Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Avenida Universidad, 8 – Apdo. 28
20560 Oñati – Gipuzkoa – Spain
Tel. (+34) 943 783064 / opo@iisj.net / https://opo.iisj.net

A cautionary tale: children, dark patterns and normative perspectives

OÑATI SOCIO-LEGAL SERIES VOLUME 16, ISSUE 1 (2026), 176-208: DERECHO Y ECONOMÍA POLÍTICA EN AMÉRICA LATINA: PROBLEMAS Y PERSPECTIVAS PARA UNA AGENDA TRANSNACIONAL
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL.2351
RECEIVED 29 APRIL 2025, ACCEPTED 12 JANUARY 2026, VERSION OF RECORD PUBLISHED 2 FEBRUARY 2026

VITÓRIA OLIVEIRA*

Abstract

This article explores the intersection of dark patterns — deceptive design practices that manipulate user behavior—with children's digital experiences, examining how universal cognitive vulnerabilities intersect with context-specific susceptibilities. After reviewing scholarship on dark patterns and synthesizing fragmented empirical research on children's encounters with manipulative design, the article applies Mathur, Mayer, and Kshirsagar's (2021) normative framework to assess harms across individual welfare, collective welfare, regulatory objectives, and autonomy in children's contexts. Drawing on vulnerability theory, children's rights instruments, and childhood studies, it situates children within this taxonomy to clarify how developmental characteristics and relational dependencies shape exposure to manipulation in digital environments. Children constitute a particularly revealing analytical lens for understanding digital vulnerability: while developmental characteristics heighten their exposure to manipulation, dark patterns exploit cognitive features universally shared. By engaging both particularist and universalist accounts, the article argues that protective measures developed with children in mind may establish baseline standards addressing digital vulnerability more broadly.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. I am grateful to Matias Guiloff and Ricardo Valenzuela for organizing the workshop "Law and Political Economy in Latin America: Problems and Perspectives for a Transnational Agenda"and this special issue. I benefited from presenting earlier versions of this work at the "Legal Technologies and the Bodies Conference" at Sciences Po Law School and the "Legal Technologies and the Law at a Technological Crossroad Conference" at the University of Sheffield, and I thank all participants and discussants for their valuable feedback. I owe particular thanks to Prof. Diogo Coutinho, Prof. Mateja Durovic, Talita Ferrantelli, Eric George, Paulo Henrique de Oliveira, and João Francisco Coelho for their comments on earlier drafts. I am also grateful to the anonymous reviewers for their constructive critiques and to Leire Kortabarria for coordinating the peer review process. Any remaining errors are my own.
* Vitória Oliveira, PhD Candidate in Economic Law and Political Economy at the University of São Paulo and researcher at the Law and Public Policy Group. Email: vitoria.oliveira@usp.br / vitoria_oliveira@live.com Phone: +5511968583215. Largo São Francisco, 95 - Centro Histórico de São Paulo, São Paulo - SP, 01005-010.

Key words

Dark patterns; children's rights; digital vulnerability

Resumen

Este artículo explora la intersección entre los patrones oscuros —prácticas de diseño engañosas que manipulan el comportamiento de los usuarios— y las experiencias digitales de los niños, examinando cómo las vulnerabilidades cognitivas universales se entrecruzan con las susceptibilidades específicas del contexto. Tras revisar los estudios académicos sobre los patrones oscuros y sintetizar las investigaciones empíricas fragmentadas sobre los encuentros de los niños con el diseño manipulador, el artículo aplica el marco normativo de Mathur, Mayer y Kshirsagar (2021) para evaluar los daños al bienestar individual, al bienestar colectivo, a los objetivos normativos y a la autonomía en los contextos infantiles. Nos basamos en la teoría de la vulnerabilidad, los instrumentos de derechos del niño y los estudios sobre la infancia, y situamos a los niños dentro de esta taxonomía para aclarar cómo las características del desarrollo y las dependencias relacionales determinan la exposición a la manipulación en los entornos digitales. Los niños constituyen una lente analítica especialmente reveladora para comprender la vulnerabilidad digital: mientras que las características del desarrollo aumentan su exposición a la manipulación, los patrones oscuros explotan características cognitivas universalmente compartidas. Al combinar explicaciones particularistas y universalistas, sostenemos que las medidas de protección desarrolladas pensando en los niños pueden establecer normas básicas que aborden la vulnerabilidad digital de manera más amplia.

Palabras clave

Patrones oscuros; derechos de la infancia; vulnerabilidad digital

Table of contents

1. Introduction 179
2. Dark patterns 183
3. Dark patterns and children 184
4. Normative perspectives 187
    4.1. Individual welfare 188
    4.2. Collective welfare 191
    4.3. Regulatory objectives 195
    4.4. Individual autonomy 197
5. Discussion and concluding remarks 198
References 199

1. Introduction

Vulnerability occupies a central place in contemporary legal and policy debates, particularly in fields concerned with social welfare and state responsibilities. Yet the concept remains deeply contested. At its core lies a persistent tension between universalist accounts of vulnerability, which understand vulnerability as an inescapable feature of the human condition, and particularist approaches, which emphasise the heightened exposure of specific groups to harm and therefore justify differentiated legal protections. This article engages with that tension and argues that contemporary digital environments destabilise this divide and reveal the inadequacy of treating universalist and particularist approaches as mutually exclusive.

Martha Fineman's vulnerability theory provides a seminal universalist starting point. In its canonical formulation, vulnerability is understood as universal, inevitable, and constant, grounding a conception of substantive equality that moves beyond formal anti-discrimination frameworks (Fineman 2008, 2013). Foregrounding the shared fragility of the human condition, Fineman shifts attention from individual fault and group identity to the structural role of institutions in producing resilience or, conversely, deepening disadvantage. The state, on this view, bears responsibility not merely for preventing discrimination, but for ensuring equitable access to the social, economic, and legal institutions that mediate vulnerability over the life course – a positive conception of state responsibility that extends beyond formal non-discrimination.

This universalist orientation has generated ongoing debate. A recurring concern is that treating vulnerability as universally distributed may obscure how disadvantage is produced through historical processes and reinforced by institutional structures. In this line of critique, group-based protections are understood as a pragmatic response to the uneven ways in which vulnerability materialises in social life, particularly when states must prioritise regulatory attention and allocate limited resources. Nina Kohn's intervention is especially relevant in this regard. Drawing on elder care policy, she shows that vulnerability theory, as originally articulated, offers limited guidance when policymakers are required to determine which vulnerabilities warrant intervention and how competing claims should be assessed. At the same time, she highlights the risk of paternalism when vulnerability is inferred from status alone, rather than being assessed through contextual analysis and attention to institutional design (Kohn 2014).

Against this backdrop, the article adopts a relational and layered account of vulnerability, drawing on Luna's critique of both universalist and particularist approaches. On this account, vulnerability is not a fixed attribute, nor a condition evenly shared across populations, but a dynamic and situational phenomenon that emerges from social, economic, and technological relationships (Luna 2009). Vulnerability is universal insofar as all individuals are susceptible to harm; it is particular in how that susceptibility is shaped through interactions with specific contexts, dependencies, and power asymmetries. These layers are cumulative rather than mutually exclusive: individuals can be simultaneously universally and differentially vulnerable (Malgieri 2023, Rossi *et al.* 2024).

Digital environments make this tension especially salient. Contemporary platform architectures are designed to identify and commercialise moments of susceptibility, frequently through behavioural design strategies that exploit cognitive biases and

information asymmetries, while manipulating constraints on attention and decision-making capacity (Helberger *et al.* 2022). In such settings, vulnerability takes shape through concrete design and data practices embedded in interface arrangements that actively structure users' capacities for understanding, resistance, and self-determination. Digital vulnerability is therefore neither purely universal nor purely particular, but emerges from the interaction between generalised platform architectures and situated user experiences. This dynamic accounts for vulnerability theory's renewed traction in debates on digital regulation (Herzog *et al.* 2022, Rossi *et al.* 2024, DiPaola and Calo 2024).

Children occupy a particularly revealing position within this landscape. On the one hand, childhood has long been recognised in law as a status warranting special protection, grounded in developmental considerations and evolving capacities as articulated in the United Nations Convention on the Rights of the Child (hereinafter UNCRC) and General Comment No. 25. On the other hand, children are deeply embedded in digital environments shaped by the same infrastructural logics that govern adult participation online,[1] including data extraction, persuasive design techniques, attention-maximising strategies, and algorithmic curation (OECD 2022). Children thus interact with generalised digital architectures while simultaneously bearing distinctive developmental and relational vulnerabilities.

The interplay between universal platform architectures and children's specific developmental characteristics helps explain the recent surge of child-specific digital regulations and policy instruments across jurisdictions. such as age-appropriate design codes and restrictions on behavioural targeting, alongside enhanced duties of care and specific disclosure requirements have often been more detailed — and more ambitious — than parallel, general-purpose digital legislation (Information Commissioner's Office — ICO — 2020, OECD 2022). This divergence reflects a regulatory intuition that children's rights frameworks offer a particularly robust normative grounding for addressing structural harms embedded in digital design (Bernstein 2023). In this sense, child-specific digital regulation operates as a testing ground for regulatory strategies that have proven more difficult to articulate, legitimise, enforce, and scale when framed exclusively in universal terms.

Alongside these regulatory developments, children's rights by design approaches have emerged as a framework for embedding child protection from the outset of the design process, influenced by earlier developments such as Privacy by Design (Hartung 2020, Henriques and Hartung 2021, CNIL 2021, Djeffal 2022). Children's rights by design seeks to translate normative commitments — such as the best interests of the child and protection from economic exploitation, alongside recognition of evolving capacities — into concrete design and governance requirements for digital systems (UNCRC; General Comment No. 25; Livingstone and Otani 2023, Livingstone and Pothong 2023). These frameworks position children as rights-holders whose interests must be considered at the level of system architecture, rather than addressed solely through downstream enforcement or individual choice. While grounded in child-specific norms, children's

[1] In some cases, these systems are plausibly designed with children in mind, not to protect them, but to capitalise on their heightened susceptibility to engagement and influence, a concern underscored by whistleblower accounts from within the platform industry.

rights by design carries broader implications for digital governance, as environments that meet these standards tend to mitigate structural risks for users more generally.

Emphasising the asymmetry of power between young users and digital platforms does not entail portraying children as passive or helpless subjects. A relational and layered understanding of vulnerability offers a way to recognise children's agency while remaining attentive to the structural conditions that shape their exposure to harm (Luna 2009). From this perspective, vulnerability arises from specific configurations of context and dependence within structures of institutional power, rather than from fixed personal characteristics. As Malgieri summarises, "all individuals are vulnerable, but some individuals possess more layers of vulnerability based on particular contexts and relational balances" (Malgieri 2023). This perspective aligns with research on children's digital lives showing that children can be competent and resourceful users, capable of developing strategies to navigate and resist online risks, even as these capacities are exercised within environments that systematically constrain meaningful choice and disproportionately affect them in specific settings (Livingstone *et al.* 2023, Rossi *et al.* 2024).

The article uses dark patterns[2] as a focal example precisely because they crystallise the relationship between vulnerability and design. Dark patterns refer to "business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice" (OECD 2022). Developed within the Human–Computer Interaction community to denounce manipulative design techniques (Brignull 2010), the concept explicitly rests on the exploitation of human cognitive biases and vulnerabilities. Dark patterns therefore offer a particularly suitable entry point for examining how universal cognitive limitations intersect with context-specific vulnerabilities, and how these dynamics are intensified in children's digital experiences.

Despite growing attention to dark patterns, existing scholarship exhibits two related limitations. First, even as research has documented the prevalence and effectiveness of manipulative design practices, it has engaged less systematically with questions of vulnerability. Studies examining how social and structural factors shape susceptibility to dark patterns remain fragmented, and comparative analyses that might distinguish universal features of manipulation from context-specific vulnerabilities are rare. Second, scholarship on dark patterns has largely originated within the Human-Computer Interaction community, focusing primarily on identifying, classifying, and measuring manipulative design techniques. While this work has generated rich empirical and conceptual insights, it has engaged less systematically with normative questions grounded in legal categories and modes of reasoning to justify regulatory intervention.

These limitations are particularly pronounced in relation to children. Studies focusing on children are rarely conducted alongside analyses of adult users, making it difficult to assess which effects of manipulative design are age-specific and which reflect more general dynamics of digital vulnerability—a gap that constrains normative analysis. Moreover, established frameworks for assessing dark patterns' harms (such as Mathur

[2] The Human-Computer Interaction (HCI) community is gradually shifting from the term "dark patterns" to "deceptive patterns" to avoid racial biases. Following Rossi *et al.* (2024), I will use both terms interchangeably, along with similar terms that emphasise the manipulative nature of such designs.

et al. 2021) have not been systematically applied to children's contexts. This represents a significant normative gap, as children's developmental characteristics, relational dependencies, and the existence of robust child-focused regulatory frameworks — which explicitly address layered, context-dependent forms of vulnerability and translate them into concrete design and governance obligations — provide a particularly revealing lens for examining how vulnerability operates in digital environments and for developing regulatory responses that address manipulation at the level of design.

To address these gaps, the article applies an established normative taxonomy of dark patterns to children's digital experiences (Mathur *et al.* 2021)**.** Methodologically, the research combines two complementary strategies. First, an exploratory review of scholarship on dark patterns and children's encounters with manipulative design, drawing primarily on empirical studies in HCI, developmental psychology, and childhood studies. Second, a targeted literature search guided by the normative perspectives' framework — individual welfare, collective welfare, regulatory objectives, and autonomy — to identify relevant contributions in legal scholarship and child-specific regulatory instruments such as the UNCRC, General Comment No. 25, and Age Appropriate Design Codes. Rather than conducting a systematic literature review with strict inclusion/exclusion criteria, the article develops a conceptual synthesis that situates children as an analytical lens to examine how different conceptions of harm and vulnerability operate in contexts of persuasive design. This allows assessment of existing normative frameworks' scope and limits when confronted with children's situated experiences, clarifying how child-specific regulatory strategies might inform broader approaches to digital governance.

Through this approach, this article makes three contributions. First, it systematises existing evidence on children's encounters with dark patterns, drawing together fragmented research across multiple fields. Second, it examines how normative perspectives on harm apply to children's digital experiences, with particular attention to how children's developmental and relational characteristics shape their exposure to manipulative design. Third, it reflects on how regulatory approaches grounded in children's rights might inform wider strategies for addressing digital vulnerability. While child-specific protections have distinct limits when extended to general-purpose regulation, they engage with a broader dynamic: digital platforms increasingly deploy infrastructural and behavioural strategies that render all users susceptible to harm, regardless of age or status. This suggests that universalist accounts of vulnerability remain essential for understanding how these systems operate and that protective measures developed with children in mind may establish baseline standards benefiting all users.

The article is organized as follows. Section 2 provides an overview of dark patterns, tracing the concept's origins and reviewing taxonomies of manipulative design practices. Section 3 examines the empirical literature on children's encounters with dark patterns, documenting how manipulative design operates in contexts where children are primary users. Section 4 applies the normative framework developed by Mathur *et al.* (2021) to assess how dark patterns affect children across four dimensions: individual welfare, collective welfare, regulatory objectives, and individual autonomy. Section 5 discusses how both particularist and universalist dimensions of vulnerability are

necessary to understand dark patterns' effects, and explores how regulatory measures developed with children in mind may establish baseline standards that benefit all users.

2. Dark patterns

The concept of "dark patterns" was coined in 2010 by UX designer Harry Brignull to refer to user interfaces that are strategically designed to deceive or manipulate users into actions they might otherwise avoid (Brignull 2010). In his work, Brignull draws a clear distinction between dark patterns and anti-patterns, emphasising the intentional and strategic nature of the former. While anti-patterns typically result from errors, poor design choices, or unintended consequences, dark patterns rely on deliberate tactics aimed at exploiting human psychology for strategic ends. As Brignull notes, these designs are "carefully crafted with a solid understanding of human psychology" and do not serve the user's best interests (*ibid*.).

In practical terms, the harms associated with dark patterns include inducing users to make unintended purchases and extracting consent or personal data through misleading interfaces, while prolonging user engagement beyond what users intend and obstructing exit, cancellation, or privacy-protective choices through friction, deception, or emotional pressure (OECD 2022).

In this sense, dark patterns exemplify the key properties of digital vulnerability identified by Helberger *et al.* (2022). First, they are architectural, as they operate through online choice architectures that systematically steer users towards harmful or undesired outcomes (CMA 2022). Second, they are relational, insofar as they exploit vulnerabilities that develop and intensify over time through repeated interactions between users and digital systems. Third, they are closely tied to privacy asymmetries, undermining meaningful consent and relying on extensive data collection to personalise and optimise manipulation (Helberger *et al.* 2022).

Narayanan *et al.* (2020) situate the emergence of dark patterns within a longer trajectory of commercial and technological practices, identifying three interrelated trends. The first concerns deceptive practices in retail, which range from legally tolerated techniques, such as psychological pricing, to more problematic practices, including false claims of scarcity or urgency, and clearly unlawful conduct such as bait-and-switch advertising. The second trend relates to the diffusion of behavioural influence techniques originally associated with public policy and behavioural economics, which have been repurposed by firms in adversarial, profit-oriented contexts rather than paternalistic ones. The third trend, growth hacking, refers to data-driven strategies aimed at accelerating user acquisition and engagement through continuous experimentation, optimisation, and A/B testing. Together, these trends help explain how long-standing commercial practices, behavioural insights, and data-intensive experimentation converged in contemporary digital interfaces.

The coining of the term "dark patterns" provided both a vocabulary and an agenda for addressing manipulative online practices, which was rapidly taken up by the Human–Computer Interaction (HCI) community. From a relatively small number of early contributions, research on dark patterns expanded into a distinct and active field, with a growing presence in HCI conference proceedings and journals (Gray *et al.* 2024). A decade after the term was introduced, Luguri and Strahilevitz (2021) characterised this

literature as developing in three waves. The first wave focused on identifying and classifying dark patterns, producing influential taxonomies that systematised different forms of manipulation (Conti and Sobiesk 2010, Zagal *et al.* 2013, Bösch *et al.* 2016, Gray *et al.* 2018). A key contribution to this phase was Brignull's own initiative to catalogue examples through an online "Hall of Shame", which also popularised terms such as "Bait and Switch", "Confirmshaming", and "Roach Motel".

The second wave shifted attention to the prevalence of dark patterns, relying on empirical studies to document how widespread these practices are across platforms and sectors (Mathur *et al.* 2019, Gunawan *et al.* 2021). Evidence from app ecosystems and web interfaces suggests that manipulative designs are far from marginal. Di Geronimo *et al.* (2020), for example, found that 95% of the 240 apps sampled from the US Google Play Store contained at least one dark pattern, while nearly half included seven or more. In the context of consent mechanisms, Utz *et al.* (2019) showed that 57.4% of the most popular websites in the European Union steered users towards privacy-unfriendly choices.

The third wave of scholarship has focused on the effectiveness of dark patterns, examining how successfully they influence user behaviour and how users respond to different forms of manipulation (Luguri and Strahilevitz 2021, Bongard-Blanchy *et al.* 2021, Lupiáñez-Villanueva *et al.* 2022, Zac *et al.* 2023). Within this strand, researchers have begun to engage more directly with questions of vulnerability. Some studies adopt a particularist perspective, suggesting that susceptibility to dark patterns varies across populations. Luguri and Strahilevitz (2021), for instance, argue that less educated participants are more likely to fall for manipulative interfaces. Other findings point in a different direction. Zac *et al.* (2023) show that dark patterns are effective across a diverse population varying in age, income, and education, challenging assumptions embedded in the notion of an "average consumer" and suggesting that all users are, to some degree, vulnerable to such practices.

Despite these advances, relatively few studies in this third wave have examined how social and structural factors shape vulnerability to dark patterns, particularly in relation to historically marginalised communities. Existing efforts remain fragmented, with a limited number of studies focusing on older users (Bongard-Blanchy *et al.* 2021, Sánchez Chamorro, Toebosch, and Lallemand 2024) or less educated users (Bongard-Blanchy *et al.* 2021, Luguri and Strahilevitz 2021). As a result, while the literature has generated rich descriptive and experimental insights, it has only partially engaged with the normative implications of how vulnerability is shaped and reinforced through digital design.

Children represent a particularly significant yet fragmented area of research in this regard. The following section synthesises the emerging body of work on dark patterns and children, drawing together empirical studies on children's experiences, research on parental and developer perspectives, and contributions from civil society organisations and legal scholars to clarify how manipulative design operates in children's digital environments.

3. Dark patterns and children

If this abusive behaviour has been shown to be effective with adults (Luguri and Strahilevitz 2021, Bongard-Blanchy *et al.* 2021, Zac *et al.* 2023), what impact might it have

on children and adolescents? As young people constitute the most digitally connected age group (UNICEF 2017), they have become a particularly attractive consumer segment for digital platforms and, consequently, a salient target of dark patterns. Paediatrician Jenny Radesky, speaking at the US Federal Trade Commission (FTC) Workshop "Bringing Dark Patterns to Light" (2021),[3] identifies five significant characteristics — or layers of vulnerability — that make dark patterns especially pernicious for children: (i) immature executive functions; (ii) the tendency to form imaginative relationships with characters; (iii) heightened sensitivity to rewards; (iv) limited familiarity with data privacy; and (v) incomplete understanding of virtual currencies.

Given that dark patterns are considered "far from a niche practice" (OECD 2022), it is not surprising that evidence points to their widespread presence in children's online environments. A growing number of studies have examined websites and applications frequently used by children. Radesky *et al.* (2022), for example, show that manipulative patterns are present in approximately 80% of the apps most used by children aged 3 to 5. Other research has focused on specific sectors, such as education, social media, and gaming. Lehtosalo and Woods (2023) demonstrate that websites specifically targeted at children (2%) tend to rely on consent dialogues addressed to parents or guardians to ensure valid consent. Sousa and Oliveira (2023), based on a small sample of popular mobile games, find evidence of temporal, monetary, and psychological dark patterns. Similarly, Albuquerque *et al.* (2023), analysing the user journeys of child influencers ("kidfluencers"), identify the presence of dark patterns across six out of twelve recognised types on major platforms, including Instagram, YouTube, and TikTok.

Echoing earlier efforts in childhood studies to incorporate children's voices into research (Kleine *et al.* 2016), a growing body of work focuses on documenting children's own experiences with manipulative design (Fitton *et al.* 2021, Schäfer *et al.* 2024, Renaud *et al.* 2024, Sánchez Chamorro, Lallemand, and Gray 2024). These studies typically involve children aged 10 to 17 and do not include longitudinal designs or systematic comparisons across age groups. Across these contributions, children are shown to possess a certain degree of awareness and to have developed strategies to resist dark patterns, particularly once they are introduced to the concept. In several instances, participants reported sensing that something was "up to no good" (Renaud *et al.* 2024) or "fishy" (Schäfer *et al.* 2024), even when they struggled to articulate precisely how the manipulation operated. At the same time, these studies indicate greater susceptibility when children encounter more sophisticated scenarios or specific types of dark patterns (Renaud *et al.* 2024, Schäfer *et al.* 2024). Notably, younger children and children from the Global South remain largely absent from this body of research.

Beyond children themselves, HCI scholarship has also examined the role of parents and caregivers. Parents are often portrayed as bearing primary responsibility for protecting children online, a role that can become burdensome. Nonetheless, their influence on children's awareness of dark patterns is consistently highlighted as a critical factor by researchers engaging directly with children (Renaud *et al.* 2024, Sánchez Chamorro, Lallemand, and Gray 2024, Schäfer *et al.* 2024). Sánchez Chamorro, Lallemand, and Gray

[3] *Bringing Dark Patterns to Light* workshop transcript available at: https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf

(2024) argue that parents may contribute to greater exposure to dark patterns, since applications frequently mediate parent-child interactions, and may themselves be vulnerable to manipulation. At the same time, parents can support children in developing coping strategies and raising awareness of manipulative practices, while providing opportunities to discuss feelings of manipulation online. In some cases, adults' negative experiences with dark patterns may even foster increased caution or mistrust of technology among children.

As emphasised by General Comment No. 25, responsibility for children's digital well-being extends beyond parents and caregivers to encompass states, businesses, and civil society organisations. Bessant *et al.* (2023), for instance, surveyed parents to examine perceptions of responsibility for children's online experiences. While parents acknowledged their own role, they also attributed responsibility to "companies which sell a product, service or app; those who design adverts; app, web and game designers; and industry regulatory bodies" (*ibid*.).

Questions of industry accountability have also been explored through engagement with developers and designers. Melzer *et al.* (2021) document recurring tensions around shared responsibility, with some developers shifting responsibility onto parents while experts emphasise the accountability of "authorities, developers, and platforms such as the App Store and Google Play" (*ibid*.). The absence of clear guidelines or legislation intensifies this negotiation over responsibility, forcing developers to navigate "competing priorities" (Pothong *et al.* 2024) between children's rights and commercial objectives, often relying on experience or intuition rather than expert guidance (Melzer *et al.* 2021). These dynamics are particularly pronounced in applications relying on zero-price business models, which tend to adopt more aggressive engagement strategies (Dreier *et al.* 2017) and are widely accessed by children due to their limited purchasing power (Fitton *et al.* 2021). As one developer interviewed by Melzer *et al.* (2021) acknowledged, free-to-play games are a significant driver of addictive behaviours.

In response to these challenges, several authors have proposed frameworks aimed at supporting more ethical design practices, particularly in the gaming sector. Fitton and Read (2019), Fitton, Bell, and Read (2021), and Wang *et al.* (2023) offer tools intended to assist developers in identifying and mitigating risks to young users. Fitton, Bell, and Read (2021) introduce the Risk in Games Assessment, which draws on the 4Cs framework (content, contact, conduct, and commerce) to prompt reflection on potential harms. Earlier, Fitton and Read (2019) developed the App Dark Design framework, which establishes a taxonomy of harmful design practices in free-to-play applications. From a complementary perspective, Wang *et al.* (2023) propose a taxonomy of beneficial design mechanisms aimed at promoting children's digital autonomy.

Civil society organisations have played a central role in framing the harms of dark patterns in relation to children. The 5Rights Foundation's report Disrupted Childhood, for example, documents a range of persuasive design practices and their effects on children's social, mental, and physical development. Building on the OECD framework, the report adapts dark patterns to children's digital lives, identifying five categories: (i) dopamine hits and anticipation; (ii) social proof and fear of missing out; (iii) forced action; (iv) interface interference; and (v) obstruction (5Rights Foundation 2023). Similarly, the Fairplay coalition (formerly the Campaign for a Commercial-Free

Childhood) argues that the concept of dark patterns should encompass all forms of behavioural influence aimed at stimulating engagement or purchases among children (Fairplay 2021). Given that neither children nor their parents or guardians can fully shield young users from exposure to manipulative design, Fairplay advocates for more specific regulation of practices that affect children's psychosocial development.

Finally, a smaller body of work adopts regulatory and rights-based perspectives on the state's responsibility for children's digital well-being. Leiser (2023)[4] analyses children's user journeys and potential encounters with dark patterns through the lens of European legal frameworks and the United Nations Convention on the Rights of the Child, alongside General Comment No. 25. Van der Hof *et al.* (2022) pursue a similar approach in their analysis of behavioural design in games. Based on their examination of consent notices, which were frequently unsuitable for children, Lehtosalo and Woods (2023) argue that such practices may violate Article 8 of the GDPR.

These contributions document the prevalence and mechanisms of dark patterns in children's digital environments, yet they offer limited guidance on how to assess the harms they produce. While the empirical literature establishes that children are exposed to manipulative design across platforms and sectors, it rarely articulates the normative foundations required to evaluate these practices or translate concerns into regulatory obligations. The following section addresses this gap by examining how different normative frameworks can be applied to assess dark patterns in children's digital experiences.

4. Normative perspectives

Most of the scholarship on dark patterns has concentrated on describing and systematising the phenomenon (Gray *et al.* 2024), with particular emphasis on developing taxonomies or measuring the prevalence and effectiveness of manipulative design practices across digital environments (Luguri and Strahilevitz 2021). This body of work has been largely driven by the HCI community, where research has focused on understanding manipulative design practices through the analysis of interfaces, user interactions, and their behavioural effects, often without advancing explicit normative or regulatory claims. While these contributions have generated rich empirical and conceptual insights, they tend to engage with normativity in ways that are not systematically grounded in legal categories or modes of reasoning, which limits their ability to speak directly to questions of legal reasoning and regulatory design.

This reflects broader disciplinary differences in how normativity is mobilised across epistemic fields. As Calo (2025) observes, scholarship at the intersection of law and technology frequently operates with divergent conceptions of what it means to make a normative claim. In fields such as HCI and Science and Technology Studies (STS), normativity is often implicit, emerging through critiques of design practices, descriptions of harm, or appeals to user welfare, without necessarily advancing prescriptive judgments about how institutions should act. By contrast, legal scholarship tends to treat normativity as explicitly prescriptive, concerned with justification and the

[4] Leiser, M.R., 2023. *Protecting Children from Dark Patterns and Deceptive Design.* SSRN (withdrawn). Copy on file with the author.

allocation of responsibility among states, firms, and other actors. As a result, discussions of dark patterns have frequently diagnosed problems of manipulation and harm without fully engaging with the normative foundations required to translate these diagnoses into legal or regulatory obligations.

An important attempt to bridge this gap is offered by Mathur, Mayer, and Kshirsagar (2021), who explicitly identify and systematise the normative concerns raised by dark patterns. Rather than treating manipulation solely as a design flaw or behavioural anomaly, they outline four normative lenses through which the use of behavioural techniques by digital platforms can be assessed, including concerns related to autonomy, welfare, distributive effects, and procedural fairness. Their framework represents a rare effort within the dark patterns literature to move beyond description and to clarify the moral and normative stakes of manipulative design.

For the purposes of this study, these normative lenses are adapted to analyse children's contexts and interactions with dark patterns. Drawing on existing research on children's digital experiences, domestic legal instruments — such as the Age Appropriate Design Codes in the United Kingdom — and international legal frameworks, including the UN Convention on the Rights of the Child and General Comment No. 25, this section situates children within this taxonomy to clarify how each normative concern operates when applied to children's situated vulnerabilities. The section examines how developmental characteristics and relational dependencies intersect with the specific contexts of children's digital use — including gaming, social media, and educational platforms — and how regulatory instruments specific to childhood reshape the evaluation of harm across individual welfare, collective welfare, regulatory compliance, and autonomy. The subsections explore how dark patterns manifest in children's digital environments and draws on paradigmatic cases and existing evidence to document their effects.

4.1. Individual welfare

Individual welfare concerns focus on direct harms to users, including financial loss, privacy invasion, and cognitive burden. In children's contexts, these harms take on specific characteristics due to developmental vulnerabilities and the design of platforms targeting young users. The following subsections examine how each form of individual welfare harm operates in children's digital experiences.

4.1.1. Financial loss

Financial loss, identified by Mathur, Mayer, and Kshirsagar (2021) as one of the detrimental effects on individual welfare, is described as "the most straightforward welfare consequence for users" (*ibid*.) and is one of the most frequently cited harms by scholars and policymakers (Santos *et al.* 2024). According to Susser and Grimaldi (2021), dark patterns can manifest in two ways that result in financial losses. They can either "induce buyers to purchase what they would not" or "enable sellers to charge more for products than buyers would otherwise pay", as demonstrated in Luguri and Strahilevitz (2021)'s experimental study that encouraged users to subscribe to expensive services using dark patterns. Examples of dark patterns that result in financial losses include adding products to shopping carts without users' consent or misleading users into believing they are signing up for a one-time offer or free trial when, in fact, they are

committing to recurring fees and advertisements disguised as non-advertising content (Mathur *et al.* 2021).

This is particularly evident in the tactics employed by the gaming industry to sustain engagement and maximise revenues, such as microtransactions and loot boxes, to which children are heavily exposed. By "blurring the lines between pay and play" (Nguyen and McNealy 2021), children are incentivised to make in-app purchases — intentionally or not — that not only harm them economically but also increase their vulnerability to gambling-like behaviour in the future (Ash *et al.* 2022), resulting in more significant economic and health issues. As discussed by van der Hof *et al.* (2020), "children and their families are (...) exposed to a commercialisation of play", such as "the delivery of commercial messages through in-game advertising, advergames, or even interactive, connected toys" and "gambling elements (...) integrated into children's games, such as slot machines or loot boxes". These techniques are often employed in free-to-play games, as children's spending power is limited (Fitton *et al.* 2021). Evidence of accidental or excessive purchases made by young users is mounting in surveys (Childnet International and Phonepay Plus 2015, Ofcom 2019) and popular anecdotes shared by children (Hannah and Andrews 2020) and parents (Tims 2020). Extracting revenues from children through manipulative design patterns goes against the UNCRC prohibition of economic exploitation of children (article 32), which should be understood broadly (Swepston 2012).

In the past, the US FTC has challenged tech giants such as Google (FTC 2014b), Apple (FTC 2014a), and Amazon (FTC 2016) over billing interfaces that facilitated unauthorised in-app purchases made by children without proper parental consent. The companies reached settlement agreements requiring them to refund consumers a total of more than 50 million dollars (OECD 2022).

4.1.2. Invasion of privacy

Invasion of privacy, another individual welfare harm identified by Mathur, Mayer, and Kshirsagar (2021) and the most studied harm in the scholarship (Santos *et al.* 2024), consists of choices about user's personal information that do not align with their preferences, such as sharing more personal information than they would otherwise volunteer (*ibid*.). Users can give up more data than intended through dark patterns that include privacy-invasive defaults that expose user data and privacy-respecting choices that are hard to access, alongside the use of fear or other emotion-laden language to drive users away from making privacy-respecting choices (Mathur *et al.* 2021).

Privacy is not only a value in itself for children but also connects to other essential developmental areas — autonomy, identity, intimacy, and trust, alongside the development of pro-social behaviour, resilience, critical thinking, and capacities for sexual exploration (Livingstone *et al.* 2019). However, the attention-driven business model can jeopardise children's development for profit. Research indicates that children are often more concerned about interpersonal privacy (related to their parents, friends, or malicious individuals) than commercial privacy, which entails the use of their data online (Livingstone *et al.* 2019, Desimpelaere *et al.* 2020), particularly among younger children.

According to SuperAwesome, a company operating in the *kidtech* market, by the time a child reaches 13 years of age, 72 million data points will have been collected about them (SuperAwesome 2018). Through dark patterns, an increasing amount of data can be extracted from children without their full understanding, exploiting their immature sense of privacy and their difficulties in grasping how their data will be used. The findings of Renaud *et al.* (2024) and Sanchez Chamorro, Lallemand, and Gray (2024) echo this, demonstrating how infrequently children consider privacy harms when confronted with dark patterns. Additionally, Lehtosalo and Woods (2023) reveal that the vast majority of consent banners on European websites do not obtain appropriate parental consent.

While children's privacy encompasses various dimensions (UNICEF 2017), it is the decisional aspect of privacy — focus on "an individual's ability to make significant decisions without interference" (Levesque 2017) — that raises greater concerns regarding the effects of dark patterns. Data obtained from children through dark patterns that violate their privacy will be directed towards monetisation "through sales to third parties or customising the child's online experience based on behavioural data, thereby ensuring prolonged engagement" (Leiser 2023).

Defaults, for instance, are often employed in digital environments to steer users away from their best interests and rob them of their agency (5Rights Foundation 2023) because humans typically prefer options that do not demand extra effort, a phenomenon known as "status quo bias" (Thaler *et al.* 2012). Concerning defaults, the UK Age Appropriate Design Code issued by the Information Commissioner's Office has indicated that "many children will just accept whatever default settings you provide and never change their privacy settings" and, therefore, has urged digital service providers to set children's configurations to 'high privacy' by default

The UNCRC guarantees children's right to privacy, whereas General Comment No. 25 cautions that practices aimed at influencing children's behaviour, such as profiling and behavioural targeting, present a significant risk to children. It calls for states to adopt a privacy-by-design approach in their legislation and to establish "design standards that identify, define, and prohibit practices that manipulate or interfere with children's right to freedom of thought and belief in the digital environment, for example, by emotional analytics or inference."

In a recent settlement agreement, the Federal Trade Commission, the creator of the popular video game Fortnite, ordered Epic Games to pay $252 million for "collecting personal information from children under the age of 13 who played Fortnite (...) without notifying their parents or obtaining their verifiable consent" and for employing defaults that harm children and teenagers by enabling live text and voice communications that led to harassment. In this suit, the design of the interface is challenged as a means to promote harm to privacy and children's rights (FTC 2022).

4.1.3. Cognitive burden

Cognitive burden, a third form of individual welfare harm in Mathur, Mayer, and Kshirsagar (2021)'s , refers to the ways dark patterns impose costs on users' time, attention, and mental resources, often making it more difficult to complete desired tasks or resist unwanted choices. In digital environments, where information overload is

commonplace, dark patterns can create an additional obstacle, causing users to expend more "time, energy, and attention" (i.e. "cognitive tax") than intended on a specific task, often leading them to choose the easiest available option to escape this conundrum. Cognitive burdens can be perpetrated through interfaces that "obstruct users from cancelling the online services they are subscribed to by requiring them to phone in only during certain hours (...) and those that repeatedly prompt the user to accept certain choices" (Mathur *et al.* 2021).

In games, children can experience cognitive burdens due to temporal dark patterns (Zagal *et al.* 2013) that cheat players out of their time, such as "repetitive play to earn in-game resources" (grinding), which forces players to spend more time on the game (Fitton and Read 2019). Cognitive harms can also be compounded by monetary dark patterns that exploit children's time and attention to extract financial resources. These include payment structures that offer in-game advantages to reduce the time needed to achieve goals, such as Pay for Permanent Enhancements, Pay for Expendable Updates, Pay to Skip/Progress, and Pay to Win (Zagal *et al.* 2013, Fitton and Read 2019). Additionally, another form of exploitation of cognitive loads in games involves using complex exchange rates between in-game currency and real-life currency, which can confuse children about the value of real money spent (van der Hof *et al.* 2022) – similar to the "poker chips" used by casinos to increase expenses for poker players (Fairplay 2021). The combined tactics mentioned above, such as grinding, along with never-ending content and levels, put children on an endless treadmill that "pressures children to play as much as possible, convincing them that there is always more to do in a game" (Fairplay 2021).

A shared strategy by social media and games that results in cognitive harm consists of increasing seamlessness (5Rights Foundation 2023) by eliminating friction or stopping points to prolong user engagement at the expense of natural breaks and biological needs, especially sleep. In social media, children often encounter infinite scrolling (or "doom scrolling") and autoplay features, spending more time than intended and finding it challenging to stop (5Rights Foundation 2021). By continuously presenting new content without natural stopping points, these design choices undermine children's capacity to self-regulate, even when they recognise that their engagement has become excessive.

In more extreme cases and depending on users' predisposition to compulsive behaviour, dark patterns may aim to establish habits that could potentially induce addiction in young people. A survey conducted by the mental health charity YoungMinds, involving 2,000 individuals aged 16 to 24, reported that "more than a third (34%) of young people wish to leave social media sites at least once a week, but feel they cannot", "42% displaying early signs of addictive behaviour", and "89% agreed to some extent that social media contributes to harmful behaviours" (YoungMinds 2022).

4.2. Collective welfare

Beyond harms to individual users, dark patterns can generate collective welfare concerns that extend across markets and societies. These include distortions to market competition, reductions in price transparency, erosion of trust in digital services, and unanticipated societal consequences such as political polarisation. When children are the primary users of platforms employing manipulative design, these collective harms

acquire distinct features. Dominant platforms may establish exploitative practices as industry standards, while children's limited purchasing power and developmental vulnerabilities intensify how manipulation affects entire user populations and market structures. The following subsections examine how these dynamics unfold in children's digital environments.

4.2.1. Competition

The current landscape of digital environments, dominated by large conglomerates in multiple digital markets, has brought competition law to the forefront. Despite varying applications across jurisdictions, competition law is vital in tackling abuses of economic power in digital markets; significant fines have been imposed, new legislation introduced, and antitrust objectives thoroughly debated. Dark patterns have gradually emerged within the realm of competition law (Day and Stemler 2019, Willis 2020). Although academic discourse is still limited, earlier enforcement actions have begun to establish precedent. For instance, one of the largest fines imposed by the European Commission exemplifies a market manipulation strategy through design, as illustrated in the Google Shopping Case, resulting in a EUR 2.42 billion fine. Google prominently displayed its so-called "Product Listing Ads" above other textual search results, employing a more attention-grabbing layout, thereby granting Google an unfair competitive advantage over rival products (European Commission 2017).

Examples of dark patterns can raise competition concerns — particularly when employed by dominant players — include "pre-selected checkboxes" and "the use of emotions and fear," which facilitate locking the user in the ecosystem (European Commission 2019). The obstruction of users' choices by digital providers — for instance, by making subscriptions easier while adding obstacles to cancellation (such as requiring phone calls to terminate the service) — can also heighten switching costs and create barriers to entry for emerging competitors (Mathur *et al.* 2021).

Competition in digital markets is often associated with the "winner takes all or most" phenomenon, which posits that digital providers typically compete "for" the market rather than merely for shares of it. This dynamic frequently results in high market concentration among dominant players. Multi-homing, the practice of using multiple platforms for the same function, and portability, the ability to transfer personal information and preferences to a competing platform, may be hindered either by deliberate platform design choices or by network effects and data lock-in inherent to digital services, compelling users to remain within a specific environment. For minors, if the leading platform uses dark patterns, this tactic can become the dominant design in the market (Hummel 2023), as competitors often replicate these practices in a "follow the leader" fashion (European Commission 2019). When manipulative practices become the industry standard, children face elevated costs — both monetary and qualitative — across available platforms. This creates barriers for services that prioritise child welfare over engagement metrics, as less harmful alternatives struggle to compete against platforms optimised for data extraction and prolonged use.

Although competition law does not traditionally frame its objectives in terms of child protection, the concept of market power intersects directly with concerns about economic exploitation. As van der Hof *et al.* (2020) observe, economic exploitation

requires both a material interest — "a certain gain or profit through the production, distribution or consumption of goods and services" — and the taking of "unjust advantage of another for one's own advantage or benefit," which includes manipulation, misuse, and disrespect for human dignity. When dominant platforms exploit their position of power to embed such practices into children's digital environments, they create conditions where economic exploitation becomes structurally embedded in market design. The accumulation of market power thus enables not only anticompetitive conduct but also the systematic manipulation of vulnerable users. In markets where children are the primary user base, this dynamic is particularly pronounced: dominant platforms can normalise exploitative practices, making it difficult for children to access services that do not prioritise data extraction or prolonged engagement over their well-being.

4.2.2. Price transparency

Deceptive pricing strategies are not new and are not necessarily unlawful. Psychological pricing — the practice of setting prices just below a round number (e.g. 1.99 instead of 2.00) — has long been used to influence consumers' perceptions of value and is generally considered lawful in many jurisdictions (Narayanan *et al.* 2020). In digital markets, however, pricing practices acquire distinct characteristics. Online providers are able to fragment prices and obscure the real cost of transactions through interface design, default settings, and the use of intermediary currencies. These practices reduce price transparency and, as a result, "impede consumers from making informed decisions" (Mathur *et al.* 2021). Competition and consumer protection authorities have increasingly recognised that such design-mediated pricing practices may distort consumer choice even in the absence of outright misrepresentation (OECD 2022, CMA 2022).

These concerns are amplified in the context of children's digital consumption. As noted by paediatrician Jenny Radesky during the FTC Workshop "Bringing Dark Patterns to Light", children's limited understanding of virtual currencies and pricing mechanisms constitutes a specific layer of vulnerability. Deceptive pricing strategies embedded in dark patterns are therefore particularly detrimental to children, who may struggle to translate virtual expenditures into real-world monetary values. The report Between Gaming and Gambling (Ash *et al.* 2022), funded by the Economic and Social Research Council, documents how game developers frequently rely on virtual currencies while failing to adopt standardised methods for tracking or displaying actual expenses. This lack of standardisation makes it difficult for children to assess how much they have spent, often leading to systematic underestimation of in-app purchases.

Regulatory and self-regulatory bodies have begun to address these practices. According to the OECD (2022), the Children's Advertising Review Unit (CARU), a self-regulatory organisation within the US advertising industry, has scrutinised the use of intermediary or virtual currencies as a form of dark pattern. Competition and consumer protection authorities have raised similar concerns regarding price opacity, drip pricing, and choice architecture in digital markets more broadly (OECD 2022, CMA 2022). Yet enforcement remains fragmented across jurisdictions and regulatory bodies. Scholars have documented persistent limitations of self-regulatory approaches in protecting children from commercial exploitation, including lack of effective enforcement, low levels of transparency, and guidelines that remain "deliberately subjective" in their application

(Verdoodt 2018). These structural weaknesses help explain why opaque pricing mechanisms and virtual currency systems remain widespread in games and applications targeting children, despite regulatory attention.

4.2.3. Trust in the market

When users become aware of the manipulative goals of dark patterns and deceptive design strategies, collective trust in the market can be undermined. Mathur, Mayer, and Kshirsagar (2021) argue that "users who become aware of them may become sceptical of and resistant to interface elements that look like dark patterns." For instance, Luguri and Strahilevitz (2021)'s experiment aimed to simulate a shopping experience and establish a relationship with customers to measure market manipulation. The results revealed that the most insidious dark patterns — the ones participants were more likely to succumb to — were mild, as they are subtler and fail to provoke consumer backlash. Participants who recognised the more aggressive dark patterns were generally in a worse mood than those who did not.

Children may experience negative emotions due to dark patterns and deception. Following the initial excitement of a purchase, players often feel shame after spending excessively on in-game transactions. At the same time, unsuccessful attempts to acquire rare items can result in feelings of frustration and disappointment, and even hostility towards parents when they impose restrictions on access to games and in-game purchases (Ash *et al.* 2022).

Constant exposure to advertisements can also cause distress for children. Advertisements employing dark patterns may utilise strategies such as the carrot-and-stick approach (i.e. paying to skip ahead to gain advantages or avoid waiting periods or "grinding"), content integration that blurs the boundary between entertainment and advertising, and bombardment through repeated or persistent prompts (Fairplay 2021). Content integration is particularly adept at manipulating children, as they struggle to discern the persuasive intent of such advertisements compared to traditional ads (Clarke and Svanaes 2014), with younger children being especially disadvantaged in recognising web page advertisements (Ali *et al.* 2009).

Experiencing manipulation or observing it early in life can foster a generalised distrust of the market later on. While caution is vital, overly fatalistic perspectives may hinder children's development of digital skills (Renaud *et al.* 2024) and make it more difficult for them to recover from adversity (Sánchez Chamorro, Lallemand, and Gray 2024).

4.2.4. Unanticipated societal consequences

A final collective welfare concern identified by Mathur, Mayer, and Kshirsagar (2021) involves unanticipated societal consequences — instances where design choices lead to outcomes that the designer did not originally foresee. A recent example of collective well-being being compromised without public knowledge is the Cambridge Analytica scandal. The FTC has accused the company of employing deceptive tactics to gather personal information from millions of Facebook users (FTC 2019). Brignull, the UX expert who coined the term "dark patterns", discusses how manipulative design practices were part of this conduct: "enabling social media businesses to extract fake consent from users regarding the use of their personal data, and enabling them to use

principles of addiction to make their products so compelling that they can dominate users' consumption of news and understanding of the world at large" (Brignull 2023).

Evidence suggests that design can shape children's political behaviour. Tyler and Iyengar (2023)'s research demonstrates that "adolescents today are just as polarised as adults" and that children as young as 11 years old already exhibit group favouritism and out-group distrust. According to Brian Hughes, Associate Director at the Polarization & Extremism Research & Innovation Lab (PERIL), the radicalisation of children primarily occurs due to increased exposure. In the past, vulnerable young individuals were unlikely to encounter propagandists or recruiters often. Nowadays, "it's frankly impossible not to come across that kind of propaganda. Any time we log on to our digital devices, we encounter extremist propaganda, hate, and their various cognates" (Children and Screens 2023). Katie Paul, director of the Tech Transparency Project, argues that "platforms are dangerous by design, targeting youth, amplifying extremism, and profiting in the process," (*ibid*.) whether through the automated creation of content for extremists or the recommendation of harmful material by social media platforms.

Auto-play and recommendations are user interface features central to political polarisation, alongside other detrimental effects such as increased anxiety and sleep deprivation, physical fatigue, and symptoms associated with depression (Chaudhary *et al.* 2022). A 2019 investigation by *The New York Times* revealed how YouTube guided users like 16-year-old Matheus Dominguez towards far-right radicalisation in Brazil.

> YouTube's recommendation system is engineered to maximise watch time, among other factors, the company says, but not to favour any political ideology. The system suggests what to watch next, often playing the videos automatically, in a never-ending quest to keep us glued to our screens.
>
> But the emotions that draw people in — like fear, doubt and anger — are often central features of conspiracy theories, and in particular, experts say, of right-wing extremism.
>
> As the system suggests more provocative videos to keep users watching, it can direct them toward extreme content they might otherwise never find. It is to lead users to new topics to pique new interest — a boon for channels like Mr. Moura's that use pop culture as a gateway to far-right ideas. (Fisher and Taub 2019)

4.3. Regulatory objectives

Another normative approach discussed by Mathur, Mayer, and Kshirsagar (2021) is the regulatory objectives lens, which "uses democratically created rules and standards to assess when dark patterns inflict individual and collective harms, such as diminishing individual financial welfare and undermining fair market competition, respectively" (*ibid*.). This lens "takes the existing legal framework as a given in making this judgement about an interface" (*ibid*.).

Beyond domestic child protection laws, the UNCRC (the most widely supported human rights treaty) offers guidance on how dark patterns can adversely affect children, as emphasised by General Comment No. 25. As noted by Leiser (2023), the UNCRC's perspective on the economic exploitation of children is crucial for analysing dark patterns. Leiser states that "digital platforms employing deceptive designs, whether focusing on direct or data-driven monetisation, perpetrate sophisticated economic

exploitation, capitalising on children's naivety and the absence of comprehensive regulatory oversight."

In several passages, General Comment No. 25 urges stakeholders in the digital environment to consider children's best interests in their designs, arguing that "the digital environment was not originally designed for children, yet it plays a significant role in children's lives" (paragraph 12). Recognising children's vulnerability during their development, particularly in the early stages, General Comment No. 25 mandates precautions (paragraph 15). It requires state parties to ensure the design of age-appropriate measures (paragraph 19) and to implement regulations with design standards for the industry (paragraph 24) that adhere to the highest standards of ethics, privacy, and safety (paragraph 39). The "Privacy by Design" approach, a movement championed in the 1990s by Ann Cavoukian to ensure that privacy is a guiding concern in the development and design of technologies, must also be integrated into the design of digital products to prevent problematic digital practices "such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering, and mass surveillance" (paragraphs 68, 69, and 70).

Translating these international standards into concrete design obligations, several jurisdictions have adopted Age Appropriate Design Codes that directly address dark patterns. The UK's Information Commissioner's Office pioneered this approach, issuing a code that prohibits nudge techniques that "lead or encourage children to provide unnecessary personal data or turn off privacy protections," "exploit unconscious psychological processes," and "might lead children to lie about their age." The code encourages platforms to implement pro-privacy nudges and strategies tailored to different age groups.

In the United States, California approved the first Age-Appropriate Design Code Act with unanimous legislative support, explicitly employing the terminology of dark patterns. The legislation prohibits design features that harm children's physical health, mental health, or well-being, and requires platforms to assess risks posed by their design, including exposure to harmful content. Maryland followed with legislation that defines the "best interest of a child" to mean platforms must not design in ways that benefit the company to the detriment of child users or result in reasonably foreseeable harm. The law requires platforms to set minors' accounts to the highest privacy settings by default. More recently, Nebraska's legislation focuses on user controls that allow minors to block unwanted contact, control design features, opt into chronological feeds instead of personalised ones, opt out of in-app purchases, and limit screen time. Vermont requires platforms to prohibit overnight notifications by default and prevent features that could lead to compulsive use. However, these state-level initiatives have faced intense resistance from the technology industry. NetChoice, representing major companies including Amazon, Google, Meta, and X, has filed lawsuits challenging these laws on constitutional grounds, resulting in California's law being enjoined pending appeal.

Brazil illustrates how existing children's rights frameworks can be adapted to address dark patterns in the digital environment. Grounded in constitutional provisions establishing shared responsibility for child protection and the robust framework of the Estatuto da Criança e do Adolescente (ECA), Brazil enacted the "ECA Digital" to extend

these protections to online spaces. The legislation establishes duties of prevention and protection owed by digital platforms to child users, targeting manipulative practices that induce compulsive use and prohibiting profiling for advertising purposes. Brazil exemplifies how emerging economies can address digital challenges to child welfare by adapting established constitutional and legal frameworks rather than building new regulatory architectures from scratch.

4.4. Individual autonomy

Lastly, the fourth normative lens used by Mathur, Mayer, and Kshirsagar (2021) is individual autonomy, which addresses dark patterns as a "user interface that undermines individual decision-making." This occurs either by altering choice architecture in a way that leads users to make selections they would not have made otherwise, were it not for the modified choice architecture, or through denying users choice, obscuring available options, burdening the exercise of choice, or fostering compulsive use patterns. From the early definitions of dark patterns, autonomy has been a primary concern within the scholarship on deceptive design.

For children and adolescents, autonomy is said to encompass three domains, as defined by Wang *et al.* (2023): (i) cognitive autonomy (i.e. "self-governance of the mental action or process of acquiring knowledge and understanding — evaluating thoughts, voicing opinions, making decisions independently, and self-assessing"); (ii) behavioural autonomy (i.e. the ability to make decisions independently and, more importantly, to follow through on these decisions with actions rather than merely conforming to or imitating others"); and (iii) emotional autonomy (i.e. "the ability to free oneself from emotional dependence").

Dark patterns can cause harm across these domains. Concerning cognitive autonomy, dark patterns are characterised by their ability to exploit cognitive biases (Waldman 2020) and, for children, vulnerabilities linked to their development (Fairplay 2021), thereby undermining users' choices, which are influenced by detailed behavioural profiles that facilitate manipulation (Richards *et al.* 2023). For example, visual indicators suggesting a scarcity of time (scarcity bias and loss aversion bias) are frequently employed in children's apps to prolong gameplay and encourage purchases (Radesky *et al.* 2022).

Regarding behavioural autonomy, the primary aim of dark patterns is to shape users' behaviour to favour the interests of digital platforms through choice architecture (CNIL 2019). Beyond minor behavioural manipulations, design patterns become particularly concerning for children when they effectively foster habits (Langvardt 2019), "even when this conflicts with other essential daily activities, such as sleeping or eating" (5Rights Foundation 2023). Compulsive use of social media can be triggered by design strategies rooted in seamlessness, such as infinite scroll and autoplay, while games typically rely on variable rewards (*ibid*.)

Ultimately, children's ability to manage their emotions (emotional autonomy) can be negatively impacted when digital platforms exploit their desire for acceptance or approval from others (need for social validation). The fear of missing out, described as "a pervasive apprehension that others might be having rewarding experiences from which one is absent" (Przybylski *et al.* 2013), coupled with dopamine hits from

notifications, has been shown to effectively manipulate children's emotions and prolong their usage of digital platforms (5Rights Foundation 2023).

5. Discussion and concluding remarks

Dark patterns have become a focal point in debates on digital design, regulation, and user protection. Yet existing evidence-based research has only partially addressed how the harms associated with manipulative design are distributed across different populations, particularly in relation to children. While scholarship on dark patterns has documented their prevalence and effectiveness, it has engaged less systematically with questions of vulnerability, particularly as shaped by developmental characteristics and structural asymmetries. By examining children's encounters with dark patterns through the normative framework proposed by Mathur, Mayer, and Kshirsagar (2021), this article has sought to address this gap, clarifying how individual and collective welfare, autonomy, and regulatory objectives are affected when vulnerability is understood as layered, relational, and context-dependent.

Placing this discussion within vulnerability theory helps illuminate both the potential and the limits of child-specific regulatory approaches. Fineman's universalist account highlights vulnerability as a shared feature of the human condition, shaped by institutional arrangements that distribute resilience unevenly over time. At the same time, critiques developed by Kohn and Luna draw attention to the fact that vulnerability materialises differently across contexts and relationships, requiring careful regulatory judgement. Children's digital experiences make this tension particularly visible. While empirical research shows that children can act competently and develop strategies to navigate digital environments (Livingstone *et al.* 2023, Renaud *et al.* 2024), their interactions remain structured by design choices that systematically exploit developmental asymmetries and constraints on attention.

Acknowledging children's specific vulnerabilities therefore requires particular caution. There is a fine line between recognising heightened exposure to harm and treating children as lacking agency. A relational and layered understanding of vulnerability, as articulated by Luna (2009) and developed in more recent work on digital vulnerability (Malgieri 2023, Rossi *et al.* 2024), offers a way to approach this tension. On this account, vulnerability shapes the conditions under which agency is exercised, without eliminating it. Regulatory responses should therefore focus on the design of digital environments and on how responsibility is allocated within platform architectures, rather than on categorical assumptions about individual incapacity.

The child-specific regulatory instruments examined in this article, including children's rights by design approaches grounded in the UN Convention on the Rights of the Child and General Comment No. 25, reflect this normative orientation. These frameworks translate legal commitments such as the best interests of the child and evolving capacities into expectations for design and governance. They also resonate with the regulatory objectives lens identified by Mathur, Mayer, and Kshirsagar (2021), which assesses harm by reference to democratically articulated legal standards. By embedding protective considerations at the level of system architecture, these approaches reduce reliance on individual awareness and place responsibility more squarely on platform operators.

The empirical literature reviewed here has made important advances in documenting children's encounters with dark patterns and in foregrounding questions of vulnerability and design. A recurring limitation, however, is that studies focusing on children are rarely conducted alongside analyses of adult users. This makes it difficult to assess which effects of manipulative design are specific to childhood and which reflect more general dynamics of digital vulnerability. It is in response to this gap that this article has drawn on scholarship from childhood studies to complement existing research on dark patterns, using insights from that literature to help identify how children's situated experiences both overlap with and diverge from those of other users.

While empirical clarity remains limited regarding how dark patterns affect different groups differently, emerging scholarship suggests that digital vulnerability extends well beyond childhood. From a particularist perspective, certain populations — including children, but also adults facing educational, economic, or cognitive disadvantages — may experience heightened exposure to harm due to asymmetries in power, information, and resources. Yet a universalist account reveals that dark patterns exploit cognitive biases and attentional constraints inherent to human cognition, rendering all users vulnerable to manipulation regardless of age or circumstance. If protective measures are justified for children due to developmental constraints and asymmetries, the underlying rationale applies more broadly: dark patterns manipulate features of human decision-making that are universally shared, even as their effects are unevenly distributed across different contexts and populations.

This universalist dimension has important regulatory implications. Regulating dark patterns with children in mind can establish baseline standards that benefit all users. As Richards, Hartzog, and Francis (2023) note, many of the rationales for protecting children also apply to adults facing educational, economic, or cognitive constraints. Regulatory measures developed to safeguard children tend to shape baseline expectations for acceptable design, influencing digital environments beyond the child-specific context. When grounded in a relational understanding of vulnerability, such approaches address manipulation at the level of design while preserving agency and generating positive externalities across digital markets.

References

5Rights Foundation. 2023. *Disrupted Childhood: The Cost of Persuasive Design* [online]. Report. Available at: https://5rightsfoundation.com/resource/updated-report-disrupted-childhood-the-cost-of-persuasive-design/

Albuquerque, N.F., Valença, G., and Falcão, T.P., 2023. How Social Media Platforms Manipulate Kidinfluencers? Analysing the Adoption of Deceptive Design Patterns by Big Techs. *Proceedings of the XXII Brazilian Symposium on Human Factors in Computing Systems* [online]. Maceió Brazil: ACM, 1–10. Available at: https://doi.org/10.1145/3638067.3638123

Ali, M., *et al*., 2009. Young Children's Ability to Recognize Advertisements in Web Page Designs. *British Journal of Developmental Psychology* [online], 27(1), 71–83. Available at: https://doi.org/10.1348/026151008X388378

Ash, J., Gordon, R., and Mills, S., 2022. *Between Gaming and Gambling: Children, Young People, and Paid Reward Systems in Digital Games* [online]. Loughborough University. Available at: https://hdl.handle.net/2134/21640190

Bernstein, G., 2023. *Unwired: Gaining Control over Addictive Technologies* [online]. Cambridge University Press.

Bessant, C., *et al*., 2023. Exploring parents' knowledge of dark design and its impact on children's digital well-being. *AoIR Selected Papers of Internet Research* [online], December. Available at: https://doi.org/10.5210/spir.v2023i0.13395

Bongard-Blanchy, K., *et al*., 2021. "I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!" - Dark Patterns from the End-User Perspective. *DIS '21: Proceedings of the 2021 ACM Designing Interactive Systems Conference* [online], 763–76. Available at: https://doi.org/10.1145/3461778.3462086

Bösch, C., *et al*., 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies* [online], 2016(4), 237–54. Available at: https://doi.org/10.1515/popets-2016-0038

Brignull, H., 2010. Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff. *90 Percent Of Everything* [online], 8 July. Available at: https://www.90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/

Brignull, H., 2023. *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You*. 1st ed. Eastbourne: Testimonium.

California Legislature. *California Age-Appropriate Design Code Act. AB-2273 (2022).*

Calo, R., 2025. *Law and Technology: A Methodical Approach.* 1st ed. Oxford University Press.

Chaudhary, A., *et al*., 2022. "Are You Still Watching?": Exploring Unintended User Behaviors and Dark Patterns on Video Streaming Platforms. *DIS '22: Proceedings of the 2022 ACM Designing Interactive Systems Conference* [online], 776–91. Available at: https://doi.org/10.1145/3532106.3533562

Childnet International and Phonepay Plus. 2015. *Young People's Experiences with in-App Purchases* [online]. Available at: https://www.childnet.com/wp-content/uploads/2021/11/Young-peoples-experiences-of-in-app-purchases.pdf

Children and Screens, 2023. *Youth and online polarization and radicalization: FAQ and tips for parents* [online]. August. Available at: https://www.childrenandscreens.org/learn-explore/research/youth-and-online-polarization-and-radicalization/

Clarke, B., and Svanaes, S., 2014. *Literature Review of Research on Online Food and Beverage Marketing to Children* [online]. Produced for the Committee of Advertising Practice (CAP). December. Available at: https://www.asa.org.uk/static/uploaded/d54b3c2c-f3d1-4bbe-ac0acab9cd351c30.pdf

Commission Nationale de l'Informatique et des Libertés (CNIL), 2019. *Shaping Choices in the Digital World* [online]. IP Reports, no. 6. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

Commission Nationale de l'Informatique et des Libertés (CNIL), 2021. *Recommendation 6: Strengthen the Information and Rights of Children by Design* [online]. 9 August. Available at: https://www.cnil.fr/en/recommendation-6-strengthen-information-and-rights-children-design

Competition and Markets Authority (CMA), 2022. *Online Choice Architecture - How Digital Design Can Harm Competition and Consumers* [online]. Discussion Paper. 5 April. Available at: https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers

Conti, G., and Sobiesk, E., 2010. Malicious Interface Design: Exploiting the User. *WWW '10: Proceedings of the 19th international conference on World wide web* [online], 271–80. Available at: https://doi.org/10.1145/1772690.1772719

Day, G., and Stemler, A., 2019. Are Dark Patterns Anticompetitive? *SSRN Electronic Journal* [online]. Available at: https://doi.org/10.2139/ssrn.3468321

Desimpelaere, L., Hudders, L., and Van De Sompel, D., 2020. Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study. *Media and Communication* [online], 8(4), 163–74. Available at: https://doi.org/10.17645/mac.v8i4.3232

Di Geronimo, L., *et al.*, 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* [online], 1–14. Available at: https://doi.org/10.1145/3313831.3376600

DiPaola, D., and Calo, R., 2024. Socio-Digital Vulnerability. *SSRN Electronic Journal* [online], 7 January. Available at: https://doi.org/10.2139/ssrn.4686874

Djeffal, C., 2022. Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment. *Laws* [online], 11(6), 84. Available at: https://doi.org/10.3390/laws11060084

Dreier, M., *et al.*, 2017. Free-to-Play: About Addicted Whales, at Risk Dolphins and Healthy Minnows. Monetarization Design and Internet Gaming Disorder. *Addictive Behaviors* [online], 64 (January), 328–33. Available at: https://doi.org/10.1016/j.addbeh.2016.03.008

European Commission, 2017. *Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service* [online]. Press release. 27 June. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_17_1784

European Commission, 2019. *Competition Policy for the Digital Era* [online]. Luxembourg: Publications Office. Available at: https://data.europa.eu/doi/10.2763/407537

Fairplay, 2021. *Comments of Campaign for a Commercial-Free Childhood and Center for Digital Democracy in the matter of request for public comment on the Federal Trade Commission's request for comments regarding topics to be discussed at Dark Patterns Workshop* [online]. 27 May. Available at: https://fairplayforkids.org/wp-content/uploads/2021/05/darkpatterns.pdf

Federal Trade Commission (FTC), 2014a. *Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent* [online]. Press release. 15 January. Available at: https://www.ftc.gov/news-events/news/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million-settle-ftc-complaint-it-charged-kids

Federal Trade Commission (FTC), 2014b. *Google to Refund Consumers at Least $19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges* [online]. Press release. 4 September. Available at: https://www.ftc.gov/news-events/news/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it-unlawfully-billed-parents-childrens

Federal Trade Commission (FTC), 2016. *Federal Court Finds Amazon Liable for Billing Parents for Children's Unauthorized In-App Charges* [online]. Press release. 27 April. Available at: https://www.ftc.gov/news-events/news/press-releases/2016/04/federal-court-finds-amazon-liable-billing-parents-childrens-unauthorized-app-charges

Federal Trade Commission (FTC), 2019. *FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield* [online]. Press release. 6 December. Available at: https://www.ftc.gov/news-events/news/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving-consumers-about-collection-facebook

Federal Trade Commission (FTC), 2021. *Bringing Dark Patterns to Light* [online]. Workshop transcript. Available at: https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf

Federal Trade Commission (FTC), 2022. *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges* [online]. Press release. 19 December. Available at: https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations

Fineman, M.A., 2008. The Vulnerable Subject: Anchoring Equality in the Human Condition. *Yale Journal of Law and Feminism*, 20(1).

Fineman, M.A., 2013. Equality, Autonomy, and the Vulnerable Subject in Law and Politics. *In:* M.A. Fineman and A. Grear, eds., *Vulnerability: Reflections on a New Ethical Foundation for Law and Politics.* Burlington: Ashgate.

Fisher, M., and Taub, A., 2019. How YouTube radicalized Brazil. *New York Times* [online], 11 August. Available at: https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html

Fitton, D., and Read, J.C., 2019. Creating a Framework to Support the Critical Consideration of Dark Design Aspects in Free-to-Play Apps. *IDC '19: Proceedings of the 18th ACM International Conference on Interaction Design and Children* [online], 407–18. Available at: https://doi.org/10.1145/3311927.3323136

Fitton, D., Bell, B.T., and Read, J.C., 2021. Integrating Dark Patterns into the 4Cs of Online Risk in the Context of Young People and Mobile Gaming Apps. *In:* C. Ardito *et al*., eds., *Human-Computer Interaction – INTERACT 2021. Lecture Notes in Computer Science* [online]. Cham: Springer International, 701–11. Available at: https://doi.org/10.1007/978-3-030-85610-6_40

Gray, C.M., *et al*., 2018. The Dark (Patterns) Side of UX Design. *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* [online], 1–14. Available at: https://doi.org/10.1145/3173574.3174108

Gray, C.M., *et al*., 2024. An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building. *CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* [online], 1–22. Available at: https://doi.org/10.1145/3613904.3642436

Gunawan, J., *et al*., 2021. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. *Proceedings of the ACM on Human-Computer Interaction* [online], 5(CSCW2), 1–29. Available at: https://doi.org/10.1145/3479521

Hannah, F., and Andrews, J., 2020. Loot boxes: I blew my university savings gaming on Fifa. *BBC* [online], 9 July. Available at: https://www.bbc.com/news/business-53337020

Hartung, P., 2020. *The Children's Rights-by-Design Standard for Data Use by Tech Companies* [online]. Issue brief no. 5. UNICEF. Available at: https://www.unicef.org/innocenti/media/1096/file/UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf

Helberger, N., *et al*., 2022. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. *Journal of Consumer Policy* [online], 45(2), 175–200. Available at: https://doi.org/10.1007/s10603-021-09500-5

Henriques, I., and Hartung, P., 2021. Children's Rights by Design in AI Development for Education. *The International Review of Information Ethics* [online], 29(March). Available at: https://doi.org/10.29173/irie424

Herzog, L., Kellmeyer, P., and Wild, V., 2022. Digital Behavioral Technology, Vulnerability and Justice: Towards an Integrated Approach. *Review of Social Economy* [online], 80(1), 7–28. Available at: https://doi.org/10.1080/00346764.2021.1943755

Hummel, L.M.F., 2023. Innovation as a Competitive Constraint on Online Platforms in European Competition Law: The Industry Life Cycle and Dominant Designs in Digital Markets. *In:* K. Mathis and A. Tor, eds., *Law and Economics of the Digital*

Transformation. ILEC 2023. Economic Analysis of Law in European Legal Scholarship, vol 15 [online]. Cham: Springer Nature Switzerland, 281–304. Available at: https://doi.org/10.1007/978-3-031-25059-0_11

Information Commissioner's Office (ICO), 2020. *Age Appropriate Design: A Code of Practice for Online Services* [online]. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

Kleine, C., Pearson, G., and Poveda, S., 2016. *Participatory Methods: Engaging Children's Voices and Experiences in Research.* University of London.

Kohn, N.A., 2014. Vulnerability Theory and the Role of Government. *Yale Journal of Law & Feminism*, 26.

Langvardt, K., 2019. Regulating Habit-Forming Technology. *SSRN Electronic Journal* [online]. Available at: https://doi.org/10.2139/ssrn.3351936

Lehtosalo, S., and Woods, D.W., 2023. *Deceptive Patterns in Consent Dialogs on Children's Websites* [online]. Conference paper. INFORMATIK 2023 - Designing Futures: Zukünfte gestalten. Available at: https://doi.org/10.18420/INF2023_65

Levesque, R.J.R., 2017. *Adolescence, Privacy, and the Law: A Developmental Science Perspective*. New York: Oxford University Press.

Livingstone, S., and Otani, M., 2023. Why We Need Child Rights by Design. *Context* [online], 17 July. Available at: https://www.context.news/digital-rights/opinion/why-we-need-child-rights-by-design

Livingstone, S., and Pothong, K., 2023. *Child Rights By Design - Child Rights by Design Principles* [online]. 5rights Foundation, Digital Futures Commission. Available at: https://childrightsbydesign.5rightsfoundation.com/page/child-rights-by-design/#

Livingstone, S., Mascheroni, G., and Stoilova, M., 2023. The Outcomes of Gaining Digital Skills for Young People's Lives and Wellbeing: A Systematic Evidence Review. *New Media & Society* [online], 25(5), 1176–1202. Available at: https://doi.org/10.1177/14614448211043189

Livingstone, S., Stoilova, M., and Nandagiri, R., 2019. *Children's Data and Privacy Online Growing up in a Digital Age* [online]. January. London School of Economics and Political Science. Available at: https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf

Luguri, J., and Strahilevitz, L.J., 2021. Shining a Light on Dark Patterns. *Journal of Legal Analysis* [online], 13(1), 43–109. Available at: https://doi.org/10.1093/jla/laaa006

Luna, F., 2009. Elucidating the concept of vulnerability: Layers not labels. *IJFAB: International Journal of Feminist Approaches to Bioethics* [online], 2(1), 121–139. Available at: https://doi.org/10.3138/ijfab.2.1.121

Lupiáñez-Villanueva, W.F., *et al*., 2022. *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation* [online].

10 June. Open Evidence. Available at: https://open-evidence.com/2022/06/10/behavioural-study-on-unfair-commercial-practices-in-the-digital-environment-dark-patterns-and-manipulative-personalization/

Malgieri, G., 2023. *Vulnerability and Data Protection Law* [online]. 1st ed. Oxford University Press. Available at: https://doi.org/10.1093/oso/9780192870339.001.0001

Mathur, A., *et al.*, 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction* [online], 3(CSCW), 1–32. Available at: https://doi.org/10.1145/3359183

Mathur, A., Mayer, J., and Kshirsagar, M., 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. *CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* [online], 1–18. Available at: https://doi.org/10.1145/3411764.3445610

Melzer, A.K., *et al.*, 2021. Towards Suitable Free-to-Play Games for Children. *In:* J.B. Hauge et al, eds., *Entertainment Computing – ICEC 2021. Lecture Notes in Computer Science* [online]. Cham: Springer International, 264–76. Available at: https://doi.org/10.1007/978-3-030-89394-1_20

Narayanan, A., *et al.*, 2020. Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces. Research article. *Queue* [online], 18(2), 67–92. Available at: https://doi.org/10.1145/3400899.3400901

Nguyen, S., and McNealy, J., 2021. *I, Obscura - Illuminating Deceptive Design Patterns in the Wild* [online]. Stanford PACS. Available at: https://pacscenter.stanford.edu/wp-content/uploads/2021/07/I-Obscura-Zine.pdf

OECD, 2022. *Dark Commercial Patterns. OECD Digital Economy Papers 336* [online]. Available at: https://doi.org/10.1787/44f5e846-en

Ofcom, 2019. *Children and Parents: Media Use and Attitudes Report 2018* [online]. 2 February. Available at: https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2018

Pothong, K., *et al.*, 2024. Applying Children's Rights to Digital Products: Exploring Competing Priorities in Design. *Proceedings of the 23rd Annual ACM Interaction Design and Children Conference* [online], 93–104. Available at: https://doi.org/10.1145/3628516.3655789

Przybylski, A.K., *et al.*, 2013. Motivational, Emotional, and Behavioral Correlates of Fear of Missing Out. *Computers in Human Behavior* [online], 29(4), 1841–48. Available at: https://doi.org/10.1016/j.chb.2013.02.014

Radesky, J., *et al.*, 2022. Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children. *JAMA Network Open* [online], 5(6), e2217641. Available at: https://doi.org/10.1001/jamanetworkopen.2022.17641

Renaud, K., *et al.*, 2024. "We're Not That Gullible!" Revealing Dark Pattern Mental Models of 11-12-Year-Old Scottish Children. *ACM Transactions on Computer-Human Interaction* [online], 31(3), 1–41. Available at: https://doi.org/10.1145/3660342

Richards, N., Hartzog, W., and Francis, J., 2023. *Comments of the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis* [online]. Regulatory comment. Saint Louis: Cordell Institute for Policy in Medicine & Law. Available at: https://scholarship.law.bu.edu/faculty_scholarship/3386/

Rossi, A., *et al*., 2024. Who Is Vulnerable to Deceptive Design Patterns? A Transdisciplinary Perspective on the Multi-Dimensional Nature of Digital Vulnerability. *Computer Law & Security Review* [online], 55(November), 106031. Available at: https://doi.org/10.1016/j.clsr.2024.106031

Sánchez Chamorro, L., Lallemand, C., and Gray, C.M., 2024. "My Mother Told Me These Things Are Always Fake" - Understanding Teenagers' Experiences with Manipulative Designs. *Designing Interactive Systems Conference* [online], 1469–82. Available at: https://doi.org/10.1145/3643834.3660704

Sánchez Chamorro, L., Toebosch, R., and Lallemand, C., 2024. Manipulative Design and Older Adults: Co-Creating Magic Machines to Understand Experiences of Online Manipulation. *Designing Interactive Systems Conference* [online], 668–84. Available at: https://doi.org/10.1145/3643834.3661513

Santos, C., Morozovaite, V., and De Conca, S., 2024. No Harm No Foul: How Harms Caused by Dark Patterns Are Conceptualised and Tackled under EU Data Protection, Consumer and Competition Laws. *SSRN* [online], 26 June. Available at: https://doi.org/10.2139/ssrn.4877439

Schäfer, R., *et al*., 2024. Growing Up With Dark Patterns: How Children Perceive Malicious User Interface Designs. *Nordic Conference on Human-Computer Interaction* [online], 1–17. Available at: https://doi.org/10.1145/3679318.3685358

Sousa, C., and Oliveira, A., 2023. The Dark Side of Fun: Understanding Dark Patterns and Literacy Needs in Early Childhood Mobile Gaming. *European Conference on Games Based Learning* [online], 17(1), 599–610. Available at: https://doi.org/10.34190/ecgbl.17.1.1656

SuperAwesome, 2018. *SuperAwesome launches Kid-Safe Filter to prevent online ads from stealing children's personal data* [online]. Press release. 6 December. Available at: https://www.superawesome.com/superawesome-launches-kid-safe-filter-to-prevent-online-ads-%20from-stealing-childrens-personal-data/

Susser, C., and Grimaldi, V., 2021. Measuring Automated Influence: Between Empirical Evidence and Ethical Values. *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* [online], 242–53. Available at: https://doi.org/10.1145/3461702.3462532

Swepston, L., 2012. *A Commentary on the United Nations Convention on the Rights of the Child, Article 32: Protection from Economic Exploitation* [online]. Leiden: Brill Nijhoff. Available at: https://doi.org/10.1163/9789004231467

Thaler, R.H, Unstein, C.R.S., and Balz, J.P., 2012. Choice Architecture. *In:* E. Shafir, ed., *The Behavioral Foundation of Policy* [online]. Princeton University Press. Available at: https://doi.org/10.13140/2.1.4195.2321

Tims, A., 2020. My kids spent £600 on their iPads without my knowledge. *The Guardian* [online], 11 March. Available at: https://www.theguardian.com/money/2020/mar/11/my-kids-spent-600-on-their-ipads-without-my-knowledge

Tyler, M., and Iyengar, S., 2023. Learning to Dislike Your Opponents: Political Socialization in the Era of Polarization. *American Political Science Review* [online], 117(1), 347–54. Available at: https://doi.org/10.1017/S000305542200048X

UNICEF, ed., 2017. *Children in a Digital World. The State of the World's Children* [online]. New York: UNICEF. Available at: https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf

United Nations Committee on the Rights of the Child, 2021. *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment. CRC/C/GC/25* [online], 2 March. Available at: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

United Nations. Convention on the Rights of the Child. Adopted November 20, 1989. *United Nations Treaty Series* [online], vol. 1577, p. 3. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

Utz, C., *et al.*, 2019. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [online], 973–90. Available at: https://doi.org/10.1145/3319535.3354212

Van der Hof, S., *et al.*, 2020. The Child's Right to Protection against Economic Exploitation in the Digital World. *The International Journal of Children's Rights* [online], 28(4), 833–59. Available at: https://doi.org/10.1163/15718182-28040003

Van der Hof, S., *et al.*, 2022. "Don't Gamble With Children's Rights"—How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment. *Frontiers in Digital Health* [online], 4(May), 822933. Available at: https://doi.org/10.3389/fdgth.2022.822933

Verdoodt, V., 2018. Strengthening Advertising Self-Regulation to Ensure Meaningful Protection for Children in the Digital Environment. *SSRN Electronic Journal* [online], 1 January. Available at: https://doi.org/10.2139/ssrn.3460508

Waldman, A.E., 2020. Cognitive Biases, Dark Patterns, and the "Privacy Paradox". *Current Opinion in Psychology* [online], 31(February), 105–9. Available at: https://doi.org/10.1016/j.copsyc.2019.08.025

Wang, G., *et al.*, 2023. 12 Ways to Empower: Designing for Children's Digital Autonomy. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* [online], 1–27. Available at: https://doi.org/10.1145/3544548.3580935

Willis, L.E., 2020. Deception by Design. *Harvard Journal of Law & Technology*, 34(1).

YoungMinds, 2022. *Putting a Stop to the Endless Scroll* [online]. January. Available at: https://www.youngminds.org.uk/media/qsppe0f3/youngminds-putting-a-stop-to-the-endless-scroll-january-2023.pdf

Zac, A., *et al*., 2023. Dark Patterns and Online Consumer Vulnerability. *SSRN Electronic Journal* [online]. Available at: https://doi.org/10.2139/ssrn.4547964

Zagal, J.P, Björk, S., and Lewis, C., 2013. *Dark Patterns in the Design of Games* [online]. Available at: https://files01.core.ac.uk/download/pdf/301007767.pdf