to digital fairness and consumer rights. By examining consultations with key stakeholders—including child advocacy organisations, regulatory authorities, and industry representatives—this section identifies evidence-based recommendations for developing child-centred digital policies. Central to these proposals is the recognition that protecting minors requires more than technical safeguards; it necessitates a cohesive regulatory response capable of anticipating and adapting to emerging digital threats. For example, the proliferation of algorithmically curated content presents new challenges in ensuring that young users are not unduly influenced by personalisation mechanisms or exposed to potentially harmful material. Establishing enforceable standards for greater transparency in content personalisation and data usage would empower children and their guardians to make more informed decisions about digital interactions.

This section also underscores the need to regulate AI-driven personalisation techniques that target minors with tailored advertising, nudges, or engagement-maximisation strategies, raising critical questions about the ethical responsibilities of digital service providers and the long-term implications of these practices for child welfare and autonomy.

Additionally, this section examines the role of enforcement mechanisms in fostering a digital environment where children can participate safely. Key recommendations include strengthening cooperation between national and EU-level authorities to streamline enforcement and ensure that Member States apply regulatory standards consistently and effectively. This section also highlights the necessity of integrating an educational component within the broader regulatory framework, advocating for digital literacy initiatives that equip children with the critical skills to recognise and navigate manipulative design tactics. As these recommendations unfold, they aim to embed fairness and transparency into every aspect of digital design, ensuring that young users remain shielded from harmful influences and exploitative commercial strategies. A holistic approach is essential—one that incorporates preventative measures and enforceable standards to establish a regulatory ecosystem that protects young users today and evolves to address future digital challenges. These recommendations are integral to building a resilient and adaptive framework that aligns with the EU's broader digital ambitions, setting a precedent for safeguarding children's rights and well-being in an era of rapid technological transformation.

The primary objective of this section is to outline specific, evidence-based measures designed to enhance protections for minors against deceptive design techniques while also contributing to the broader discourse on regulatory reform. This research builds on the findings of the Digital Fitness Check, translating its broader insights into actionable, targeted interventions aimed at protecting children in an increasingly sophisticated digital landscape. As deceptive design tactics become more deeply embedded in AI-driven personalisation systems and system architectures, the urgency of implementing robust regulatory safeguards grows. Personalisation techniques, behavioural nudges, and engagement-maximisation mechanisms are increasingly integrated into digital services at a structural level, making their effects more difficult to detect and regulate. Identifying and implementing effective protective measures is therefore critical to ensuring that future regulatory frameworks remain adaptive and resilient against emerging digital threats, particularly those that exploit the vulnerabilities of young users.

6.1 THE INADEQUACY OF CURRENT EU DIGITAL DESIGN REGULATIONS

The EU's current digital design acquis, encompassing regulations such as the Digital Services Act (DSA), Digital Markets Act (DMA), UCPD, Data Act, and GDPR, cannot address the more profound, system-embedded deceptive design techniques that impact minors. While these instruments provide a foundational regulatory layer for visible dark patterns—such as misleading interface choices and coercive design elements— they fall short in tackling more insidious, non-visible manipulative practices embedded in digital services' system architecture and algorithmic processes.[cclxxvi]

At the interface level, user interface dark patterns are governed by various EU frameworks. The DSA, for instance, restricts specific online platforms from deploying manipulative designs that impair user autonomy. Similarly, the DMA uses dark patterns to restrict gatekeeper platforms that unfairly influence user decisions. Meanwhile, the GDPR's Article 25 calls for data protection by design and default, indirectly addressing dark patterns by mandating transparency and fairness in data handling practices. The UCPD further supports this framework by prohibiting business-to-consumer manipulative practices, and amendments to its blacklist now specifically mention several types of deceptive practices.[cclxxvii]

> *"The deeper problem lies with 'darker' and 'darkest' patterns—deceptive techniques embedded in system architecture and algorithmic processes, often undetected by surface-level regulations.”*

However, as scholars have pointed out, these frameworks primarily focus on manipulations at the user interface (UI) level, which are readily observable and enforceable. The deeper problem lies with "darker" and "darkest" patterns—deceptive techniques that operate within the system architecture and algorithmic logic, going undetected by surface-level regulations and standard auditing. These can include the design of recommendation algorithms that subtly exploit cognitive biases, creating hyper-nudging effects that guide young users' choices in difficult-to-detect or counteract ways. Deterministic algorithms, for instance, can craft specific outcomes by analysing individual behavioural patterns, while stochastic algorithms introduce unpredictability that makes even expert evaluation challenging.[cclxxviii]

In the context of protecting minors, this gap in regulatory scope is especially concerning. Children lacking the cognitive development to understand and resist such manipulative tactics are particularly vulnerable. Current regulatory instruments do not extend far enough to enforce meaningful protections against these "systemic" forms of manipulation, which often exploit vulnerabilities related to age, social environment, and economic circumstances. The EU's AI Act addresses some aspects of these deeper manipulations by prohibiting certain AI practices that target vulnerable populations, including children. However, the criteria for enforcement under this Act—such as the demonstration of "significant harm" or "material distortion" of a user's behaviour—set a high threshold that may fail to capture many of the subtle yet cumulatively harmful effects of these manipulations.[cclxxix] Expanding regulatory oversight to encompass system architecture and algorithmic logic ensures that protections extend beyond visible user interfaces to the deeper, often imperceptible mechanisms that shape user experiences and influence decision-making. Many manipulative practices operate at the system level, where deterministic and stochastic processes dynamically adjust content, interactions, and engagement strategies based on behavioural data. Addressing these forms of manipulation requires a regulatory approach that integrates transparency obligations with robust enforcement mechanisms, ensuring that platforms disclose their interface-level tactics and underlying algorithmic structures that drive them. Without such measures, deceptive design will continue to evolve in ways that evade traditional UI-focused regulatory interventions. Achieving meaningful digital fairness for minors necessitates a multifaceted strategy that blends preventative safeguards with corrective enforcement mechanisms, moving beyond the scope of existing consumer protection regulations. The limitations of current regulatory frameworks—many designed in an era before AI-driven personalisation and engagement-maximisation techniques became dominant—underscore the urgency of adapting legal instruments to reflect the realities of modern digital environments. The following table presents a comparative analysis of key EU regulatory acts relevant to dark patterns, particularly those likely to affect children. It examines each regulation's focus areas, strengths, limitations, and applicability to deceptive design practices, offering a comprehensive overview of how existing legal instruments intersect with the challenges posed by manipulative digital architectures:

Table 6.1: The EU Framework for Regulating Deceptive Design

Regulation	Focus Areas	Strengths	Limitations	Applicability to Deceptive Design
GDPR	Data protection, privacy, transparency, and user consent	Strong privacy protections; accountability in data handling; user autonomy via consent	Primarily focused on data privacy; limited in addressing manipulative design; high enforcement threshold	Addresses dark patterns indirectly through consent requirements; some deterrent against opaque data use
DSA	User safety, transparency, content moderation, and accountability on digital platforms	Targets large platforms; mandates risk assessment and reporting for user safety.	This only applies to user interface dark patterns, is limited to "online platforms," and is inconsistently enforced.	Limits regulation to the UI; manipulative designs on user choices; applicable to content moderation and UI
DMA	Fair competition and user protection with gatekeeper oversight	Imposes obligations on gatekeepers; promotes fair competition and user protection	Focused only on significant platforms; less impact on small or medium-sized entities	Reduces dark patterns by gatekeepers; curbs manipulative designs in large tech firms
UCPD	Consumer rights, prohibition of misleading practices, and B2C transaction transparency	Comprehensive consumer protections; supports informed choices; bans deceptive marketing.	Primarily covers visible manipulation (UI-level); lacks provisions for system-level manipulations.	Prohibits misleading B2C practices; addresses deceptive advertising and sales tactics
Data Act	Data access, sharing, & portability; rights over non-personal data; obligations for fair data use	Establishes more precise rules on data access and sharing, enhancing transparency and fairness in data-driven markets	Primarily focused on B2B and B2G data access; limited direct consumer protection provisions.	Indirect relevance—enhanced data access rights may improve transparency around data-driven manipulative practices but does not directly regulate

Regulation	Focus Areas	Strengths	Limitations	Applicability to Deceptive Design
				deceptive design
AI Act	Prevents psychological manipulation and exploitation of vulnerable groups by AI systems	Protects against AI-driven manipulative tactics; systemic approach to manipulation	High evidentiary thresholds; challenges in proving 'significant harm'; complex AI enforcement	Targets deceptive AI techniques; protects vulnerable groups; addresses systemic manipulations.

6.2 THE ENFORCEMENT CHALLENGE

Despite the increasing presence of regulatory frameworks addressing dark patterns, the enforcement landscape in the EU reveals substantial gaps and persistent challenges. Regulations such as the GDPR, DSA, DMA, Data Act, and UCPD collectively establish a legal foundation for overseeing manipulative design tactics. Yet, their enforcement remains inconsistent and often narrowly focused on interface-level manipulations. These frameworks largely overlook the more sophisticated deceptive techniques embedded within system architectures, including algorithm-driven hyper-nudging, behavioural personalisation, and manipulative decision architectures that operate beyond children's awareness.[cclxxx]

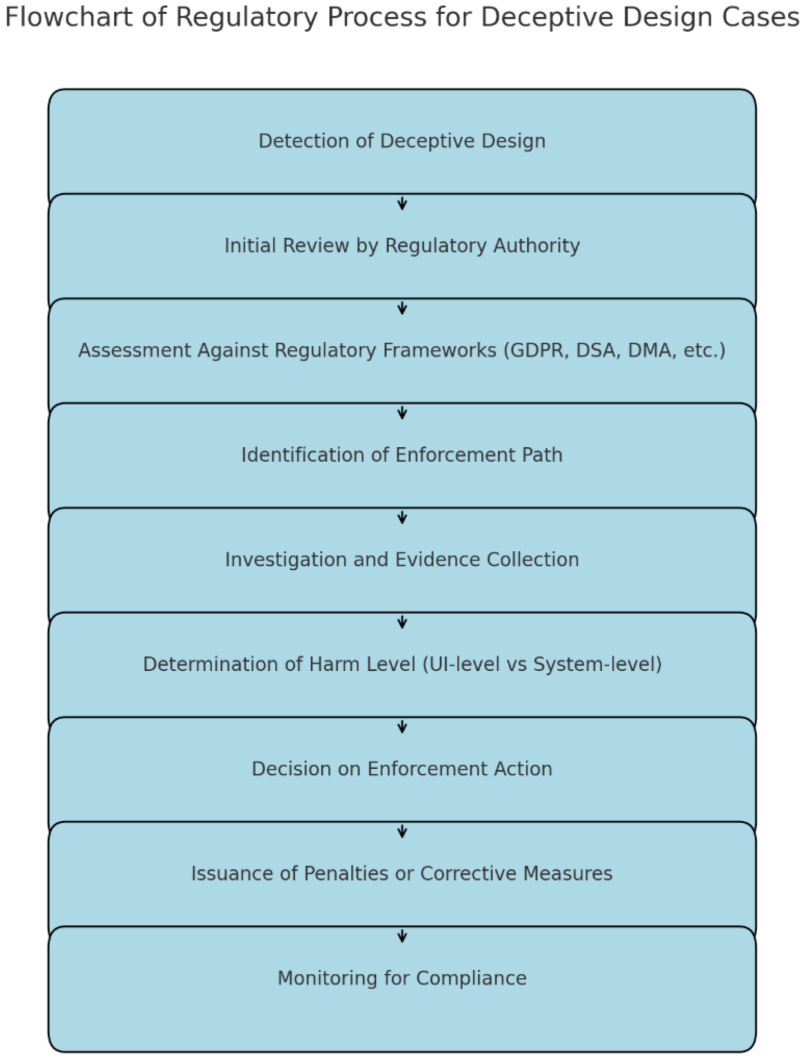
The lack of a cohesive, cross-regulatory approach is a critical shortcoming in the current enforcement landscape. While the GDPR indirectly addresses dark patterns through its principles of fairness, transparency, and data protection by design[cclxxxi], enforcement remains highly fragmented and disproportionately reliant on individual Member State Data Protection Authorities (DPAs), whose capacities and resources vary significantly. As a result, many manipulative data-driven practices escape meaningful scrutiny or penalties, allowing companies to continue deploying these tactics with minimal regulatory consequences.

As personalisation and automation increasingly dominate digital ecosystems, these enforcement challenges become even more pronounced. Dark patterns are no longer confined to UI-level manipulations; they are now deeply embedded within system logic, recommender algorithms, and behavioural prediction models. Traditional enforcement agencies often need more technical expertise, investigative tools, and cross-disciplinary resources to effectively detect, assess, and penalise these covert manipulations. For instance, despite the GDPR being in force since 2018, persistent enforcement gaps remain, as seen in the struggles of regulators such as the ACM (Authority for Consumers and Markets) and the Dutch DPA to implement meaningful interventions against companies that continue deploying manipulative practices. This issue is exacerbated by resource constraints, technical knowledge gaps, and the inherent difficulty of coordinating across multiple enforcement bodies, all hindering efforts to regulate complex, cross-border digital practices effectively.[cclxxxii]

The enforcement limitations are evident in cases where regulatory frameworks overlap but need to converge on a unified enforcement strategy. The UCPD, for example, is effective in prohibiting certain types of business-to-consumer manipulations. Still, it only covers dark patterns in transactional contexts, leaving many data-driven manipulations outside its scope. Similarly, the DSA and DMA establish rules for user protection in online platforms, targeting dark patterns that distort user choice. Still, their mandates primarily apply to platform-level or gatekeeper-level responsibilities rather than covering the full range of manipulative practices within digital service ecosystems. Furthermore, the DSA's requirement that platforms not use designs that "materially distort" user decision-making lacks precise definitions, creating ambiguity around which designs qualify as manipulative and how regulatory authorities can enforce these regulations. Despite regulatory frameworks, the persistence of UI dark patterns underscores a pressing need for reformed enforcement protocols that better reflect the complex realities of today's digital environments. One critical area for improvement lies in standardising definitions and enforcement practices across Member States to ensure that regulatory action is timely, consistent, and proportionate to the level of harm caused by dark patterns. This challenge grows as the high evidentiary thresholds required for enforcement make it difficult to act, particularly in cases where "significant harm" or "material distortion" must be demonstrated before regulatory action can occur. These high thresholds can render enforcement impractical, especially when the harm is diffuse or long-term, as is often the case with children and other vulnerable users.

The **flowchart** illustrates the multiple enforcement pathways in determining **the relevant regulatory authority** and ensuring compliance with the diverse legal frameworks governing dark patterns:

Diagram 6.2 Flowchart of the Regulatory Process for Deceptive Design Cases


Flowchart of Regulatory Process for Deceptive Design Cases
Detection of Deceptive Design
Initial Review by Regulatory Authority
Assessment Against Regulatory Frameworks (GDPR, DSA, DMA, etc.)
Identification of Enforcement Path
Investigation and Evidence Collection
Determination of Harm Level (UI-level vs System-level)
Decision on Enforcement Action
Issuance of Penalties or Corrective Measures
Monitoring for Compliance

Another significant enforcement gap is the lack of specialised regulatory teams to address the technical and behavioural intricacies of dark patterns embedded within system architecture and AI-driven personalisation techniques. While regulators can detect and sanction visible dark patterns—such as misleading buttons, deceptive countdown timers, or obstructive consent flows—they lack the necessary technical tools and behavioural expertise to identify covert and system-level manipulations. This distinction between user interface-level manipulation and system architecture manipulation is crucial for effective enforcement. Yet, regulators frequently prioritise surface-level deceptive tactics while neglecting the algorithmic and data-driven mechanisms that fuel manipulative practices. Without a clear enforcement strategy targeting these deeper, systemic dark patterns, regulatory bodies remain inadequately equipped to protect users from the most insidious forms of deception.

There is an urgent need for cross-border coordination and collaboration among enforcement authorities to establish a unified and robust regulatory framework capable of addressing dark patterns at all levels of digital system design. DPAs, consumer protection bodies, and competition regulators can strengthen their capacity to detect and combat visible and hidden manipulative techniques by developing shared standards, pooled resources, and cross-disciplinary expertise. A potential model for this collaboration is creating a European-level task force dedicated to dark patterns and deceptive design. Such a body would centralise expertise, develop technical tools for system architecture analysis, and coordinate enforcement strategies across jurisdictions. Additionally, it could streamline data-sharing mechanisms between national regulators, ensuring that companies cannot exploit jurisdictional fragmentation to evade accountability.

A crucial aspect of strengthening enforcement protocols lies in re-evaluating the scope and applicability of existing legal frameworks to ensure they adequately address the emerging challenges of personalised and automated manipulative practices. Moving beyond piecemeal, sector-specific enforcement, a comprehensive regulatory strategy should integrate data protection, consumer rights, and AI governance into a cohesive framework that prioritises the protection of vulnerable groups, particularly minors, from all forms of digital manipulation. To effectively hold digital platforms accountable, enforcement mechanisms must be reformed to include:

1. Expanded technical expertise within regulatory bodies, incorporating behavioural science and AI governance specialists to detect covert manipulation techniques.
2. Centralised regulatory coordination, ensuring that cross-agency collaboration mitigates enforcement gaps and prevents regulatory arbitrage.
3. Proactive detection frameworks incorporating automated audit mechanisms, AI-based compliance monitoring, and system-level scrutiny of hyper-nudging and personalised manipulation strategies.

Enhancing the efficacy of dark pattern enforcement requires a full-spectrum regulatory approach that accounts for prominent and concealed manipulative practices. While existing enforcement mechanisms target surface-level manipulations, they lack robust mechanisms to scrutinise and regulate deceptive design embedded within system architecture. Addressing this critical enforcement shortfall requires a regulatory strategy prioritising a holistic and forward-looking view of deceptive design.

One key recommendation is expanding enforcement visibility across all levels of manipulation by integrating technical expertise, advanced forensic analysis, and AI-driven audit mechanisms into regulatory oversight. This could involve establishing a European task force on deceptive design, leveraging resources from multiple enforcement agencies to enable cross-jurisdictional investigations, enhanced detection tools, and coordinated regulatory action. Additionally, introducing pan-European assessment standards for identifying and evaluating dark patterns would ensure a coherent and uniform enforcement approach across Member States, addressing the existing disparities in regulatory capacity and enforcement strength.

Moreover, by implementing sophisticated audit mechanisms that incorporate both AI-based detection and system-level behavioural impact assessments, regulators can begin to combat complex algorithmic manipulations such as hyper-nudging, personalised engagement-maximisation tactics, and covert content steering effectively. These proactive enforcement measures would increase regulatory scrutiny over deceptive platform architectures and serve as a deterrent, reducing the prevalence of harmful design strategies that evade enforcement.[cclxxxiii]

6.3 AMBIGUITIES IN ENFORCEMENT UNDER THE DSA AND GDPR

The enforcement of dark patterns under the DSA and GDPR remains ambiguous and inconsistent, particularly within the Netherlands, where the enforcement approach of the Dutch Data Protection Authority (DPA) and the Authority for Consumers and Markets (ACM) has notable limitations. The DSA and GDPR aim to address manipulative design tactics that compromise user autonomy; however, they focus heavily on high-profile cases against significant platforms, neglecting the widespread use of dark patterns across smaller websites, especially those frequented by children. This focus on "big fish" cases assumes that action against large companies will establish precedents and create a deterrent effect.

> *"Enforcement measures, as they stand, are reactive rather than proactive, failing to address the nuances of highly adaptive digital manipulations."*

However, dark patterns persist across thousands of smaller platforms, meaning the actual impact of these high-profile cases on the broader ecosystem remains limited.

The Dutch DPA's approach of targeting well-known global platforms, such as Meta or Google, reflects a strategy prioritising visibility and impact. While these cases draw attention, they need to do more to address the day-to-day manipulation users encounter across a vast array of smaller websites and applications. Children are disproportionately impacted, as they are more likely to engage with sites deploying overt dark patterns—like manipulative consent banners or gamified purchase prompts—that slip through the cracks of current enforcement efforts. This trickle-down approach fails to address the scale and breadth of the problem, leaving children and other vulnerable users inadequately protected from deceptive design on smaller, often under-regulated platforms.

Further complicating this issue is the slow pace of enforcement in the Netherlands. The Dutch DPA's lengthy investigatory processes often mean that cases take years to resolve, which needs to be better suited to the fast-paced nature of digital innovation. As platforms and technologies evolve quickly, regulatory delays allow manipulative practices to proliferate unchecked, weakening the DSA's intended impact. The result is a gap between regulatory intention and enforcement reality, as businesses need more time to adapt or pivot their tactics before penalties are applied. This delay also fails to deter smaller platforms from adopting manipulative practices since the likelihood of rapid enforcement could be higher.

Because the DSA uses broad and open regulatory language, these challenges become more complex, adding new layers of enforcement ambiguity. For example, while the DSA prohibits platforms from materially distorting users' ability to make informed choices, the lack of specificity around what constitutes a "material distortion" or "informed choice" creates significant leeway. This vagueness complicates enforcement, as platforms can argue that their design choices must meet the threshold for manipulation under the DSA. The GDPR faces similar issues, as its principles of fairness and transparency, while foundational, are also broadly defined. These ambiguities make it challenging for regulators to hold platforms accountable for specific design tactics, primarily when dark patterns operate within the system architecture or involve algorithm-driven content personalisation.

A more direct and comprehensive approach is necessary to strengthen the enforcement framework. One recommendation is to adopt a proactive, rather than reactive, enforcement strategy, focusing on high-profile cases and frequent audits and spot-checks of smaller websites, especially those aimed at children. Establishing a dedicated unit within the Dutch DPA or ACM to specialise in detecting and penalising dark patterns at scale would increase accountability and deterrence. Moreover, enhancing collaboration between the DPA, ACM, and European regulators could streamline enforcement and improve cross-border oversight, making it more difficult for platforms to exploit jurisdictional loopholes.

Finally, regulatory language in both the DSA and GDPR needs refinement. Reform could take a page out of the Modernisation Directive to update current legal frameworks; for example, clearly defining terms like "material distortion" and creating explicit criteria for manipulative practices would reduce enforcement ambiguities, providing regulators with a more robust framework for action. In a rapidly evolving digital landscape, enforcement bodies must adapt to ensure that regulatory frameworks remain relevant and practical. A shift towards nimbler, child-focused enforcement practices would significantly enhance the protection of vulnerable users from manipulative design tactics, supporting the DSA and GDPR's broader objectives of transparency and user autonomy.

6.4 THE EU AI ACT: ADDRESSING SYSTEM-LEVEL DECEPTIVE DESIGN TECHNIQUES

The EU AI Act introduces critical prohibitions on manipulative AI techniques under Article 5(1)(a) and (b), representing a significant regulatory effort to safeguard user autonomy against deceptive design tactics embedded within system architectures. These provisions extend beyond traditional consumer protection frameworks by directly targeting AI-driven manipulations that operate below the user interface, exploiting users' cognitive and psychological vulnerabilities in often imperceptible ways.

Article 5(1)(a) prohibits AI systems that employ subliminal or manipulative techniques to distort user behaviour materially, reflecting an understanding that digital persuasion strategies increasingly rely on subtle and non-transparent mechanisms that bypass conscious awareness. Article 5(1)(b) strengthens this protection by explicitly prohibiting AI systems that exploit vulnerabilities arising from age, disability, or socio-economic conditions, particularly where such exploitation risks causing significant harm. These provisions signal a regulatory shift towards recognising and addressing the more profound, systemic manipulations embedded within AI-driven architectures.

At its core, Article 5(1)(a) seeks to prevent AI-driven distortions of user behaviour that impair decision-making autonomy. This extends beyond overt coercion to include subtler, behaviourally informed techniques outside conscious awareness. Examples include algorithmically mediated visual or auditory cues that subtly steer users toward actions, content, or choices without their explicit recognition. Such techniques may leverage cognitive biases, heuristics, and predictive behavioural modelling, allowing AI systems to nudge or shape user preferences in ways that are not transparent. The significance of this prohibition lies in its broad scope, capturing not only manipulative user interfaces but also algorithmic decision-making processes that systematically influence behaviour.

By explicitly addressing these subliminal and systemic manipulative practices, Article 5(1)(a) and (b) introduce a critical legal mechanism for mitigating the most insidious forms of AI-driven deception. Unlike previous regulatory approaches that primarily targeted user-facing dark patterns, these provisions seek to tackle the structural and algorithmic architectures that underpin manipulative digital environments. In doing so, the EU AI Act moves towards a more comprehensive consumer protection model that recognises the increasingly opaque nature of AI-driven influence and the necessity of legal interventions that go beyond visible design manipulations.[cclxxxiv]

Article 5 of the EU AI Act introduces prohibitions on AI techniques that exploit subliminal or manipulative tactics to distort user behaviour, with specific protections for vulnerable groups such as children and the elderly. However, high thresholds for "material distortion" and "significant harm" limit its applicability, leaving room for subtler manipulations to persist.

However, the high evidentiary threshold for what qualifies as "material distortion" or "significant harm" poses substantial limitations on the practical enforceability of this prohibition. Under Article 5(1)(a), for regulatory intervention to be triggered, the manipulative technique must either have the intent or effect of substantially impairing a user's ability to make autonomous and informed choices, leading them to decisions they would not otherwise make. This requirement introduces a complex causality test, demanding evidence that a specific AI-driven manipulation directly led to distorted decision-making—a challenge in environments where multiple factors influence user behaviour.

Compounding this issue is the ambiguity surrounding the threshold of "significant harm." For a practice to fall under Article 5(1)(b), the harm must be more than a mere inconvenience, extending to physical, psychological, societal, or economic consequences. While this broad conceptualisation aims to capture AI-driven exploitations with severe impacts, it simultaneously raises the enforcement bar, making it challenging to apply regulatory action to many forms of manipulation that may be harmful but do not meet the threshold of "significance."

This dual requirement—demonstrating both material distortion and significant harm—introduces systemic barriers to enforcement, effectively narrowing the scope of the prohibition. Subtle but persistent AI-driven manipulations, such as hyper-personalised engagement tactics, behavioural micro-targeting, or dynamic pricing strategies that exploit cognitive biases, may exert substantial influence over user behaviour yet fail to meet the strict evidentiary standards required for enforcement. As a result, many AI-driven deceptive design strategies may escape regulatory scrutiny, particularly where the harm manifests cumulatively over time rather than as an immediate, tangible impact.

The challenge for regulators, therefore, lies in operationalising these legal concepts in a manner that accounts for the evolving and often opaque nature of AI-driven manipulation. Without more precise definitions, burden-of-proof adjustments, or interpretative guidance, the risk remains that Article 5(1)(a) and (b) will be under-enforced, allowing systemic AI manipulations to persist unchecked within digital ecosystems designed to subtly but consistently influence user choices.[cclxxxv]

On the other hand, Article 5(1)(b) aims to protect vulnerable groups from AI systems that exploit specific susceptibilities, such as those related to age or disability. By targeting these vulnerabilities, the provision acknowledges that certain users may be disproportionately affected by AI-driven manipulations, such as children who may be unaware of the persuasive intent behind digital content or elderly users who might struggle with complex consent flows. The goal is to safeguard users who may be less able to critically assess or resist these influences, which can lead to exploitative or harmful outcomes. Importantly, this provision covers both intentional and incidental exploitation, where AI systems may impact vulnerable groups regardless of explicit targeting by developers.[cclxxxvi]

"The EU AI Act addresses manipulative AI techniques that distort user behaviour, yet its effectiveness is constrained by the high evidentiary thresholds of significant harm and material distortion, limiting its reach to only the most extreme cases."

In practical terms, these provisions represent a significant advancement in AI regulation, addressing manipulative tactics that have traditionally evaded scrutiny due to their subtlety or integration within broader system architecture. However, the requirement for significant harm and material behavioural distortion means that only the most extreme cases are likely to fall under these prohibitions. This threshold leaves a regulatory gap, as many deceptive design practices can still exploit users without meeting the strict criteria of Article 5. Critics argue that while the AI Act marks an essential step in regulating manipulative AI, the high evidentiary thresholds limit its applicability, allowing a range of deceptive tactics to persist without consequence.[cclxxxvii]

Moreover, the enforcement of Article 5(1)(a) and (b) presents significant operational challenges, particularly given the subtlety and sophistication of system-level manipulations that operate within opaque algorithmic frameworks. Unlike surface-level deceptive design, which can often be detected through interface analysis, AI-driven manipulative techniques are embedded within system architectures, making them difficult to identify, assess, and regulate effectively. Regulatory bodies must develop advanced technical capabilities to detect, interpret, and measure the impact of these manipulations when their effects unfold cumulatively over time rather than through immediate, observable distortions of user behaviour.

Addressing these enforcement gaps requires enhanced regulatory resources and cross-disciplinary expertise. Regulators must expand their investigatory capabilities by incorporating AI specialists, digital psychologists, and behavioural scientists to examine the intersection of algorithmic decision-making, cognitive manipulation, and legal compliance. Establishing dedicated enforcement units within data protection, competition, and consumer authorities would strengthen compliance monitoring and enforcement actions under Article 5. Collaboration with independent AI ethics bodies, civil society organisations, and academic institutions could also enhance regulators' ability to audit AI-driven systems for manipulative design patterns and provide independent compliance verification.

Beyond enforcement, Article 5's current framing may require further regulatory refinement to ensure its practical applicability. The narrow definition of "significant harm" introduces a high evidentiary threshold, which may undermine enforcement efforts against subtler, yet still damaging, AI-driven manipulations. Expanding the conceptualisation of harm to include direct and immediate consequences and cumulative psychological, behavioural, and systemic impacts would broaden the scope of regulatory interventions. Similarly, clarifying the conditions under which "material distortion" applies would reduce interpretative ambiguity, allowing enforcement agencies to act more decisively against AI-driven deceptive practices.

Alternatively, supplementary regulatory guidance could provide more precise industry benchmarks for assessing acceptable versus prohibited AI manipulations. Establishing explicit criteria for distinguishing lawful AI-driven persuasion from unlawful manipulation—such as thresholds for opacity, coercion, and autonomy infringement—would enable greater legal certainty for regulators and industry stakeholders. By combining regulatory refinement, enhanced enforcement capabilities, and interdisciplinary oversight, policymakers can ensure that Article 5 effectively safeguards against AI-driven exploitation, reinforcing user autonomy, digital fairness, and consumer protection in increasingly algorithmically mediated environments.

6.5 PROTECTING MINORS THROUGH ARTICLE 5(1)(B) OF THE EU AI ACT

Article 5(1)(b) of the EU AI Act represents a critical regulatory safeguard against AI-driven deceptive design tactics that exploit children’s cognitive vulnerabilities. By explicitly recognising minors as a protected category, this provision acknowledges that children’s decision-making autonomy is particularly susceptible to algorithmic influence, necessitating specific regulatory interventions to prevent AI systems from exploiting their developmental limitations. It prohibits AI systems from leveraging vulnerabilities linked to age, disability, or socio-economic status to manipulate behaviour in ways that could lead to significant harm, marking an important step toward child-centred AI governance.

Children’s cognitive and psychological development stages make them highly impressionable, with a limited capacity to recognise manipulative intent in digital interactions. This heightened susceptibility makes them ideal targets for AI-driven engagement-maximisation strategies, including gamified reward loops, algorithmic nudging, hyper-personalised content curation, and micro-targeted persuasive techniques. Unlike adults, children lack the executive function and critical reasoning skills to identify and resist manipulative digital architectures when these techniques operate subtly and pervasively.

Including children under Article 5(1)(b) is essential to mitigating the risks associated with AI-driven behavioural influence. Many algorithmic strategies designed to enhance engagement or monetisation appear benign—such as seamless autoplay features, streak-based incentives, or adaptive content feeds—but function as coercive mechanisms that systematically shape user behaviour. In child-directed digital environments, such tactics can reinforce compulsive usage patterns, distort perceptions of choice, and normalise commercial exploitation, effectively compromising developmental autonomy.

Article 5(1)(b) prohibits AI-driven exploitation of children's vulnerabilities, introducing a necessary regulatory mechanism to counteract the increasing sophistication of AI-powered persuasive design. However, its effectiveness will depend on enforcement capacity, clear definitional criteria for what constitutes exploitation, and proactive regulatory oversight. Ensuring this provision is effectively operationalised will require ongoing scrutiny of AI-driven digital ecosystems, interdisciplinary regulatory expertise, and structured frameworks for identifying and assessing manipulative design patterns that target children.[cclxxxviii]

The protection framework under Article 5(1)(b) is structured around four interdependent criteria:

(1) the deployment of an AI system,

(2) the exploitation of vulnerabilities,

(3) the material distortion of behaviour, and

(4) the causation of significant harm.

These elements collectively establish a stringent threshold for regulatory intervention while raising complex enforcement challenges, particularly in cases involving minors.

The first criterion, deployment, encompasses introducing and using AI systems in the market, ensuring that regulatory oversight applies from the point of access rather than solely at the stage where harm has already materialised. This early-stage recognition underscores the need for proactive scrutiny of AI systems designed for or accessible to children, spanning social media, gaming, educational technology, and entertainment platforms. Given the high-risk nature of these digital environments, regulatory bodies must implement continuous compliance monitoring—tracking AI systems from their initial release through active usage—to identify and mitigate risks before they become entrenched in platform design and user behaviour.[cclxxxix]

The second criterion, exploitation of vulnerabilities, reflects a critical acknowledgement that AI-driven systems can disproportionately affect certain groups based on age, disability, or socio-economic status. Children lack the cognitive maturity, digital literacy, and critical reasoning skills to recognise manipulative intent in algorithmically mediated environments. AI-powered personalisation engines, persuasive notification systems, gamified interfaces, and social comparison triggers all function as mechanisms of behavioural influence, subtly shaping children's interactions in ways that may compromise their autonomy and decision-making capacity. These techniques exploit children’s cognitive and emotional states, enhancing engagement while remaining largely opaque due to the non-transparent nature of algorithmic decision-making.

The third element, material distortion of behaviour, is central to understanding how AI-driven manipulative systems transcend mere persuasion, veering into coercion and deceptive design practices. This criterion captures alterations in decision-making autonomy, particularly in environments where algorithmic architectures are explicitly optimised for engagement, retention, and monetisation. In child-facing digital ecosystems, these AI systems frequently exploit cognitive shortcuts, emotional triggers, and impulsive tendencies to shape user behaviour in ways that deviate from rational or autonomous decision-making processes.

A key example is the inducement of compulsive platform engagement through hyper-personalised recommendation engines, intermittent reinforcement loops, and gamified reward structures. These mechanisms leverage children’s heightened sensitivity to immediate gratification—an established characteristic of developing cognitive control—to skew behavioural outcomes in a direction that aligns with platform profit motives rather than user welfare. Common manifestations include addictive usage patterns, impulsive digital transactions, and heightened anxiety linked to fear of missing out (FOMO). Given children’s susceptibility to these design strategies, Article 5(1)(b) provides an essential regulatory tool to address AI-driven behavioural distortions that compromise young users' autonomy.

The fourth criterion, causation of significant harm, highlights the long-term consequences of AI-driven exploitations in child-directed digital environments. While regulatory discussions often focus on tangible financial or physical harm, psychological and developmental impacts—such as anxiety, self-esteem erosion, compulsive digital dependency, and behavioural conditioning—are equally significant yet often underappreciated in traditional enforcement models. AI-driven persuasive notifications, gamified incentives, and reward-driven feedback loops create reinforcement cycles that entrench habitual digital behaviours, leading to prolonged screen time, attention fragmentation, and an increased risk of digital over-reliance.

Empirical research underscores AI-driven persuasive systems' profound and lasting impact on children’s cognitive and behavioural development. Early exposure to algorithmically optimised engagement mechanisms can instil habitual digital dependencies, reinforcing impulsive decision-making tendencies and increasing vulnerability to future manipulative design strategies. These risks extend beyond immediate exploitations, manifesting in long-term developmental challenges related to attention regulation, emotional resilience, and autonomy in digital interactions. As AI systems evolve to refine their predictive capabilities, the capacity to influence children’s behaviour in imperceptible yet persistent ways grows, necessitating a regulatory approach that anticipates overt manipulation and the cumulative psychological effects of sustained algorithmic exposure.

Despite Article 5(1)(b)'s intent to mitigate such harms, its practical enforcement faces structural challenges due to the high evidentiary threshold required for regulatory intervention. Establishing that an AI system has materially distorted behaviour, exploited cognitive vulnerabilities, and caused significant harm involves a level of data collection and behavioural analysis that exceeds the current capabilities of many enforcement bodies. Manipulative techniques often operate at a systemic level, embedded within personalisation engines, engagement-maximisation algorithms, and reinforcement-learning models that shape user interactions over time. Tracing the precise mechanisms through which an AI-driven system influences a child's decision-making trajectory—and linking these effects to legally actionable harm—remains a considerable challenge.

A key obstacle lies in demonstrating the causal relationship between algorithmic influence and measurable harm, mainly when effects are gradual and cumulative rather than immediate and overt. For example, children exposed to adaptive engagement strategies may experience a progressive shift in attention regulation, risk perception, or compulsive interaction patterns. Yet, these effects may not meet the legal threshold of significant harm until they manifest in observable behavioural dysfunctions. This complexity underscores the need for a more robust regulatory infrastructure that enables continuous monitoring of AI-driven manipulations, integrating behavioural science, algorithmic auditing, and cross-disciplinary expertise into enforcement frameworks.

Ensuring the effectiveness of Article 5(1)(b) requires moving beyond traditional regulatory models toward proactive, pre-emptive oversight. Recognising that AI-driven persuasive systems do not operate in isolation. Still, as part of broader digital ecosystems, regulatory interventions must account for algorithmic influence's subtle but compounding nature. By incorporating early-stage risk assessments, real-time compliance mechanisms, and AI-specific investigative methodologies, enforcement bodies can more effectively address the evolving landscape of AI-driven manipulative design, safeguarding children's autonomy and digital well-being against both immediate exploitations and long-term behavioural conditioning.

Article 5(1)(b) thus provides a framework for identifying and limiting exploitative AI practices directed at minors, yet its full potential lies in lowering the high enforcement threshold. The AI Act could better shield young users from digital manipulations that exploit their unique susceptibilities by refining definitions of harm and material distortion and introducing child-specific standards. These steps would create a safer digital environment for children and uphold the EU's commitment to protecting its youngest citizens in an increasingly AI-driven world.

6.6 CHALLENGES WITH ARTICLE 5(1)(B): HIGH THRESHOLDS FOR PROTECTION

Article 5(1)(b) of the EU AI Act represents a well-intentioned attempt to safeguard vulnerable groups, particularly children, from harmful manipulative practices in AI-driven systems. However, its high legal and evidentiary thresholds pose significant challenges for effective enforcement, especially in addressing the nuanced yet damaging forms of manipulation that often affect young users. This provision prohibits AI practices that exploit vulnerabilities arising from age, disability, or socio-economic situations, intending to distort behaviour in ways likely to cause significant harm materially. However, while these protections are vital, the high bar set by Article 5(1)(b) limits its applicability, leaving children susceptible to many harmful but subtle manipulative tactics embedded in system architecture.

One of the primary hurdles is the requirement to demonstrate a *material distortion of behaviour*. This standard demands evidence of a substantial shift in user decision-making directly attributed to AI influence. This criterion is complex to fulfil, particularly with minors who, due to their developmental stage, are more easily influenced by digital nudges but may not exhibit a measurable or transparent change in behaviour that observers can connect to the AI system's actions. Children naturally gravitate toward interactive digital environments that use reward loops, social validation cues, and notifications to trigger cognitive and emotional responses. While these strategies influence behaviour, they do not necessarily produce the stark behavioural changes that Article 5(1)(b) appears to require, creating a gap between harm and enforceability. Moreover, AI systems often rely on highly personalised algorithms that evolve continuously based on user interactions. For children, the continuous evolution of personalised algorithms may lead to exposure to nudges or suggestions finely tuned to exploit individual traits, such as impulsivity or a need for social validation. Identifying and proving that these adaptive algorithms lead to a "material distortion" of behaviour becomes a complex task, often requiring data beyond the reach of enforcement agencies. The dynamic nature of these interactions and the opacity of many algorithmic processes make it challenging to establish a direct, causal link between specific system designs and behavioural outcomes, mainly when the effects may accumulate gradually rather than manifest in a single, measurable distortion.[ccxc]

Challenges w/ Article 5(1)(b) of EU AI Act

High threshold for material distortion.

Strict requirement for significant harm.

Evidentiary burden on regulators.

Dynamic and adaptive nature of AI algorithms.

Difficulty addressing cumulative and diffuse harms.

Opacity of AI processes and system architecture.

Lack of child-specific provisions.

Inconsistent enforcement across Member States.

Delayed detection and reactive enforcement approaches.

Focus on immediate, tangible harm over long-term impacts.

Challenges in defining and identifying exploitation of vulnerabilities.

Limited resources and technical expertise among regulators.

The second major challenge in applying Article 5(1)(b) lies in the *significant harm* criterion, which raises the higher enforcement bar. For intervention, harm must be present and meet a substantial threshold, covering impacts beyond minor inconveniences to physical, psychological, social, or financial harm. In the context of children, this requirement is problematic; many harms associated with digital manipulation are cumulative and intangible, manifesting over time as behavioural dependencies, mental health impacts, or altered social behaviours. For instance, the compulsive use of social media or gaming platforms, driven by AI-powered engagement strategies, can lead to patterns of behaviour that impair academic performance or social well-being. Nevertheless, these effects may not immediately qualify as "significant harm" under the legal standards despite their potentially profound long-term impacts.

Furthermore, enforcing this provision would often require a substantial evidentiary base to demonstrate that harm has occurred or is likely to happen, adding another layer of difficulty. Collecting the necessary evidence to substantiate significant harm—especially in cases where digital influence operates below conscious awareness—is a challenging endeavour, often requiring a combination of psychological, behavioural, and technical data. Children, who are generally less able to articulate the sources of their digital experiences, are doubtful about reporting or recognising these subtle manipulations, further hindering the evidentiary process. The regulatory burden to gather and assess this data for a broad spectrum of potential harms, many of which may be indirect or diffuse, can deter authorities from acting altogether.

Additionally, the threshold of significant harm confines regulatory intervention to cases that surpass a specific and identifiable harm threshold. However, many of the harms minors experience are low-level but persistent, such as reduced attention span, dependence on instant validation, or exposure to subtly exploitative advertising, which are difficult to quantify within the rigid framework of significant harm. This evidentiary threshold prevents regulators from addressing AI practices that might accumulate into substantial long-term effects, exposing children to manipulative practices that can shape their behaviour over time in harmful ways.

Considering these challenges, revising or refining Article 5(1)(b) could improve its practical efficacy in protecting minors. A more flexible interpretation of "material distortion" and "significant harm" could allow regulators to account for cumulative or indirect harms that may not immediately satisfy high thresholds but pose risks to young users. For example, revising the evidentiary standards to include cumulative harm or introducing presumptions around the impact of specific design patterns on minors could help address the limitations posed by these thresholds.

Alternatively, a framework of presumptive vulnerability for children could streamline enforcement and promote a more preventative stance against manipulative AI practices by classifying specific manipulative methods as harmful when applied to minors, regardless of immediate harm. This approach would reflect the EU's commitment to safeguarding children by lowering the evidentiary burden on enforcement authorities and recognising the unique vulnerabilities of minors in digital environments. Adopting a more flexible or contextually sensitive interpretation of Article 5(1)(b) would allow regulators to address better the nuanced and evolving ways AI can exploit young users, ensuring that the law provides meaningful, proactive protections in a digital landscape increasingly shaped by AI-driven influences. The findings of this research highlight four critical areas where legislative or regulatory action is required:

Prohibit Addictive Design Features: Establish clear restrictions on engagement-driven mechanics such as countdown timers, streak-based rewards, and gamified progression systems that exploit children's cognitive vulnerabilities and encourage compulsive use.

Mandate Transparency Requirements: Require platforms to disclose how personalisation algorithms operate, particularly regarding how they influence minors' behaviour and decision-making. This would enable regulators and civil society organisations to assess and mitigate risks associated with AI-driven content targeting.

Standardise Cross-Border Enforcement: Strengthen cooperation among national regulatory authorities and EU bodies to ensure consistent enforcement of digital fairness principles, preventing jurisdictional discrepancies that allow harmful practices to persist in certain Member States.

Adopt Fairness by Design: Introduce binding obligations requiring child-specific protections to be embedded at the design stage of digital services, shifting the responsibility from end-users to service providers and ensuring that digital environments are inherently safe for minors.

By implementing these measures—through revisions to existing legislation or new legal instruments—the EU can ensure that regulatory protections keep pace with the rapidly evolving digital landscape. A proactive, harmonised approach to consumer protection will safeguard children's rights, well-being, and autonomy in an increasingly data-driven and algorithmically mediated online environment.

SECTION 7: THE EU LEGAL FRAMEWORK FOR REGULATING DECEPTIVE DESIGN

7.1 CHILDREN AND DECEPTIVE DESIGN

User Interface Dark patterns targeting children exemplify a critical intersection of commercial and psychological exploitation, behavioural manipulation, and insufficient regulatory specificity. These practices are embedded within digital interfaces, aiming to influence children's choices in ways they might not otherwise take, exploiting their cognitive vulnerabilities and emotional dependencies. Despite existing consumer protection frameworks in the EU, dark patterns' increasing sophistication and subtlety require a more nuanced and robust legislative response. At their core, dark patterns targeting children exploit developmental characteristics such as limited critical reasoning, heightened suggestibility, and emotional dependency on validation. As observed in the CERRE report on harmful online choice architecture, design tactics like gamification, reward systems, and manipulative interface designs amplify engagement at the expense of autonomy.[ccxci] For instance, designers configure reward loops or "loot boxes" in games to invoke gambling-like behaviours, a strategy identified as particularly exploitative when offered on platforms frequented by minors.[ccxcii]

The regulatory environment addressing such practices is fragmented, creating legal and practical challenges. For example, the UCPD prohibits misleading and aggressive practices under Art. 5–9, including those that distort the economic behaviour of the "average consumer."[ccxciii] However, its application to vulnerable groups, such as children, hinges on demonstrating a transactional impact that is challenging to quantify in digital contexts.[ccxciv] Additionally, the GDPR's provisions on children's data processing under Art. 8 offer safeguards against profiling but do not explicitly regulate the deployment of manipulative interfaces.[ccxcv]

Dark Patterns Targeting Children

Exploitative Practices: Highlights how dark patterns exploit children's developmental vulnerabilities, including limited critical reasoning and emotional dependencies, through deceptive design features like gamification and reward systems.

Examples of Harm: Discusses manipulative tactics such as fake countdown timers, loot boxes, and misleading prompts that distort children's decision-making and encourage compulsive behaviours.

Regulatory Gaps: This section identifies deficiencies in existing frameworks like the UCPD and GDPR, which inadequately address non-interface manipulative practices embedded in algorithms and system architectures.

Impact on Children: Emphasises the risks posed to children, including excessive screen time, mental health challenges, and coercive financial decisions influenced by deceptive digital designs.

Recommendations for Action: Advocates for extending regulations to cover algorithmic manipulations, enforcing stricter transparency requirements, and adopting behavioural testing to mitigate risks unique to child users.

In the context of children, the structural asymmetry between platforms and users is stark. A 2024 report on the commercial exploitation of children online highlights how dark patterns intensify the commercial pressure on minors through features such as false urgency claims, obfuscated cancellation processes, and relentless upselling. These tactics exploit children's limited decision-making capacity and emotional bonds with characters or narratives embedded within the digital experience.[ccxcvi]

Such practices undermine the rights enshrined in Article 24 of the Charter of Fundamental Rights, which mandates special protections for children. Legislative initiatives such as the DSA introduce transparency and accountability measures for large online platforms, yet their scope remains constrained. Article 25 DSA prohibits dark patterns in user interfaces but does not extend to the regulation of recommender systems or other structural manipulations. While it restricts interface-based manipulative designs that distort or influence user decision-making, it does not comprehensively address the opaque forms of deceptive design embedded within algorithmic architectures. Future legislative efforts must extend these prohibitions to encompass non-interface dark patterns, particularly those that operate at the systemic level through algorithmic personalisation, engagement-maximisation techniques, and behavioural targeting.

As the CERRE report recommends, integrating behavioural testing and enhanced transparency obligations could mitigate the risks of covert manipulative strategies.[ccxcvii] For instance, mandating disclosures regarding algorithmic decision-making and imposing age-appropriate adjustments within recommender systems could help counteract the exploitative asymmetries embedded within digital platforms.[ccxcviii] While Article 25 DSA establishes a critical baseline in prohibiting manipulative interface designs, its failure to address algorithmic and systemic manipulations represents a significant regulatory blind spot.[ccxcix] Closing this gap is essential to ensuring comprehensive consumer protections, particularly for children, who remain the most susceptible to digital exploitation.

Current regulatory measures frequently fail to account for the nuanced vulnerabilities of children, instead focusing on broader consumer harms that do not adequately reflect the distinct risks posed by child-facing digital environments.[ccc] The Digital Fairness Fitness Check underscores the necessity of targeted interventions to combat manipulative design strategies affecting children, advocating for a more integrated approach that aligns existing consumer protection directives with emerging regulatory imperatives.[ccci] The principle of proportionality in consumer law necessitates a regulatory framework that evolves to accommodate the specific needs of children as a distinct consumer demographic. Moving beyond general prohibitions on unfair practices requires the introduction of more prescriptive regulatory obligations for digital environments designed for children. The implementation of a "digital duty of care" framework—akin to provisions within Australia's Online Safety Act—could provide a viable model for compelling platforms to prioritise user welfare over extractive engagement strategies, ensuring that commercial incentives do not continue to operate at the expense of fundamental rights and digital well-being.[cccii]

The European Commission's exploration represents a promising avenue for addressing these challenges. By harmonising existing directives under a unified framework, the Act could clarify the legality of specific dark patterns, impose stricter penalties for violations, and mandate age-appropriate design standards for platforms targeting minors. However, the CERRE report cautions that such measures must avoid regulatory overlaps and ensure coherence with broader EU objectives on consumer protection, competition, and digital governance.

The persistent exploitation of dark patterns targeting children underscores a fundamental failure to adapt consumer protection frameworks to the complexities of the digital age. Addressing this challenge necessitates legislative innovation and a paradigm shift towards ethical digital design principles that prioritise the autonomy and rights of children. Young users will continue to be systematically exploited without decisive regulatory intervention, eroding trust in the digital ecosystem and perpetuating structural inequities. The prevalence of these manipulative practices highlights the pressing need for a comprehensive and harmonised regulatory response that extends beyond the scope of existing legal instruments. As the persistent gaps identified in the Digital Fitness Check illustrate, frameworks such as the GDPR, UCPD, and DSA remain insufficient in addressing the evolving and often opaque manipulative strategies embedded within system architectures and algorithmic decision-making processes.

To effectively curtail the commercial and psychological exploitation of children, future regulatory frameworks must introduce targeted, enforceable obligations that reflect the specific developmental vulnerabilities of young users. A central regulatory challenge lies in countering manipulative design strategies that operate below the user interface—beyond the explicit deceptive practices currently targeted under Article 25 of the DSA. Algorithmic personalisation, engagement-maximisation mechanisms, and system-level nudges frequently function imperceptibly, leveraging behavioural data to reinforce compulsive usage patterns and optimise consumption. Children are particularly susceptible to such techniques due to their developmental immaturity and limited capacity to assess digital content critically. The principle of proportionality in consumer protection law mandates recognising children as a distinct consumer demographic requiring bespoke safeguards. Regions must adopt a multi-pronged approach that integrates explicit prohibitions, enhanced transparency obligations, and preventative oversight mechanisms to mitigate these exploitative practices. For instance, banning non-interface dark patterns—such as algorithmic nudges prioritising profit over user welfare—would be crucial in addressing the hidden coercive architectures that govern children's digital interactions.

Transparency requirements must extend beyond interface design to encompass disclosures about algorithmic personalisation processes and the data-driven logic underpinning digital environments. Additionally, platforms should be required to implement behavioural testing methodologies to assess and mitigate the potential harms associated with their design choices, ensuring compliance with child-centric regulatory standards and fostering a digital ecosystem that actively prioritises user well-being over commercial exploitation.

A critical regulatory innovation would be introducing a "digital duty of care" specifically for platforms catering to minors. Inspired by the principles articulated in Australia's Online Safety Act, this obligation would compel platforms to assess and mitigate their systems' psychological and behavioural risks. A duty of care framework could incentivise businesses to prioritise ethical design and operational practices, embedding child welfare into their core operations.

The CERRE report highlights the imperative of harmonising regulatory protections across EU Member States to mitigate enforcement disparities and reduce regulatory fragmentation risks. Drawing from existing legislative instruments while incorporating more prescriptive measures tailored to child-directed digital environments, a unified legal framework would enhance consistency and efficacy in safeguarding young users. Such an approach is essential to address existing lacunae in digital governance and anticipate the regulatory challenges posed by the rapid evolution of digital technologies. Without a coherent and forward-thinking framework, legal protections risk becoming obsolete due to increasingly sophisticated manipulative design strategies. The persistent deployment of dark patterns to exploit children underscores a profound governance failure—one in which commercial imperatives systematically take precedence over fundamental rights and ethical obligations. This structural imbalance perpetuates digital environments that are inherently asymmetrical, privileging platform profitability over the autonomy and well-being of young users. The absence of robust and enforceable protections exacerbates these systemic inequities, reinforcing power asymmetries that leave children particularly vulnerable to exploitation. Strengthening regulatory safeguards through a comprehensive and anticipatory legal framework is thus critical to ensuring that children's rights are not merely recognised in principle but actively protected in practice.

7.1.1 THE UNIQUE VULNERABILITIES OF MINORS IN THE DIGITAL AGE

The European Union has long led global consumer protection and digital regulation. However, the rapid pace of technological change, particularly the rise of AI-driven manipulations targeting minors, has exposed significant gaps in the existing legal framework. In this context, policymakers must consider whether incremental amendments to existing EU legislation can sufficiently address these gaps or whether a comprehensive new regulatory instrument is required. The case for patching up existing EU law—including the GDPR, DSA, UCPD, and AI Act—rests on the premise that these frameworks already provide a strong foundation. However, relying solely on these instruments raises questions about their adequacy and coherence in addressing the nuanced and covert manipulations prevalent in targeting children. This discussion examines the limitations of the current regulatory framework, the unique vulnerabilities of minors in the digital space, and the challenges of revising existing legislation in lieu of introducing a new law.

Children represent a particularly vulnerable group in the digital ecosystem. Their cognitive development, limited capacity to assess risks, and heightened susceptibility to emotional manipulation make them prime targets for exploitative practices. AI-driven systems exacerbate these vulnerabilities by leveraging behavioural data to personalise interactions, nudges, and recommendations, often in ways that are neither visible nor intuitively understood. For example, social media platforms frequently employ infinite scrolling, autoplay features, and engagement loops that exploit children's impulse control and desire for social validation. Gaming applications utilise loot boxes and variable rewards to create compulsive behaviours, tapping into psychological mechanisms that children struggle to resist. Educational apps and IoT devices like smart toys increasingly rely on algorithmic personalisation, which, while ostensibly designed to enhance learning experiences, often prioritises engagement metrics over children's well-being. These practices not only erode children's autonomy but also have long-term implications for their mental health, privacy, and decision-making abilities. Despite these risks, EU legislation has struggled to keep pace with the sophistication and pervasiveness of AI-driven manipulations, leaving children inadequately protected.

7.2 LIMITATIONS OF THE EXISTING LEGAL FRAMEWORK

7.2.1 THE DSA: LIMITED SCOPE AND FOCUS ON INTERFACES

The DSA represents a significant step in regulating digital platforms, mainly through provisions such as Article 25, which prohibits manipulative design in online interfaces. However, its scope is limited to online platforms, excluding many digital environments frequented by children, such as educational apps, IoT devices, and standalone software. These exclusions create significant blind spots in the regulation of child-focused digital services. Moreover, the DSA's emphasis on visible manipulative practices, such as dark interface patterns, fails to address the covert manipulations embedded within system architectures. Techniques like algorithmic nudging and dynamic content adaptation operate beneath the surface, shaping user behaviour in difficult-to-detect regulated ways. These systemic manipulations are particularly harmful to minors, as they exploit behavioural data to influence interactions in subtle yet profound ways. Addressing these gaps would require expanding the DSA's scope and introducing provisions targeting system-level manipulations—a challenging endeavour given that the regulation has only recently been enacted.

Article 25 prohibits online platforms from designing, organising, or operating their interfaces in a manner that deceives, manipulates, or materially distorts or impairs users' ability to make free and informed decisions. This provision is one of the first EU-wide explicit legal measures against deceptive design, setting a standard for interface transparency and fairness. The regulation focuses on online platforms, defined under the DSA as services that store and disseminate user-generated content to the public. This means the provision excludes other digital services, such as operating systems, smart devices, and enterprise software, even though they may deploy similar manipulative tactics. The emphasis is on consumer-facing platforms, such as social media networks, online marketplaces, and app stores, where user autonomy is most vulnerable.

Key Regulatory Principles

The prohibition under Article 25 encompasses several design manipulations that impair decisional autonomy. According to Recital 67, dark patterns can take various forms, including:

- **Making some choices more prominent** to steer users in a particular direction.
- **Repeatedly prompting users** to make a decision they have already declined.
- **Creating friction in cancellation processes** to make unsubscribing or terminating a service harder than subscribing.

Article 25 does not require intent to manipulate users; even designs that incidentally result in decisional impairment can fall under its prohibition. This shifts the focus from proving intent (which is difficult to establish in algorithmic or behavioural nudging) to evaluating user impact, a significant regulatory evolution.

Limitations and Exceptions

Despite its broad reach, Article 25(2) carves out exceptions for practices already regulated under the Unfair Commercial Practices Directive (UCPD) and the General Data Protection Regulation (GDPR). This exception raises concerns that many dark patterns will remain regulated under pre-existing laws, potentially leading to enforcement inconsistencies. For example, manipulative consent mechanisms in cookie banners may fall under GDPR, excluding them from Article 25 enforcement. Further ambiguity arises regarding the interpretation of “material distortion”—a threshold differentiating minor nudging from unlawful manipulation. Without clear guidance, enforcement may vary across EU jurisdictions.

Risk Mitigation and Compliance

Very large online platforms (VLOPs), defined as those with over 45 million active users in the EU, face additional obligations under Article 35 of the DSA. They must conduct risk assessments and mitigate systemic risks related to interface manipulations. This requirement acknowledges that dark patterns can cause collective harm, reinforcing the EU’s broader regulatory approach to platform accountability.

Summary Table: Article 25 of the DSA

Aspect	Details
Prohibition	Online platforms must not design, organise, or operate their interfaces in a way that deceives, manipulates, or materially distorts users' ability to make free and informed decisions.
Examples of Prohibited Practices	- Making certain choices disproportionately prominent (nudging) - Repeated prompts interfering with the user experience - Making service termination harder than subscribing

Exceptions	- Practices already covered by the GDPR (e.g., misleading consent mechanisms) - Practices covered by the UCPD (e.g., false urgency messages)
Scope	Applies only to online platforms (services that store and disseminate user content) and excludes other digital services like operating systems and IoT devices.
Regulatory Threshold	Requires a material distortion or impairment of user decision-making, leaving room for interpretation and potential enforcement challenges.
VLOP Obligations	Very Large Online Platforms (VLOPs) must assess and mitigate risks associated with manipulative design (Article 35 DSA).

7.2.2 THE GDPR: RELIANCE ON TRANSPARENCY AND CONSENT MECHANISMS

The GDPR is a pivotal regulatory framework within the European Union that emphasises data protection, rights, and privacy through accountability, fairness, transparency and informed consent principles. However, its reliance on transparency and consent mechanisms often proves inadequate in the face of AI-driven manipulations. Articles 5 and 7 require fairness and freely given consent for data processing, yet manipulative practices undermine these principles by influencing how platforms secure consent and later use the data. For instance, cookie banners and privacy notices focus on upfront disclosures but fail to address ongoing manipulations within system architectures. Practices like infinite scrolling or personalised engagement loops exploit behavioural data to keep users engaged long after consent, effectively bypassing GDPR protections. Enforcement challenges further weaken the GDPR's efficacy. Data Protection Authorities (DPAs) face resource constraints and procedural delays, often prioritising high-profile cases involving significant platforms while leaving smaller operators unregulated. This fragmented enforcement landscape disproportionately affects children who are likelier to engage with less prominent apps and services.

Transparency requirements compel organisations to disclose their data processing practices clearly, while informed consent mandates that users receive sufficient information to make autonomous decisions regarding their data. These principles form the backbone of the GDPR's protective aims, placing individuals in control of their data and demanding that organisations obtain genuine, explicit agreement to data collection and processing activities. However, while these measures have advanced data protection in Europe, their effectiveness is increasingly questioned in the context of manipulative digital design, especially concerning the protection of minors.

GDPR Limitations in Addressing Deceptive Design

Transparency and consent mechanisms assume rational decision-making, unsuitable for minors.

GDPR fails to address hidden manipulative tactics embedded in system architectures.

Child-specific protections under GDPR lack enforceability.

The GDPR's approach to consent assumes a rational actor model, presuming that users can make informed decisions if given clear, accessible information.[ccciii] This assumption, however, needs to adequately account for the unique vulnerabilities of minors, who often need more cognitive maturity to interpret, process, or critically evaluate consent information. Children and adolescents are less likely to comprehend the long-term implications of data sharing, particularly as it pertains to the complex and, at times, opaque methods by which digital platforms utilise their data in practical terms, minors are ill-equipped to fully understand how platforms harvest, profile, and employ their information to personalise and manipulate digital experiences. Therefore, although organisations may achieve GDPR compliance by ticking the boxes of transparency and consent, these requirements do not guarantee that minors will grasp the ramifications of their choices, leaving them vulnerable to exploitative and manipulative design practices.

Moreover, the GDPR's transparency and consent provisions have inherent limitations when applied to the subtle, often hidden nature of manipulative design tactics, which operate at a system level that remains largely invisible to users. While dark patterns are regulated explicitly under frameworks like the GDPR and the DSA, it is essential to note that not all deceptive design strategies are considered dark patterns. Other manipulative techniques, such as interface nudging, data-sharing prompts disguised as beneficial options, and gamified engagement loops, may not fall under these definitions yet still frequently bypass users' conscious consent. These designs exploit cognitive biases and developmental vulnerabilities, steering user behaviour through technically GDPR-compliant methods that raise concerns, mainly when aimed at young users. For example, while a platform may ostensibly seek consent to collect a minor's data, the consent flow itself may be designed to favour opt-in choices or obscure alternatives, resulting in decisions that may not genuinely reflect the user's intention.[ccciv]

A further complication lies in the GDPR's lack of specificity regarding child-centred protections, especially in the face of AI-enhanced manipulative tactics. Although the regulation includes some considerations for children, notably in Recital 38, it lacks robust, enforceable provisions addressing minors' unique vulnerabilities in AI-driven digital environments. While effective in some adult contexts, reliance on transparency and consent becomes increasingly tenuous when applied to complex, data-driven designs tailored by algorithms to influence and predict user behaviour.[cccv] Due to their developmental stage, minors may need to know how personalised algorithms shape their digital experiences. They also need to possess the cognitive tools to critically evaluate these influences, which platforms often embed within the very structure of their interfaces.

While the GDPR marks significant progress towards data rights in Europe, its emphasis on transparency and consent does not sufficiently protect young users from manipulative design practices. A child may technically "consent" to data processing without truly understanding the depth and implications of their decision, allowing platforms to exploit this regulatory gap. Addressing these issues necessitates a move beyond traditional transparency and consent models, advocating for specific, child-centred regulatory protections within the GDPR framework. Such provisions would need to account for the developmental limitations of minors, implementing more stringent requirements around data use, algorithmic transparency, and AI-driven personalisation tactics that may undermine the autonomy and well-being of young users.

7.2.3 THE UCPD: INADEQUATE COVERAGE OF SYSTEM-LEVEL MANIPULATIONS

The UCPD establishes a legal framework prohibiting misleading, aggressive, and unfair commercial practices. Yet, its effectiveness in addressing AI-driven manipulative design techniques embedded within system architectures remains significantly constrained. While the directive is well-suited to tackling overtly deceptive practices, its scope is structurally ill-equipped to regulate non-transparent, algorithmically mediated manipulations that operate beyond user awareness. A fundamental limitation of the UCPD lies in its reliance on traditional conceptions of deception and consumer harm, which prioritise observable, interface-level misconduct over the systemic and behavioural mechanisms that shape user decision-making at a structural level. While the directive prohibits misleading actions and aggressive commercial tactics, algorithmically optimised personalisation, real-time urgency prompts, and dynamic pricing discrimination frequently escape regulatory scrutiny because they do not conform to conventional definitions of deception. These practices exploit cognitive biases, data-driven behavioural profiling, and probabilistic engagement models, subtly steering users towards predefined commercial outcomes while maintaining a veneer of consumer choice.

For children, these limitations are particularly pronounced. Unlike adults, minors lack the cognitive maturity, digital literacy, and informed scepticism to identify and resist algorithmically mediated persuasion techniques. AI-driven recommendation systems, gamified reward loops, and data-driven engagement-maximisation strategies manipulate psychological vulnerabilities unique to children—such as immediacy bias, susceptibility to social validation, and underdeveloped impulse control—without meeting the UCPD's high evidentiary threshold for deception or coercion. Because these techniques do not rely on explicitly false representations but instead subtly distort decision-making autonomy over time, they evade the directive's enforcement mechanisms. Moreover, the UCPD's heavy reliance on user perception and direct consumer impact further weakens its applicability to system-level manipulations. Many AI-driven deceptive design strategies operate below the interface level, shaping engagement through dynamic interface adaptations, algorithmic reinforcement learning, and predictive analytics that are neither directly observable nor immediately actionable by individual consumers. In such cases, children are particularly disadvantaged, as they are less capable of recognising when they are subject to personalised persuasion strategies that exploit their behavioural tendencies rather than presenting neutral choices.

Enforcement challenges further exacerbate these shortcomings. The UCPD's case-by-case enforcement model, which often requires ex-post harm assessments, is inherently ill-suited to AI-driven manipulation, where exploitative design choices are continuously refined through algorithmic learning. Unlike static deceptive practices—such as misleading product claims or false scarcity notifications—AI-powered deception evolves dynamically, making traditional regulatory approaches insufficient to address digital manipulation's iterative and adaptive nature.

To ensure meaningful consumer protection in child-facing digital environments, regulatory frameworks must extend beyond the UCPD's narrow focus on interface-level deception to encompass manipulative design's structural and behavioural dimensions. This requires a paradigm shift from identifying discrete violations toward anticipating and mitigating systemic risks embedded within AI-driven consumer interactions. Without such reforms, the UCPD will remain an incomplete safeguard, leaving children particularly vulnerable to increasingly sophisticated and opaque forms of digital exploitation.

7.2.4 THE AI ACT: HIGH THRESHOLDS FOR APPLICABILITY

The AI Act introduces a targeted regulatory approach to AI governance. Article 5(1)(b) explicitly prohibits AI systems that exploit vulnerabilities linked to age, disability, or socio-economic conditions in ways that materially distort behaviour. While this provision marks a significant regulatory advancement, its high enforcement threshold severely limits its practical applicability in addressing AI-driven manipulative design tactics targeting minors. A key challenge lies in demonstrating "significant harm," which demands resource-intensive investigations and complex evidentiary standards. Many of the harms associated with manipulative AI-driven systems—such as addictive design, algorithmic reinforcement loops, and hyper-personalised engagement strategies—manifest incrementally over time, making them difficult to quantify within traditional regulatory frameworks. Unlike immediate, tangible harms (e.g., financial fraud or physical safety risks), AI-driven manipulations often erode autonomy, shape behaviour cumulatively, and reinforce compulsive engagement patterns. Yet, such effects are rarely immediately observable or easily measurable under existing legal standards. Further complicating enforcement is the requirement to prove intent, which imposes a significant burden of proof on regulators. Establishing that an AI system was explicitly designed to exploit children's vulnerabilities necessitates detailed forensic analysis of system architectures, training data, optimisation objectives, and decision-making processes. This challenge is further exacerbated by the adaptive nature of AI, where machine learning models continuously evolve in response to user interactions rather than operating based on fixed, pre-programmed rules. As a result, many exploitative AI systems may not exhibit explicit intent to manipulate children, even though their design incentivises engagement-maximisation strategies that disproportionately affect young users.

Additionally, the AI Act's focus on prohibiting only the most extreme form of behavioural manipulation means that many covert and emergent deceptive practices remain unregulated. AI-driven persuasive mechanisms, nudging frameworks, and dynamic content delivery models often operate within legal grey areas, subtly shaping user interactions without crossing clear regulatory thresholds. This regulatory gap leaves minors particularly exposed, as they lack the cognitive maturity and digital literacy to identify and resist sophisticated algorithmic persuasion techniques. To address these limitations, enforcement strategies must evolve to incorporate more potent investigative tools, clearer evidentiary thresholds, and proactive oversight mechanisms. Without expanded regulatory capacity and refined legal interpretations, Article 5(1)(b) risks being underutilised, leaving many of the most insidious AI-driven manipulative tactics unchecked.

7.3 TOWARDS A CHILD-CENTRIC DIGITAL FAIRNESS FRAMEWORK: ADDRESSING THE GAPS IN EU LEGISLATION

The interplay between existing EU legislative frameworks, including the GDPR, DSA, and AI Act, highlights persistent regulatory gaps in protecting children from manipulative digital practices embedded within system architectures. While these regulatory instruments establish robust consumer protection mechanisms, they were designed with a broad, generalised focus, often failing to account for the specific vulnerabilities of minors. This lack of a child-centric regulatory lens creates enforcement blind spots, mainly in AI-driven environments where subtle, system-level manipulations evade conventional oversight. For example, Article 25 of the DSA introduces prohibitions against manipulative *interface designs*. Yet, its applicability is narrowly confined to "online platforms", excluding standalone gaming applications, educational tools, and IoT devices like smart toys. Given that children frequently interact with digital spaces outside traditional online platforms, this limitation leaves significant gaps in regulatory coverage, particularly in environments where AI-driven persuasive techniques operate covertly.

The fragmented enforcement of the GDPR further underscores the need for a more cohesive regulatory approach. Articles 5 and 7 of the GDPR, which articulate principles of fairness and transparency in data processing, are insufficient in addressing AI systems that exploit children's behavioural data. While transparency mechanisms such as cookie banners provide upfront disclosures, they fail to address ongoing manipulative practices embedded within system architectures. Algorithmic nudging, behavioural reinforcement loops, and hyper-personalised engagement strategies continue to operate beneath the surface, dynamically adapting to user behaviour in ways that evade traditional regulatory scrutiny.

Amending frameworks like the GDPR and DSA to bridge these gaps presents substantial challenges. Both laws are relatively recent—the GDPR marking its fifth anniversary in 2023 and the DSA only recently entering into force—and revisiting them so soon risks disrupting regulatory stability, a cornerstone of EU policymaking. Additionally, piecemeal amendments may create inconsistencies, leading to a patchwork regulatory landscape where new provisions conflict with existing rules or fail to address emergent digital threats comprehensively. At the same time, one potential approach could involve expanding the scope of the DSA to cover non-platform environments; such a revision would require redefining key legal concepts and introducing potential ambiguities in enforcement.

The AI Act's Article 5(1)(b) represents an essential regulatory advance by explicitly prohibiting AI systems that exploit children's vulnerabilities. However, its practical application remains highly challenging, primarily due to its stringent evidentiary requirements for demonstrating "significant harm" and intent. Proving that an AI system deliberately exploits children's vulnerabilities requires extensive documentation and analysis, particularly when AI-driven recommendation engines evolve autonomously in response to engagement metrics. For example, social media algorithms that amplify harmful content to minors may exacerbate anxiety, self-esteem issues, or compulsive digital consumption, yet demonstrating that these systems intentionally exploit children—rather than merely optimising for engagement—presents a substantial legal and evidentiary hurdle.

These challenges raise fundamental concerns about the adequacy of existing regulatory frameworks in safeguarding minors from complex, adaptive AI-driven manipulations. Without more precise enforcement criteria, lower evidentiary thresholds for harm, and more muscular regulatory coordination across Member States, covert AI-driven manipulative design techniques will continue to evade meaningful oversight.

A more integrated and child-centric regulatory approach is needed to ensure that protections extend beyond high-profile platforms, including smaller, lesser-known operators that often escape scrutiny. For example, introducing mandatory child-focused impact assessments for all AI-driven systems, irrespective of their classification under the AI Act's risk categories, could provide an additional safeguard against the long-term harms associated with digital manipulation. Such measures would address cumulative risks, including the addictive effects of infinite scrolling, gamified engagement loops, and algorithmic content curation that reinforces compulsive usage patterns.

Furthermore, regulatory enforcement mechanisms require refinement to clarify evidentiary standards for demonstrating significant harm and intent under Article 5(1)(b) of the AI Act. Lowering the threshold for harm to include cumulative and diffuse impacts, such as the erosion of autonomy, increased susceptibility to digital coercion, or the exacerbation of social insecurities, would improve accountability for AI developers while ensuring that platforms cannot evade liability under overly restrictive interpretations of harm. Additionally, explicit recognition of children's unique vulnerabilities as an independent regulatory criterion would align EU digital policy with emerging research on child development, cognitive biases, and digital dependency.

However, strengthening protections for minors in digital environments must be balanced against concerns about regulatory complexity and potential barriers to innovation. Overregulation risks disproportionately impacting SMEs and emerging tech firms, which may lack the compliance infrastructure to navigate burdensome regulatory obligations. A tiered regulatory model, where obligations scale based on platform size, market power, and risk profile, could help streamline enforcement while maintaining robust child protection measures. Under such a model, large platforms with extensive behavioural data processing capabilities would be subject to more stringent requirements. At the same time, smaller operators could benefit from simplified compliance tools and proportionate reporting obligations.

Additionally, regulatory reform's political and institutional challenges cannot be overlooked. Consensus-building among Member States is often fraught with competing national priorities, particularly where digital regulation intersects with economic interests. Countries with strong digital economies may resist additional regulatory burdens, arguing that existing laws are sufficient if enforced effectively. Conversely, Member States with weaker enforcement infrastructures may advocate for greater centralisation of oversight mechanisms at the EU level to address cross-border regulatory inconsistencies. Balancing these divergent perspectives will ensure that future regulatory initiatives remain enforceable and politically viable.

Despite these challenges, the case for a more comprehensive, child-centric regulatory framework remains compelling. Existing legislation, while providing a strong foundation, fails to address the nuanced and often covert nature of AI-driven manipulations targeting minors. The limitations of the GDPR, DSA, and AI Act—combined with enforcement fragmentation and jurisdictional inconsistencies—underscore the need for a more structured and harmonised regulatory response. By prioritising children's digital rights, strengthening oversight mechanisms, and addressing interface-level and system-level manipulations, the EU can set a global benchmark for child protection in the digital age, reinforcing its broader commitment to fairness, transparency, and fundamental rights in algorithmically mediated environments.

7.4 CHALLENGES OF REVISING EXISTING LEGISLATION

Amending existing legislation to address the gaps outlined above poses significant challenges. Because the DSA and AI Act have only recently taken effect, revising their provisions risks introducing regulatory uncertainty and causing compliance fatigue among stakeholders. Moreover, piecemeal amendments to individual frameworks may exacerbate inconsistencies and overlaps, undermining the coherence of the EU's digital regulatory landscape. For example, expanding the DSA's scope to include non-platform environments would require redefining key terms and extending obligations to a broader range of entities. Such changes could dilute the regulation's platform focus while imposing disproportionate burdens on smaller operators.

Similarly, lowering the threshold for "significant harm" under the AI Act would necessitate re-evaluating its risk classification criteria, potentially creating confusion among developers and regulators alike. The GDPR's reliance on consent mechanisms further complicates efforts to address covert manipulations. Strengthening these provisions would require redefining consent standards and introducing new obligations for ongoing transparency and accountability. However, such changes risk overburdening DPAs, who are already struggling with enforcement challenges.

7.5 RECOMMENDATIONS FOR ACHIEVING COMPREHENSIVE PROTECTION FOR CHILDREN

Whether the necessary regulatory reforms are standalone legislation or a series of targeted amendments to existing laws remains uncertain. Regardless of the approach, ensuring meaningful protection for minors against AI-driven deceptive design requires, at a minimum, the following measures. These recommendations are critical for bridging the gaps in the current legal framework, ensuring that robust safeguards are implemented effectively through enhancements to existing legislation and more vigorous enforcement mechanisms:

1. **Expand the Digital Services Act's Scope** Extend the DSA's personal and material scope to cover all digital services frequently used by children, not just those explicitly classified as online platforms. Incorporate provisions that regulate covert manipulative practices embedded within system architectures, ensuring comprehensive oversight of digital environments that shape children's interactions and choices.
2. **Strengthen GDPR Enforcement Capabilities** Establish a centralised enforcement model or develop specialised units within existing authorities to prioritise minor cases. Improve coordination between

national enforcement bodies to enhance cross-border regulatory action, ensuring consistent application and strong protections across Member States.

3. **Refine the AI Act's Provisions on Manipulative Practices.** Modify Article 5(1)(b) by redefining the threshold for "significant harm" to account for cumulative and long-term impacts, particularly those affecting children's cognitive development, autonomy, and mental health. Establish clear evidentiary standards to facilitate enforcement, particularly in cases where AI-driven manipulation operates adaptively and dynamically, making intent and impact challenging to prove under existing legal tests.
4. **Introduce Proactive Compliance Measures** Require mandatory algorithmic audits and impact assessments for AI-driven digital services targeting children. These mechanisms should be designed to preemptively identify and mitigate risks associated with manipulative design, enhancing the protective capabilities of existing regulatory frameworks before harm occurs.
5. **Encourage Ethical Industry Practices.** Promote voluntary adoption of child-centred design principles through certification programmes and industry-led compliance initiatives. These measures would complement legal requirements, foster a culture of accountability, and encourage industry-wide best practices that prioritise children's well-being over commercial imperatives.

By focusing on these priorities, the European Union can strengthen its regulatory framework to provide comprehensive and adaptive protections for children, ensuring that safeguards evolve in step with AI-driven manipulative practices. Protecting minors in the digital environment demands a coherent and coordinated regulatory approach that balances robust enforcement with forward-looking reforms.

While existing frameworks such as the GDPR, DSA, UCPD, and AI Act provide a strong foundation, their inability to address system-level manipulations and AI-driven behavioural exploitation underscores the need for targeted legal and enforcement refinements. Immediate regulatory improvements should focus on:

- Expanding the DSA's applicability beyond traditional online platforms to capture non-platform digital services, including gaming environments, educational tools, and connected devices.
- Refining the AI Act's evidentiary requirements to ensure that proving significant harm does not exclude cases where AI-driven manipulations operate subtly but persistently.
- Incorporating explicit regulatory provisions to address system-level manipulations, ensuring that AI-driven persuasion techniques are not merely assessed through traditional UI-focused consumer protection models.
- Enhancing enforcement capacity and coordination, ensuring legal protections are applied uniformly and without prolonged delays.

Achieving these goals requires a strategic balance between regulatory ambition and practical enforceability. While comprehensive legislative reform may offer a unified framework, delays in implementation could hinder immediate protections. Conversely, incremental amendments—if well-coordinated—could rapidly address existing regulatory gaps while maintaining legal predictability. The European Union must carefully navigate these considerations, ensuring its legal framework evolves to protect minors effectively without stifling innovation or imposing disproportionate compliance burdens.

7.6 ADDRESSING ADDICTIVE DESIGN

The phenomenon of addictive design in digital services epitomises a profound tension within contemporary regulatory frameworks—one between the protection of individual autonomy and the commercial imperatives of profit-driven digital platforms. By exploiting cognitive biases and behavioural predispositions, these designs transform user interfaces into intricate systems of manipulation, entrenching dependency and distorting decision-making processes. Such practices challenge foundational consumer protection principles and raise pressing questions regarding the adequacy of existing legislative mechanisms to counter the pervasive commodification of attention.

Addressing Addictive Design in Digital Services

Explores the tension between protecting individual autonomy and the commercial motivations of profit-driven platforms that exploit cognitive and behavioural vulnerabilities.

Highlights manipulative tactics such as infinite scrolling, variable reward structures, and algorithmic personalisation, which entrench user dependency and distort decision-making.

Examines economic drivers, including ad revenue models and in-app purchase systems like loot boxes, which rely on addictive behaviours for profitability.

Identifies regulatory gaps in current frameworks (e.g., GDPR, UCPD, and DSA) that fail to adequately address structural manipulations and digital dependency, particularly for vulnerable groups like children.

Reviews emerging legislative efforts, including transparency obligations in the DSA and risk assessment frameworks in the AI Act, which aim to counter manipulative design practices.

Proposes a paradigm shift, advocating for integrated ethical design principles, accountability mechanisms, and international collaboration to combat addictive practices comprehensively.

Emphasises the urgency of safeguarding children and adolescents, citing their heightened susceptibility to digital exploitation and the associated risks to mental health and well-being.

At its core, addictive design operates through mechanisms that systematically undermine informed choice and volitional engagement. Infinite scrolling, variable reward structures, and algorithmic personalisation are exemplary tactics that capitalise on users' psychological vulnerabilities, including the fear of missing out (FoMO) and the innate responsiveness to intermittent rewards. As observed in the European Parliament's 2023 resolution, platforms deliberately engineer these features to extend engagement durations and amplify consumption behaviours, often at the expense of user well-being. The strategic deployment of recommender systems—optimised to prioritise platform objectives rather than user interests—exemplifies this dynamic. Such systems embed a structural asymmetry between users and platforms, where platforms subordinate users' autonomy to their commercial imperatives.

Economic motivations underpin the proliferation of these practices. Digital platform monetisation models rely on maximising user engagement as a vehicle for ad revenue and in-app purchases. Mechanisms such as loot boxes, which mimic gambling dynamics, illustrate the extent to which platforms exploit behavioural psychology to drive profit. The CERRE report on harmful online choice architecture elucidates this intersection of commerce and manipulation, highlighting how such practices disrupt market fairness and erode consumer trust.[cccvi] These issues align with broader concerns identified in the European Commission's Fitness Check of EU consumer law, which critiques the inadequacy of existing frameworks in addressing emerging challenges posed by dark patterns and manipulative personalisation.[cccvii] While Art. 5 of Directive 2005/29/EC (UCPD) prohibits misleading and aggressive commercial practices, its application to nuanced digital phenomena such as addictive design remains constrained by interpretative ambiguities.

This regulatory lacuna becomes particularly concerning in the context of vulnerable groups, most notably children and adolescents. The 2024 report on the commercial exploitation of children underscores the susceptibility of young users to targeted advertising, gamified content, and algorithmic manipulation. By leveraging minors' developmental immaturity, such practices exacerbate risks of excessive screen time, mental health issues, and exposure to harmful content. These dynamics not only contravene the protections articulated in Art. 24 of the EU Charter of Fundamental Rights but also challenge the efficacy of the GDPR's safeguards under Art. 8, which impose heightened restrictions on processing children's data. However, as these laws primarily address data protection concerns, they do not sufficiently constrain the structural designs perpetuating digital dependency.

Recent legislative initiatives attempt to recalibrate this imbalance. The DSA, through Arts. 25 and 35 introduce transparency obligations for recommender systems, seeking to illuminate their operational logic. However, transparency alone is insufficient to redress the entrenched asymmetry of power that enables addictive practices. The nascent AI Act offers a more substantive intervention by proposing risk assessment frameworks under Arts. 13 and 14, which account for algorithmic systems' societal and individual harms. Simultaneously, the European Parliament's call for a digital "right not to be disturbed" reflects a conceptual shift towards empowering users to disengage from attention-seeking features, thereby restoring agency within the digital ecosystem.[cccviii]

Despite these developments, a fundamental tension persists in regulatory instruments' capacity to address the deeply embedded economic incentives that drive addictive design. Current frameworks—spanning the GDPR, UCPD, and DSA—remain disparate and fragmented, limiting their ability to mitigate the harms of manipulative system architectures comprehensively. Moreover, while flexible, the principle-based approaches that characterise these instruments often result in protracted legal uncertainty, delaying the emergence of jurisprudence capable of providing normative clarity.

The persistence of addictive design thus signals a broader crisis in the governance of the digital environment. It reveals the limitations of existing legal structures and the wider ethical failures of a system that privileges profit over the public good. Addressing this crisis demands a paradigm shift in regulatory strategy that integrates ethical design principles, enforces robust accountability mechanisms, and fosters international coordination to confront the transnational nature of digital exploitation. Without such measures, the digital economy risks becoming irreversibly defined by its most exploitative practices, perpetuating a cycle of dependency that undermines both individual autonomy and collective trust in the digital age.

7.7 DARK PATTERNS AND EXPLOITATION OF VULNERABILITIES

Empirical studies on dark patterns, including the 2022 investigation and subsequent regulatory sweeps, underscore manipulative design strategies' pervasive and insidious nature across digital platforms. Evidence reveals that an overwhelming majority of widely used websites and applications—up to 97%—deploy at least one form of deceptive design, with regulatory audits by ICPEN and GPEN further corroborating that 75.7% of digital services incorporate exploitative mechanisms such as artificial urgency, concealed material information, and obstructive cancellation processes. These tactics have profound implications, particularly for children, who are disproportionately susceptible to coercive digital architectures. Research demonstrates that exposure to dark patterns can precipitate psychological distress, financial exploitation through predatory monetisation schemes such as loot boxes, and cognitive overload, which systematically undermines informed decision-making. The cumulative effect of these manipulative techniques is a measurable increase in anxiety and a corresponding decline in user confidence, particularly among vulnerable populations.

Despite existing regulatory interventions, the current legal framework remains inadequate in addressing the full complexity of deceptive design practices, particularly those that operate beyond the interface level. While the UCPD provides a foundational consumer protection mechanism, it is ill-equipped to confront digital manipulation's systemic and algorithmic dimensions. Its regulatory scope is constrained by interpretive ambiguities, particularly about emergent phenomena such as addictive design and personalised manipulation, which exploit behavioural vulnerabilities at scale. Furthermore, national implementation and enforcement disparities contribute to a fragmented regulatory landscape, leading to significant inconsistencies in consumer protections across Member States. A comprehensive and harmonised regulatory strategy is essential to address deceptive design's multifaceted nature, encompassing overt manipulative tactics and more opaque algorithmic exploitation embedded within backend system architectures. Crucially, interventions must extend beyond the prohibition of identifiable dark patterns to incorporate structural safeguards against algorithmically driven coercion. Regulatory mechanisms should integrate fairness-by-design principles akin to the data protection by design obligations enshrined in the GDPR, compelling platforms to embed consumer welfare considerations—particularly for vulnerable demographics such as children—throughout the entire lifecycle of digital service development.

Concurrently, the proliferation of addictive design mechanisms—such as autoplay, engagement streaks, and gamified reward structures—raises significant concerns regarding their role in fostering compulsive digital behaviours. These engagement-maximising strategies, deliberately engineered to capitalise on psychological vulnerabilities, pose considerable risks to user autonomy and well-being, with children particularly susceptible to the deleterious effects of digital dependency. Addressing these economic incentives necessitates a robust regulatory response that directly confronts the monetisation strategies underpinning compulsive platform engagement. Beyond prohibitory measures targeting the most egregious forms of addictive design, regulatory frameworks should impose obligations for rigorous behavioural impact assessments, mandating platforms to evaluate and mitigate the psychological consequences of their design choices. A duty of care framework should further compel digital service providers to take proactive measures in minimising harm associated with compulsive digital engagement, ensuring that platform architectures prioritise user well-being over extractive engagement imperatives.

Enforcement remains a critical challenge despite regulatory advancements. While transparency measures introduced by instruments such as the DSA represent progress, they do not address the deeper structural issues underpinning manipulative design. The EU must develop more sophisticated enforcement mechanisms, including automated systems capable of detecting deceptive practices at scale, and establish a centralised European dark pattern database to facilitate consistent and coordinated regulatory action. Regulators should introduce anti-circumvention provisions akin to those in the DMA, ensuring that platforms cannot exploit loopholes to perpetuate exploitative practices under the guise of compliance. The persistent prevalence of dark patterns and addictive design mechanisms highlights the structural deficiencies of existing regulatory frameworks and underscores the urgent need for a fundamental reorientation in digital governance. A paradigm shift is necessary—one that moves beyond reactive enforcement and towards proactive regulatory oversight that prioritises user autonomy, safeguards vulnerable populations, and embeds ethical considerations into the digital design at a systemic level. Without decisive intervention, the digital economy risks being increasingly defined by exploitative architectures that entrench power asymmetries, reinforcing a system where commercial imperatives consistently override fundamental rights and child protection.

7.8 CONCLUSION

This section offers a robust and forward-looking framework to address the complex regulatory gaps and challenges presented by digital platforms targeting children. By recognising the dual role of the recommendations—either as incremental amendments akin to the Modernisation Directive or as the foundation for an ambitious legislative initiative —this analysis underscores the adaptability and timeliness of the proposed measures. The recommendations navigate critical issues in protecting children's rights within digital environments, offering nuanced solutions across multiple dimensions of policy and legislation. They emphasise the urgency of addressing manipulative design features, algorithmic exploitation, and the inherent power asymmetries between platforms and their youngest users. Each recommendation balances legal precision with a forward-looking perspective, anticipating emerging risks and aligning with international commitments such as the UN Convention on the Rights of the Child (UNCRC). A recurring theme throughout this section is the necessity of harmonisation and coherence. The recommendations ensure compatibility with established principles by anchoring these proposals within existing frameworks—such as the GDPR, DSA, and UCPD—and suggesting targeted amendments. At the same time, they advocate for transformative additions that account for the unique vulnerabilities of children. For instance, integrating "Fairness by Design" principles into Article 25 GDPR or introducing comprehensive prohibitions on psychological triggers represents a paradigm shift in digital governance.

The section also highlights the critical role of enforcement and oversight in ensuring these legal and regulatory mechanisms achieve their intended outcomes. Enhanced monitoring capabilities for regulators, mandatory audits, and clear penalties for non-compliance are vital components of this framework. Moreover, including participatory mechanisms—such as feedback channels for children and parents—adds a dynamic layer to the regulatory design, fostering continuous improvement and accountability. In addition to the legal and regulatory recommendations, the section emphasises the importance of embedding ethical design principles into digital ecosystems. From mandating child-specific transparency obligations to enforcing stringent data minimisation practices, the proposed measures ensure that platforms comply with the law and align with broader societal values. This dual focus on legal compliance and ethical integrity is essential for creating a digital environment where children can safely engage, learn, and grow. Ultimately, this section is a call to action for policymakers, industry stakeholders, and civil society to prioritise the rights and well-being of children. Whether implemented as part of incremental legal updates or through the comprehensive vision of substantial law reform, these recommendations represent a decisive step towards safeguarding children from exploitation and manipulation. The EU can set a global benchmark for regulatory innovation and social responsibility in the digital age by fostering a more equitable, transparent, and child-centric digital ecosystem.

ANNEX I: DECEPTIVE DESIGN AND DARK PATTERNS IN EU LAW

Deceptive Design Tactic	Description	Examples	Relevant Legislation	Notes
Push Notifications and Instant Alerts	Platforms use frequent notifications to create FOMO, disrupting focus and encouraging re-engagement.	Constant notifications from gaming apps or social media.	**GDPR:** Articles 5(1)(a), 5(1)(c), 12, 25. **UCPD:** Annex I, No. 28 (prohibited commercial practices). **DSA:** Article 25 (prohibition of deceptive design). **AI Act:** Article 5(1)(b) (exploitation of vulnerabilities due to age or socio-economic status). **DMA:** Article 13(6). **Data Act:** Article 6(1).	GDPR applies if personal data is used to personalise notifications, nudging children into engagement loops (Articles 5(1)(b), 8). Article 8 GDPR requires verifiable parental consent for children under 13-16 (depending on Member State law), meaning push notifications prompting children to engage, consent to data sharing, or make in-app purchases could be unlawful if consent were not validly obtained. UCPD applies only in B2C contexts (Article 2(d)) but prohibits direct exhortations to children (Annex I, No. 28), meaning notifications urging children to make purchases or influence their parents may be unlawful. AI Act Article 5(1)(b) applies only if the notifications materially distort behaviour and cause significant harm (e.g., addiction, financial harm). If AI-driven notifications merely create engagement loops but do not meet the 'significant harm' threshold, enforcement under the AI Act is unlikely. The DSA's Article 25(1) applies only to UI-based DD, so algorithmically triggered push notifications designed to re-engage children are not covered unless they involve misleading UI elements. Article 25(2) ensures UCPD takes precedence. The DMA applies only to gatekeepers (Article 6(5)), meaning smaller apps targeting children would not be regulated. Data Act is relevant only if IoT-connected toys or smart devices use push notifications to manipulate children's interactions (Article 6(1)).

Variable Rewards and Loot Boxes	Incorporates gambling-like mechanics in games to encourage compulsive behaviours and spending.	Randomised loot boxes in gaming apps.	**GDPR:** Articles 5(1)(b), 5(1)(c), 6, 25. **UCPD:** Annex I, No. 16 (misleading practices). **DSA:** Article 34 (risk mitigation obligations for platforms). **AI Act:** Article 5(1)(a) (subliminal manipulation and deceptive AI). **DMA:** Article 6(5) (restrictions on manipulative user steering). **Data Act:** Article 4 (fairness in data access).	GDPR applies if personal data is used to personalise loot box probabilities (Articles 5(1)(b), 22), meaning AI-driven dynamic pricing of loot boxes based on children's behavioural patterns may be unlawful. Article 8 requires parental consent for profiling children, but randomised loot boxes without personal data processing would fall outside the GDPR scope. UCPD prohibits direct exhortations to children to make purchases (Annex I), meaning loot box mechanisms designed to push children into repeat spending unlawful Article 5(1)(b) prohibits AI-driven reward manipulation that exploits children's cognitive vulnerabilities, but only if the behaviour is distorted and causes significant harm (e.g., addiction, financial loss). DSA Article 25(1) applies if UI misleads (e.g., obscured loot box probabilities), but where financial loss occurs due to coercive mechanics, UCPD Annex I, No. 28 takes precedence. Scope remains issue for regulating gaming DMA applies only to gatekeepers (Article 6(5)), meaning most game developers escape its scope. Data Act is relevant if smart toys use algorithmic personalisation of in-game purchases based on children's behavioural data (Article 6(1)).

Misleading Visual Cues and Interface Manipulations	Bright visuals and misleading navigation paths direct children toward in-app purchases or data sharing.	Buy Now buttons camouflaged in animations.	**GDPR:** Articles 5(1)(a), 12(1), 25. **UCPD:** Annex I, No. 7 (misleading omissions). **DSA:** Article 25 (prohibition of deceptive design). **AI Act:** Article 5(1)(b) (exploitation of vulnerabilities). **DMA:** Article 13(6). **Data Act:** Article 6(1).	The GDPR applies if misleading visual cues involve deceptive personal data processing, particularly in obtaining consent from children (Articles 4(1), 5(1)(a), 8). Article 12 applies where visual cues mislead users into consenting. Article 7(3) ensures withdrawal is as easy as giving consent. Article 8 mandates that consent for data processing must be obtained from a parent or guardian for children under 13-16 (depending on Member State laws), meaning manipulative design nudging children into providing consent may violate transparency and fairness principles. The UCPD applies only in B2C transactions (Article 2(d)). Still, Annex I, No. 28 explicitly prohibits "direct exhortations" to children to buy products or persuade parents to do so (e.g., UI cues tricking children into in-app purchases). However, if a platform's manipulative interface does not involve a commercial transaction, the UCPD would not apply (e.g., social media platforms using misleading UI to encourage data sharing). The AI Act's Article 5(1)(b) prohibits AI systems that exploit children's vulnerabilities through deceptive interface manipulations, but only if the distortion of behaviour meets the cumulative test (exploitation + distortion + significant harm). Article 25(1) applies only to UI-based deception, such as bright colours or animations designed to mislead children into subscribing to services or sharing data. Article 25(2) clarifies that if UCPD already covers issues (e.g., deceptive UI leading to in-game purchases), the DSA does not create additional obligations. DMA applies only to gatekeepers (Article 6(5)), meaning smaller platforms that target children may escape its scope. The Data Act applies only if smart toys or IoT devices collect data from children. This means that deceptive UI in interactive toys or connected apps that encourage children to share personal information without parental consent could be scrutinised under the Data Act's transparency and control provisions (Article 4, 6(1)).

Subscription Traps and Obstructive Cancellations	Lures users into free trials that auto-renew into paid subscriptions, complicating cancellations.	Free trial offers lead to recurring fees and obscure cancellation paths.	**GDPR:** Articles 7(3), 12(1), 25. **UCPD:** Annex I, No. 29 (coercive contract mechanisms). **DSA:** Article 25 (manipulative design rules). **AI Act:** Article 5(1)(b) (exploitation of socio-economic vulnerabilities). **DMA:** Article 6(12) (restrictions on unfair retention practices). **Data Act:** Article 3(3) (consumer control over data).	GDPR applies if cancellation is obstructed through deceptive personal data processing (Article 5(1)(b)), such as requiring more steps to delete an account than to create one. Children's data should be easier to erase under Article 17 GDPR ("right to be forgotten"), but hidden settings may hinder compliance. UCPD prohibits misleading retention tactics (Annex I, No. 29), but only in B2C transactions, meaning non-commercial retention traps (e.g., school e-learning platforms) are outside its scope. Article 5(1)(b) of the AI Act prohibits AI-driven subscription traps that exploit children's lack of cognitive maturity to understand financial commitments, but only if harm results. DSA's Article 25(1) applies only to UI-based deception, meaning AI-powered behavioural nudges keeping children subscribed are not directly covered. Article 25(2) ensures that if UCPD applies, the DSA does not add additional obligations. DMA Article 6(12) applies only to gatekeepers (e.g., Apple, Google). UCPD Annex I, No. 29 covers coercive contract mechanisms (e.g., free trials auto-renewing with obstructive cancellation) Data Act applies only if IoT devices complicate cancellation (e.g., forcing smart toy resets to terminate a subscription). For standard UI deception, UCPD and GDPR are more relevant).

Addictive Design in Gaming and Social Media	Features like autoplay, infinite scrolling, and gamification exploit psychological vulnerabilities to maximise user engagement.	Infinite scrolling on social media, autoplay features on streaming apps, and gamified notifications in mobile games.	**GDPR:** Articles 5(1)(a), (b), 22, 25. **UCPD:** N/A (does not explicitly regulate addiction). **DSA:** Articles 25 (prohibition of deceptive design), 34 (systemic risk mitigation). **AI Act:** Article 5(1)(b) (exploitation of age-related vulnerabilities). **DMA:** Article 6(5); **Data Act:** Article 9.	GDPR applies if personal data is used to reinforce addictive behaviour (Articles 5(1)(b), 22), meaning AI-driven personalisation of autoplay, infinite scroll, or engagement loops for children may be unlawful if it significantly impacts autonomy and decision-making. Article 8 requires parental consent for data-driven profiling of children, meaning adaptive engagement mechanics (e.g., algorithmic content ranking designed to retain children) may be non-compliant if permission is not obtained correctly. The UCPD does not explicitly regulate addictive designs, but Article 6 (misleading omissions) could apply if platforms fail to disclose the harmful impact of engagement-maximising mechanics on children. The AI Act's Article 5(1)(b) prohibits AI-driven addictive loops that exploit children's cognitive vulnerabilities, but only if the behaviour is materially distorted and results in significant harm (e.g., mental health issues, loss of self-control over screen time). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning addictive mechanics at the algorithmic/system level (e.g., reinforcement learning-driven engagement maximisation) are not covered unless they involve misleading UI elements (e.g., "one more video" autoplay nudges). Article 25(2) clarifies that UCPD takes precedence if the addictive design leads to financial exploitation. The DMA applies only to gatekeepers (Article 6(5)), meaning that most gaming and social media platforms aimed at children are outside its scope. The Data Act applies if IoT devices or smart toys use addictive engagement mechanisms (e.g., connected toys rewarding extended play with additional content) (Article 6(1)).

Gambling-like Features and In-Game Purchases	Many games incorporate gambling-like features, such as loot boxes and virtual currencies for in-game purchases.	Loot boxes and virtual currencies in online games.	**GDPR:** Articles 5(1)(a), (b), 25; **UCPD:** Annex I, No. 16 (misleading about probabilities). **DSA:** N/A (platform risk accountability applies). **AI Act:** Article 5(1)(a) (subliminal manipulation in digital services). **DMA:** Article 6(5); **Data Act:** Article 7(1).	GDPR applies if personal data is used to personalise in-game purchases or dynamic pricing (Articles 5(1)(b), 22), meaning AI-driven pricing models that target children based on spending habits may be unlawful. Article 8 requires verifiable parental consent for profiling children, meaning some in-game purchases may not comply. The UCPD prohibits direct exhortations to children to make purchases (Annex I, No. 28), meaning in-game currency prompts that pressure children to buy more may be unlawful. The AI Act's Article 5(1)(b) prohibits AI-driven reinforcement loops designed to exploit children's impulsivity, but only if harm occurs. The DSA's Article 25(1) covers misleading UI cues (e.g., false scarcity or unclear purchase buttons), but systemic behavioural reinforcement techniques remain outside its scope. Article 25(2) ensures UCPD takes precedence. The DMA applies only to gatekeepers (Article 6(5)), meaning most game developers escape its scope. The Data Act applies if smart toys or connected devices nudge children into making purchases via IoT interfaces (Article 6(1)).

Algorithmic Personalisation and AI-Driven Targeting	Platforms use AI-driven personalisation to tailor content and advertisements, encouraging compulsive engagement.	Social media apps recommend addictive content based on user activity.	**GDPR:** Articles 5(1)(b), 12, 13, 22, 25; **UCPD:** Articles 6-7 (misleading omissions in algorithmic targeting). **DSA:** Article 26 (transparency obligations for profiling and targeting). **AI Act:** Article 5(1)(b) (exploitation of vulnerabilities through profiling). **DMA:** Article 6(3) (fairness in platform ranking). **Data Act:** Article 8.	GDPR applies if AI-driven personalisation involves personal data processing, particularly profiling or automated decision-making that influences children's content, advertising, or engagement patterns (Articles 5(1)(b), 22). Article 8 of GDPR requires verifiable parental consent for profiling children, meaning AI-based content recommendation engines that adapt based on children's behaviour without explicit parental approval may be unlawful. EDPB Guidelines 03/2022 highlight deceptive UI practices that manipulate consent under GDPR (e.g., misleading consent toggles, privacy-invasive defaults) The UCPD applies if algorithmic targeting results in misleading omissions or coercive practices (Articles 6-7), such as personalised ads disguised as organic content or dynamic pricing tailored to children's spending patterns. The AI Act's Article 5(1)(b) prohibits AI systems that exploit children's vulnerabilities, but only if they materially distort behaviour and cause significant harm (e.g., reinforcing compulsive engagement or social validation anxiety). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning system-level algorithmic personalisation that influences children's behaviour is not directly regulated unless UI elements mislead them (e.g., "Recommended for you" buttons that disguise ads). Article 25(2) clarifies that GDPR remains the primary law for AI-driven targeting. The DMA applies only to gatekeepers (Article 6(3)), meaning most children's platforms escape its scope. The Data Act applies if IoT devices or smart toys use AI-driven personalisation (e.g., connected toys adapting speech patterns based on children's emotional states) (Article 6(1)).

Photo Editing and Filters for Social Approval	Platforms offer editing tools and filters that subtly encourage children to alter their appearance to meet perceived social standards.	Beauty filters distort self-image.	**GDPR:** Articles 5(1)(a), 6. **UCPD:** Annex I, No. 22 (coercive commercial practices). **DSA:** N/A (platform risk assessment applies). **AI Act:** N/A (does not regulate aesthetic manipulation). **DMA:** Article 6(12). **Data Act:** Article 6(2).	GDPR applies if AI-driven filters or editing tools process children's biometric or personal data (Articles 4(1), 5(1)(a)), meaning AR-based beauty filters that modify facial features may be unlawful if used without explicit parental consent (Article 8 GDPR). Profiling children based on their photo editing habits for ad targeting is also restricted (Article 22 GDPR). The UCPD applies only in B2C transactions (Article 2(d)), meaning social media platforms using filters for non-commercial engagement loops (e.g., likes, shares) would not be covered unless linked to direct exhortations to children (Annex I, No. 28). The AI Act's Article 5(1)(b) prohibits AI-driven editing tools that exploit children's body image vulnerabilities, but only if the system materially distorts behaviour and leads to significant harm (e.g., self-esteem issues, body dysmorphia, or increased pressure to conform to unrealistic standards). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning systemic algorithmic reinforcement of filtered beauty norms is not covered unless UI deception is involved (e.g., hidden disclosures about filter use). Article 25(2) clarifies that GDPR remains the primary regulation for filter biometric processing. The DMA applies only to gatekeepers (Article 6(5)), meaning most platforms children use escape its scope. The Data Act applies if smart mirrors, connected cameras, or AR-powered IoT devices use real-time photo enhancement on children (Article 6(1)).

Artificial Scarcity and Urgency Prompts	False urgency, such as countdown timers and limited-time offers, pressures children into impulsive decisions.	Countdown timers pressuring purchases.	**GDPR:** Articles 5(1)(a), (b), 25. **UCPD:** Annex I, No. 7 (false scarcity practices). **DSA:** Article 25 (prohibition of urgency-based dark patterns). **AI Act:** Article 5(1)(b) (exploitation of cognitive vulnerabilities). **DMA:** Article 6(5). **Data Act:** Article 9.	GDPR applies if scarcity-based tactics involve deceptive personal data processing (Articles 4(1), 5(1)(a)), such as using AI to detect children's engagement patterns and trigger "limited-time" offers at psychologically vulnerable moments. Article 8 of GDPR requires parental consent to profile children for urgency-based nudging. The UCPD prohibits false urgency tactics (Annex I, No. 7), meaning countdown timers or "only a few left" messages that mislead children into impulsive purchases may be unlawful. The AI Act's Article 5(1)(b) prohibits AI systems that exploit children's cognitive biases toward scarcity, but only if they distort behaviour and lead to significant harm (e.g., compulsive buying habits or distress over missing out). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning AI-driven scarcity tactics that operate at the system level (e.g., algorithmically generated urgency prompts) are not directly regulated unless they use misleading UI (e.g., fake "low stock" indicators). Article 25(2) ensures that if UCPD applies, the DSA does not impose additional obligations. The DMA applies only to gatekeepers (Article 6(5)), meaning most platforms targeting children escape its scope. The Data Act applies if IoT-connected toys or devices use artificial scarcity prompts to manipulate engagement (Article 6(1)).

Dopamine Hits from 'Likes' and Notifications	Social interactions, such as likes and comments, create dopamine-driven feedback loops, fostering dependency.	Social media fosters engagement dependency.	**GDPR:** Articles 5(1)(a), 6. **UCPD:** N/A (does not directly regulate addictive design). **DSA:** Article 25 (prohibition of manipulative engagement design). **AI Act:** N/A (does not restrict dopamine loops). **DMA:** Article 6(3). **Data Act:** Article 6(2).	GDPR applies if dopamine-driven reinforcement loops rely on personal data processing (Articles 4(1), 5(1)(a)). AI-driven social validation cycles that personalise notifications to keep children engaged may be unlawful without explicit parental consent (Article 8 GDPR). The UCPD does not directly regulate dopamine-driven mechanisms, but Articles 6-7 could apply if platforms omit information about the mental health risks of excessive social validation cycles. The AI Act's Article 5(1)(b) prohibits AI-driven engagement systems that exploit children's psychological vulnerabilities, but only if they materially distort behaviour and lead to significant harm (e.g., compulsive checking of notifications, anxiety over likes, or social withdrawal). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning AI-driven social validation reinforcement (e.g., dynamic-like counts, peer comparison rankings) is not covered unless UI deception is involved. Article 25(2) clarifies that GDPR remains the primary regulation for social validation mechanics using personal data. The DMA applies only to gatekeepers (Article 6(5)), meaning most children's platforms escape its scope. The Data Act applies if smart toys, connected wearables, or social IoT devices use AI-driven engagement feedback loops to reinforce dopamine-triggering behaviours (Article 6(1)).

In-App Purchases and 'Freemium' Traps	Many free apps entice children to make in-app purchases, exploiting their limited understanding of digital economies.	Games offering in-app purchases for progress boosts.	**GDPR:** Articles 5(1)(b), 12. **UCPD:** Annex I, No. 22 (coercive commercial practices). **DSA:** Article 25 (prohibition of deceptive freemium models). **AI Act:** N/A (focuses on subliminal AI). **DMA:** Article 6(5). **Data Act:** Article 7(1).	GDPR applies if in-app purchases or freemium traps rely on personal data processing (Articles 4(1), 5(1)(a)), meaning AI-driven dynamic pricing of in-app purchases or rewards based on children's behaviour may be unlawful if parental consent was not obtained (Article 8 GDPR). Article 22 GDPR restricts automated decision-making that significantly affects individuals, meaning pricing models that adapt to children's spending habits through behavioural tracking may violate fairness principles. The UCPD prohibits direct exhortations to children to make purchases (Annex I, No. 28), meaning apps or games that pressure children into spending—especially by manipulating emotions ("Your friends bought this power-up!")—may be unlawful. The AI Act's Article 5(1)(b) prohibits AI-driven monetisation strategies that exploit children's cognitive vulnerabilities, but only if they materially distort behaviour and lead to significant harm (e.g., compulsive spending or financial harm to parents). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning system-level algorithmic pricing strategies are not covered unless UI deception is involved (e.g., hiding total costs, using misleading "buy" buttons, or making cancellation difficult). Article 25(2) ensures that if UCPD applies, the DSA does not impose additional obligations. The DMA applies only to gatekeepers (Article 6(5)), meaning most gaming and children's app developers escape its scope. The Data Act applies if IoT-connected toys or devices use dynamic pricing mechanisms to encourage purchases (e.g., smart learning apps adjusting pricing based on children's engagement levels) (Article 6(1)).

Constant Distractions through Multi-Tasking Encouragement	Platforms send notifications, messages, and alerts across multiple apps, fragmenting attention and increasing screen time.	Notifications disrupt focus and increase screen time.	**GDPR:** Articles 5(1)(a), (b). **UCPD:** N/A (does not regulate cognitive overload). **DSA:** Article 25 (prohibition of disruptive notifications). **AI Act:** N/A (AI manipulative design applies in other contexts). **DMA:** Article 6(12). **Data Act:** Article 6(2).	GDPR applies if multi-tasking distractions rely on personal data processing, such as AI-driven notifications or real-time engagement prompts tailored to children (Articles 4(1), 5(1)(a)). Article 8 of GDPR requires verifiable parental consent for profiling children, meaning platforms using engagement-based tracking to trigger real-time distractions may be unlawful if permission is not obtained. The UCPD does not directly prohibit distraction-based design, but Articles 6-7 could apply if platforms omit information about the cognitive impact of constant interruptions on children. The AI Act's Article 5(1)(b) prohibits AI-driven distraction mechanisms that exploit children's cognitive vulnerabilities, but only if they materially distort behaviour and lead to significant harm (e.g., attention deficits, stress, or sleep disruption). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning AI-driven distraction loops that operate at the system level (e.g., multi-tasking prompts or forced app-switching) are not covered unless UI deception is involved (e.g., forced pop-ups with misleading close buttons). Article 25(2) clarifies that GDPR remains the primary regulation for distraction-based tracking. The DMA applies only to gatekeepers (Article 6(5)), meaning most children's platforms escape its scope. The Data Act applies if smart toys or connected devices use AI-driven distractions to keep children engaged (e.g., IoT-based game notifications pulling children back into apps) (Article 6(1)).

Autoplay and Infinite Scrolling	Features like autoplay and infinite scrolling reduce natural stopping points, making disengaging challenging.	Endless scrolling makes it difficult to stop.	**GDPR:** Articles 5(1)(a), (b), 25. **UCPD:** Annex I, No. 7 (manipulative design omissions). **DSA:** Article 25 (prohibition of infinite scrolling). **AI Act:** Article 5(1)(b) (exploitation of user attention vulnerabilities). **DMA:** Article 6(5); **Data Act:** Article 9.	GDPR applies if autoplay or infinite scrolling relies on personal data processing (Articles 4(1), 5(1)(a)), meaning AI-driven recommendation systems that endlessly serve content to children may be unlawful without verifiable parental consent (Article 8 GDPR). Article 22 of GDPR restricts automated decision-making that significantly affects individuals, meaning personalised infinite scrolling designed to retain children may face scrutiny. The UCPD does not explicitly regulate autoplay or infinite scrolling, but Articles 6-7 could apply if platforms omit information about how endless engagement loops affect children's well-being. The AI Act's Article 5(1)(b) prohibits AI-driven autoplay or infinite scroll features that exploit children's cognitive vulnerabilities, but only if they materially distort behaviour and lead to significant harm (e.g., excessive screen time, sleep deprivation, or compulsive viewing habits). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning algorithmically driven infinite scrolling mechanisms are not covered unless UI deception is involved (e.g., hiding exit options or misleading pause buttons). Article 25(2) ensures that if UCPD applies (e.g., for content monetisation tactics), the DSA does not impose additional obligations. The DMA applies only to gatekeepers (Article 6(5)), meaning most children's platforms escape its scope. The Data Act applies if IoT devices or smart toys use algorithmic autoplay mechanisms (e.g., interactive toys that continually trigger new activities to prevent disengagement) (Article 6(1)).

Data Collection and Profiling	Platforms collect extensive data on children's interactions, creating detailed profiles that inform targeted engagement and advertising.	Children unknowingly contribute personal data to profiling.	**GDPR:** Articles 5(1)(a), (b), 25. **UCPD:** Annex I, No. 7 (misleading profiling practices). **DSA:** Article 25 (prohibition of deceptive tracking). **AI Act:** Article 5(1)(b) (exploitation through extensive data collection). **DMA:** Article 6(5). **Data Act:** Article 9.	GDPR vigorously protects children's data (Article 8), requiring parental consent before processing personal data for profiling. If a child unknowingly consents to tracking, the processing is unlawful. Article 22 of GDPR restricts automated decision-making affecting children, meaning AI-driven profiling of children for marketing is heavily scrutinised. The UCPD does not directly address data collection but prohibits misleading omissions about tracking (Articles 6-7). The AI Act's Article 5(1)(b) prohibits AI systems that exploit children's data vulnerabilities, but only if profiling materially distorts behaviour and causes harm. The DSA's Article 25(1) applies to UI-based dark patterns that mislead children into sharing data, but Article 25(2) clarifies that GDPR remains the primary law for data collection. The DMA applies only to gatekeepers (Article 6(5)), meaning most children's apps escape its scope. The Data Act is particularly relevant for smart toys and IoT devices that collect children's behavioural data, meaning toys that profile children's speech patterns or emotions could be scrutinised under Article 6(1).

Inadequate Transparency and Consent Mechanisms	Consent prompts are often simplified to expedite agreement, encouraging children to share data without fully understanding the implications.	Simplified consent mechanisms misleading children.	**GDPR:** Articles 5(1)(a), (b), 12. **UCPD:** Annex I, No. 7 (misleading consent mechanisms). **DSA:** Article 25 (prohibition of deceptive consent flows) **AI Act:** Article 5(1)(b) (exploitation of lack of informed consent). **DMA:** Article 6(5). **Data Act:** Article 9.	GDPR has strict rules for obtaining children's consent (Article 8), meaning simplified, deceptive, or hidden consent prompts designed to trick children into agreeing to data collection are unlawful. Article 12 GDPR requires transparent, intelligible information on how data is used, meaning consent pop-ups that obscure key privacy details or force misleading "accept all" options could violate data protection principles. The UCPD prohibits misleading omissions and coercive consent tactics (Articles 6-7), meaning websites or apps that disguise data collection agreements within non-essential settings could be unlawful in a B2C context. The AI Act's Article 5(1)(b) prohibits AI-driven consent mechanisms that exploit children's limited digital literacy, but only if the behaviour is distorted and results in significant harm (e.g., large-scale tracking without understanding the risks). The DSA's Article 25(1) applies only to UI-based deceptive design, meaning dark patterns in consent mechanisms (e.g., pre-checked boxes, unclear opt-outs) are covered. Still, algorithmic consent manipulation at the system level is not. Article 25(2) clarifies that if GDPR applies, the DSA does not impose additional obligations. The DMA applies only to gatekeepers (Article 6(5)), meaning most platforms targeting children escape regulation. The Data Act applies if IoT devices or smart toys use deceptive consent flows to encourage children to share personal data (Article 6(1)).

ANNEX II: RECOMMENDATIONS

Protecting Children from Deceptive and Manipulative Digital Practices: A Regulatory Framework

The rapid evolution of digital technologies and platforms has created a landscape fraught with challenges for protecting children's rights. In this environment, manipulative design techniques and algorithmic decision-making systems disproportionately exploit children's vulnerabilities. This Annex presents a structured and forward-looking set of 20 recommendations to address these pressing concerns, offering a dual-purpose legal and regulatory reform roadmap. These recommendations serve two complementary functions. First, they provide a blueprint for incremental legal amendments consistent with the Modernisation Directive, which updated EU consumer protection laws to reflect the digital age better. Second, they offer a comprehensive framework should policymakers pursue a more ambitious, cohesive initiative to systematically close regulatory gaps and establish robust protections for children across the EU. Recognising that existing frameworks such as the GDPR, DSA, and UCPD provide foundational protections but fail to address children's unique risks, this Annex identifies and addresses fundamental shortcomings in the current legal landscape. The recommendations are designed to ensure that regulatory protections evolve in tandem with the complexities of modern digital ecosystems, striking a balance between prevention and enforcement. This section analyses twenty deceptive design techniques prevalent in digital environments, particularly those disproportionately affecting children. These techniques are contextualised through short case studies, illustrating the mechanisms through which manipulative digital architectures operate and the extent to which they exploit children's cognitive and developmental vulnerabilities. Each case study follows a structured format:

1. **Synopsis of the Problem:** This section provides an overview of the deceptive practice, detailing how it manifests in digital environments, manipulates or coerces users—particularly children—into making choices that do not align with their best interests, and the commercial incentives driving these practices.

2. **Impact on Children:** This section examines why the technique is especially harmful to children, considering cognitive immaturity, limited digital literacy, and susceptibility to persuasive design. Where relevant, empirical research and behavioural science substantiate claims regarding the disproportionate impact of these manipulative strategies.

3. **Regulatory and Legislative Recommendations:** Tailored solutions for regulatory intervention, focusing on maximum harmonisation where feasible to establish explicit, enforceable prohibitions against deceptive digital practices. This ensures that platforms prioritise user protection over commercial gain.

4. **Targeted Amendments for Incremental Reform:** In cases where minimum harmonisation is more appropriate, the analysis identifies specific legal provisions requiring amendment to extend protections to children. This includes targeted modifications to existing legislation, such as the UCPD, DSA, GDPR, and sector-specific laws, to ensure deceptive practices targeting children are effectively prohibited.

Addressing systemic exploitation requires a balance of proactive measures and robust enforcement. This framework advocates for a dynamic interplay between:

- **Preventative Measures:** Transparency obligations, ethical design requirements, and accountability mechanisms that ensure platforms prioritise children's welfare.

- **Enforcement Mechanisms:** Fines, operational restrictions, and other penalties for non-compliant platforms to create strong deterrents against exploitative practices.

Ultimately, this Annex seeks to inspire a paradigm shift in regulating digital environments, advocating for robust and harmonised protections prioritising children's well-being, autonomy, and rights. Whether pursued incrementally or through a comprehensive legislative initiative, these recommendations provide a clear and actionable vision for safeguarding the most vulnerable users in our increasingly digital world.

INTRODUCE CHILD-SPECIFIC DARK PATTERN PROHIBITIONS: EXPLICITLY BAN DARK PATTERNS TARGETING MINORS IN THE DFA, FOCUSING ON ADDICTIVE DESIGNS AND MANIPULATIVE CHOICE ARCHITECTURES.

INTRODUCE CHILD-SPECIFIC DARK PATTERN PROHIBITIONS

Digital platforms exploit the cognitive and emotional vulnerabilities of children through dark patterns—deceptive design techniques that manipulate behaviour. These tactics, including gamified rewards, false urgency claims, and obfuscation of critical choices, disproportionately affect minors, who have a limited capacity to discern commercial intent. By undermining autonomy, fostering compulsive engagement, and exposing children to economic harm, these practices pose a significant threat to their well-being. Despite the protections offered by the UCPD, GDPR, and DSA, current legal frameworks fail to address these vulnerabilities adequately. Comprehensive reform is urgently required to protect children from digital exploitation. While the UCPD prohibits unfair commercial practices, it does not explicitly address the manipulation of children in digital contexts. The GDPR, though robust in its data protection principles, inadequately restricts the use of children's behavioural data to construct manipulative choice architectures. Similarly, the DSA's prohibition of visible dark patterns does not extend to algorithmic or systemic manipulations that dominate the digital ecosystem. These regulatory gaps allow platforms to deploy opaque systems to exploit children's behavioural and emotional vulnerabilities.

Remedies: Amendments to Existing Laws

1. **Expand the UCPD Annex I** Specific child-targeted dark patterns should be explicitly blacklisted. Practices such as gamified reward loops, loot boxes linked to real-world spending, and deceptive mechanisms that promote in-app purchases must be prohibited. These amendments would establish clear and enforceable standards, ensuring platforms cannot exploit children through manipulative interface design.
2. **Enhanced Protections Against Profiling and Manipulative Consent Mechanisms** Protections against profiling and manipulative consent mechanisms must be substantially enhanced to counter the exploitation of children's behavioural data. Current GDPR provisions, particularly Article 8, require a sharper focus on the specific vulnerabilities of minors in digital environments. This could involve establishing explicit prohibitions on designing consent flows that intentionally exploit children's impulsivity, lack of digital literacy, or inability to grasp long-term consequences. Platforms should also be barred from leveraging behavioural data to create predictive profiles that encourage compulsive behaviours, such as excessive spending or prolonged engagement with addictive content. Strengthening these provisions involves stricter limits on data collection and processing and mandating child-centric consent designs. For example, platforms could employ simple, gamified designs that are intuitive and informative for children instead of complex or vague consent interfaces. Additional layers of protection could include requiring parental verification in clear and transparent terms, ensuring that consent is meaningful and not a rubber-stamping exercise. By addressing these critical gaps, the GDPR can more effectively safeguard children's rights to privacy and autonomy in digital spaces.
3. **Broaden the Scope of DSA Article 25** The DSA should extend its prohibition of dark patterns beyond visible user interface manipulations to include algorithmic and systemic practices. This expansion would address the increasingly sophisticated methods platforms use to exploit children's vulnerabilities.

BAN HIDDEN AND DECEPTIVE ADVERTISEMENTS: PROHIBIT IN-GAME AND APP-BASED ADVERTISING THAT IS NOT CLEARLY DISTINGUISHED FROM CONTENT, PARTICULARLY ADS THAT ENCOURAGE PURCHASES THROUGH PLAYFUL OR INTERACTIVE FEATURES.

7.2.2 BAN HIDDEN AND DECEPTIVE ADVERTISEMENTS

Hidden and deceptive advertisements in games and apps manipulate user behaviour by blurring the boundaries between content and marketing. These tactics disproportionately harm children, who often cannot distinguish between entertainment and advertising. Interactive ads, such as those embedded in mini-games or gamified rewards, encourage impulsive purchases and foster unhealthy consumer habits. Although EU law, including the UCPD, prohibits misleading commercial practices under Article 5, it does not adequately address the unique challenges posed by hidden advertisements in digital environments. The DSA's transparency requirements focus on advertising disclosures but fail to prevent ads from integrating seamlessly into gameplay or app interfaces. These practices exploit minors' developmental limitations, embedding calls to action that mimic entertainment and gameplay mechanics. The absence of explicit safeguards for hidden and interactive advertisements targeting children leaves a significant regulatory gap. The manipulative nature of these practices undermines fundamental principles of fairness and informed consumer choice, particularly for vulnerable groups like children. A robust regulatory framework must address these gaps to safeguard children's rights and create a more transparent and ethical digital ecosystem.

Remedies: Amendments to Existing Laws

1. **Amend the UCPD to Blacklist Hidden and Interactive Ads** Annex I of the UCPD should explicitly prohibit advertisements that use gamification or other interactive features to disguise their commercial intent. Adding these practices to the UCPD's blacklist would give regulators across Member States the authority to target and penalise platforms that deploy deceptive ads in games and apps aimed at children.

2. **Strengthen Transparency Provisions in the DSA** Article 24 of the DSA must mandate that in-game and app-based advertisements targeting minors feature clear, age-appropriate labelling. These requirements should include distinct visual markers, such as bolded "Ad" labels, and auditory cues, such as brief sounds indicating commercial content. This approach aligns with Article 7 of the UCPD, ensuring clarity and non-misleading communication.

Legal Provisions for Amendment

1. **UCPD** Annex I must explicitly blacklist interactive and hidden advertisements targeting children. These amendments should ensure regulators universally recognise gamified advertising practices as unfair and subject them to strict enforcement.

2. **DSA** Strengthening Article 24 would ensure that advertisements embedded in gameplay or app interfaces meet stringent labelling and transparency requirements. Expanding these provisions to address gamified ads would align the DSA with broader consumer protection objectives.

RESTRICT USE OF PERSUASIVE DESIGN TECHNIQUES: BAN OR RESTRICT THE USE OF SPECIFIC PERSUASIVE DESIGN TECHNIQUES IN CHILDREN'S ONLINE ENVIRONMENTS, ESPECIALLY THOSE INTENDED TO INDUCE REPETITIVE OR ADDICTIVE ENGAGEMENT.

RESTRICT THE USE OF PERSUASIVE DESIGN TECHNIQUES

Explanation Persuasive design techniques, such as gamification, infinite scrolling, and variable reward schedules, exploit behavioural psychology and cognitive biases, including children's underdeveloped impulse control and reward-driven behaviours. These strategies foster compulsive engagement, undermining autonomy and informed decision-making, as outlined in the BEUC position paper and the CERRE report on harmful choice architecture. Deliberately engineered to exploit behavioural vulnerabilities, these methods drive repetitive engagement and often result in addictive behaviours. Children less equipped to resist such influences due to cognitive and emotional vulnerabilities are particularly susceptible to these persuasive strategies.

These mechanisms amplify risks of mental health harm, including anxiety, depression, and attention disorders. Excessive screen time driven by engagement-maximising designs disrupts sleep patterns and physical activity, leading to long-term developmental consequences. Reports on the commercial exploitation of children emphasise the significant risks associated with these practices, highlighting how such designs exacerbate psychological and physical challenges. By targeting minors, these techniques also blur ethical boundaries, undermining children's autonomy and their ability to make informed decisions.

Monetised techniques, such as gamified rewards and loot boxes, further push children into overspending while exposing them to covert marketing and data exploitation. These mechanisms frequently blur the line between entertainment and manipulation, creating a heightened risk of consumer exploitation. Current EU frameworks, such as the UCPD, prohibit misleading or aggressive practices but fail to address manipulative behavioural techniques that induce explicit compulsive engagement. Similarly, while the DSA and the AI Act provide transparency and accountability measures for specific digital environments, they lack explicit bans on persuasive designs that exploit children's vulnerabilities.

Significant legal and policy gaps remain despite regulatory advances, demanding urgent reform. Exploiting behavioural psychology through persuasive design techniques, such as gamification, infinite scrolling, and variable rewards, represents a pressing regulatory and ethical challenge. These mechanisms, designed to maximise engagement, have led to concerning outcomes, particularly for children. The BEUC position paper and CERRE report underscore the urgent need for regulatory updates to safeguard children from manipulative digital practices that compromise their well-being and autonomy.

Suggested Remedies

Standards for Transparency in Content Recommendation Systems

1. **Explainability:** Platforms must provide clear, age-appropriate explanations of how recommendation algorithms operate and the factors influencing content display. These explanations should include interactive visualisations, simplified descriptions, and child-friendly language to ensure accessibility and understanding for younger audiences.
2. **Data Disclosure:** Platforms should transparently disclose data collection and usage practices, including retention policies, sharing protocols, and profiling methods used for personalisation. Such disclosures empower children and their guardians to understand and control their digital interactions.
3. **Content Labelling:** Sponsored content, advertisements, and potentially harmful or misleading information must be clearly labelled using distinct visual cues and standardised labels. Transparent explanations of these formats should be accessible to ensure children can differentiate between organic and paid content.

Child-Specific Safeguards in Digital Environments

1. **Age-Based Filtering:** Platforms can prevent children from encountering inappropriate or harmful content by implementing granular, adaptable filtering options tailored to different age groups. These filters should be updated regularly to address emerging risks and reflect the evolving digital landscape.

2. **Non-Manipulative Design:** Prohibit features that exploit children's cognitive vulnerabilities, such as dark patterns and addictive mechanics. Implementing such measures requires adopting a child-centric design philosophy prioritising children's well-being over commercial interests.
3. **Human Oversight:** Platforms should introduce human oversight and moderation for AI-driven content recommendations. Such oversight should involve independent auditors, child development experts, and ethical AI review boards to ensure adherence to child protection standards.

Proposed Legal Amendments

Unfair Commercial Practices Directive (UCPD):

- Amend Annex I to explicitly ban persuasive design techniques targeting children, such as infinite scrolling, variable reward schedules, and gamified interactions. Categorise these as unfair commercial practices that exploit cognitive vulnerabilities.

Digital Services Act (DSA):

1. Expand Article 24 to require platforms to provide detailed, child-friendly explanations of content recommendation algorithms and their implications for children's digital experiences.
2. Strengthen Article 25 by explicitly prohibiting manipulative practices targeting children through AI-driven profiling and content recommendations.

Artificial Intelligence Act (AI Act):

- Reinforce Amend Article 5(1)(b) to prohibit AI systems' exploitation of children's vulnerabilities. The amendment should require platforms to conduct Child Rights Impact Assessments (CRIAs) to evaluate content recommendation systems' potential harm to children's autonomy, decision-making, and well-being. Align Articles 13–14 with child-specific safeguards, mandating ethical AI audits, transparent design logic disclosure, and compliance reporting.

The EU can address significant legal and policy gaps to protect children from exploitative content and manipulative design by combining transparency measures, child-specific safeguards, and regulatory enforcement mechanisms. These measures promote ethical digital environments where children can engage responsibly, autonomously, and safely.

PROHIBIT THE USE OF PSYCHOLOGICAL TRIGGERS IN CHILD-ORIENTED APPS: FORBID THE USE OF PSYCHOLOGICAL TRIGGERS, SUCH AS TIME-BASED REWARDS AND FLASHING COLOURS, AIMED AT PROLONGING ENGAGEMENT AMONG YOUNG USERS.

PROHIBIT USE OF PSYCHOLOGICAL TRIGGERS IN CHILD-ORIENTED APPS

Explanation

Psychological triggers in child-oriented apps represent a pervasive and harmful form of digital manipulation, exploiting the cognitive and emotional vulnerabilities of young users. Developers deliberately design these triggers—such as time-based rewards, flashing colours, countdowns, and persistent notifications—to captivate attention, prolong engagement, and foster dependency. By leveraging principles from behavioural psychology, these techniques exploit a child's underdeveloped impulse control, limited ability to detect manipulation, and heightened sensitivity to external stimuli. The result is not only compulsive use but also significant harm to children's autonomy, well-being, and mental health. Children, as a uniquely vulnerable demographic, lack the cognitive maturity to evaluate or resist such manipulative techniques critically. Children's susceptibility to external influences due to their developmental stage makes them vulnerable to psychological triggers that shape behaviours, preferences, and decision-making processes. Unlike adults, who generally have greater self-regulation and awareness of manipulative tactics, children are more easily affected. As a result, they may experience adverse outcomes such as excessive screen time, disrupted sleep patterns, heightened anxiety, and a reduced ability to make independent decisions.

These practices distort children's ability to make informed decisions, fostering addictive behaviours that can have far-reaching developmental consequences. Over time, the impact of these manipulations becomes more severe, contributing to social isolation, cognitive impairments, and entrenched behavioural dependencies. The harm extends beyond the individual, influencing societal norms around ethical design and prioritising engagement metrics over child welfare. Despite their detrimental effects, psychological triggers often escape regulatory scrutiny due to gaps in existing frameworks. Regulations intended to address harmful manipulative practices usually impose high evidentiary thresholds, such as requiring proof of significant harm or a material distortion of behaviour. These thresholds make it challenging to enforce rules against pervasive but subtle techniques, allowing platforms to embed psychological triggers into child-oriented apps with impunity.

Current consumer protection laws fail to categorise psychological triggers as inherently manipulative or unfair, leaving a significant regulatory void. Without explicit legal prohibitions, platforms continue to deploy mechanisms such as flashing notifications, countdown timers, and gamified rewards. Developers strategically design these features to bypass children's cognitive defences, manipulating their behaviour in ways they cannot recognise or resist. The cumulative impact of these practices is profound. These triggers undermine fundamental principles of fairness and transparency by fostering digital environments that prioritise engagement over well-being. They create a digital ecosystem where commercial interests outweigh the developmental needs of children, compromising their autonomy and mental health. Addressing this issue requires a comprehensive legal framework that explicitly recognises and prohibits psychological triggers in digital environments targeting children. Amendments to existing laws must lower evidentiary thresholds and categorise these triggers as manipulative practices that violate child protection standards. Complementary measures should ensure that all digital designs targeting children are subject to stringent oversight, prioritising well-being, autonomy, and ethical responsibility. By enforcing such protections, regulators can foster a digital ecosystem prioritising children's development and welfare over commercial objectives.

Suggested Remedies

A robust regulatory framework is required to explicitly prohibit psychological triggers in child-oriented digital environments, ensuring that children's rights, autonomy, and well-being are protected. These remedies should address such manipulative practices' technical and ethical dimensions, closing existing regulatory gaps and fostering consistent enforcement across the EU.

1. **Define Psychological Triggers with Precision**

The AI Act establishes a comprehensive and nuanced definition of psychological triggers, describing them as stimuli or mechanisms for exploiting behavioural or cognitive vulnerabilities.

Examples include:

- **Time-Based Rewards:** Systems that condition user behaviour through countdowns or timed incentives.
- **Flashing Colours and Notifications:** Visual stimuli engineered to capture attention and sustain engagement.
- **Gamified Interactions:** Features such as points, badges, and leaderboards that manipulate competitive instincts and reinforce compulsive behaviours.
- **Persistent Prompts:** Repeated nudges encouraging continued use, such as reminders to log in or unlock features within a specified timeframe.

This definition must encompass overt and covert techniques, acknowledging the cumulative and indirect harm caused by such mechanisms. It should further clarify that intent to manipulate is not a prerequisite for enforcement; the presence of exploitative outcomes is sufficient to trigger regulatory action.

2. Ban Psychological Triggers in Child-Oriented Apps

Law reform must institute a categorical prohibition on psychological triggers within any digital environment targeting individuals under 18. This prohibition should:

- Apply universally across all child-oriented apps, irrespective of platform size, business model, or sector.
- Include environments where children make up a significant user demographic, even if the app does not explicitly target minors in its marketing.
- Preclude reliance on harm thresholds, ensuring that triggers are banned outright without requiring evidence of a "significant probability of harm," as stipulated in **Article 5(1)(b)** of the AI Act.
- Extend to hybrid features, such as reward systems combined with persistent notifications, which amplify manipulative effects.

3. Mandate Comprehensive Transparency Requirements

Platforms hosting child-oriented apps must comply with rigorous transparency obligations, including:

- **Disclosure of Behavioural Techniques:** Platforms must publish detailed reports on all behavioural and psychological mechanisms employed within their apps. These reports should explain these mechanisms' intent, functionality, and anticipated effects in accessible terms.
- **Regular Independent Audits:** Platforms should undergo periodic third-party audits to verify compliance with the prohibition on psychological triggers. These audits must assess app features' technical implementation and real-world impact.
- **Public Reporting:** Audit findings should be publicly available to foster accountability and build trust among stakeholders, including parents, educators, and regulators.

4. Require Behavioural Testing for Compliance

Platforms must conduct behavioural testing to evaluate the psychological effects of their apps on children. This testing should:

- Be scientifically rigorous, employing controlled trials, surveys, and user behaviour analysis methods.
- Focus on identifying unintended consequences, including compulsive engagement, diminished autonomy, and adverse mental health outcomes.
- Include diverse participant groups to account for varying levels of vulnerability among children based on age, socio-economic status, and cognitive development.
- Mandate submission of test results to regulators for review and enforcement.

Testing protocols should align with the principles of Article 13 of the AI Act, which requires risk assessments for high-risk systems. However, regulators must also tailor these assessments to address child-specific vulnerabilities.

5. Introduce Penalties for Non-Compliance

The enforcement framework should include stringent penalties to deter non-compliance, such as:

- **Substantial Fines:** Penalties proportionate to the severity and scale of violations ensure that fines are sufficient to disincentivise profit-driven manipulation.
- **Revenue-Based Sanctions:** Fines for repeat offenders depend on a percentage of global turnover, similar to the penalty structure under Article 83 of the GDPR.
- **Operational Restrictions:** Temporary suspension of services for platforms found to violate the prohibition on psychological triggers repeatedly.
- **Enhanced Liability for Executives:** Holding senior executives personally accountable for compliance failures, particularly in cases involving wilful negligence or intent to deceive.

6. Strengthen Regulatory Oversight

Regulators must be equipped with the necessary tools and authority to ensure effective enforcement and to:

- Conduct real-time monitoring of digital environments targeting children.
- Collaborate with independent auditors, child protection advocates, and technical experts to identify and eliminate manipulative practices.
- Establish dedicated hotlines and reporting mechanisms for parents and educators to flag potentially harmful app features.
- Create an EU-wide database of non-compliant platforms to facilitate cross-border enforcement.

Legal Provisions that Need Amending:

1. AI Act (Article 5(1)(b)): Broadening Interpretation and Enforcement Guidelines

Article 5(1)(b) of the AI Act prohibits systems that exploit vulnerabilities related to age, disability, or other characteristics in a manner likely to cause significant harm. However, the current threshold of "significant probability of harm" poses a substantial barrier to enforcement, particularly against subtle yet pervasive manipulative practices like psychological triggers. To address these challenges, the European Commission, in collaboration with the European Data Protection Board (EDPB), should issue interpretative guidelines to:

- Lower the threshold for enforcement by focusing on **potential harm**, recognising the cumulative and indirect nature of psychological manipulation in child-oriented systems.
- Emphasise that manipulative triggers, such as flashing colours or gamified rewards, inherently distort autonomy and informed decision-making, meeting the exploitation criteria without immediate or quantifiable harm.
- Require platforms to conduct **Child Rights Impact Assessments (CRIAs)** as part of risk management under **Article 9**, ensuring that systems targeting children are subject to robust evaluation of their psychological effects.
- Clarify enforcement responsibilities for national authorities under **Article 64**, encouraging proactive monitoring and collaboration across Member States to address cross-border violations.

Recital 29 of the AI Act highlights the importance of protecting the most vulnerable users, such as children, from AI-driven manipulation. This emphasis should underpin broader interpretations of Article 5(1)(b), aligning its application with the evolving digital landscape and the unique vulnerabilities of children.

2. Unfair Commercial Practices Directive (Directive 2005/29/EC): Expanding Annex I to Address Psychological Triggers

The **Unfair Commercial Practices Directive (UCPD)** provides a robust foundation for consumer protection but lacks explicit provisions addressing psychological triggers in digital environments. Annex I, which lists practices deemed unfair in all circumstances, should be amended to explicitly categorise psychological triggers targeting children as unfair commercial practices.

The amendment should:

- Define **psychological triggers** as stimuli manipulating behavioural or cognitive vulnerabilities, such as time-based rewards, gamified interactions, and persistent notifications.

- Harmonise the treatment of these practices across the EU, ensure consistent enforcement under Article 3 of the UCPD, and establish the directive's scope.

- Align enforcement with the DSA by mandating transparency obligations for platforms using behavioural techniques in child-oriented apps. Such commitments would address manipulative design through consumer law and platform governance frameworks.

To ensure effective implementation, the Commission should issue **interpretative guidance** under **Article 16**, clarifying how existing provisions apply to digital environments and providing examples of prohibited practices targeting children. These guidelines should also encourage Member States to adopt complementary measures under **Article 4**, fostering a cohesive approach across national jurisdictions.

Psychological triggers represent a particularly insidious form of manipulation, exploiting the most vulnerable users—children. The EU can establish a robust and unequivocal prohibition by addressing the inadequacies of current frameworks, including the high threshold under Article 5(1)(b) of the AI Act. A total ban on these triggers, complemented by amendments to existing laws such as the UCPD, would ensure robust protections against the exploitation of minors in the digital environment. These measures would foster a safer, more ethical digital ecosystem that prioritises the welfare and rights of children.

BAN IN-APP PURCHASES TARGETED AT CHILDREN: LIMIT OR PROHIBIT THE USE OF IN-APP PURCHASES DESIGNED TO APPEAL SPECIFICALLY TO CHILDREN, ESPECIALLY IN ENVIRONMENTS THAT ENCOURAGE IMPULSIVE PURCHASING.

BAN IN-APP PURCHASES TARGETED AT CHILDREN

Explanation: In-app purchases designed to appeal specifically to children exploit their developmental vulnerabilities, fostering impulsive decision-making and encouraging excessive spending. Tactics such as virtual currencies, loot boxes, countdown offers, and gamified rewards obscure real-world costs, creating environments that incentivise children to spend without understanding the financial implications. These mechanisms are deliberately opaque and exploit children's limited capacity for critical evaluation. Research, including the ACM case against Fortnite[cccix], highlights such practices' damaging psychological and economic impacts.[cccx] The UCPD prohibits misleading and aggressive practices under Arts. 5–9 lacks explicit provisions targeting manipulative in-app purchase systems in child-oriented environments.

Similarly, while the **DSA** requires transparency for advertisements under Art. 24, it does not explicitly address in-app purchase mechanics designed to exploit children's vulnerabilities. Art. 5(1)(b) of the AI Act establishes a prohibition on exploitative systems but requires proof of "significant probability of harm," which sets a high evidentiary threshold. These legal gaps leave children vulnerable to exploitative digital environments. These practices of the UN Convention on the Rights of the Child (UNCRC), which mandates protection from economic exploitation, undermine rights to autonomy and development under Article 24 of the EU Charter of Fundamental Rights. A targeted legislative response is necessary to address these challenges and protect children's rights in the digital economy.

Suggested Remedies:

1. **Prohibit Manipulative In-App Purchase Designs:** Introduce a ban on manipulative in-app purchasing mechanisms in child-oriented environments. Under the UCPD's Annex I, practices such as loot boxes, virtual currencies, gamified purchasing features, and countdown timers should be considered unfair and prohibited. Such measures would harmonise prohibitions across all Member States and create enforceable platform rules.[cccxi]
2. **Mandate Age-Appropriate Transparency** In-app purchases in child-focused environments must prominently display real-world monetary costs. Virtual currencies, which obscure financial transparency, should not be allowed in applications targeting minors. The DSA's transparency obligations under Art. 24 should expand to mandate child-specific measures.
3. **Strengthen Age Verification Systems:** Platforms should implement robust, GDPR-compliant age-verification mechanisms to ensure children do not access environments with exploitative purchasing systems. These mechanisms must uphold data minimisation principles while effectively restricting access.[cccxii]
4. **Lower Harm Threshold Under the AI Act:** Interpret Article 5(1)(b) to reduce the evidentiary threshold for proving harm in cases involving children. Regulators should be empowered to address systems targeting children without requiring significant harm to be demonstrated. Such an approach would facilitate regulating systems that exploit minors through in-app purchasing mechanisms.

Conclusion: Manipulative in-app purchases targeting children undermine their financial autonomy and psychological well-being. A comprehensive, harmonised regulatory framework integrating prohibitions, transparency, and enforcement mechanisms across the UCPD, DSA, and AI Act is essential.

REQUIRE BEHAVIOURAL TESTING OF CHILD-DIRECTED PLATFORMS: MANDATE BEHAVIOURAL TESTING FOR PLATFORMS TO ASSESS IF THEIR DESIGNS MANIPULATE OR HARM CHILDREN, WITH REGULAR AUDITS AND ACCESS FOR REGULATORS TO TEST

REQUIRE BEHAVIOURAL TESTING OF CHILD-DIRECTED PLATFORMS

Explanation: Child-directed platforms often use design choices, algorithms, and features that manipulate behaviour or encourage harmful engagement patterns. These include persuasive design techniques, dark patterns, and addictive mechanisms that exploit children's cognitive and emotional vulnerabilities. Such practices lead to excessive screen time, impulsive behaviours, and financial exploitation. Evidence from the CERRE report on harmful online choice architecture and the NCC's 2024 report on the commercial exploitation of children confirms the prevalence and detrimental impact of such designs.[cccxiii] While the UCPD addresses misleading and aggressive practices under Articles 5–9, it does not mandate systematic behavioural testing to identify or prevent harmful impacts on children. The DSA requires VLOPs to conduct risk assessments and mitigate systemic risks (Arts. 34–35), but these provisions are not specific to child-directed platforms. Similarly, the AI Act imposes obligations on high-risk systems.[cccxiv] However, this does not address behavioural testing for child-specific interactions. These gaps in existing frameworks leave platforms unchecked in their ability to design and deploy features that manipulate children, contravening Article 32 of the UN Convention on the Rights of the Child (UNCRC) and children's rights to autonomy and protection under Article 24 of the EU Charter of Fundamental Rights. Mandating behavioural testing ensures child-directed platforms comply with ethical standards and regulatory requirements.

Suggested Remedy:

- **Mandate Regular Behavioural Testing:** Platforms targeting or accessible to children must be required to conduct both **pre-launch and ongoing behavioural testing** of their user interfaces, algorithms, and core features to identify manipulative, harmful, or exploitative design elements. These tests should evaluate whether features such as dark patterns, variable reward mechanisms, or gamified interactions exploit children's cognitive or emotional vulnerabilities.
    - **Pre-launch testing** should assess whether design elements likely encourage compulsive behaviours, excessive engagement, or financial harm.
    - **Ongoing testing** should occur annually to assess platforms' continued compliance with child-specific legal protections under Article 32 of the UNCRC and the principles of fairness under the UCPD.[cccxv]
    - The EU should standardise testing frameworks based on metrics developed in consultation with child psychologists, behavioural scientists, and regulatory authorities. Such standardisation would ensure consistency with Article 24 of the EU Charter of Fundamental Rights.[cccxvi]
- **Ensure Regulator Access and Independent Audits:** Platforms must submit behavioural testing results to regulators, such as national consumer protection authorities or digital services coordinators, for review. These findings should also be subject to independent audits by certified third parties to validate methodologies and conclusions.
    - Testing reports should detail any identified risks, corrective actions taken, and the ongoing measures adopted to ensure compliance with child protection standards.
    - Align this requirement with Article 40 of the DSA, which already mandates reporting on systemic risks, and expand its scope to include explicitly behavioural testing of child-directed platforms.
    - Regulators should be empowered to request ad hoc testing, especially where there is evidence or suspicion of harm, such as excessive screen time or compulsive purchasing. Failure to comply with such requests should result in substantial fines tied to the platform's annual revenue, as permitted under Article 52 of the DSA.
- **Revise the AI Act:** Expand the scope of Article 9 to require behavioural testing for high-risk AI systems that interact with or target children. These tests must examine whether recommender systems, personalisation algorithms, or automated decision-making tools exploit children's cognitive vulnerabilities or undermine their autonomy.

  - Platforms must submit testing protocols and results to national supervisory authorities and demonstrate that their systems comply with Article 5(1)(b) requirements, which prohibits systems from exploiting vulnerabilities due to age or other characteristics.
  - Testing must explicitly assess potential harms caused by attention-maximising algorithms and propose corrective measures to mitigate these risks.
- **Parental Oversight Tools:** Platforms should disclose behavioural testing outcomes to parents and guardians in a simplified and accessible format, enabling them to understand the platform's potential risks.
  - This information should include clear metrics on screen time impacts, the likelihood of impulsive behaviours, and financial risks associated with platform features.
  - Such transparency measures should align with Article 24 of the DSA, which requires clear consumer disclosures. They must use age-appropriate and inclusive language as outlined in Recital 38 of the GDPR.
  - Platforms failing to provide such information to parents or using overly technical or obfuscated language should face sanctions.

These enhanced proposals respond to gaps identified in vital regulatory frameworks, including the DSA, AI Act, and UCPD, and align with findings in reports such as the NCC's 2024 report on commercial exploitation of children, the CERRE study, and the Fitness Check on EU Consumer Law. By mandating behavioural testing, regulators can ensure child-directed platforms prioritise the well-being of their most vulnerable users, holding platforms accountable for manipulative and harmful design practices. Integrating these measures across the DSA and AI Act will create a comprehensive and harmonised legal framework to protect children in the digital ecosystem.

Legal Provisions That Need Amending:

1. **Digital Services Act (Regulation (EU) 2022/2065):** Expand **Articles 34–35** to require behavioural risk assessments and testing for platforms accessible to children, including independent audits and submission of findings to regulators.
2. **AI Act:** Amend **Article 9** to include mandatory behavioural testing for high-risk AI systems that interact with or target children, ensuring these systems do not manipulate or harm their users.
3. **Unfair Commercial Practices Directive (Directive 2005/29/EC):** Incorporate a requirement for behavioural testing of designs and algorithms targeting children—failure to conduct such testing is an unfair practice under Article 5.
4. Introduce explicit obligations for child-directed platforms to conduct behavioural testing, disclose findings to regulators, and undergo independent audits. Include penalties for platforms found to use manipulative or harmful designs.

Conclusion: Mandating behavioural testing for child-directed platforms is critical to ensuring ethical design and protecting children's rights in the digital space. By pre-emptively identifying manipulative or harmful elements, these requirements would create accountability and align platforms with international and EU obligations, including the UNCRC and EU Charter of Fundamental Rights. Integrating behavioural testing across the UCPD, DSA, and AI Act would ensure a harmonised framework, fostering a safer, more transparent digital environment for children.

INCORPORATE FEEDBACK MECHANISMS FOR CONTINUOUS IMPROVEMENT: REQUIRE PLATFORMS TO IMPLEMENT FEEDBACK CHANNELS SPECIFICALLY FOR CHILDREN AND PARENTS, ALLOWING THEM TO REPORT ISSUES WITH DESIGN FEATURES THAT FEEL UNFAIR OR MANIPULATIVE.

INCORPORATE FEEDBACK MECHANISMS FOR CONTINUOUS IMPROVEMENT

Explanation: Children and parents often encounter digital design features that feel unfair, manipulative, or harmful, such as dark patterns, addictive design, or gamified purchasing systems. However, existing regulatory frameworks need explicit platform requirements to enable direct feedback channels for these users, leaving concerns unaddressed. Reports like the CERRE study on harmful choice architecture and the European Commission's Fitness Check on Consumer Law underscore the importance of user-driven oversight mechanisms in identifying and mitigating harmful practices in real-time.[cccxvii] Current EU legislation partially addresses systemic risks and transparency but does not mandate feedback mechanisms for children and parents. The DSA requires user risk assessments and redress mechanisms.[cccxviii], but these provisions are neither tailored to child-specific concerns nor designed to support iterative platform improvements based on direct user input.

Similarly, the UCPD lacks provisions requiring platforms to incorporate user feedback into compliance processes.[cccxix] The absence of such mechanisms disproportionately affects children and their guardians, who are less likely to navigate traditional complaint systems effectively. Empowering these groups through tailored feedback channels aligns with Article 24 of the EU Charter of Fundamental Rights (children's rights to care and protection) and Article 32 of the UN Convention on the Rights of the Child (UNCRC) (protection against exploitation).

Suggested Remedy:

1. **Mandate Child-Centric Feedback Channels:** Platforms targeting or accessible to children should establish dedicated feedback mechanisms that allow children and parents to report manipulative, harmful, or unfair design features directly. These mechanisms must:
   - Be accessible through child-friendly interfaces and use age-appropriate language.
   - Enable parents to submit feedback on behalf of their children.
   - Collect structured data on complaints, categorising them by design issues (e.g., dark patterns, addictive features, or misleading costs).
   - Provide feedback summaries and explain actions taken to the user, enhancing trust and transparency.
2. **Establish Regulatory Oversight and Escalation Pathways:** For oversight, feedback mechanisms must connect to regulatory bodies, such as national digital service coordinators or consumer protection authorities. Escalation pathways should ensure platforms refer unresolved or systemic complaints to regulators for investigation.
   - These pathways should also include provisions addressing direct user-reported risks, aligning with the DSA's Article 40, which requires transparency in compliance with risk mitigation measures.[cccxx]
   - Platforms must submit quarterly reports on user feedback trends to regulators, detailing the volume of complaints, identified risks, and steps taken to address recurring issues.
   - **Require Iterative Improvements Based on Feedback:** Platforms must continuously implement feedback loops to improve their design systems. Platforms should incorporate user-reported issues into periodic risk assessments, as mandated under DSA Articles 34–35 for very large online platforms (VLOPs). Feedback should inform updates to recommender systems, interface designs, and purchasing mechanisms, ensuring compliance with child-specific protections outlined in the **Fitness Check on EU Consumer Law** and **CERRE report.**[cccxxi]

- Failures to address recurring complaints should result in fines or operational restrictions under **Article 52 of the DSA**.

3. **Incorporate Feedback into AI Act Compliance:** Amend **Article 9 of the AI Act** to require child-directed platforms using recommender systems or personalised algorithms to incorporate user feedback channels into their risk management systems. Platforms must demonstrate that feedback informs the iterative improvement of their AI systems and mitigates risks of manipulation or harm.

Legal Provisions That Need Amending:

1. **Digital Services Act (Regulation (EU) 2022/2065):** Expand **Articles 17 and 40** to require platforms to establish dedicated feedback mechanisms for children and parents. Include obligations to escalate unresolved issues to national regulators and integrate feedback into risk mitigation measures.
2. **Unfair Commercial Practices Directive (Directive 2005/29/EC):** Amend the directive to require platforms targeting children to incorporate user feedback into their compliance processes, categorising the failure to do so as an unfair practice under Article 5.
3. **AI Act (Draft):** Interpret **Article 9** to include user feedback as a mandatory component of risk management for child-directed systems, ensuring continuous improvement based on real-world interactions and complaints.

Conclusion: Feedback mechanisms tailored to children and parents are essential for identifying and mitigating manipulative or harmful design elements in digital platforms. Mandating such systems would foster accountability, empower users, and support iterative platform improvements, aligning with the EU's broader commitment to fairness, transparency, and child protection. By integrating these requirements into the DSA, UCPD, and AI Act, the EU can ensure a harmonised and participatory approach to safeguarding children in the digital ecosystem.

LIMIT DATA COLLECTION FROM CHILDREN, PARTICULARLY FOR PURPOSES OF PERSONALISATION OR TARGETED ADVERTISING, AND REQUIRE EXPRESS PARENTAL CONSENT WHERE NECESSARY

DATA PROTECTION & PRIVACY

Explanation: The digital landscape has led to pervasive data collection practices that disproportionately impact children due to their vulnerability and limited capacity to provide informed consent. Features like personalised advertising and targeted content often exploit data collected from minors, contravening their rights under GDPR Articles 5(1)(a), (b), and 6(1), which emphasise fairness, purpose limitation, and the need for a lawful basis for processing. The 2022 EDPB decision concerning TikTok's practices highlights systemic issues with age verification and inadequate consent mechanisms that expose children's data to potential misuse.[cccxxii] While the GDPR recognises children as a special category deserving heightened protection[cccxxiii], enforcement still needs consistency. Cases like Instagram's public-by-default settings for minors reveal systemic flaws, as platforms nudge children into data-sharing behaviours without their understanding the implications.[cccxxiv] The UNCRC, particularly Article 32, obligates states to protect children from economic exploitation, which includes practices arising from personal data commodification.

Suggested Remedy:

1. **Prohibit Behavioural Targeting of Minors:** Interpret GDPR Article 6 to categorically prohibit the use of children's data for behavioural advertising and profiling. Platforms should not process data for these purposes unless strictly necessary for a service explicitly requested by the child or their legal guardian.
2. **Parental Consent Mechanisms:** Reenvisage Article 8 GDPR to mandate robust parental verification systems for data processing involving minors. Recent binding decisions[cccxxv] underscore the necessity for effective mechanisms to verify parental consent and ensure it is informed, explicit, and traceable.[cccxxvi]
3. **Introduce Specific Transparency Requirements:** Extend GDPR Article 12 to include child-specific transparency obligations. Privacy notices for minors must use plain, age-appropriate language and leverage visuals and interactive formats to explain how platforms will use their data and outline their associated rights. The UK’s ICO's guidance on children and the GDPR provides a framework for implementing these measures effectively.[cccxxvii]
4. **Establish Data Minimisation Mandates:** Build on GDPR Article 25 (Data Protection by Design and Default) to enforce strict data minimisation requirements for child-directed platforms. Platforms should restrict data collection to what is necessary for delivering core functionality and conduct routine audits to ensure compliance.
5. **Strengthen Enforcement and Penalties:** Regulators must increase scrutiny and impose substantial fines for non-compliance involving minors. Case precedents, such as the €345 million fine against TikTok for unfair practices, demonstrate the necessity of robust enforcement measures.[cccxxviii]

Legal Provisions That Need Amending:

- **Article 6 GDPR:** Prohibit the use of children's data for profiling and behavioural advertising.
- **Article 8:** Introduce mandatory parental consent verification protocols.
- **Article 25:** Expand data protection by design requirements specific to children's online environments.
- **Article 35:** Mandate DPIAs for services likely to impact children disproportionately.

1. **Digital Services Act (DSA):** Amend Article 24 to include child-specific transparency and accountability measures for data processing practices.

A comprehensive regulatory framework addressing children's vulnerabilities is critical to safeguarding their data privacy and autonomy. By prohibiting behavioural advertising, mandating robust parental consent mechanisms, and enforcing stringent data minimisation principles, the EU can uphold its commitments under the GDPR and UNCRC, ensuring a fairer digital ecosystem for minors. Integrating these measures into existing laws like the GDPR, UCPD, and the DSA will foster a safer and more equitable online environment for children.

MANDATE AGE VERIFICATION MECHANISMS: REQUIRE DIGITAL PLATFORMS TO IMPLEMENT ROBUST, PRIVACY-PRESERVING AGE VERIFICATION TO LIMIT CHILDREN'S EXPOSURE TO AGE-INAPPROPRIATE CONTENT AND HARMFUL DESIGN.

MANDATE AGE VERIFICATION MECHANISMS

Explanation: The increasing prevalence of children accessing digital platforms presents unique challenges for protecting their rights under GDPR and other regulatory frameworks. Article 25 GDPR implicitly supports measures like age verification to prevent exposure to age-inappropriate or harmful content. However, practical implementation has yet to catch up. For instance, the EDPB's binding decision regarding TikTok highlighted significant deficiencies in age verification mechanisms, as existing measures allowed children to bypass controls quickly, exposing them to data risks and manipulative design (e.g., nudging via "public by default" settings).[cccxxix] Similarly, the DSA emphasises transparency and user control but does not mandate robust age-verification systems for platforms hosting child-directed content.[cccxxx] This gap leaves minors vulnerable to exposure to content or interactions designed for adult users, violating their rights under Article 32 of the UNCRC and undermining protections against economic exploitation.[cccxxxi]

Suggested Remedy:

1. **Mandatory Age-Verification Systems:** Require platforms accessible to children to integrate robust, privacy-preserving age-verification mechanisms. Platforms should use technologies verifying a user's age without collecting or retaining unnecessary personal data, complying with GDPR data minimisation and purpose limitation principles.[cccxxxii] Mechanisms like zero-knowledge proofs and secure multi-party computation can provide viable solutions.
2. **Harmonised Standards Across the EU:** Amend the DSA to introduce EU-wide technical and procedural standards for age-verification systems. Article 24 of the DSA should be updated to mandate that platforms hosting child-directed content implement verification measures proportionate to the sensitivity of the content or activity offered.
3. **Audit and Accountability Measures:** Platforms must subject their verification processes to regular national data protection authorities (DPAs) audits, with results shared transparently. Such audits align with Article 40 of the DSA, which requires transparency in compliance.
4. **Special Protections for Minors Under GDPR:** Expand Article 25 of the GDPR to include age-verification requirements for platforms explicitly targeting children. Additionally, regulators should provide clear guidelines under Article 8 of the GDPR to ensure that consent mechanisms for minors include verifiable parental involvement where necessary.[cccxxxiii]
5. **Guidance and Support for Compliance:** Create an EU-wide toolkit for platforms, including technical guidance and best practices for age verification. Platforms should also be required to provide clear, child-friendly explanations of their verification processes.

Legal Provisions to Amend:

- **GDPR (Regulation (EU) 2016/679):** Amend Articles 8 and 25 to mandate privacy-preserving age-verification mechanisms explicitly for ISS directed at children.
- **Digital Services Act (Regulation (EU) 2022/2065):** Strengthen Article 24 to include age-verification obligations, ensuring platforms prioritise child safety and transparency.
- **Audiovisual Media Services Directive (Directive (EU) 2018/1808):** Expand obligations under Articles 6a and 9 to address age verification for video-sharing platforms hosting child-directed content.

Mandating age-verification mechanisms is critical to ensure children's digital environments are safe and age-appropriate. The EU can address current regulatory gaps by amending the GDPR, DSA, and AVMSD and introducing explicit measures through law reform. Such measures must balance protecting children and safeguarding fundamental privacy rights, leveraging privacy-enhancing technologies to ensure compliance without infringing user freedoms. Robust, harmonised age-verification standards will significantly bolster protections for minors in the digital age.

CREATE DESIGN STANDARDS THAT PREVENT MANIPULATIVE TACTICS IN APPS AND WEBSITES ACCESSED BY CHILDREN, DRAWING FROM GDPR'S "PRIVACY BY DESIGN" PRINCIPLES TO INCLUDE "FAIRNESS BY DESIGN"

DEVELOP "CHILD-FAIR" DESIGN STANDARDS

Explanation: Digital environments increasingly exploit behavioural and psychological tendencies, especially among children, through manipulative tactics such as dark patterns, excessive gamification, and misleading choice architecture. The CERRE report and BEUC's consultation paper identify how design choices distort user autonomy and disproportionately affect vulnerable populations, including minors.[cccxxxiv] These harmful designs conflict with consumer protection laws like the UCPD and contravene the principles of fairness and transparency central to the GDPR and the DSA.[cccxxxv] Existing frameworks, including **GDPR Article 25** (Data-Protection-by-Design-And-Default), already mandate proactive measures for protecting privacy. Expanding these principles to enforce **Fairness by Design** would ensure that digital platforms prioritise user rights and avoid designs that manipulate or deceive children. Reports such as the Digital Fairness Fitness Check emphasise the need for more robust standards to address these issues.[cccxxxvi]

Suggest Remedies:

1. **Mandate "Fairness by Design" Standards in Legislation:**
   - Extend Article 25 GDPR to encompass fairness as a fundamental design principle. Platforms must design interfaces and features to be understandable and accessible to children without exploiting their developmental vulnerabilities.
   - Age-specific testing is required to assess the fairness of design elements before launch. Platforms must demonstrate that their designs do not rely on psychological manipulation to drive engagement or monetisation.[cccxxxvii]

2. **Blacklist Manipulative Tactics:**
   - Amend **UCPD Annex I** to prohibit manipulative tactics for children, such as gamified reward systems or hidden costs in digital environments. These prohibitions should cover designs that lead to compulsive behaviours or obscure critical information, aligning with recommendations from the CERRE and BEUC reports.[cccxxxviii]

3. **Harmonise Standards Across Existing Frameworks:**
   - Incorporate fairness principles into the DSA under Article 24 by requiring platforms to eliminate dark patterns from child-oriented interfaces. Article 40 transparency obligations should include reporting on fairness compliance in child-focused digital spaces.[cccxxxix]

4. **Introduce Fairness Audits and Monitoring:**
   - Require platforms to conduct regular independent audits assessing fairness in design, with findings submitted to regulatory bodies like the **Consumer Protection Cooperation Network (CPCN)**. Audits should include child-specific fairness metrics and evidence of proactive compliance.

5. **Educational and Parental Empowerment Tools:**
   - Mandate clear, concise disclosures about design mechanisms that could influence child behaviour. For instance, platforms should summarise their fairness policies and user testing outcomes in a format accessible to parents and educators.

6. **Empower Regulators to Act Pre-emptively:**
   - Equip authorities with the power to investigate and sanction platforms that fail to meet "Fairness by Design" standards, even before platforms demonstrate significant harm. This approach

aligns with the **precautionary principle** embedded in GDPR and strengthens proactive enforcement.[cccxl]

Legal Provisions to Amend or Introduce:

1. **General Data Protection Regulation:**
   - Amend Article 25 to explicitly include "Fairness by Design" as a core requirement for data controllers designing child-facing services[cccxli]

2. **Unfair Commercial Practices Directive:**
   - Update Annex I to blacklist manipulative designs targeting children. Extend Articles 5–9 to include fairness obligations in user interface and choice architecture.[cccxlii]

3. **Digital Services Act:**
   - Strengthen Article 24 by mandating the inclusion of fairness metrics in transparency reporting. Article 40 should require fairness audits for platforms accessed by children.[cccxliii]

Conclusion:

Embedding "Fairness by Design" principles across EU legal frameworks is essential for protecting children in the digital environment. The EU can ensure a robust, forward-looking approach that safeguards minors' autonomy, privacy, and rights by leveraging existing laws like GDPR and UCPD and harmonising them with newer regulations like the DSA. These measures will also foster trust and accountability, creating a safer and more equitable digital landscape for all users.

ESTABLISH A LABELLING SYSTEM TO CERTIFY CHILD-FRIENDLY DIGITAL APPLICATIONS, HELPING PARENTS IDENTIFY COMPLIANT APPS AND WEBSITES WITH TRANSPARENT, NON-MANIPULATIVE DESIGN FEATURES.

INTRODUCE COMPLIANCE LABELS FOR CHILD-FRIENDLY APPS:

Explanation: The digital landscape presents a significant challenge for parents seeking to protect their children online. The sheer volume of apps and websites, coupled with the often-opaque nature of their design features, makes it difficult to discern those who genuinely prioritise child safety and well-being. This challenge becomes even more complex with the rapid advancement of AI, which introduces new layers of difficulty and potential risks to children's online experiences. A transparent, trustworthy labelling system would empower parents to make informed choices and foster a more child-friendly digital environment.

Suggested Remedy

I propose establishing a robust labelling system to certify child-friendly digital applications. This system would:

1. **Develop Comprehensive Criteria:** Define specific, measurable criteria for certification, encompassing:

    - **Data protection:** Strict compliance with the GDPR, the new DFA, and child-specific data protection measures ensures that children's data is processed fairly, transparently, and appropriately.
    - **Transparency:** Clear, age-appropriate privacy policies and terms of service, written in plain language and utilising child-friendly formats to enhance comprehension.
    - **Non-manipulative design:** Avoid dark patterns, addictive designs, and exploitative marketing practices to protect children's cognitive and emotional vulnerabilities from exploitation.
    - **Age-appropriateness:** Content filtering and moderation align with children's developmental needs, and robust mechanisms are incorporated to prevent exposure to harmful or inappropriate content.
    - **AI ethics:** Compliance with ethical AI principles, including fairness, explainability, and accountability, ensuring AI-driven features are used responsibly and do not perpetuate harmful biases.

2. **Establish an Independent Certification Body:** Create an independent, multi-stakeholder body composed of child development experts, data protection authorities, and technology specialists to rigorously assess and certify apps and websites based on the defined criteria.

3. **Design a Recognizable Label:** Develop a visually distinctive and easily recognisable label to be prominently displayed on certified apps and websites, signifying compliance with child-friendly standards. This label should include a QR code or link that provides parents with detailed information about the app or website's features and data processing practices.

4. **Promote Public Awareness:** Conduct extensive public awareness campaigns to educate parents, educators, and children about the labelling system, its benefits, and how to identify certified apps and websites. These campaigns should utilise diverse media channels and child-friendly formats to reach a broad audience.

5. **Ensure Ongoing Monitoring and Evaluation:** Establish mechanisms for ongoing monitoring and evaluation of certified apps and websites to ensure continued compliance with the labelling system criteria. These mechanisms should include regular audits, user feedback processes, and a transparent procedure for decertifying apps or websites that no longer meet the standards.

Legal Provisions That Need Amending

1. **Digital Services Act (DSA):**

    - **Article 28:** Mandate child-friendly labels for all certified platforms targeting children, making compliance a legal requirement.

- **Article 34:** Require platforms to conduct comprehensive risk assessments addressing child safety, data protection, and compliance with the labelling system criteria. These assessments should be independently audited and made publicly available.

Conclusion By establishing a robust labelling system to certify child-friendly digital applications, the EU can empower parents to make informed choices and promote a safer, more transparent online environment for children. With a strengthened legal framework and ongoing efforts to promote digital literacy, this initiative will contribute to a digital world prioritising children's rights and well-being.

ENHANCED PROTECTIONS AGAINST EXPLOITATIVE CONTENT: RECOMMEND STANDARDS THAT REQUIRE TRANSPARENCY AND CLEAR LABELLING IN CONTENT RECOMMENDATION SYSTEMS TO PREVENT MANIPULATIVE DESIGNS FROM TARGETING YOUNG USERS

ENHANCED PROTECTIONS AGAINST EXPLOITATIVE CONTENT

Explanation: The widespread use of content recommendation systems in digital environments has significantly changed how individuals, particularly children, engage with online platforms. These systems, often driven by algorithmic processes optimised for engagement, pose critical risks by exposing young users to exploitative content. Such content includes algorithmically amplified harmful material, undisclosed advertising, and manipulative narratives designed to exploit children's cognitive and emotional vulnerabilities. Exposure to exploitative content can severely impact children's mental health, autonomy, and overall development.

Recommendation systems amplify extreme, sensational, or emotionally charged content to maximise user retention, prioritising engagement and profit over safety. This approach disproportionately affects children, who lack the cognitive maturity to recognise persuasive intent or differentiate between organic and algorithmically promoted content. As a result, children are particularly vulnerable to harmful behavioural patterns, social pressures, and exposure to unsafe or inappropriate content. Exploitative content, such as misinformation, damaging stereotypes, or hyper-commercialised narratives, reinforces unhealthy behaviours and creates long-term developmental risks.

The opacity of these systems compounds the risks. Platforms typically fail to disclose the mechanisms driving their recommendation algorithms, the data used for personalisation, or the commercial motivations influencing recommendations. This lack of transparency makes it nearly impossible for children—or their guardians—to understand the origins or potential harms of exploitative content. Current disclosures are often dense, technical, and designed for regulatory compliance rather than accessibility, leaving young audiences particularly underserved.

Despite progress under frameworks like the DSA, GDPR, and AI Act, the regulatory landscape is insufficient to tackle these challenges comprehensively. The DSA provides general transparency and accountability provisions but does not explicitly target exploitative content propagated by recommendation systems targeting children. Similarly, the GDPR regulates the use of personal data but does not address how companies leverage that data for manipulative content strategies. While the AI Act focuses on high-risk AI systems, it lacks precise requirements for mitigating algorithmic amplification of harmful or exploitative content in child-facing platforms. These gaps allow platforms to continue deploying systems that perpetuate exploitative content, prioritising engagement metrics over the welfare of young users.

Algorithmic amplification of exploitative content stems directly from optimisation strategies to maximise user interaction. These strategies create a dangerous feedback loop in which platforms prioritise harmful, emotionally charged material for its ability to drive user retention, normalising manipulation as part of the digital experience. Children, being highly impressionable and less equipped to assess such content critically, are disproportionately affected. Beyond individual harm, this systemic issue erodes societal trust and undermines digital environments, fostering a culture where manipulation and misinformation thrive.

Regulatory intervention must evolve to address this growing threat. Meaningful transparency standards must ensure that platforms disclose how content is curated, personalised, and recommended. These disclosures must be age-appropriate and accessible, enabling children and guardians to understand the mechanisms behind content delivery. Standardised labelling is critical to differentiate between organic, sponsored, and algorithmically amplified content, ensuring platforms identify exploitative material. Regulators must focus on proactive prevention, requiring platforms to assess, mitigate, and disclose risks related to exploitative content as part of their core operational processes.

By embedding these protections within frameworks like the DSA, GDPR, and AI Act—or through new initiatives such as the new DFA—the EU can establish a regulatory model that safeguards children's rights while addressing the systemic propagation of exploitative content. This proactive shift is essential for fostering a safer digital ecosystem and ensuring fairness, transparency, and accountability in content recommendation systems.

Suggested Remedies Addressing exploitative content in recommendation systems requires precise regulatory measures, leveraging existing legal frameworks and proposing targeted amendments where gaps persist. This section outlines how laws such as the **DSA**, **AI Act**, and **GDPR** can be enhanced or supplemented while identifying areas that may necessitate new legislation like the **DFA**.

Leverage the Digital Services Act (DSA). The DSA provides a strong foundation for regulating algorithmic systems, but its provisions require extension and specificity to address exploitative content in child-facing recommendation systems.

- **Reinterpret Article 24**:
  - Introduce specific obligations for platforms targeting children, requiring precise, age-appropriate transparency about how recommendation systems operate.
  - Mandate detailed disclosures about the data used to personalise recommendations and explain the potential risks of algorithmic amplification.
- **Expedite the Article 25 Code of Conduct**:
  - Explicitly prohibit the use of manipulative recommendation practices, such as dark patterns or engagement-maximising designs that amplify exploitative content for children.
  - Require content labelling for algorithmically amplified content, distinguishing between organic, sponsored, and behaviourally targeted recommendations.
- **Introduce Article 26a (New Provision)**:
  - Require platforms to implement child-specific risk assessments that evaluate the likelihood of recommendation systems exposing children to harmful or exploitative content.
  - These assessments should be submitted to regulators annually and publicly available in child-accessible formats.

Enforce the General Data Protection Regulation (GDPR). While the GDPR regulates personal data use, it does not fully address the exploitation of that data through recommendation systems targeting children. The GDPR can be clarified and expanded to cover these issues:

- **Expand Articles 12–14** (Transparency Requirements):
  - Require platforms to disclose, in a format understandable to children, how profiling and automated decision-making influence the recommendations they receive.
  - Clarify that profiling practices leading to exploitative recommendation systems violate **Article 5(1)(a)** (lawfulness, fairness, and transparency).
- **Strengthen Article 22** (Automated Decision-Making):
  - Prohibit fully automated decisions in content recommendation systems targeting children unless explicit safeguards exist, such as opt-in requirements for behavioural profiling and clear options to turn off personalisation.
  - Require platforms to provide children with simplified explanations of their rights to contest or opt out of automated recommendations.

Adapt the Artificial Intelligence Act (AI Act) The AI Act, as a framework for high-risk AI systems, offers an opportunity to address recommendation systems' disproportionate effects on children:

- **Article 5(1)(b)**:
  - Lower the enforcement threshold from "significant probability of harm" to "reasonable likelihood of harm," ensuring that exploitative recommendation systems targeting children are more easily classified as prohibited.
- **Expand Articles 13–14**:
  - Mandate **Child Rights Impact Assessments (CRIAs)** for all recommendation systems classified as high-risk AI and used by platforms with significant child user bases.
  - Platforms must disclose the algorithmic logic behind recommendations in non-technical terms suitable for young audiences.

Introduce a New Legislative Framework: While regulators can strengthen existing laws, a comprehensive legislative approach may be required to plug persistent regulatory gaps. The DFA could provide a unified framework specifically targeting child-facing digital environments.

- **Child-Centric Labelling Requirements**:

  - Mandate standardised visual markers for algorithmically amplified, sponsored, and harmful content in child-facing systems. These markers should include clear warnings and interactive explanations accessible to children.
- **Prohibit Exploitative Practices**:
  - Define and prohibit "exploitative recommendation practices," including amplifying harmful content, manipulative behavioural nudges, and dark patterns.
- **Require Regular Algorithm Audits**:
  - Introduce mandatory independent audits of recommendation systems targeting children, ensuring compliance with transparency, fairness, and ethical design principles.
- **Behavioural Testing for Compliance**:
  - Obligate platforms conduct behavioural testing to identify whether their recommendation systems expose children to exploitative content. Regulators must have access to test results, and platforms found non-compliant should face penalties or operational restrictions.

Develop Codes of Conduct and Industry Standards In addition to legislative measures, enforceable industry standards can complement regulatory frameworks:

- **Platform-Specific Codes**:
  - Platforms must develop and adhere to codes of conduct under **DSA Article 35**, focusing on ethical content recommendations for children. These codes should include commitments to transparency, content labelling, and minimising harm.
- **Multi-Stakeholder Guidance**:
  - Establish a coalition of regulators, child rights organisations, and industry representatives to issue guidelines on algorithmic transparency and ethical content curation for child-facing systems.

Create Clear Penalty Structures Effective enforcement requires meaningful consequences for non-compliance:

- **Escalating Penalties**:
  - Platforms failing to meet transparency and labelling standards should face fines proportionate to their global turnover, mirroring **GDPR Article 83**. Repeat offenders should face operational restrictions, including suspension of child-targeted services.
- **Public Accountability Mechanisms**:
  - Require platforms to publish detailed transparency and compliance reports annually, including disclosures about the nature and prevalence of exploitative content in their recommendation systems.

These remedies create a comprehensive regulatory structure by leveraging laws such as the DSA, GDPR, and AI Act while introducing new frameworks like the DFA. This approach holds platforms targeting children accountable, reduces exploitative content, and establishes transparency and fairness as the cornerstones of digital governance.

EMPOWER AUTHORITIES TO MONITOR "HIGH-RISK" CHILD PLATFORMS: GIVE REGULATORY BODIES ENHANCED POWERS TO PROACTIVELY MONITOR PLATFORMS FREQUENTLY USED BY MINORS, ENFORCING COMPLIANCE WITH CHILD-FOCUSED FAIRNESS STANDARDS.

EMPOWER AUTHORITIES TO MONITOR "HIGH-RISK" CHILD PLATFORMS:

Explanation

The increasing prevalence of digital platforms frequented by minors necessitates enhanced regulatory oversight to protect their rights, well-being, and autonomy. These platforms, ranging from social media networks to gaming applications, employ advanced algorithms and behavioural design techniques that disproportionately affect children, who are particularly vulnerable to manipulation and exploitation. The lack of robust, proactive monitoring mechanisms for these "high-risk" child platforms has created a regulatory vacuum, allowing harmful practices to proliferate unchecked. Children's cognitive and emotional vulnerabilities render them less equipped to critically evaluate or resist manipulative tactics such as personalised content recommendations, psychological triggers, and dark patterns. These mechanisms exploit behavioural psychology to maximise engagement, often leading to addictive behaviours, excessive screen time, and exposure to harmful content. Furthermore, platforms leveraging algorithmic profiling and targeted advertising risk compromising children's privacy and autonomy, which directly conflicts with ethical design principles and existing legal protections under the **AI Act**, **DSA**, and **GDPR**.

While providing valuable guidance, current regulatory frameworks primarily rely on reactive measures that address harm only after it has occurred. For instance, the **DSA** mandates risk assessments and mitigation strategies for very large online platforms. Still, enforcement mechanisms need to be more cohesive and sufficient for addressing subtle, cumulative harms to children. Similarly, **Article 5(1)(b) of the AI Act** prohibits systems from exploiting age-based vulnerabilities. Still, it imposes a high threshold for proving a "significant probability of harm," limiting its applicability to proactive regulation.

A key barrier to effective oversight lies in the inherent complexity of these platforms' algorithmic systems and choice architectures. Platforms frequently update their interfaces, algorithms, and policies, making it difficult for regulators to keep pace. Moreover, the opaque nature of algorithmic decision-making complicates efforts to assess compliance with child-focused fairness standards. Without real-time access to technical data and behavioural testing results, authorities often cannot identify or address manipulative practices before they cause harm. Cross-border platforms present additional challenges, as jurisdictional differences in enforcement capabilities and legal interpretations hinder coordinated regulatory actions. This fragmentation delays responses to violations and creates uneven protections for children across the EU.

Empowering regulatory authorities with enhanced, proactive monitoring powers is essential to address these gaps. By granting real-time access to platform algorithms, decision-making logic, and behavioural impact assessments, authorities can ensure compliance with fairness standards before harmful practices escalate. Moreover, a shift towards preventative regulation aligns with the EU's broader goals of fostering transparency, accountability, and ethical innovation in the digital ecosystem.

Proactive monitoring would also create a level playing field for digital platforms, incentivising compliance and ethical design. Platforms adhering to child-centric fairness standards would no longer be at a competitive disadvantage to those prioritising engagement and profit over user welfare. Additionally, enhanced oversight would bolster public trust in digital services, reassuring parents, educators, and policymakers that platforms actively protect children from exploitation in online environments. Finally, the rapid evolution of digital technologies underscores the need for dynamic regulatory approaches. Empowering authorities to monitor high-risk child platforms proactively ensures that regulatory frameworks remain adaptable and effective in safeguarding children's rights amid technological advancements. These measures represent a critical step toward creating a safer, more equitable digital ecosystem for the youngest and most vulnerable users.

STRENGTHEN ENFORCEMENT AGAINST HARMFUL ALGORITHMS: EMPOWER REGULATORY BODIES TO REVIEW AND CHALLENGE ALGORITHMS THAT MANIPULATE YOUNG USERS, ENSURING THESE ALGORITHMS DO NOT EXPLOIT COGNITIVE VULNERABILITIES.

STRENGTHEN ENFORCEMENT AGAINST HARMFUL ALGORITHMS:

Establishing High-Risk Designation for Child Platforms: Platforms that cater significantly to minors—or where minors constitute a substantial portion of the user base—should be designated as "high-risk" under existing and forthcoming regulatory frameworks, such as the **Artificial Intelligence Act (AI Act)** and **DSA**. This designation should reflect the heightened duty of care owed to children due to their unique vulnerabilities.

Criteria for High-Risk Designation:

- Platforms where minors represent a significant share of users (e.g., educational apps, gaming platforms, or social media with youth-oriented features).
- Systems employing behavioural profiling, psychological triggers, or algorithmic recommendation engines that target or disproportionately impact children.
- Digital environments offer monetised features, such as in-app purchases or loot boxes, which can exploit children's limited understanding of financial consequences.

Designated platforms should be subject to additional obligations under **Article 6 of the AI Act**, which outlines requirements for high-risk systems, and **Articles 24 and 26 of the DSA**, which mandate transparency and risk assessments.

Proactive Monitoring by Regulatory Authorities Regulatory bodies must have enhanced powers to monitor high-risk child platforms proactively, ensuring compliance with child protection standards before harm materialises. These powers should include:

1. **Real-Time Monitoring Tools:** Authorities should deploy advanced monitoring systems in real-time to identify potential violations, such as manipulative design elements or unsafe content. These tools should leverage platforms' technological sophistication, including AI-driven analytics, to ensure comprehensive oversight.

2. **Mandatory Reporting by Platforms:** High-risk platforms should be required to submit regular, detailed reports to regulatory bodies, including:

   - Summaries of design logic and behavioural techniques targeting children.
   - Data on content moderation practices and algorithmic decision-making.
   - Results of Child Rights Impact Assessments (CRIAs) mandated under **Article 9 of the AI Act**.

   These reporting obligations should align with the **transparency measures outlined in Articles 13–15 of the DSA**, fostering accountability and enabling regulators to identify risks proactively.

3. **Auditing Powers:** Regulators must have the authority to conduct unannounced audits of high-risk platforms. These audits should encompass technical evaluations of platform algorithms, behavioural testing of child-facing systems, and reviews of compliance with child-centric design standards.

4. **Cross-Border Collaboration:** Given digital platforms' global reach, authorities must enhance cross-border cooperation under **Articles 61–64 of the DSA**, facilitating information-sharing and coordinated enforcement actions across Member States.

Strengthening Enforcement and Accountability Mechanisms: Proactive monitoring must be coupled with robust enforcement tools to ensure that platforms prioritise compliance. These tools should include:

1. **Escalating Penalties:** Platforms found non-compliant with child-focused fairness standards should face escalating penalties, ranging from fines proportionate to global turnover (per **Article 83 of the GDPR**) to operational restrictions or temporary bans for repeated violations.

2. **Injunctive Relief:** Regulators should have the power to issue immediate injunctive relief, compelling platforms to cease harmful practices or modify design elements that exploit children.

3. **Public Naming and Shaming:** Authorities should maintain a publicly accessible registry of non-compliant platforms, which would provide transparency and enable parents, educators, and advocacy groups to make informed choices.

4. **Executive Accountability:** Introduce personal liability for senior executives of high-risk platforms, ensuring they prioritise compliance with child protection standards at the highest organisational levels.

Legal Provisions and Interpretative Guidelines Empowering authorities to monitor high-risk child platforms requires enhancements to existing laws and the issuance of detailed interpretative guidelines to ensure consistent application across the EU:

1. **Artificial Intelligence Act (AI Act):**
   - Expand the scope of **Article 64** to include proactive monitoring of high-risk platforms used by children, ensuring that authorities can act without waiting for harm to materialise.
   - Mandate **Child Rights Impact Assessments (CRIAs)** under **Article 9** for all high-risk platforms, focusing on AI systems' potential psychological and developmental impact on minors.
2. **Digital Services Act (DSA):**
   - Strengthen **Article 24**, requiring high-risk platforms to implement ongoing risk assessments specific to child protection.
   - Amend **Article 13** to include a dedicated section on transparency obligations for platforms with minor user bases, mandating detailed reporting on algorithmic systems and behavioural techniques.

Conclusion Proactive monitoring of high-risk child platforms is essential to protect minors in an increasingly complex digital ecosystem. By granting regulatory bodies enhanced powers, supported by robust legal provisions and interpretative guidelines, the EU can ensure that platforms prioritise fairness, transparency, and the well-being of their youngest users. These measures will prevent harm and establish a global standard for child protection in digital governance, reinforcing the EU’s commitment to upholding the rights of vulnerable populations in the digital age.

ENFORCE PENALTIES FOR NON-COMPLIANCE WITH CHILD SAFETY STANDARDS: SET STRICT PENALTIES AND FINES FOR PLATFORMS FOUND NON-COMPLIANT WITH CHILD SAFETY AND FAIRNESS STANDARDS TO CREATE STRONG DISINCENTIVES AGAINST EXPLOITATIVE PRACTICES

ENFORCE PENALTIES FOR NON-COMPLIANCE WITH CHILD SAFETY STANDARDS:

Explanation Penalties for non-compliance with child safety standards in digital environments must be robust, dissuasive, and proportionate to the harm caused. Platforms have increasingly relied on AI-driven technologies, personalised content, and monetisation strategies that frequently target children, often bypassing their unique vulnerabilities. As a legally recognised vulnerable group, children require heightened protection to safeguard their rights, safety, and well-being in digital spaces.

1. The Growing Risk to Children in Digital Environments

Children now interact extensively with online education, entertainment, and social engagement platforms. Many platforms exploit this engagement through dark patterns, manipulative design, and harmful recommendation systems. These practices:

- Exploit cognitive biases, such as impulsivity and limited capacity for critical reasoning, to encourage extended engagement or in-app purchases.
- Expose children to inappropriate, harmful, or exploitative content, including age-inappropriate advertisements or addictive reward systems like loot boxes.[cccxliv]
- Create asymmetric power dynamics where children are at a disadvantage, unable to fully understand the consequences of their interactions due to their developmental stage.[cccxlv]

2. Economic and Psychological Harm

The harm caused by these exploitative practices extends beyond immediate financial losses. Key impacts include:

- **Economic Harm**: Due to gamified purchasing features, children often spend money unknowingly or under pressure, leading to financial distress for families. Systems such as loot boxes or virtual currencies obscure real-world costs, making spending challenging to track.[cccxlvi]
- **Psychological Harm**: The use of addictive design, such as countdown timers or urgency nudges, can lead to overuse, which negatively impacts mental health. Extended screen time and exposure to manipulative designs contribute to anxiety, sleep issues, and reduced social interactions.[cccxlvii]

3. The Role of Penalties in Driving Compliance

Penalties are critical for ensuring platforms adhere to child safety and fairness standards. Without substantial deterrents, companies frequently perceive non-compliance as a manageable cost of doing business. However, when penalties are proportionate to platform revenues and publicised, they create a powerful incentive for compliance. Effective enforcement measures also build public trust in the regulatory system by demonstrating that authorities will not allow breaches to occur.

4. Regulatory and Enforcement Gaps

Current enforcement mechanisms across Member States are inconsistent. Many regulators face resource constraints or lack the tools to impose significant sanctions, particularly in cross-border cases. The introduction of the Modernisation Directive (EU) 2019/2161 partially addressed this issue by harmonising penalties, but challenges remain:

- **Cross-Border Coordination**: Platforms often operate transnationally, making enforcement fragmented and ineffective.
- **Transparency Issues**: Many enforcement actions lack visibility, reducing public awareness and the reputational risks of platforms engaging in harmful practices.[cccxlviii]
- **Disproportionate Penalties**: Existing penalties may not scale with platform revenues, particularly for major global players whose financial impact from fines is minimal compared to their profits.

5. Legislative Basis for Enhanced Penalties[cccxlix]

The GDPR, Modernisation Directive, and DSA provide a foundation for robust enforcement. For example:

- **GDPR:** Article 83 allows for administrative fines of up to 4% of annual global turnover, ensuring financial penalties are proportionate to violators' economic power.
- **Modernisation Directive**: Articles 13 and 24 mandate harmonised penalties for unfair commercial practices, requiring Member States to implement effective and dissuasive fines.
- **DSA:** Provides a framework for holding digital platforms accountable for systemic violations, including harm to children caused by unsafe design or practices.[cccl]

6. Public Expectations and Reputational Incentives

Parents, guardians, and the broader public increasingly expect digital platforms to prioritise child safety. Explicit and publicised penalties for non-compliance signal a commitment to accountability. Furthermore, public enforcement outcomes create reputational risks for violators, incentivising better compliance with child safety standards beyond the immediate financial implications of fines. By addressing these issues through enhanced penalty frameworks, Member States can ensure that platforms prioritise the well-being of children and foster trust in digital environments. This approach aligns with the EU's broader goals of protecting vulnerable consumers and maintaining high standards of fairness in the digital economy.

INTRODUCE DYNAMIC PARENTAL CONTROLS FOR AI-DRIVEN CONTENT: I RECOMMEND DEVELOPING ADAPTIVE PARENTAL CONTROL FEATURES FOR AI-DRIVEN PLATFORMS. THESE FEATURES WOULD ALLOW PARENTS TO ADJUST CONTROLS BASED ON A CHILD'S AGE AND ENGAGEMENT PATTERNS, EMPOWERING THEM TO MONITOR CONTENT MORE EFFECTIVELY.

INTRODUCE DYNAMIC PARENTAL CONTROLS FOR AI-DRIVEN CONTENT

Explanation: The rapid advancement of AI-driven platforms presents new challenges for parents in safeguarding their children online. While traditional parental controls offer basic measures, they often need more flexibility to adapt to the evolving digital landscape and the specific needs of individual children. AI-powered platforms, with their personalised content recommendations and sophisticated algorithms, require a more nuanced approach to parental controls.

Suggested Remedy: I recommend developing adaptive parental control features for AI-driven platforms to empower parents in the digital age. These features would:

1. **Prioritise Age-Based Customization:** Allow parents to adjust controls based on their child's age and maturity level, ensuring content aligns with developmental needs.
2. **Monitor Engagement Patterns:** Track children's interactions with AI-driven platforms, providing insights into content consumption and potential risks.
3. **Facilitate Real-Time Adjustments:** Empower parents to modify controls in response to observed engagement patterns, enabling proactive intervention.
4. **Promote Transparency and Explainability:** Explain AI-driven recommendations and parental control features clearly to foster informed decision-making.

Legal Provisions That Need Amending

1. **Digital Services Act (DSA):**
   - **Article 25:** Expand the scope of prohibited manipulative practices to include those explicitly targeting children based on AI-driven profiling.
   - **Article 28:** Strengthen platform requirements to provide robust, dynamic parental control features for AI-driven content.

Conclusion By introducing dynamic parental controls for AI-driven content, the EU can empower parents to safeguard their children effectively in the evolving digital landscape. These adaptive features and a robust legal framework will promote a safer and more child-friendly online environment.

FACILITATE EASIER REPORTING FOR PARENTS AND GUARDIANS: ESTABLISH CLEAR, ACCESSIBLE REPORTING CHANNELS FOR PARENTS TO REPORT MANIPULATIVE PRACTICES IN CHILDREN'S APPS, WITH FOLLOW-UP ACTIONS REQUIRED BY REGULATORS.

FACILITATE EASIER REPORTING FOR PARENTS AND GUARDIANS:

Explanation: The digital environment presents a complex challenge for protecting children's rights. While offering valuable opportunities for learning, playing, and skill development, it also exposes children to cyberbullying, harmful content, and privacy violations. With their still-developing understanding of online risks and consequences, children are particularly vulnerable to manipulative design practices employed by some apps. These practices often exploit cognitive biases and children's inexperience to encourage excessive engagement, in-app purchases, and data sharing, potentially leading to addiction, financial exploitation, and privacy harm.

Suggested Remedy: To better protect children's rights online, it is crucial to facilitate easier reporting for parents and guardians. The following measures provide effective solutions:

1. **Establish a Centralised Reporting Portal:** Create a user-friendly online platform to report manipulative practices in children's apps. This portal should be accessible to parents and guardians across all EU member states, with clear instructions and support in multiple languages.
2. **Simplify Reporting Procedures:** Design the reporting process to be straightforward and efficient. Implement a standardised form to capture essential information, such as the child's age, the app's name and developer, and a description of the manipulative practice.
3. **Ensure Accessibility and Support:** Provide guidance and support to parents and guardians throughout the reporting process. Offer helplines, live chat assistance, and FAQs to address questions or concerns.
4. **Mandate Follow-Up Actions by Regulators:** Impose a legal obligation on regulators to acknowledge, investigate, and take appropriate action on all reported incidents. These actions should include enforcement measures against developers employing manipulative practices, such as warnings, fines, or app removal.
5. **Promote Awareness and Education:** Conduct public awareness campaigns to inform parents and guardians about the risks of manipulative practices in children's apps and the importance of reporting. Offer educational resources on how to identify these practices and protect children online.[cccli]

Legal Provisions That Need Amending: The implementation of these measures requires amendments to the following legal provisions:

1. **General Data Protection Regulation (GDPR):**
   - **Article 8:** Strengthen parental responsibility and control over children's data processing by mandating robust parental verification systems for all online services children access.[ccclii]
   - **Article 12:** Introduce child-specific transparency obligations, requiring platforms to provide privacy notices in plain, age-appropriate language.[cccliii]
   - **Article 25:** Expand data protection by design requirements to include specific safeguards for children's online environments, such as minimising data collection and avoiding manipulative design practices.[cccliv]
   - **Article 35:** Mandate Data Protection Impact Assessments (DPIAs) for all services likely to impact children disproportionately, focusing on child-specific risks and mitigation measures.[ccclv]

2. **Digital Services Act (DSA):**

    - **Article 24:** Include child-specific transparency and accountability measures for data processing practices, requiring platforms to provide clear, accessible information to parents and guardians about how they use children's data.[ccclvi]
    - **Article 34:** Mandate systemic risk assessments for platforms accessed by children, focusing on identifying and mitigating risks related to manipulative design and data exploitation.[ccclvii]

Conclusion

By facilitating easier reporting for parents and guardians, the EU can take a significant step towards protecting children's rights online. Establishing clear reporting channels, simplifying procedures, and mandating follow-up actions by regulators will empower parents and guardians to actively participate in safeguarding their children from manipulative practices in apps. These measures, combined with the suggested amendments to the GDPR, DSA, and the new DFA, will contribute to a safer, fairer, and more equitable digital environment for children.

DEVELOP EDUCATIONAL PROGRAMS ON DIGITAL LITERACY: WORK WITH SCHOOLS AND CHILD ADVOCACY ORGANISATIONS TO EDUCATE CHILDREN ON RECOGNISING AND RESISTING DARK PATTERNS, EQUIPPING THEM WITH EARLY DIGITAL LITERACY SKILLS. THIS ALIGNS TO EMPOWER CHILDREN AS INFORMED DIGITAL CITIZENS FROM A YOUNG AGE.

DEVELOP EDUCATIONAL PROGRAMS ON DIGITAL LITERACY

Explanation: The digital world is an integral part of children's lives, offering unprecedented opportunities for learning, communication, and creativity. However, it also presents potential risks, including exposure to harmful content, cyberbullying, and manipulative marketing practices. These dark patterns frequently exploit cognitive biases and vulnerabilities, particularly in children with less experience and understanding of online environments.

Suggested Remedy: To empower children as informed digital citizens, educators must develop programs focused on digital literacy. These programs should:

1. **Start Early:** Introduce digital literacy concepts in primary school, adapting teaching methods to different age groups.
2. **Focus on Critical Thinking:** Teach children to evaluate online information critically, identify manipulative tactics, and make informed choices.
3. **Incorporate Interactive Learning:** Use games, simulations, and real-life examples to make learning engaging and relevant.
4. **Partner with Experts:** Collaborate with child advocacy organisations, technology experts, and educators to develop evidence-based programs.
5. **Provide Resources for Parents and Teachers:** Offer workshops, online materials, and support to help adults guide children's online experiences.

Legal Provisions That Need Amending

1. **Digital Services Act:**
    - **Article 24:** Strengthen platform requirements to provide clear, age-appropriate information about data processing practices.
    - **Article 25:** Expand the scope of prohibited manipulative practices to include those specifically targeting children.

Conclusion

By developing educational programs on digital literacy, the EU can empower children to navigate the digital world safely and responsibly. These programs and strengthened legal frameworks will help create a more equitable and child-friendly online environment.

ENHANCE THE SCOPE OF UNFAIR COMMERCIAL PRACTICES: UPDATE THE UCPD TO ENCOMPASS DIGITAL FAIRNESS FOR CHILDREN, EXPLICITLY ADDRESSING DIGITAL DESIGNS THAT COMPROMISE CHILDREN'S DECISION-MAKING AUTONOMY.

ENHANCE THE SCOPE OF UNFAIR COMMERCIAL PRACTICES

Explanation: The digital world offers children unprecedented opportunities for learning, connecting, and playing, but it also exposes them to new forms of commercial exploitation. While the UCPD prohibits misleading and aggressive practices that distort consumer behaviour, regulators must significantly expand it to address the unique vulnerabilities of children in the digital age. Children's developing cognitive abilities, emotional susceptibility, and limited online experience make them particularly vulnerable to manipulative digital designs employed by some businesses. These designs can exploit children's trust, naivety, and desire for social acceptance to promote excessive engagement, risky behaviours, and unwanted purchases.

Suggested Remedy: To enhance child protection online, regulators should update the UCPD to:

1. **Explicitly Address Children's Vulnerabilities:** Include a separate chapter or section dedicated to digital fairness for children, recognising their unique vulnerabilities and developmental needs.
2. **Expand the Definition of Unfair Commercial Practices:** Broaden the definition to include practices that exploit children's cognitive, emotional, and social vulnerabilities, such as:
    - **Dark patterns:** Misleading interfaces that trick children into making unintended choices (e.g., hidden subscription fees, disguised ads).
    - **Addictive designs:** Features that encourage excessive engagement, dependence, and even addiction (e.g., infinite scroll, randomised rewards).
    - **Personalized marketing:** Targeted advertising that exploits children's interests, insecurities, and desire for social acceptance.
    - **Manipulative social influence:** Techniques that pressure children into making purchases or engaging in risky behaviours to gain social approval or avoid exclusion.
3. **Strengthen the "Blacklist" of Prohibited Practices:** Expand Annex I of the UCPD to include specific examples of digital design practices deemed unfair or misleading when targeting children.
4. **Introduce Child-Specific Data Protection Measures:** Incorporate provisions inspired by the GDPR and the Age-Appropriate Design Code to ensure that children's data is processed fairly and transparently.
5. **Provide Clear Guidance for Businesses:** Offer detailed guidance and examples of prohibited practices to help businesses understand their obligations and promote the development of child-friendly digital environments.

Legal Provisions That Need Amending

1. **Unfair Commercial Practices Directive (UCPD):**
    - **Article 5:** Expand the definition of "vulnerable consumer" to explicitly include children and address their online vulnerabilities.
    - **Annexe I:** Certain digital design practices exploit the unique vulnerabilities of children, making them particularly harmful when used in online platforms and services aimed at younger audiences. Include a separate section with examples of digital design practices identified as unfair when targeting children.
        1. Manipulative Gamification: Platforms often employ game-like mechanics, such as streaks, badges, or rewards, to create compulsive usage patterns. When directed at children, these tactics exploit their underdeveloped impulse control to keep them engaged for extended periods.
        2. Excessive In-App Purchases: Apps and games encourage children to spend money through tactics like limited-time offers, countdown timers, or confusing interfaces that

obscure actual costs, pressuring them into making purchases they do not fully understand.

3. Deceptive Advertising: Platforms blur the lines between content and advertisements by embedding ads within gameplay or social media feeds, making it difficult for children to identify them as promotional material.
4. Obstructive Interfaces: Services complicate processes like unsubscribing, disabling notifications, or exiting apps, intentionally creating frustration loops to discourage children from disengaging.
5. Data Exploitation for Personalisation: Platforms leverage personal data to serve highly tailored and persuasive content, further deepening children's engagement without their awareness of how platforms use their data.
6. Emotionally Manipulative Notifications: Apps use emotionally charged language in notifications to elicit feelings of urgency or guilt, such as "Your friend misses you!" or "Do not let your team down!" targeting children's social and emotional vulnerabilities.

Conclusion By expanding the UCPD to address children's unique online vulnerabilities, the EU can take a decisive step towards creating a safer and more equitable digital world for its youngest citizens. These amendments, combined with ongoing efforts to promote digital literacy and empower children as informed digital citizens, will help ensure that children can benefit from the opportunities of the digital world while avoiding unfair or exploitative commercial practices.

IMPOSE TRANSPARENCY ON AI-DRIVEN CONTENT RECOMMENDATIONS: MANDATE THAT PLATFORMS DISCLOSE AI-DRIVEN CONTENT RECOMMENDATIONS FOR CHILDREN, ENABLING TRANSPARENCY ABOUT HOW CONTENT IS SELECTED AND WHY.

IMPOSE TRANSPARENCY ON AI-DRIVEN CONTENT RECOMMENDATIONS

Explanation: AI-powered content recommendation systems are central to children's digital experiences, influencing their interactions with online environments. These systems curate and personalise content based on user data, employing increasingly complex and opaque algorithms. While such technologies can enhance engagement and provide tailored educational or recreational experiences, they pose significant risks to children’s well-being. Due to their developmental stage, children are particularly vulnerable to the psychological impacts of AI-driven recommendations. Their limited critical reasoning skills, emotional impulsivity, and inherent trust in authority figures make them less equipped to identify or resist manipulative or exploitative practices. Systems designed to maximise engagement, often at the expense of user welfare, can exploit these vulnerabilities. Key risks associated with these recommendation systems include:

1. **Addictive Content Consumption:** Algorithms often prioritise content to maximise time spent on platforms, leading children to engage in excessive screen time. Research has demonstrated that such prolonged usage can impair social development, contribute to mental health issues, and reduce physical activity.

2. **Exposure to Inappropriate or Harmful Material:** AI systems, driven by engagement metrics rather than ethical considerations, may inadvertently expose children to harmful content, such as violent or explicit material, misinformation, or content that promotes unhealthy behaviours.

3. **Manipulative Commercial Practices:** Recommendation algorithms frequently integrate targeted advertising and in-app purchase prompts. These can exploit children's cognitive and emotional vulnerabilities, leading to unintentional spending or engagement with unsuitable products.

4. **Loss of Privacy and Data Exploitation:** The data collection that underpins AI recommendations involves invasive profiling, frequently raising ethical and legal concerns around consent and data protection. Children, in particular, may unknowingly provide sensitive information, further amplifying these concerns.

A significant challenge in regulating these systems is their opacity. The algorithms and data inputs driving content personalisation are typically proprietary and shielded from scrutiny. This lack of transparency undermines the ability of regulators, parents, and even platform operators to evaluate whether these systems adhere to child welfare principles, ethical norms, or legal obligations. Moreover, AI technologies' dynamic and evolving nature makes it difficult to anticipate all potential harms. Current safeguards, such as age-restriction policies or opt-in mechanisms, often must address these systemic issues. Without clear accountability and robust oversight, platforms can prioritise commercial interests over the rights and well-being of child users. Addressing these challenges requires a regulatory framework that recognises children's unique vulnerabilities, ensures the ethical use of AI technologies, and enforces transparency and accountability across the lifecycle of recommendation systems. Only by embedding child welfare principles into the design, deployment, and oversight of these systems can we create a digital environment that prioritises the rights and development of young users.

Suggested Remedies

1. Mandatory Algorithmic Transparency

Explanation: Platforms must disclose the logic, functionality, and objectives of content recommendation algorithms targeting children. These disclosures ensure platforms design and operate such systems ethically, aligning with child welfare principles and enabling scrutiny from parents, regulators, and civil society.

Justification:

- Article 13 of the General Data Protection Regulation (GDPR) mandates that individuals, including children, are informed about automated decision-making, including meaningful information about the logic involved and its likely consequences.

- Article 22 of the GDPR regulates automated decision-making processes, further supported by Article 5(1)(b) of the AI Act, which prohibits AI practices that exploit vulnerabilities of specific groups, including children.

Platforms should clearly and accessibly explain the design of their recommendation algorithms and the processes used to select content for children, tailoring this information to an age-appropriate levelConduct independent audits to assess the ethical implications and risks of these algorithms, ensuring compliance with EU regulations and child-specific transparency standards.

2. Data Minimisation and Privacy Safeguards

Explanation: Platforms must adhere to strict data minimisation principles, ensuring only essential data are collected to deliver recommendations. These practices must be embedded into the design of content recommendation systems to align with children's rights to privacy and protection.

- Article 5(1)(c) of the GDPR specifies that personal data collection should be adequate, relevant, and limited to what is necessary for processing.
- Article 25 of the GDPR calls for data protection by design and default, requiring platforms to incorporate safeguards from the outset.
- Recital 38 of the GDPR explicitly acknowledges the need for enhanced data protection for children, recognising their vulnerability.

Implementation:

- Limit data collection to non-sensitive categories, avoiding behavioural profiling or collection of data such as location, health, or biometric information without explicit, informed consent from parents or guardians.
- Platforms must embed privacy-enhancing technologies into their systems to ensure children's data are anonymised where possible and only used to support their best interests.

3. Prohibition of Manipulative AI Practices

Explanation: Prohibiting manipulative tactics protects children from undue commercial or psychological pressures.

Justification:

- Article 5(1)(b) of the AI Act explicitly prohibits using AI systems that exploit vulnerabilities of individuals based on age or other factors, causing material distortion of behaviour.
- The UCPD, particularly its Annex I blacklist, prohibits practices that exploit consumer vulnerabilities, which should extend to AI-driven manipulations targeting minors.

Implementation:

- Ban AI features such as urgency prompts, countdown timers, or gamified designs that pressure children into making hasty decisions.
- Prohibit targeted advertising for children that leverages data to manipulate purchasing decisions or engagement behaviours.
- Platforms should implement clear, upfront disclosures of monetised content and in-app purchase prompts in child-directed environments.

4. Independent Monitoring and Enforcement

Explanation: Strong enforcement mechanisms are essential to ensure consistent compliance across Member States and create accountability for platforms. Independent monitoring ensures that AI systems targeting children operate within legal and ethical boundaries.

Justification:

- Article 63 of the GDPR establishes a consistency mechanism to ensure harmonised application of regulations across Member States.
- The AI Act proposes the establishment of national supervisory authorities to oversee compliance with its provisions, which should include child-specific enforcement priorities.

Implementation:

- Establish specialised supervisory authorities to monitor AI systems targeting children, ensuring they adhere to transparency, data minimisation, and ethical design standards.
- Strengthen collaboration between Data Protection Authorities (DPAs) and consumer protection bodies to address cross-border challenges effectively.
- Impose significant penalties for platforms that fail to comply with child-specific safeguards, using the GDPR's fines provisions as a deterrence model.
-

Legal Provisions That Need Amending

1. General Data Protection Regulation (GDPR) The GDPR currently provides robust protections for personal data but requires targeted amendments to address the unique vulnerabilities of children interacting with AI-driven content recommendation systems:

- **Article 5(1)(c) (Data Minimisation):** Introduce explicit provisions mandating that data collection for AI systems targeting children must be strictly necessary for delivering age-appropriate recommendations. Extend the application of Recital 38 to specify stricter requirements for children's data processing.

- **Article 25 (Data Protection by Design and Default):** Expand the scope to include requirements for content recommendation algorithms explicitly targeting children. Platforms should be required to embed child-specific privacy controls into their systems, ensuring that data collection and processing align with the child's best interests.

- **Articles 12–14 (Transparency Obligations):** Strengthen existing transparency obligations by requiring platforms to provide child-friendly explanations of how AI-driven recommendations operate. Include a mandate for independent audits of algorithmic transparency.

2. AI Act The AI Act addresses high-risk systems and their impact on vulnerable groups but must explicitly extend its application to content recommendation systems targeting children:

- **Article 5(1)(b) (Prohibited Practices):** Expand the prohibition on AI systems that exploit vulnerabilities to include manipulative content recommendations targeted at minors. Specify examples of banned practices, such as gamified nudges, urgency prompts, and hyper-personalised advertising.

- **Article 29 (Transparency for High-Risk Systems):** Add specific requirements for content recommendation algorithms targeting children. Platforms should disclose the logic and operation of these systems and any measures taken to mitigate risks to children's well-being.

- **Article 64 (Monitoring and Enforcement):** Ensure supervisory authorities prioritise enforcement of child-specific provisions, establish clear guidelines for evaluating compliance, and address non-conformity in cross-border cases.

3. Digital Services Act (DSA) The DSA provides a framework for transparency and accountability in online platforms but requires further refinement to safeguard children:

- **Article 24 (Transparency Obligations):** Mandate specific transparency measures for content recommendation systems targeting minors, including disclosures on how content is selected, the sources of recommendations, and any commercial considerations involved.

- **Article 17 (Protection of Minors):** Extend this provision to prohibit platforms from employing AI-driven mechanisms that amplify harmful or manipulative content aimed at children. Include requirements for platforms to implement age-appropriate filters and parental controls.

- **Article 35 (Risk Assessment):** Require platforms to conduct child-specific risk assessments for their AI-driven recommendation systems, evaluating the potential psychological and behavioural impacts of recommended content.

4. Unfair Commercial Practices Directive (UCPD)

The UCPD's Annex I blacklist of unfair practices should be updated to address AI-driven manipulative tactics targeting children explicitly:

- **Annex I (Blacklisted Practices):** Add provisions banning specific manipulative practices, such as countdown timers, in-game nudges, and hyper-personalised advertising in child-directed environments.

- **Article 6 (Misleading Actions):** Expand the definition of misleading actions to include AI systems that distort children's behaviour through covert design or algorithmic manipulation, ensuring the directive covers digital and AI-driven contexts comprehensively.

Summary of Amendments By refining these legal provisions, the GDPR, AI Act, DSA, and UCPD can create a cohesive and enforceable framework for safeguarding children against the risks posed by AI-driven content recommendations. These amendments would address transparency, data minimisation, and prohibiting manipulative practices, ensuring platforms operate ethically and align with children's rights.

BIBLIOGRAPHY

[i] Kelsey Campbell-Dollaghan, 'The Year Dark Patterns Won' *CO.DESIGN* (21 December 2016) https://www.fastcompany.com/co-design accessed 29 May 2017.

[ii] Harry Brignull, 'Dark Patterns: Deception vs. Honesty in UI Design' *A List Apart* (1 November 2011) https://alistapart.com accessed 29 May 2017. Note: darkpatterns.org is now 'Deceptive Patterns' https://www.deceptive.design accessed 29 November 2024.

[iii]

[iv] UNICEF, *The State of the World's Children 2017: Children in a Digital World* (UNICEF 2017) https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf accessed 29 November 2024.

[v] Norwegian Consumer Council, 'Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy' (Norwegian Consumer Council 2018) <https://www.forbrukerradet.no/undersokelse/2018/deceived-by-design>.

[vi] S.E. Domoff, A.L. Borgen, J.S. Radesky, Interactional theory of childhood problematic media use, Human behavior and emerging technologies 2.4 (2020) 343-353. doi: 10.1002/hbe2.217

[vii] UNICEF, *Policy Guidance on AI for Children, Draft Version 1.0* (UNICEF 2020) https://www.unicef.org/innocenti/media/1326/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf accessed 29 November 2024.

[viii] Fosh T, *Hooked: Why We Are Addicted and How to Break Free* (Watkins Media Limited 2024); Ahn SJ, Johnsen K and Ball C, 'Points-Based Reward Systems in Gamification Impact Children's Physical Activity Strategies and Psychological Needs' (2019) 46 *Health Education & Behavior* 417.

[ix] JWT Marketing Communications, 'Fear of Missing Out' (JWT Intelligence, 7 March 2012) http://www.jwtintelligence.com/wp-content/uploads/2012/03/F_JWT_FOMO-update_3.21.12.pdf accessed 29 November 2024.

[x] European Parliament, 'Addictive Design of Online Services and Consumer Protection in the EU Single Market' (2023) OJ C 4164.

[xi] Abel JP, Buff CL and Burr SA, 'Social Media and the Fear of Missing Out: Scale Development and Assessment' (2016) 14 *Journal of Business & Economics Research* 33.

[xii] European Data Protection Supervisor, 'Resolution on Children's Digital Rights' (43rd Closed Session of the Global Privacy Assembly, October 2021) https://www.edps.europa.eu/system/files/2021-10/21-10-25-gpa-resolution-childrens-digital-rights-final-adopted_en.pdf accessed 29 November 2024.

[xiii] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

[xiv] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

[xv] European Commission, 'Review of EU Consumer Law' (European Commission) https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en accessed 29 November 2024.

[xvi] Ofcom, 'Looking Ahead to Online Regulation: Transparency Reporting' (Ofcom, 2024) https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/looking-ahead-to-online-regulation-transparency-reporting/ accessed 29 November 2024.

[xvii] EDPB Guidelines on Dark Patterns: European Data Protection Board, 'Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces' (adopted 14 March 2022) https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en accessed 29 November 2024.

[xviii] Gray CM, Santos C, Bielova N, Toth M and Clifford D, 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective' in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (ACM 2021) 1.

[xix] Silverman ME, Jedd K and Luciana M, 'Neural Networks Involved in Adolescent Reward Sensitivity: A Review of Functional Connectivity Studies' (2017) 37 *Journal of Neuroscience* 10855 https://www.jneurosci.org/content/37/45/10855 accessed 29 November 2024.

[xx] Rodrigo Smiderle and others, 'The Impact of Gamification on Students' Learning, Engagement and Behavior Based on Their Personality Traits' (2020) 7 Smart Learning Environments 3.

[xxi] Arianna Rossi and others, 'Who Is Vulnerable to Deceptive Design Patterns? A Transdisciplinary Perspective on the Multi-Dimensional Nature of Digital Vulnerability' (2024) 55 Computer Law & Security Review 106031.

[xxii] 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023).

[xxiii] Jaques, P., Pacheco, R. C. S., & Vicari, R. M., 'The impact of gamification on students' learning, engagement and behavior based on their personality traits' (2020) 7 *Smart Learning Environments* 3.

[xxiv] Melissa G Hunt and others, 'No More FOMO: Limiting Social Media Decreases Loneliness and Depression' (2018) 37 Journal of Social and Clinical Psychology 751.

[xxv] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024.

[xxvi] Every new 'like' is a reward, triggering a dopamine release. Over time, this can foster a dependency on such platforms for emotional well-being. There is a solid neuro-scientific consensus that dopamine delivery in adolescents comes from risk-taking and approval (Steinberg, L. (2008). A social neuroscience perspective on adolescent risk-taking. Developmental Review, 28, 78-106. NEUROBIOLOGÍA DE LA ADOLESCENCIA; Sherman, L. E., Payton, A. A., Hernandez, L. M., Greenfield, P. M., & Dapretto, M. (2016). The power of the like in adolescence: Effects of peer influence on neural and behavioural responses. Psychological science, 27(7), 1027-1035; "The results of neurological and psychiatric tests on social media users show that similar biological and psychological symptoms of alcohol, cigarette and drug addicts are seen in active social media users. Also, symptoms such as depression, death and suicidal thoughts, low self-esteem, loneliness and social isolation, and depression scale scores are higher in Internet addicts. The intensive use of social media damages the social functioning of the individual and society in some areas. This addiction type is related with Dopamine which is a neurochemical created in various parts of the brain and is critical for all kinds of brain functions including thinking, carrying, sleeping, mood, attention, motivation, seeking and rewarding.", see Macit, H. B., Macit, G., & Güngör, O. (2018). Research on social media addiction and dopamine driven feedback. Mehmet Akif Ersoy Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 5(3), 882-897.

[xxvii] Van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. The International Journal of Children's Rights, 28(4), 833-859.

[xxviii] Brignull H, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (Apress 2023).

[xxix] 5Rights Foundation, Designing for children: A rights-respecting framework for the digital world (5Rights Foundation 2020).

[xxx] European Commission, 'Fitness Check of EU Consumer Law on Digital Fairness' (2023), p. 2.

[xxxi] 5Rights Foundation, Disrupted Childhood: The Cost of Persuasive Design (2018) p. 6; European Commission, Fitness Check of EU Consumer Law on Digital Fairness (2023) p. 58; 5Rights Foundation, Pathways: How Digital Design Puts Children at Risk (2021) p. 17.

[xxxii] 5Rights Foundation, Disrupted Childhood (2018) 6–7; Digital Futures Commission, When Are Commercial Practices Exploitative? Ensuring Child Rights Prevail in a Digital World (2021) 85.

[xxxiii] Norwegian Consumer Council, Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy (27 June 2018) 13 https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

[xxxiv] James Ash, Rachel Gordon and Sarah Mills, Between Gaming and Gambling: Children, Young People, and Paid Reward Systems in Digital Games (ESRC, 2022) 15-16.

[xxxv] Byron T, *Safer Children in a Digital World: The Report of the Byron Review* (Department for Children, Schools and Families, 2008) 8, 12.

[xxxvi] European Commission, 'Fitness Check of EU Consumer Law: Protecting Children as Consumers' (2024) 2, 24; European Commission, 'Study to support the Fitness Check of EU Consumer Law on Digital Fairness and the Modernisation Directive (EU) 2019/2161 - Final Report Annexes' (2024) 192, 217; European Commission, 'Study to support the Fitness Check of EU Consumer Law on Digital Fairness and the Modernisation Directive (EU) 2019/2161 - Final Report Part 2' (2024) 31, 42; European Commission, 'Fitness Check and Report on the Application of the Modernisation Directive (EU) 2019/2161' (2024) 31, 53; European Commission, 'Questions and Answers on the Digital Fairness Fitness Check' (2024) 3, 8.

[xxxvii] European Commission, 'Fitness Check of EU Consumer Law' (2024) 5, 17, 18; European Commission, 'Study to support the Fitness Check of EU Consumer Law on Digital Fairness and the Modernisation Directive (EU) 2019/2161 - Final Report Part 2' (2024) 31, 42

[xxxviii] European Commission, 'Commission Staff Working Document: Fitness Check of EU Consumer Law on Digital Fairness' (2024) 153, 158; Netherlands Authority for Consumers and Markets (ACM), 'ACM Imposes Fine on Epic for Unfair Commercial Practices Aimed at Children in Fortnite' (2024) 1, 3; Norwegian Consumer Council, 'Enough Deception! Norwegian Consumers' Experiences with Deceptive Design' (2022) 5, 8; Norwegian Consumer Council, 'Deceived by Design: How Tech Companies Use Dark Patterns' (2018) 4, 6.

[xxxix] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing Up in a Digital Age' (LSE, 2019) 3, 6

[xl] Revealing Reality, 'Research into Risk Factors That May Lead Children to Harm Online' (Ofcom, 2022) 12, 24

[xli] 5Rights Foundation, 'Pathways: How Digital Design Puts Children at Risk' (5Rights Foundation, 2021) 30, 32; Revealing Reality, 'Research into Risk Factors That May Lead Children to Harm Online' (Ofcom, 2022) 24.

[xlii] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing Up in a Digital Age' (LSE, 2019) 9, 22

[xliii] European Commission, 'Study to support the Fitness Check of EU Consumer Law on Digital Fairness and the Modernisation Directive (EU) 2019/2161 - Final Report Annexes' (2024) 162, 192; European Commission, 'Study to support the Fitness Check of EU Consumer Law on Digital Fairness and the Modernisation Directive (EU) 2019/2161 - Final Report Part 2' (2024) 31, 42

[xliv] Simone van der Hof et al., 'The Child's Right to Protection against Economic Exploitation in the Digital World' (2020) 28(4) Intl J Child Rts 833, 836, 839.

[xlv] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing Up in a Digital Age' (LSE, 2019) 3, 7, 9.

[xlvi] Simone van der Hof et al., 'The Child's Right to Protection against Economic Exploitation in the Digital World' (2020) 28(4) Intl J Child Rts 833, 836, 839

[xlvii] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1–14).

[xlviii] Revealing Reality, 'Research into Risk Factors That May Lead Children to Harm Online' (Ofcom, 2022) 6, 24

[xlix] European Commission, *Fitness check and report on application of Modernisation Directive* (2019) https://commission.europa.eu/system/files/2018-07/exec_summary_online_personalisation_study_en.pdf accessed 11 November 2024, 37.

[l] Alutaybi, A., Al-Thani, D., McAlaney, J., and Ali, R., 'Combating Fear of Missing Out (FoMO) on Social Media: The FoMO-R Method' (2020) 17 International Journal of Environmental Research and Public Health 6128

[li] Children's Commissioner for England, 'Loot Boxes and Gambling' (Children's Commissioner for England, 22 October 2019) https://www.childrenscommissioner.gov.uk/blog/loot-boxes-and-gambling/ accessed 12 November 2024

[lii] Federal Trade Commission, 'FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers' (FTC, 14 September 2022) https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers accessed 12 November 2024.

[liii] Federal Trade Commission, 'Getting In and Out of Free Trials, Auto-Renewals, and Negative Option Subscriptions' (FTC, 14 September 2022) https://consumer.ftc.gov/articles/getting-and-out-free-trials-auto-renewals-and-negative-option-subscriptions accessed 12 November 2024.

[liv] American Psychological Association, 'Protecting Teens on Social Media' (APA, September 2023) https://www.apa.org/monitor/2023/09/protecting-teens-on-social-media accessed 12 November 2024.

[lv] European Parliament, 'Loot Boxes in Online Games and Their Effect on Consumers, in Particular Young Consumers' (European Parliament, 2020) https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)652727 accessed 12 November 2024.

[lvi] European Parliament, 'Artificial Intelligence and the Rights of the Child: Towards an Integrated Agenda for Research and Policy' (European Parliament, 2022) https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)733512 accessed 12 November 2024.

[lvii] Royal Society for Public Health, 'Status of Mind: Social Media and Young People's Mental Health and Wellbeing' (RSPH, 2017) https://www.rsph.org.uk/our-work/policy/social-media-and-young-people-s-mental-health-and-wellbeing.html accessed 12 November 2024.

[lviii] Mental Health Foundation, 'Body Image in Childhood' (Mental Health Foundation, 2019) https://www.mentalhealth.org.uk/explore-mental-health/articles/body-image-report-executive-summary/body-image-childhood accessed 12 November 2024.

[lix] European Consumer Organisation, 'The Dark Side of Digital: The Hidden Exploitation of Consumers in the Digital World' (BEUC, 2022) https://www.beuc.eu/publications/beuc-x-2022-007_the_dark_side_of_digital.pdf accessed 12 November 2024.

[lx] European Consumer Organisation, '"Dark Patterns" and the EU Consumer Law Acquis' (BEUC, 2022) https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf

[lxi] Lewallen J and Behm-Morawitz E, 'Pinterest or Thinterest? Social Comparison and Body Image on Social Media' (2016) 2 *Social Media + Society* 2056305116640559 https://doi.org/10.1177/2056305116640559 accessed 12 November 2024.

[lxii] Muppalla SK, Vuppalapati S, Reddy Pulliahgaru A and Sreenivasulu H, 'Effects of Excessive Screen Time on Child Development: An Updated Review and Strategies for Management' (2023) 15(6) *Cureus* e40608 https://doi.org/10.7759/cureus.40608 accessed 12 November 2024.

[lxiii] Montag C, Lachmann B, Herrlich M, Zweig K. Addictive Features of Social Media/Messenger Platforms and Freemium Games against the Background of Psychological and Economic Theories. Int J Environ Res Public Health. 2019 Jul 23;16(14):2612. doi: 10.3390/ijerph16142612. PMID: 31340426; PMCID: PMC6679162.

[lxiv] Information Commissioner's Office, 'Safeguard and Empower the Public: Annual Action Plan October 2022 - October 2023' (ICO, 2022) https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan/annual-action-plan-october-2022-october-2023/safeguard-and-empower-the-public/?q=child accessed 12 November 2024

[lxv] Livingstone S, Stoilova M and Nandagiri R, 'Children's Data and Privacy Online: Growing Up in a Digital Age' (London School of Economics and Political Science, 2018) 30, 31 https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf accessed 12 November 2024.

[lxvi] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC, and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L149/22.

[lxvii] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council [2011] OJ L304/64.

[lxviii] Article 5, Consumer Rights Directive – Information requirements for contracts other than distance or off-premises contracts; Article 6 – Information requirements for distance and off-premises contracts; Article 7 – Formal requirements for distance contracts; Article 8 – Formal requirements for off-premises contracts;

[lxix] Article 13, Consumer Rights Directive – Obligations of the trader in the event of withdrawal

[lxx] European Commission, 'Digital Fairness Act' (2024)

[lxxi] Sonia Livingstone et al., 'Children's Rights and Online Age Assurance Systems: The Way Forward' (2024) 32 *International Journal of Children's Rights* 721, 726.

[lxxii] BEUC, *Towards European Digital Fairness: BEUC framing response paper for the REFIT consultation* (2023) 13.

[lxxiii] Ayça Atabey, 'Fairness by Design: Towards a Child-Rights Approach to Digital Fairness' (Media@LSE, 2024) https://blogs.lse.ac.uk/medialse/2024/09/09/fairness-by-design-towards-a-child-rights-approach-to-digital-fairness/ accessed 11 November 2024.

[lxxiv] Ruijie Wang and others, 'Transparency in Persuasive Technology, Immersive Technology, and Online Marketing: Facilitating Users' Informed Decision Making and Practical Implications' (2023) 139 *Computers in Human Behavior* 107545 https://doi.org/10.1016/j.chb.2022.107545 accessed 11 November 2024.

[lxxv] Netherlands Authority for Consumers and Markets, 'Leidraad Bescherming Online Consument' (May 2024), pp. 56-58. This guidance outlines the need for transparency in personalization algorithms to prevent manipulative practices that may disproportionately affect children; Tanya Byron, Safer Children in a Digital World: The Report of the Byron Review (2008) pp. 81-109; Bureau Européen des Unions de Consommateurs, 'Towards European Digital Fairness' (BEUC, 2023) BEUC-X-2023-020, pp. 14-15.

[lxxvi] Tanya Byron, *Safer Children in a Digital World: The Report of the Byron Review* (Department for Children, Schools and Families 2008) 4.

[lxxvii]European Commission, *Fitness Check of EU Consumer Law on Digital Fairness* (Commission Staff Working Document, SWD(2024) 230 final, 3 October 2024). Final report part 2). ;'Questions and Answers on the Digital Fairness Fitness Check'.

[lxxviii] Ruijie Wang and others, 'Transparency in Persuasive Technology, Immersive Technology, and Online Marketing: Facilitating Users' Informed Decision Making and Practical Implications' (2023) 139 *Computers in Human Behavior* 107545 https://doi.org/10.1016/j.chb.2022.107545 accessed 11 November 2024

[lxxix] European Commission, 'Questions and Answers on the Digital Fairness Fitness Check' (2024)'Questions and Answers on the Digital Fairness Fitness Check' (n 78); European Commission, Q&A on the Digital Services Act (Press Release, 24 November 2024) https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_4909 accessed 18 December 2024.

[lxxx] European Commission, 'Fitness Check and Report on the Application of the Modernisation Directive (EU) 2019/2161' (2024);

[lxxxi] Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (First edition: 2 January 2024, Testimonium Ltd 2023).

[lxxxii] CERRE, Note 22, accessed 29 November 2024; Hilda Hadan and others, 'From Motivating to Manipulative: The Use of Deceptive Design in a Game's Free-to-Play Transition' (ACM Human-Computer Interaction 2024). Emre Kocyigit, Arianna Rossi and Gabriele Lenzini, 'A Systematic Approach for Reliable Detection of Deceptive Design Patterns' (EuroUSEC 2024).

[lxxxiii] Dr Rachel Gordon Dr. James Ash Dr Sarah Mills, 'Between Gaming and Gambling: Children, Young People, and Paid Reward Systems in Digital Games' (Economic and Social Research Council 2022).

[lxxxiv] Thomas Mejtoft and others, 'Deceptive Design: Cookie Consent and Manipulative Patterns' (34th Bled eConference 2021).

[lxxxv] Norwegian Consumer Council, 'Deceived by Design: How Tech Companies Use Dark Patterns' (2018) <https://www.forbrukerradet.no/>.

[lxxxvi] Brignull (n 85).; Bureau Européen des Unions de Consommateurs, 'Dark Patterns and the EU Consumer Law Acquis: Recommendations for Better Enforcement and Reform' (BEUC 2022).nbnfioulu-202311223286

[lxxxvii] Marc Miquel-Ribé, *Dark User Experience: From Manipulation to Deception* (Bloomsbury Publishing 2019).

[lxxxviii] Mejtoft and others (n 88); CERRE, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe (CERRE) 2024).

[lxxxix] Hadan and others (n 91); Norwegian Consumer Council, Dark Patterns in Digital Services: The Case of Social Media and E-commerce (Norwegian Consumer Council, 2022) Available at https://www.forbrukerradet.nosrn-3694575.

[xc] Rossi, A., Carli, R., Botes, M. W., Fernandez, A., Sergeeva, A., & Chamorro, L. S. (2024). Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the multi-dimensional nature of digital vulnerability. Computer Law & Security Review, 55, 106031.

[xci] Willis, L. E. (2020). Deception by design. Harv. JL & Tech., 34, 115; Mark Leiser and Cristiana Santos, 'Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface' (SocArXiv, 29 April 2023) <https://osf.io/rf3ja> accessed 25 November 2024.

[xcii] Sanchez Chamorro, L., Lallemand, C., & Gray, C. M. (2024, July). " My Mother Told Me These Things are Always Fake"-Understanding Teenagers' Experiences with Manipulative Designs. In Proceedings of the 2024 ACM Designing Interactive Systems Conference (pp. 1469-1482).

[xciii] European Parliament Text on Addictive Design: European Parliament, Addictive Design of Online Services and Consumer Protection in the EU Single Market (European Parliament Resolution P9_TA(2023)0459, 12 December 2023); Van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. The International Journal of Children's Rights, 28(4), 833-859.

[xciv] Bessant, Claire, Luei Lin Ong, Laurel Aynne Cook, Mariea Grubbs Hoy, Beatriz Pereira, Alexa Fox, Emma Nottingham, Stacey Steinberg, and Pingping Gan. "Exploring Parents' Knowledge of Dark Design and Its Impact on Children's Digital Well-Being." (2023).

[xcv] Rossi, A. and et al, 'Who is Vulnerable to Deceptive Design Patterns? A Transdisciplinary Perspective on the Multi-Dimensional Nature of Digital Vulnerability' (2024) 55 Computer Law & Security Review 106031 at page 11. ; Willis, Lauren E., Deception by Design (August 12, 2020). Loyola Law School, Los Angeles Legal Studies Research Paper No. 2020-25, 34 Harvard Journal of Law & Technology 115 (2020), Available at SSRN: https://ssrn.com/abstract=3694575.

[xcvi] Arian, S. (2024, October). Vulnerability in the Age of Metaverse and Protection of the Rights of Users Under EU Law. In The New Shapes of Digital Vulnerability in European Private Law (pp. 169-198). Nomos Verlagsgesellschaft mbH & Co. KG.

[xcvii] European Parliament Text on Addictive Design: European Parliament, Addictive Design of Online Services and Consumer Protection in the EU Single Market (European Parliament Resolution P9_TA(2023)0459, 12 December 2023);

[xcviii] Rossi, A., Carli, R., Botes, M. W., Fernandez, A., Sergeeva, A., & Chamorro, L. S. (2024). Who is vulnerable to deceptive design patterns? A transdisciplinary perspective on the multi-dimensional nature of digital vulnerability. Computer Law & Security Review, 55, 106031; Sanchez Chamorro, L., Lallemand, C., & Gray, C. M. (2024, July). " My Mother Told Me These Things are Always Fake"-Understanding Teenagers' Experiences with Manipulative Designs. In Proceedings of the 2024 ACM Designing Interactive Systems Conference (pp. 1469-1482).

[xcix] Bessant, Claire, Luei Lin Ong, Laurel Aynne Cook, Mariea Grubbs Hoy, Beatriz Pereira, Alexa Fox, Emma Nottingham, Stacey Steinberg, and Pingping Gan. "Exploring Parents' Knowledge of Dark Design and Its Impact on Children's Digital Well-Being." (2023); van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. The International Journal of Children's Rights, 28(4), 833-859.

[c] European Parliament Text on Addictive Design: European Parliament, Addictive Design of Online Services and Consumer Protection in the EU Single Market (European Parliament Resolution P9_TA(2023)0459, 12 December 2023).

[ci] Legaki, N. Z., Karpouzis, K., Assimakopoulos, V., & Hamari, J. (2021). Gamification to avoid cognitive biases: An experiment of gamifying a forecasting course. Technological Forecasting and Social Change, 167, 120725; Commission Staff Workin…).

[cii] Fitness check and repor…); 5Rights - Pathways Report: .

[ciii] Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024) .

[civ] EPRS Study on Harmful Internet Use: Olatz Lopez-Fernandez and Daria J. Kuss, Harmful Internet Use: Part I: Internet Addiction and Problematic Use (European Parliamentary Research Service, PE 624.249, January 2019).

[cv] 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023) <None>.; IMCO Report on Addictive Design: European Parliament, Draft Report on Addictive Design of Online Services and Consumer Protection in the EU Single Market (2023/2043(INI), Committee on the Internal Market and Consumer Protection, 19 July 2023)

[cvi] Leidraad on Online Consumer Protection: Autoriteit Consument & Markt, Leidraad Bescherming Online Consument (May 2024).

[cvii] Fitness Check on EU Consumer Law: European Commission, Fitness Check of EU Consumer Law on Digital Fairness (Commission Staff Working Document, SWD(2024) 230 final, 3 October 2024).; 5Rights - Pathways Report: 5Rights Foundation, Pathways: How Digital Design Puts Children at Risk (5Rights Foundation, July 2021).

[cviii]EPRS Study on Harmful Internet Use: Olatz Lopez-Fernandez and Daria J. Kuss, Harmful Internet Use: Part I: Internet Addiction and Problematic Use (European Parliamentary Research Service, PE 624.249, January 2019; Final report Annexes)

[cix] IMCO Report on Addictive Design: European Parliament, Draft Report on Addictive Design of Online Services and Consumer Protection in the EU Single Market (2023/2043(INI), Committee on the Internal Market and Consumer Protection, 19 July 2023).; Leidraad on Online Consumer Protection: Autoriteit Consument & Markt, Leidraad Bescherming Online Consument (May 2024)

[cx] Fitness Check on EU Consumer Law: European Commission, Fitness Check of EU Consumer Law on Digital Fairness (Commission Staff Working Document, SWD(2024) 230 final, 3 October 2024).

[cxi] Legaki, N. Z., Karpouzis, K., Assimakopoulos, V., & Hamari, J. (2021). Gamification to avoid cognitive biases: An experiment of gamifying a forecasting course. Technological Forecasting and Social Change, 167, 120725.

[cxii] 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023); 5Rights - Pathways Report: 5Rights Foundation, Pathways: How Digital Design Puts Children at Risk (5Rights Foundation, July 2021).

[cxiii] BEUC - Digital Fairness Consultation Paper: BEUC, *Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation* (BEUC, 20 February 2023).; 5Rights Foundation (n 21).

[cxiv] BEUC - Digital Fairness Consultation Paper: BEUC, Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation (BEUC, 20 February 2023); Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024).

[cxv]European Parliament Text on Addictive Design: European Parliament, *Addictive Design of Online Services and Consumer Protection in the EU Single Market* (European Parliament Resolution P9_TA(2023)0459, 12 December 2023). ; Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, *Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood* (November 2024).

[cxvi] Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024); Fitness Check and Report on Modernisation Directive: European Commission, *Fitness Check and Report on the Application of the Modernisation Directive (EU) 2019/2161* (European Commission, 2024).

[cxvii] Leidraad - Bescherming Online Consument: Autoriteit Consument & Markt, Leidraad Bescherming Online Consument (May 2024).

[cxviii] ; Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024)

[cxix] Fitness Check and Report on Modernisation Directive: European Commission, Fitness Check and Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024); Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024).

[cxx] Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, *Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood* (November 2024). ; European Parliament Text on Addictive Design: European Parliament, Addictive Design of Online Services and Consumer Protection in the EU Single Market (European Parliament Resolution P9_TA(2023)0459, 12 December 2023).

[cxxi] BEUC - Digital Fairness Consultation Paper: BEUC, Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation (BEUC, 20 February 2023);

[cxxii] Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024)

[cxxiii] EPRS Study on Harmful Internet Use: Olatz Lopez-Fernandez and Daria J. Kuss, Harmful Internet Use: Part I: Internet Addiction and Problematic Use (European Parliamentary Research Service, PE 624.249, January 2019).

[cxxiv]Ibid;

[cxxv] EPRS Study on Harmful Internet Use:Olatz Lopez-Fernandez and Daria J. Kuss, *Harmful Internet Use: Part I: Internet Addiction and Problematic Use* (European Parliamentary Research Service, PE 624.249, January 2019).

[cxxvi]

[cxxvii]Fitness Check on EU Consumer Law: European Commission, Fitness Check of EU Consumer Law on Digital Fairness (Commission Staff Working Document, SWD(2024) 230 final, 3 October 2024); CERRE, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe (CERRE) 2024).

[cxxviii] (BEUC - Digital Fairness Consultation Paper: BEUC, Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation (BEUC, 20 February 2023); Norwegian Consumer Council, 'Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy' (Norwegian Consumer Council 2018) <https://www.forbrukerradet.no/undersokelse/2018/deceived-by-design>.

[cxxix] BEUC, Dark Patterns in Digital Services: The Consumer Protection Implications (BEUC, 2022) https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf accessed 18 December 2024..

[cxxx] Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (First edition: 2 January 2024, Testimonium Ltd 2023); BEUC, Dark Patterns in Digital Services: The Consumer Protection Implications (BEUC, 2022) https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf accessed 18 December 2024.

[cxxxi] CERRE, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe (CERRE) 2024); Norwegian Consumer Council, 'Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy' (Norwegian Consumer Council 2018) <https://www.forbrukerradet.no/undersokelse/2018/deceived-by-design>.

[cxxxii] Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024) ; BEUC, 'Towards European Digital Fairness' (2023) <https://www.beuc.eu/>.

[cxxxiii]Fitness Check on EU Consumer Law: European Commission, Fitness Check of EU Consumer Law on Digital Fairness (Commission Staff Working Document, SWD(2024) 230 final, 3 October 2024). ; Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* (First edition: 2 January 2024, Testimonium Ltd 2023).

[cxxxiv]Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024) ; 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023).

[cxxxv] Final report Annexes; 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023).

[cxxxvi] Hof, S. van der. (2017). I Agree.. Or Do I?: A Rights-Based Analysis of the Law on Children's Consent in the Digital World. Wisconsin International Law Journal, 34(2), 409-445. Retrieved from https://hdl.handle.net/1887/58542

[cxxxvii] Simone, V. D. H., & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. Communications law, 23(1).

[cxxxviii] 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023); Hof, S. van der. (2017). I Agree.. Or Do I?: A Rights-Based Analysis of the Law on Children's Consent in the Digital World. Wisconsin International Law Journal, 34(2), 409-445. Retrieved from https://hdl.handle.net/1887/58542

[cxxxix] Simone, V. D. H., & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. Communications law, 23(1).

[cxl] Simone, V. D. H., & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. Communications law, 23(1).

[cxli] 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023).

[cxlii] 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023).

[cxliii] Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024); 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023).

[cxliv] Simone, V. D. H., & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. Communications law, 23(1).

[cxlv] Mc Cullagh, K. (2016, December). The general data protection regulation: A partial success for children on social network sites?. Forum Iuris; Simone, V. D. H., & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. Communications law, 23(1).

[cxlvi] BEUC - Digital Fairness Consultation Paper: BEUC, *Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation* (BEUC, 20 February 2023); Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024)

[cxlvii] Final Report - Annexes for Fitness Check: Mark Whittle et al, *Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161* (European Commission, 2024).

[cxlviii] BEUC - Digital Fairness Consultation Paper: BEUC, Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation (BEUC, 20 February 2023); Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024).

[cxlix] Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024).

[cl] BEUC - Digital Fairness Consultation Paper: BEUC, Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation (BEUC, 20 February 2023); Final Report - Annexes for Fitness Check: Mark Whittle et al, *Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161* (European Commission, 2024).

[cli] 5Rights Foundation (n 21).

[clii] ibid.

[cliii] European Commission (n 26).

[cliv] Final Report - Annexes for Fitness Check: Mark Whittle et al, Study to Support the Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161 (European Commission, 2024)

[clv] Article 8, GDPR.

[clvi] Norwegian Consumer Council (n 4).; European Commission (n 26).

[clvii] 5Rights Foundation (n 21).; Norwegian Consumer Council (n 4).

[clviii] 5Rights Foundation (n 21).European Commission, *Fitness Check of EU Consumer Law on Digital Fairness* (Commission Staff Working Document, SWD(2024) 230 final, 3 October 2024).; Norwegian Consumer Council (n 4).

[clix] Hof, S. van der. (2017). I Agree.. Or Do I?: A Rights-Based Analysis of the Law on Children's Consent in the Digital World. Wisconsin International Law Journal, 34(2), 409-445. Retrieved

from https://hdl.handle.net/1887/58542; The European Union gene...).

[clx]Hof, S. van der. (2017). I Agree.. Or Do I?: A Rights-Based Analysis of the Law on Children's Consent in the Digital World. Wisconsin International Law Journal, 34(2), 409-445. Retrieved from https://hdl.handle.net/1887/58542 ; 5Rights Foundation (n 21).

[clxi] Hof, S. van der. (2017). I Agree.. Or Do I?: A Rights-Based Analysis of the Law on Children's Consent in the Digital World. Wisconsin International Law Journal, 34(2), 409-445. Retrieved from https://hdl.handle.net/1887/58542

[clxii] Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024); Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024).

[clxiii] Radesky J and Hiniker A, 'From Moral Panic to Systemic Change: Making Child-Centered Design the Default' (2022) 31 *International Journal of Child-Computer Interaction* 100351.

[clxiv] Simone, V. D. H., & Lievens, E. (2018). The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. Communications law, 23(1); 5Rights Foundation, 'Disrupted Childhood: The Cost of Persuasive Design' (2023).

[clxv] 9781802208030-book-part-9781802208030-9.pdf, p. 3.

[clxvi] IPOL_STU2020648780_EN.pdf, pp. 28-31; Commission Staff Working Document Fitness Check on EU consumer law on digital fairness.pdf, pp. 35-40.

[clxvii] ssoar-2023-cole_et_al-Future_Regulation_of_Cross-Border_Audiovisual.pdf, pp. 115-124; ssrn-2728874.pdf, pp. 19-24.

[clxviii] pp. 1-2; 9781802208030-book-part-9781802208030-9.pdf, p. 3.

[clxix] BEUC-X-2024-091_Third_Party_Litigation_Funding.pdf, pp. 1-2; 9781802208030-book-part-9781802208030-9.pdf, p. 3.

[clxx] 978-3-031-60734-9.pdf, pp. 87-91; Jurisdiction_an_Issue_on_the_Intern.pdf, pp. 95-111.

[clxxi] IPOL_STU2020648780_EN.pdf, pp. 28-31; □ Commission Staff Working Document Fitness Check on EU consumer law on digital fairness.pdf, pp. 35-40.

[clxxii] ssrn-2728874.pdf, pp. 19-24; Jurisdiction_an_Issue_on_the_Intern.pdf, pp. 95-111.

[clxxiii] Mediawet 2008 (Netherlands), Dutch Media Act.

[clxxiv] Analysis of the Digital Fairness Act, Sciences Po; ACM Reaction to EU Fitness Check.

[clxxv] BEUC Consultation Paper; Commission Staff Document, Geo-Blocking Regulation Impact.

[clxxvi] Commission Staff Working Document, Fitness Check on Consumer Law; Digital Fairness Fitness Check, Tobias Timmann et al.

[clxxvii] Analysis of the Digital Fairness Act, Sciences Po.

[clxxviii] Commission Staff Working Document, Fitness Check on Consumer Law; DIGITALEUROPE Report.

[clxxix] ACM Reaction to EU Fitness Check; Final Report Annexes on Digital Fairness; European Law Institute, 'Response of the ELI to the European Commission's Public Consultation on Digital Fairness' (ELI 2024) https://www.europeanlawinstitute.eu/..

[clxxx] ACM Reaction to EU Fitness Check; Final Report Annexes on Digital Fairness; European Law Institute, 'Response of the ELI to the European Commission's Public Consultation on Digital Fairness' (ELI 2024) https://www.europeanlawinstitute.eu/..

[clxxxi] Analysis of the Digital Fairness Act, Sciences Po; BEUC Consultation Paper; Media@LSE Report on Child Rights and Digital Fairness;

[clxxxii] Commission Staff Working Document, Fitness Check on Consumer Law; ELI Consultation on Digital Fairness.

[clxxxiii] ACM Reaction to EU Fitness Check; Commission Staff Document, Geo-Blocking Regulation Impact.

[clxxxiv] Analysis of the Digital Fairness Act, Sciences Po; Commission Staff Working Document, Fitness Check on Consumer Law; Final Report Annexes on Digital Fairness.

[clxxxv] UNICEF, *Policy Guidance on AI for Children* (UNICEF 2020) https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children accessed 26 November 2024.

[clxxxvi] Media@LSE Report on Child Rights and Digital Fairness;

[clxxxvii] Commission Staff Document, Geo-Blocking Regulation Impact.

[clxxxviii] Implementation of Digital Law, Springer; Commission Staff Working Document on Digital Fairness.

[clxxxix] Commission Staff Working Document, Fitness Check on Consumer Law; Digital Fairness Fitness Check, Tobias Timmann et al; ELI Consultation on Digital Fairness.

[cxc] Analysis of the Digital Fairness Act, Sciences Po; DIGITALEUROPE Report; Final Report Annexes on Digital Fairness.

[cxci] BEUC Consultation Paper; Commission Staff Document, Geo-Blocking Regulation Impact.

[cxcii] DIGITALEUROPE Report; Media@LSE Report on Child Rights and Digital Fairness.

[cxciii] UNICEF, *Policy Guidance on AI for Children* (UNICEF 2020) https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children accessed 26 November 2024.

[cxciv] Mediawet 2008 (Netherlands), Dutch Media Act.

[cxcv] Commission Staff Working Document, Fitness Check on Consumer Law; DIGITALEUROPE Report;

[cxcvi] BEUC Consultation Paper; Commission Staff Document, Geo-Blocking Regulation Impact; Media@LSE Report on Child Rights and Digital Fairness.

[cxcvii] Digital Fairness Fitness Check, Tobias Timmann et al; Final Report Annexes on Digital Fairness; ELI Consultation on Digital Fairness.

[cxcviii] Analysis of the Digital Fairness Act, Sciences Po; Commission Staff Working Document, Fitness Check on Consumer Law.

[cxcix] Analysis of the Digital Fairness Act, Sciences Po; Commission Staff Working Document, Fitness Check on Consumer Law.

[cc] Analysis of the Digital Fairness Act, Sciences Po; ACM Reaction to EU Fitness Check; Commission Staff Working Document, Fitness Check.

[cci]Analysis of the Digital Fairness Act, Sciences Po; ACM Reaction to EU Fitness Check; Commission Staff Working Document, Fitness Check.

[ccii] Commission Staff Working Document, Fitness Check; Geo-blocking Regulation Impact Analysis; Media@LSE Report on Child Rights and Digital Fairness.

[cciii] DIGITALEUROPE Report; Media@LSE Report on Child Rights and Digital Fairness; ELI Consultation on Digital Fairness.

[cciv] ACM Reaction to EU Fitness Check; Final Report Annexes.

[ccv] BEUC Consultation Paper; Digital Fairness Fitness Check, Tobias Timmann et al.

[ccvi] Procedural Challenges in EU Enforcement, NISPA; Commission Staff Working Document on Digital Fairness.

[ccvii] Research Handbook on EU Law Enforcement; Jurisdictional Issues in the Internet Age, Krytyka Prawa.

[ccviii] Implementation of Digital Law, Springer; Commission Staff Working Document on Digital Fairness.

[ccix] BEUC Consultation Paper on Enforcement; CERRE Policy Report on Integrated Regulatory Frameworks.

[ccx] Research Handbook on EU Law Enforcement; Future Regulation of Cross-Border Audiovisual Content, SSOAR.

[ccxi] Disconnecting Sovereignty, Springer; Enforcement and Cooperation in the EU, IPOL.

[ccxii] Implementation of Digital Law, Springer; Jurisdictional Issues in the Internet Age, Krytyka Prawa.

[ccxiii] Procedural Challenges of Cross-Border Cooperation; EU Consumer Law Fitness Check; Jurisdictional Issues on the Internet.

[ccxiv] Disconnecting Sovereignty: Data Fragmentation; EU Consumer Law Fitness Check

[ccxv] Implementation of Digital Law; Cross-Border Audiovisual Content Regulation.

[ccxvi] BEUC Consultation on Consumer Protection; Enforcement Cooperation Between Member States.

[ccxvii] Research Handbook on Enforcement of EU Law; Cross-Border Audiovisual Content Regulation.

[ccxviii] Enforcement Cooperation Between Member States; Integrated Regulatory Framework for Digital Networks.

[ccxix] EU Consumer Law Fitness Check; Cross-Border Audiovisual Content Regulation.

[ccxx] Information Commissioner's Office, *Age-Appropriate Design: A Code of Practice for Online Services* (ICO 2020) https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/ accessed 26 November 2024.

[ccxxi] Fairness by Design: Child Rights Approach; EDPB Decision on TikTok Practices.

[ccxxii] Roadmap to Illuminating Dark Patterns; Consumer Law Application Report.

[ccxxiii] Roadmap to Illuminating Dark Patterns.; Fitness Check of EU Consumer Law.

[ccxxiv] EDPB Decision on TikTok Practices.

[ccxxv] Annex VI: Analysis of Problematic Practices; Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024.

[ccxxvi] Byron Review on Children and Technology; Fitness Check: Modernisation Directive.

[ccxxvii] Roadmap to Illuminating Dark Patterns; Fitness Check of EU Consumer Law.

[ccxxviii] AI Act and Consumer Protections Overview;

[ccxxix] Consumer Rights and Digital Governance Alignment.

[ccxxx] Byron Review on Digital Child Safety; Fitness Check of EU Consumer Law.

[ccxxxi] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024.; Consumer Rights and Digital Governance Alignment.

[ccxxxii] AI Act and Consumer Protections Overview; Consumer Rights and Digital Governance Alignment.

[ccxxxiii] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024.; Fitness Check of EU Consumer Law.

[ccxxxiv] Fitness Check: Modernisation Directive; Byron Review on Digital Child Safety.

[ccxxxv] Consumer Rights and Digital Governance Alignment.

[ccxxxvi] Unfair Commercial Practices Directive (UCPD)Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22.

[ccxxxvii] General Data Protection Regulation (GDPR)Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1

[ccxxxviii] Digital Services Act (DSA)Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

[ccxxxix] Digital Markets Act (DMA)Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L265/1.

[ccxl] Dark Patterns – Communications of the ACM.pdf; Digital abuse of predictable consumer behaviour must stop _ ACM.nl.pdf

[ccxli] ACM reactie op EU Fitness Check on Digital Fairness.pdf; edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[ccxlii] AP brief on DSA considerations

[ccxliii] Autoriteit Persoonsgegevens, 'Besluit tot het opleggen van een bestuurlijke boete aan TikTok Inc.' (9 April 2021).; Position paper AP - Digital Rule of Law; Rapportage AI- & Algoritmerisico's Nederland

[ccxliv] SDT uitgangspunten over reclame gericht op kinderen; Authority for Consumers and Markets (ACM), 'Guidelines on the Protection of the Online Consumer' (February 2020) https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-online-consumer.pdf accessed 18 December 2024.

[ccxlv] Mediawet advertising restrictions; AI Act implementation concerns.

[ccxlvi] Challenges in cross-border enforcement under GDPR;

[ccxlvii] Calls for algorithm registration and AI literacy; Interplay between GDPR and AI Act provisions

[ccxlviii] UCPD, Art. 5(3) and Recital 18; GDPR, Arts. 12 and 22.

[ccxlix] Autoriteit Persoonsgegevens, *TikTok fined for violating children's privacy* (Press Release, 22 July 2021) https://www.autoriteitpersoonsgegevens.nl/en/current/tiktok-fined-for-violating-childrens-privacy accessed 28 November 2024.

[ccl] Autoriteit Persoonsgegevens, 'Besluit tot het opleggen van een bestuurlijke boete aan TikTok Inc.' (9 April 2021).

[ccli] Authority for Consumers and Markets (ACM), 'Leidraad Bescherming Online Consument' (February 2020) https://www.acm.nl/system/files/documents/leidraad-bescherming-online-consument.pdf accessed 18 December 2024., pp. 4-6.

[cclii] Samenwerkingsplatform Digitale Toezichthouders (SDT), 'Uitgangspunten voor Effectieve Transparantie' (24 March 2023) accessed 18 December 2024, p. 7;

[ccliii] Mediawet, Art. 10; Samenwerkingsplatform Digitale Toezichthouders, *Uitgangspunten voor reclame en marketing gericht op kinderen online* (Guidelines, 24 March 2023) https://www.acm.nl/nl/publicaties/uitgangspunten-voor-reclame-en-marketing-gericht-op-kinderen-online accessed 28 November 2024.

[ccliv] Artilce 12, GDPR; Autoriteit Persoonsgegevens (AP), 'Rapportage AI- & Algoritmerisico's Nederland – Najaar 2023' (2023) https://www.autoriteitpersoonsgegevens.nl/uploads/2023-12/Rapportage%20AI-%20%26%20algoritmerisico%27s%20Nederland%20-%20najaar%202023.pdf accessed 18 December 2024, pp. 8-10.

[cclv] Article 22, GDPR; Samenwerkingsplatform Digitale Toezichthouders (SDT), 'Uitgangspunten voor Effectieve Transparantie' (24 March 2023) accessed 18 December 2024, p. 5-7.

[cclvi] AI Act proposed reforms, pp. 12-13; Autoriteit Persoonsgegevens, 'Position Paper: Digital Rule of Law' (2023) 14. Available at: https://www.autoriteitpersoonsgegevens.nl/uploads/2023-12/Position_Paper_Digital_Rule_of_Law.pdf [Accessed 28 November 2024], p. 14.

[cclvii] Krasodomski-Jones A and others, 'AI: The Challenge for Global Governance' (Chatham House, 7 June 2024) https://www.chathamhouse.org/sites/default/files/2024-06/2024-06-07-ai-challenge-global-governance-krasodomski-et-al.pdf accessed 18 December 2024., p. 11; Algorithm transparency and registration advocacy, pp. 8-9.

[cclviii] Association for Computing Machinery (ACM), *Principles for the Development, Deployment, and Use of Generative AI* (ACM, 2023) https://www.acm.org/binaries/content/assets/public-policy/ustpc-approved-generative-ai-principles accessed 28 November 2024.

[cclix]Autoriteit Persoonsgegevens (AP), 'AI Risk Report Summer 2024: Turbulent Rise of AI Calls for Vigilance by Everyone' (18 July 2024) https://www.autoriteitpersoonsgegevens.nl/en/current/ai-risk-report-summer-2024-turbulent-rise-of-ai-calls-for-vigilance-by-everyone accessed 28 November ; Autoriteit Persoonsgegevens (AP), *Position Paper - Een Sterke Digitale Rechtsstaat* (November 2024) 11 https://www.autoriteitpersoonsgegevens.nl/documenten/position-paper-ap-over-een-sterke-digitale-rechtsstaat#:~:text=De%20basis%20van%20een%20digitale,de%20basis%20van%20de%20rechtsstaat accessed 28 November 2024.

[cclx] Stichting Reclame Code, 'Code for Advertising Directed at Children and Young People' (2013). Available at: https://www.reclamecode.nl/nrc/code-for-advertising-directed-at-children-and-young-people/?lang=en [Accessed 28 November 2024].

[cclxi] Mediawet 2008, Art. 3 (Ministry of Education, Culture and Science, 'Media Act 2008' (14 June 2022). Available at: https://www.government.nl/documents/publications/2022/06/14/media-act-2008 [Accessed 28 November 2024].) Media Authority enforcement guidelines

[cclxii] Ministry of Education, Culture and Science, 'Media Act 2008' (14 June 2022). Available at: https://www.government.nl/documents/publications/2022/06/14/media-act-2008 [Accessed 28 November 2024].; Gerritsen J, 'Media Act 2008' (2009) 3 IRIS 1/29. Available at: https://merlin.obs.coe.int/article/4841 [Accessed 28 November 2024].

[cclxiii] Stichting Reclame Code, 'Code for Advertising Directed at Children and Young People' (2013). Available at: https://www.reclamecode.nl/nrc/code-for-advertising-directed-at-children-and-young-people/?lang=en [Accessed 28 November 2024]; Netherlands Authority for Consumers and Markets, 'Basic Principles for Advertising and Marketing Directed at Children Online' (2023). Available at: https://www.acm.nl/system/files/documents/basic-principles-for-advertising-and-marketing-directed-at-children-online.pdf [Accessed 28 November 2024].

[cclxiv] Taylor Wessing, 'Restrictions on Placement of HFSS Product Adverts' (2022). Available at: https://www.taylorwessing.com/en/insights-and-events/insights/2022/02/dl-restrictions-on-placement-of-hfss-product-adverts [Accessed 28 November 2024];

[cclxv] Autoriteit Persoonsgegevens, 'Rapportage AI- & Algoritmerisico's Nederland' (July 2023) 8-10. Available at: https://www.autoriteitpersoonsgegevens.nl/uploads/2023-07/Rapportage%20Algoritmerisico%27s%20Nederland%20-%20juli%202023.pdf [Accessed 28 November 2024]; Autoriteit Persoonsgegevens, 'Position Paper: Digital Rule of Law' (2023) 14. Available at: https://www.autoriteitpersoonsgegevens.nl/uploads/2023-12/Position_Paper_Digital_Rule_of_Law.pdf [Accessed 28 November 2024].

[cclxvi] Samenwerkingsplatform Digitale Toezichthouders, 'Guidelines on Responsible Digital Advertising to Children' (2023) 5-6. Available at: https://www.sdt.nl/guidelines-responsible-digital-advertising-children [Accessed 28 November 2024];

[cclxvii] The Ministry of the Interior and Kingdom Relations, *Responsible Algorithm Use: The Dutch National and Amsterdam City Algorithm Registers* (Technology Bloggers, 25 August 2023) https://www.technologybloggers.org/artificial-

intelligence/responsible-algorithm-use-the-dutch-national-and-amsterdam-city-algorithm-registers/#:~:text=The%20Ministry%20of%20the%20Interior,algorithms%20can%20meet%20those%20requirements accessed 28 November 2024; European Union Agency for Fundamental Rights, 'Getting the Future Right – Artificial Intelligence and Fundamental Rights' (2020) 11. Available at: https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights [Accessed 28 November 2024].

[cclxviii] ACM, *Gray and Dark Patterns: Insights from 2023 Interview Series* (2023) https://www.acm.nl/system/files/documents/gray-dark-patterns-interview-2023-acm.pdf accessed 28 November 2024.

[cclxix] ACM, *Reactie op EU Fitness Check on Digital Fairness* (2022) https://www.acm.nl/system/files/documents/acm-reactie-op-eu-fitness-check-on-digital-fairness_0.pdf accessed 28 November 2024.

[cclxx] ACM, *Guidelines for Preventing Dark Patterns in User Interfaces* (2022) https://www.acm.nl/en/publications/guidelines-preventing-dark-patterns accessed 28 November 2024.

[cclxxi] EDPB, *Guidelines on Deceptive Design Patterns in Social Media Platform Interfaces* (2022) https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en accessed 28 November 2024.

[cclxxii] EDPB Guidelines on Dark Patterns: European Data Protection Board, 'Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces' (adopted 14 March 2022) https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en accessed 29 November 2024.

[cclxxiii] ACM, *Digital Abuse of Predictable Consumer Behaviour Must Stop* (2023) https://www.acm.nl/en/publications/digital-abuse-predictable-consumer-behaviour-must-stop accessed 28 November 2024; ACM, *Reactie op EU Fitness Check on Digital Fairness* (2022) https://www.acm.nl/system/files/documents/acm-reactie-op-eu-fitness-check-on-digital-fairness_0.pdf accessed 28 November 2024.

[cclxxiv] Autoriteit Persoonsgegevens, *Position Paper: Digital Rule of Law* (2023) 14 https://www.autoriteitpersoonsgegevens.nl/uploads/2023-12/Position_Paper_Digital_Rule_of_Law.pdf accessed 28 November 2024.

[cclxxv] GDPR, Arts. 56 and 60; European Data Protection Board, *Coordinated Enforcement Framework* (2020) https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_documents_20201020_coordinatedenforcementframework_en.pdf accessed 28 November 2024.

[cclxxvi] Cristiana Santos Mark Leiser, 'Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface' (2024) 15 European Journal of Law and Technology.

[cclxxvii] ibid.

[cclxxviii] Michael Sipser, 'Introduction to the Theory of Computation' (1996) 27 ACM Sigact News 27.

[cclxxix] Surrey Safeguarding Children Partnership, 'Recognition of Significant Harm' (Surrey Safeguarding Children Partnership, 26 September 2019) https://surreyscb.procedures.org.uk/zkyqqo/managing-individual-cases/recognition-of-significant-harm accessed 25 November 2024.

[cclxxx] Mark Leiser and Cristiana Santos, 'Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface' (SocArXiv, 29 April 2023) <https://osf.io/rf3ja> accessed 25 November 2024.

[cclxxxi] Article 25, GDPR.

[cclxxxii]

[cclxxxiii] Ibid.

[cclxxxiv] Nomos eLibrary, 'The New Concept of Digital Vulnerability and the European Rules on Unfair Commercial Practices' <https://www.nomos-elibrary.de/>.

[cclxxxv] Nomos eLibrary, 'Consumer Protection and Digital Vulnerability: Common and Diverging Paths' <https://www.nomos-elibrary.de/>.

[cclxxxvi] M Leiser, 'Psychological Patterns and Article 5 of the AI Act': (2024) 1 Journal of AI Law and Regulation 5.

[cclxxxvii] Norwegian Consumer Council, 'Commercial Exploitation of Children and Adolescents Online' (November 2024) https://storage02.forbrukerradet.no/media/2024/11/commercial-exploitation-of-children-and-adolescents-online-november-2024-komprimert-2.pdf accessed 18 December 2024; Nomos eLibrary (n 302).

[cclxxxviii] Nomos eLibrary (n 306).

[cclxxxix] Nomos eLibrary (n 306).

[ccxc] Nomos eLibrary (n 302).

[ccxci] Christoph Busch and Amelia Fletcher, *Harmful Online Choice Architecture* (CERRE, May 2024) https://cerre.eu/wp-content/uploads/2024/05/CERRE-Final-Report_Harmful-Online-Choice-Architecture.pdf accessed 24 November 2024, 10.

[ccxcii] Christoph Busch and Amelia Fletcher, *Harmful Online Choice Architecture* (CERRE, May 2024) https://cerre.eu/wp-content/uploads/2024/05/CERRE-Final-Report_Harmful-Online-Choice-Architecture.pdf accessed 24 November 2024, 24.

[ccxciii] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive) [2005]

[ccxciv] As discussed in the *Study to Support the Fitness Check of EU Consumer Law on Digital Fairness* (2024) 122-123 https://cerre.eu/ accessed 24 November 2024; Reset.Tech Australia, *A Duty of Care in Australia's Online Safety Act: Policy Briefing* (April 2024) https://au.reset.tech/news/briefing-can-safety-standards-be-enforceable/ accessed 24 November 2024, 9.

[ccxcv] Centre on Regulation in Europe (CERRE), 'Harmful Online Choice Architecture' (May 2024) https://cerre.eu/ accessed 24 November 2024, 18.

[ccxcvi] VON Kommunikasjon, *Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood* (Norwegian Consumer Council, November 2024) 15 https://www.forbrukerradet.no accessed 24 November 2024.

[ccxcvii] Centre on Regulation in Europe (CERRE), *Harmful Online Choice Architecture: Definitions, Regulatory Gaps, and Recommendations* (May 2024) https://cerre.eu accessed 24 November 2024, 15.

[ccxcviii] Leiser, M. (2024). Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface. *Journal of AI law and Regulation*, *1*(1), 5-23.

[ccxcix] Leiser, M., & Santos, C. (2024). Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface. *European Journal of Law and Technology*, *15*(1).

[ccc] Commercial Exploitation Report: Norwegian Consumer Council, *Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood* (November 2024) 6; Duty of Care Report: Reset.Tech Australia, *A Duty of Care in Australia's Online Safety Act: Policy Briefing* (Reset.Tech Australia, April 2024) 15.

[ccci] European Commission, *Commission Staff Working Document: Fitness Check of EU Consumer Law on Digital Fairness* SWD(2024) 230 final, Brussels, 3 October 2024, p. 85.

[cccii] Reset.Tech Australia, A Duty of Care in Australia's Online Safety Act: Policy Briefing (April 2024) 14 https://reset.tech.au/ accessed 24 November 2024.

[ccciii] Leiser, M. (2016). The problem with 'dots': questioning the role of rationality in the online environment. *International Review of Law, Computers & Technology*, *30*(3), 191-210.

[ccciv] ICO, 'Children and the GDPR' (2018) https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf accessed 26 November 2024

[cccv] Siniša S Domazet and Lozanovska Ivona Šušak, 'Children's Data and Privacy Online: Growing up in a Digital Age' (2023) 24 Politika nacionalne bezbednosti 153.

[cccvi] Christoph Busch and Amelia Fletcher, *Harmful Online Choice Architecture* (Centre on Regulation in Europe, May 2024) 16–17.

[cccvii] European Commission, 'Fitness Check of EU Consumer Law on Digital Fairness and the Report on the Application of the Modernisation Directive (EU) 2019/2161' (2022), noting the need for legislative adjustments to address dark patterns and manipulative personalisation, particularly in the context of updating the UCPD to reflect new digital challenges (pp. 65–67). Available at: Commission Fitness Check Report

[cccviii] European Parliament, '2023 Resolution on Addictive Design' in the context of the Commission's public consultation on Digital Fairness, emphasises the introduction of a digital "right not to be disturbed" to eliminate addictive design features and foster user agency. Commission Staff Working Document Fitness Check on EU Consumer Law on Digital Fairness, pages 161-162,

[cccix] Netherlands Authority for Consumers and Markets, ACM imposes fine on Epic for unfair commercial practices aimed at children in Fortnite game (14 May 2024) https://www.acm.nl/en/publications/acm-imposes-fine-epic-unfair-commercial-practices-aimed-children-fortnite-game accessed 24 November 2024.

[cccx] CERRE Report on Harmful Online Choice Architecture Centre on Regulation in Europe (CERRE), Harmful Online Choice Architecture: Regulatory Solutions for Protecting Consumers in the Digital Age (2023) https://www.cerre.eu/publications/harmful-online-choice-architecture accessed 24 November 2024.

[cccxi] *Ibid.*

[cccxii] Livingstone S, Nair A, Stoilova M, van der Hof S, and Caglar C, 'Children's Rights and Online Age Assurance Systems: The Way Forward' (2024) 32 *International Journal of Children's Rights* 721 https://doi.org/10.1163/15718182-32030001 accessed 24 November 2024.

[cccxiii] CERRE Report on Harmful Online Choice Architecture Centre on Regulation in Europe (CERRE), Harmful Online Choice Architecture: Regulatory Solutions for Protecting Consumers in the Digital Age (CERRE, May 2024) p 7 https://www.cerre.eu/publications/harmful-online-choice-architecture accessed 24 November 2024; Report on the Commercial Exploitation of Children and Adolescents Norwegian Consumer Council, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024) p 13 https://www.forbrukerradet.no/publications/commercial-exploitation-children-adolescents-online accessed 24 November 2024.

[cccxiv] Article 6, AI Act.

[cccxv] Arts. 5–9, UCPD.

[cccxvi] Charter of Fundamental Rights of the European Union [2012] OJ C326/391

[cccxvii] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024; COMMISSION_STAFF_WORKIN...).

[cccxviii] Arts. 34, 17, DSA.

[cccxix] Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, *Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood* (November 2024).

[cccxx] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024; Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024).

[cccxxi] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024.

[cccxxii] European Data Protection Board, 'Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)' (2 August 2023) 9 https://edpb.europa.eu/system/files/2023-08/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf accessed 24 November 2024Following EDPB Decision…).

[cccxxiii] Recital 38

[cccxxiv] European Data Protection Board, 'Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)' (2 August 2023) 9 https://edpb.europa.eu/system/files/2023-08/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf accessed 24 November 2024

[cccxxv] e.g., TikTok and Instagram

[cccxxvi] European Data Protection Board, 'Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)' (2 August 2023) 9 https://edpb.europa.eu/system/files/2023-08/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf accessed 24 November 2024

[cccxxvii] Information Commissioner’s Office (ICO), Children and the GDPR (2018) http://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/ accessed 24 November 2024;

[cccxxviii] European Data Protection Board, 'Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR)' (2 August 2023) 9 https://edpb.europa.eu/system/files/2023-08/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf accessed 24 November 2024

[cccxxix] 26. European Data Protection Board (EDPB), 'Binding Decision 2/2023 on the Dispute Submitted by the Irish SA Regarding TikTok Technology Limited' (2 August 2023) https://edpb.europa.eu accessed 24 November 2024.

[cccxxx] Article 2, Digital Services Act.

[cccxxxi] Agencia Española de Protección de Datos (AEPD), Decálogo de principios para la verificación de la edad y la protección de los menores en internet (AEPD, 2024) https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf accessed 18 December 2024; European Data Protection Board (EDPB), 'Binding Decision 2/2023 on the Dispute Submitted by the Irish SA Regarding TikTok Technology Limited' (2 August 2023) https://edpb.europa.eu accessed 24 November 2024.

[cccxxxii] Article 5(1)(c)-(e), GDPR.

[cccxxxiii] Information Commissioner’s Office (ICO), Children and the GDPR (2018) http://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/ accessed 24 November 2024;

[cccxxxiv] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024; Bureau Européen des Unions de Consommateurs (BEUC), ‘Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation’ (Bureau Européen des Unions de Consommateurs (BEUC) 2023) <https://www.beuc.eu/publications/towards-european-digital-fairness>.

[cccxxxv] Commercial Exploitation of Children and Adolescents Online: Von Kommunikasjon, Commercial Exploitation of Children and Adolescents Online: How to Ensure a Rights-Respecting Digital Childhood (November 2024); CERRE, ‘Harmful Online Choice Architecture’ (Centre on Regulation in Europe (CERRE) 2024).

[cccxxxvi] European Commission, Q&A on the Digital Services Act (Press Release, 24 November 2024) https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_4909 accessed 18 December 2024.

[cccxxxvii] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024.

[cccxxxviii] Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024.

[cccxxxix] CERRE, ‘Harmful Online Choice Architecture’ (Centre on Regulation in Europe (CERRE) 2024).

[cccxl] European Commission, Q&A on the Digital Services Act (Press Release, 24 November 2024) https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_4909 accessed 18 December 2024.

[cccxli] CERRE, ‘Harmful Online Choice Architecture’ (Centre on Regulation in Europe (CERRE) 2024).

[cccxlii] Bureau Européen des Unions de Consommateurs (BEUC), ‘Towards European Digital Fairness: BEUC Framing Response Paper for the REFIT Consultation’ (Bureau Européen des Unions de Consommateurs (BEUC) 2023) <https://www.beuc.eu/publications/towards-european-digital-fairness>.

[cccxliii] European Commission, Q&A on the Digital Services Act (Press Release, 24 November 2024) https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_4909 accessed 18 December 2024; Busch C and Fletcher A, 'Harmful Online Choice Architecture' (Centre on Regulation in Europe, 29 May 2024) https://cerre.eu/publications/harmful-online-choice-architecture/ accessed 29 November 2024.

[cccxliv] Evidence of Exposure to Inappropriate Content Ash J, Gordon R, and Mills S, *Between Gaming and Gambling: Children, Young People, and Paid Reward Systems in Digital Games* (ESRC, 2022) p 15 https://esrc-bgg.com accessed 24 November 2024; European Data Protection Board (EDPB), Following EDPB Decision, TikTok Ordered to Eliminate Unfair Design Practices Concerning Children (2023) https://www.edpb.europa.eu accessed 24 November 2024.

[cccxlv] Creating Asymmetric Power Dynamics in Digital Environments European Commission, *Fitness Check of EU Consumer Law: Protecting Children as Consumers* (2023) p 2 https://www.bfd.dep.no accessed 24 November 2024.; European Commission, Final Report - Part 2: Fitness Check of EU Consumer Law on Digital Fairness (2023) p 3 https://www.eu-consumer-check.com accessed 24 November 2024.

[cccxlvi] Ash J, Gordon R, and Mills, S, Between Gaming and Gambling: Children, Young People, and Paid Reward Systems in Digital Games (ESRC, 2022) pp 6-7; European Commission, Fitness Check of EU Consumer Law on Digital Fairness and Report on the Application of the Modernisation Directive (EU) 2019/2161 (2023) p 31.

[cccxlvii] Ayça Atabey, Fairness by Design: Towards a Child-Rights Approach to Digital Fairness (Media@LSE, 2024) pp 3-4.

[cccxlviii] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness and Report on the Application of the Modernisation Directive (EU) 2019/2161* (2023) pp 342–344; European Data Protection Board, *Following EDPB Decision, TikTok Ordered to Eliminate Unfair Design Practices Concerning Children* (2023) https://www.edpb.europa.eu accessed 24 November 2024.

[cccxlix] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness and Report on the Application of the Modernisation Directive (EU) 2019/2161* (2023) pp 342–344; Norwegian Ministry of Children and Families, Fitness Check of EU Consumer Law: Protecting Children as Consumers (2023) pp 2–5.

[cccl] European Commission, *Fitness Check of EU Consumer Law on Digital Fairness and Report on the Application of the Modernisation Directive (EU) 2019/2161* (2023) pp 342–344; Christoph Busch and Amelia Fletcher, *Harmful Online Choice Architecture: Regulatory Solutions for Protecting Consumers in the Digital Age* (CERRE, 2024) pp 15-16.

[cccli] Rossi, A. and et al, 'Who is Vulnerable to Deceptive Design Patterns? A Transdisciplinary Perspective on the Multi-Dimensional Nature of Digital Vulnerability' (2024) 55 Computer Law & Security Review 106031 at page 11.

[ccclii] Ibid at page 11.

[cccliii] Ibid at page 11.

[cccliv] Ibid at page 9.

[ccclv] Ibid at page 6.

[ccclvi] Ibid at page 6.

[ccclvii] Ibid at Page 6.