ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

SCHOOL OF INTERNATINAL STUDIES COMMUNICATION AND CULTURE

DEPARTMENT OF INTERNATIONAL, EUROPEAN AND AREA STUDIES & DEPARTMENT OF COMMUNICATION, MEDIA, AND CULTURE

INTERDISCIPLINARY POSTGRADUATE STUDIES PROGRAMME

«DIGITAL TRANSFORMATION: E-DIPLOMACY, E-CAMPAIGNING AND DIGITAL LAW»

SPECIALIZATION: DIGITAL LAW

# Digital well-being in EU regulation: Addressing the challenges of the attention economy

MASTER'S DISSERTATION

Alexandra Ioannou

Athens, 2024

Three-member Committee

Yannos Paramythiotis, Adjunct Lecturer, Panteion University (Supervisor)

Vassilis Hatzopoulos, Professor, Panteion University

Pantelis Vatikiotis, Associate Professor, Panteion University

**Declaration of Non-Plagiarism and Assumption of Personal Responsibility**

I declare that the work submitted as part of my academic studies is the result of my original research. I affirm that it does not make use of the intellectual property of third parties, or any text generated by generative AI applications without proper and necessary referencing. I further confirm that any use of AI in the preparation of this work has been strictly limited to editing and proofreading purposes, without contributing to the creation of substantive content. I acknowledge and assume full legal and administrative responsibility for any instances of plagiarism or academic dishonesty that may arise from this work.

**Table of contents**

**Abstract**

This thesis explores the regulation of digital well-being in the attention economy, focusing on user autonomy, content control, and the role of platform practices. Chapter 2 examines the definitions of digital well-being, revealing its inherently subjective nature and the centrality of user agency. It discusses strategies employed by platforms to capture attention—such as personalized advertising, addictive design, and algorithmic amplification—which often undermine well-being by fostering stress, fatigue, and harmful content exposure. The chapter argues that effective regulation is essential to counter these challenges, especially given the vulnerabilities of consumers in oligopolistic markets.

Chapter 3 examines current EU regulatory frameworks, focusing on the recently enacted DSA, DMA, and AI Act. It assesses their adequacy in addressing digital well-being concerns and highlights gaps in regulating addictive platform designs and dark patterns, noting that existing laws primarily focus on overt deception and minor protection. Transparency requirements, risk assessments, and content moderation obligations introduced by the DSA represent progress but fail to provide users with meaningful tools for controlling their online experiences. Furthermore, the reliance on consent mechanisms continues to limit user choice, particularly in the context of behavioural advertising and algorithmic recommendation.

Chapter 4 concludes that digital well-being regulation remains limited by enforcement challenges, vague definitions of harm, and a reliance on user responsibility. While recent EU initiatives mark progress, gaps persist in addressing the root causes of manipulative platform practices. Stronger measures, including bans on intrusive ads and more robust personalization tools, are needed to protect users and prioritize well-being over profit.

Limitations of this study include its focus on EU law, the early implementation of the DSA, and the exclusion of smaller platforms and sectors like mobile apps. Future research should explore alternative models that better align digital platforms with user well-being.

*Key words:* Digital well-being, attention economy, platform regulation, EU law, user autonomy

## Introduction

The widespread use of the internet, particularly through social media, has resulted in several harmful effects on both individuals and society. Some of these effects have been extensively addressed by scholars and regulators such as fake news and disinformation, harms to democracy and elections, cybersecurity, and privacy. However, there are some broader societal harms that are still understudied and more nuanced in nature. These include internet addiction, which can lead to physical and psychological distress, and cognitive development issues, impacting skills such as attention span and critical reasoning. The overload of information online can overwhelm users, reducing decision-making abilities and damaging personal relationships. Social media use, in particular, has been linked to increased loneliness, cyberbullying, and the erosion of public-private boundaries, exposing individuals to privacy risks and social pressures (Brey et al., 2016).

The concept of *digital well-being* serves as a useful umbrella term to address the nuanced and often immeasurable societal harms arising from the pervasive use of digital platforms. This term provides a framework to explore and mitigate issues such as mental health risks and manipulative design practices, which extend beyond traditional regulatory concerns like privacy, market competition, and content moderation. Vanden Abeele et. al. (2024) for instance, positions digital well-being as a balance between individual autonomy and technological influences, offering a nuanced lens to evaluate the broader implications of digital platform use.

While EU regulators have acknowledged the risks posed by digital platforms, existing regulations primarily emphasize transparency, market dynamics, and privacy protections, leaving mental health and well-being largely unaddressed. Relying on platforms to self-regulate through technological solutions does little to tackle the core mechanics of the attention economy. These platforms are intentionally designed to maximize engagement through features like infinite scroll and personalized feeds—design elements that are fundamentally at odds with user mental health due to their profit-driven nature. Also, this conflict underscores broader philosophical tensions: the vision of an open, innovative, and socially connected internet versus the reality of an advertising-dependent ecosystem that prioritizes profit over the public good (Giraldo-Luque et al., 2020).

The Digital Services Act (DSA), introduced in 2022, aims to address the evolving business models of digital platforms, safeguard users and consumers, foster innovation, and establish a uniform regulatory approach across the EU (Recitals 1-4, DSA). Together with the Digital Markets Act (DMA), these laws make bold commitments: “The digital space should be a safe place for you, where your fundamental rights are protected, and businesses have a level playing field. The Digital Services Act and the Digital Markets Act protect your fundamental rights online, safeguarding your privacy and your freedom of choice in the digital world. The Digital Services Act and the Digital Markets Act ensure a safer and fairer internet for you. With these rules all businesses in the EU face a fair and open economy with higher transparency of digital platforms” (European Commission, n.d.-a).

Despite this regulatory innovation, this essay argues that the core business model of digital platforms remains fundamentally flawed. The attention economy exacerbates this issue, revealing a conflict between the overwhelming flow of information and users' finite cognitive resources. Thus, addressing the inherent tension between user well-being and attention-driven technology requires a more substantial re-evaluation of regulatory frameworks to better protect users (Syvertsen, 2020).

**Research question**

This research explores the extent to which existing EU regulations address the challenges associated with digital well-being, particularly in the context of the attention economy and dark patterns. The rationale behind EU digital platform regulations has historically centered on safeguarding consumer rights, ensuring fair market competition, and enhancing transparency. However, the emergence of harmful design practices, such as addictive interfaces and exploitative personalization, raises questions about whether these frameworks sufficiently prioritize user well-being.

## Hypothesis

The hypothesis guiding this study posits that despite increasing awareness of the risks posed by the attention economy, such as mental health harms and erosion of user autonomy, digital well-being remains inadequately addressed in EU regulation. By examining the inclinations and priorities embedded in existing regulatory approaches, this research seeks to uncover gaps and misalignments between current legal frameworks and the broader need to protect users from the psychological and social harms of digital platform practices.

## Methodology

To address these questions, I will employ an interdisciplinary approach, combining a comprehensive literature review with an analysis of existing regulatory frameworks. The literature review provides a theoretical foundation, drawing from fields such as law, digital studies, and psychology to understand the concept of digital well-being and its relevance to regulation. Simultaneously, the analysis of EU regulatory approaches, including the Digital Services Act and other relevant policies, examines how these frameworks address—or fail to address—challenges related to user well-being. This dual-method approach ensures a holistic understanding of the topic, bridging conceptual insights with practical regulatory implications.

In Chapter 2, I will discuss the concept of digital well-being, focusing on its emphasis on user autonomy and control over time spent online and the content encountered. I will explore how the attention economy, driven by targeted advertising, manipulative algorithms, and attention-capturing strategies, undermines this control, leading to stress and fatigue. I will argue that regulation is necessary to address these harms, particularly given the vulnerabilities of certain user groups and the dominance of platform oligopolies.

In Chapter 3, I will analyze the current EU regulatory framework, including consumer protection, privacy, and platform regulation laws, to evaluate their effectiveness in promoting digital well-being. Finally, In Chapter 4, I will assess the strengths and limitations of these regulations, emphasizing the need for stronger enforcement, meaningful user empowerment, and a shift in focus toward systemic platform accountability. I will propose alternative

approaches, including platform interoperability, stricter privacy protections, and greater involvement of civil society, to better support digital well-being.

## Digital well-being in the attention economy: A case for regulation

### Defining digital well-being

Digital well-being and the attention economy are closely linked concepts that explore the relationship between our use of digital technology and its impact on mental and physical health. Before examining potential regulatory approaches, it is essential to first understand what digital well-being entails. In the next section I will review how academic literature defines and conceptualizes digital well-being.

Scholars agree that digital well-being is a complex and subjective state that varies among individuals, reflecting their unique experiences and interactions with digital technologies. As noted in a 2024 report by the University of Twente, there is no universal definition of well-being; rather, researchers adopt definitions that suit their specific research questions (Annemans & Dennis, 2024). This report specifically highlights a widely cited definition by Luciano Floridi and Christopher Burr, who, in their study of digital well-being ethics, frame it simply as, "the impact of digital technologies on what it means to live a life that is *good* for a human being in an information society" (p. 1, emphasis in the original).

Vanden Abeele (2020) proposes a more nuanced definition of digital-well-being. She cautions against over-medicalizing device use (e.g. defining it as addiction) and suggests that facing challenges with technology use is a common and often normal part of modern life that shouldn't be demonized. She also considers that technology can induce both positive and negative emotions to the users, a notion that she defines as the "mobile connectivity paradox". While the use of devices, if it's mindful and purposeful, might create a sense of autonomy and growth for the user, simultaneously, those same devices can hinder the person's sense of control by distracting them from their main activities. According to Vanden Abeele:

> "Digital wellbeing is a subjective individual experience of optimal balance between the benefits and drawbacks obtained from mobile connectivity. This experiential state is comprised of affective and cognitive appraisals of the integration of digital connectivity into ordinary life. People achieve digital wellbeing when experiencing

maximal controlled pleasure and functional support, together with minimal loss of control and functional impairment" (p. 12).

Similarly, Lyngs (2019) drafts a definition of digital well-being as a state, where "people are able to exert self-control over how they use their digital devices, and in particular whether they are able to align use of digital technology with their personal long-term goals" (p. 1). Like Vanden Abeele, Lyngs emphasizes the importance of users maintaining autonomy over their device use to maximize benefits without sacrificing personal agency. Thus, the relationship between social media use and well-being is nuanced and cannot be reduced to simplistic equations like "more time online equals lower well-being." Individual experiences vary widely based on factors like exposure to harmful content or online interactions, showing that social media's impact is highly context-dependent (Montag & Elhai, 2023).

Vanden Abeele (2020) further identifies the factors that contribute to attaining (or diminishing) digital well-being. Firstly, the author explains that the sense of balance is dependent on the user's personality, mood and state of being (e.g. boredom). Secondly, it's influenced by the features and design of digital devices, which often employ elements to capture the user's attention. The last factor is related to cultural and societal expectations for availability and responsiveness. Vanden Abeele argues that there are some environments that require active negotiation of digital interactions in order to achieve one's personal and social roles.

Thus, in discussing digital well-being, scholars consider both individual circumstances, social norms and the digital environments shaping those experiences. As Al-Mansoori et al. (2022) note, "technology products and services are not neutral, rather, they play active mediating roles between humans and the real world, leading to both positive and negative consequences on their lives and wellbeing" (p. 1). Gui et al. (2017) add that, within a landscape of overabundant digital communication and the attention economy, users need specific skills to counter multitasking and manage online time. This is reflected in their proposed definition of digital well-being as "a state where subjective well-being is maintained in an environment characterized by digital communication overabundance" (p. 166).

Digital well-being could be also linked with research about work-life balance. Klingelhoefer and Meier (2023) discuss the implications of the boundary-blurring effects of social

media, particularly as flexible work arrangements and remote work become increasingly common. Even though there are no empirical studies yet on how work-related interruptions during non-work hours affect well-being, initial findings indicate “a potential to increase work-home conflicts, interruptions, and exhaustion, but also positive effects through connectedness to co-workers and improved work-related communication“ (Klingelhoefer & Meier, 2023, p.13).

A major facet of digital well-being discussed in literature is the decision of disconnecting from social media and self-moderation (e.g. digital detox). For example, Nguyen (2021) examines strategies for intentional offline time and their effects on well-being. Her study participants reported various positive effects from disconnection, including psychological benefits (e.g., relief from social pressure and information overload), improved time management and productivity (e.g., more focus and time for other interests), and physical well-being (e.g., better sleep and rest). However, disconnection can also induce negative feelings, such as loneliness.

In an effort to create a comprehensive framework for the study of digital disconnection, Vanden Abeele et al. (2024) define four primary harms people perceive from their online experiences, often motivating them to disconnect:

1. “Time displacement”: occurs when screen time replaces activities like sleeping, studying, or socializing, leading to guilt, shame, and a sense of lost control over time spent unproductively. Strategies to mitigate this involve limiting screen time, though they sometimes conflict with the perceived moral value of certain activities.
2. “Interference” describes how constant interruptions and information overload challenge focus, decision-making, and communication, implying even serious risks such as distraction while driving. Design solutions like introducing "friction" to reduce impulsive behaviors can help, but they may also heighten the stress of missing out.
3. “Boundary blurring**”** highlights the difficulty in managing competing role demands, such as balancing work and personal life, as digital media create expectations of constant availability. Limiting notification channels can help, but the necessity for 24/7 availability in some contexts complicates this.

4. “Exposure to negative or undesirable content” and technostress. Mitigation strategies like unfollowing or deleting accounts may help but depend on individual contexts and thresholds for negative experiences.

Digital well-being tools have also been introduced by some tech companies as a response to growing criticism towards problematic technology use. However, while people often appreciate the concept of digital well-being tools, they frequently find them ineffective. In practice users find restrictive tools intrusive and annoying, leading them to shift from strict usage controls to more permissive strategies over time. This reflects an ambivalence; users do not want to battle against their technology but instead prefer systems that naturally discourage undesired habits. Research suggests that internal support, such as modifications to platform design that make engagement more manageable, could complement external tools like screen-time limits, offering a more holistic approach to promoting user agency (Zhang et al., 2022).

Finally, examining digital well-being from a consumer protection perspective, the Fitness Check of EU Consumer Law on Digital Fairness (2024) identifies five main areas of concern, in addition to general trends consumers experience in the digital markets: dark patterns, addictive design, especially in gaming, where design techniques encourage excessive use; personalization practices, citing unfair monetization and lack of control over content and decision-making; influencer marketing, and sketchy digital contracts (European Commission, 2024c).

To summarize, digital well-being examines how digital technology impacts mental and physical health, focusing on balancing its benefits and drawbacks. Although definitions of digital well-being are very broad and highlight the subjective nature of what feeling well means, a common denominator is that of control, user-agency, and autonomy in the use of technology. This control operates on two key levels: managing the time spent online and influencing the content users encounter.

While much of the research focuses on self-regulation and intentional device use, scholars also highlight the broader implications of digital technologies on quality of life, questioning the balance between user responsibility and the role of platform design in shaping consumption patterns. In the following sections, I will explore these dynamics in depth: first, by analyzing the mechanisms of the attention economy and how platform design directs user engagement—

affecting time, focus, and attention—and then by examining adaptive recommender algorithms to understand their control over content. Ultimately, I will argue for the importance of considering digital well-being in regulatory frameworks.

**Mechanisms of the attention economy in digital platforms**

This section builds on the discussion of user control and platform design by examining the strategies that digital platforms employ to capture and direct user attention, thereby maximizing engagement. These strategies often undermine users' sense of autonomy, a key component of digital well-being. Internet platforms typically monetize in two ways: through transaction-based models (e.g., charging commissions to retailers) or advertising-based models that offer freemium services (Zardiashvili & Sears, 2023). Today, digital media rely almost exclusively on advertising, a model that sustains the free and open nature of the internet but raises critical questions about its impact on user agency and quality of the digital experience.

As technology evolved, online advertising has grown into a complex network of players, including hardware providers, AI systems, platforms, and data management companies. This ecosystem also incorporates tools for managing user consent and companies that specialize in content creation. With the growing automation of the ad-buying process through algorithms and AI, consumers now see highly personalized ads and product recommendations (Strycharz, 2022), the so-called targeted advertising. This practice aims to minimize wasted advertising efforts by reaching consumers most likely to engage with an ad; with AI systems often determining the user profiles to target, though, the processes used are often opaque or "black box" systems.

There are two main types of targeted advertising: contextual, which tailors ads based on the content of the page or general user details like language or location, and personalized, which relies on data about the user. Personalized targeting includes broad categories like user-provided data or detailed demographic profiling, which includes inferred attributes like financial status or interests, as well as behavioural advertising that tracks users' online activity to create highly specific psychographic profiles (Zardiashvili & Sears, 2023). Behavioural targeted advertising has especially high risks due to huge amounts of data required, the lack of algorithmic transparency

and the ability to exploit user vulnerabilities (Buri, 2022). This data is often fed into real-time bidding auctions, which take place as users load web pages, allowing advertisers to dynamically place ads based on real-time data (Strycharz, 2022). In this regard, platforms have strong incentives to keep users engaged, as prolonged online activity enables the creation of more detailed user profiles and increases exposure to advertising (Bhargava & Velasquez, 2020).

This pervasive personalization aligns with the concept of the attention economy, first introduced by Herbert A. Simon in the late 1960s, that presents information overload as an economic issue (as cited in Carpentier, 2023). While traditional media like newspapers, magazines, and television have long operated on similar principles by offering free content to capture and sell users' attention to advertisers, today's digital platforms produce an endless supply of information in comparison. However, our capacity to process this information remains limited by finite attention, time, cognitive bandwidth, and competing demands (Wu, 2019). For tech companies, capturing and maintaining user engagement is critical for profitability, as attention serves as the "currency" in the attention economy (Giraldo-Luque et al., 2020); however, this often conflicts with the goal of balanced and intentional digital media use.

Social media platforms employ specific design elements that might even lead to internet addiction, including intermittent variable rewards, the need for social validation, and the elimination of "natural stopping cues" (Bhargava & Velasquez, 2020, p. 6). Giraldo-Luque et al. (2020) identify key mechanisms that digital platforms use to capture and retain user attention. An example of such practices is push notifications and reminders designed to surprise and create novelty, while flooding users with information that demands immediate attention and triggers heightened alertness (Mujica et al., 2022). The content itself, typically audiovisual and emotionally engaging, is easy to consume and delivered in short, dynamic formats like "reels" and "shorts", that compel impulsive engagement. Each interaction with these posts can spark new cycles of attention, reinforcing the urge for constant checking and responsiveness. Additionally, Giraldo-Luque et al. (2020) argue that the intermittent rewards of likes, comments, and shares mimic gambling incentives, encouraging users to return repeatedly for unpredictable emotional payoffs.

A related concept is that of "dark patterns," which refers to user interface designs that intentionally manipulate users into actions that go against their best interests. Design manipulations were initially defined in the scope of unethical e-commerce practices, such as hidden fees or convoluted steps to unsubscribe from online services.[1] However, more specific terms have emerged in literature to describe design choices aiming at maximizing engagement. For example, “attention-capture dark patterns” are defined as designs or functionalities that exploit psychological vulnerabilities to maximize time spent, daily visits, or interactions on a digital service, often against the user’s will (Lukoff et al., 2021, as cited in Roffarello & De Russis, 2022, p. 2).

Similarly, Esposito and Ferreira (2024) mention the term “hyper-engaging dark patterns” or HEDPs. The authors describe HEDPs as a specific type of choice architecture found in digital interfaces designed to capture and sustain users’ attention. These patterns distract users from their original intentions and create a sense of lost control and awareness of time. Common mechanisms embedded in platform design include recommendation systems, autoplay, pull-to-refresh functionality, infinite scrolling, and engagement metrics like likes and comments (Esposito & Ferreira, 2024).

Adaptive algorithms, as well, play a central role, personalizing content, and interface design to align with individual preferences and past interactions. This personalization reinforces behaviour by creating a sense of reward, making these patterns highly effective in promoting prolonged use (Esposito & Ferreira, 2024). However, the algorithms’ core functions—content curation, recommendation, moderation, and targeted advertising—often lead to undesirable outcomes. Deficiencies in algorithmic tools result in errors such as inappropriate recommendations, over-blocking, or the promotion of disturbing content. Also, they amplify harmful content, such as hate speech and disinformation, by prioritizing emotionally charged or

[1] “Dark patterns are commercial practices deployed through the structure, design or functionalities of digital interfaces or system architecture that can influence consumers to take decisions they would not have taken otherwise, e.g. presenting choices in a non-neutral manner, using fake countdown timers to create urgency, using emotional manipulation to make consumers second-guess their indicated choice, phrasing questions using double negatives, misleading consent options in cookie banners” (European Commission, 2024c, p. 18).

novel content. In addition, recommendation systems can create so-called "rabbit holes" that radicalize users through increasingly divisive content (Saurwein & Spencer-Smith, 2021).

Bhargava and Velasquez (2020) claim that these systems exploit user vulnerabilities through three distinct theories of harm. They argue that the negative impact of social media use may outweigh the benefits, given the various issues associated with technology use, such as poor performance, negative mood, anxiety, low self-esteem, loss of control, and loneliness. The authors argue that platforms disrespect the users; by employing adaptive algorithms and AI, they identify what maximizes user's engagement and keep feeding them more similar content. Essentially, users contribute data that make these platforms more addictive. Furthermore, they prey on user's needs for connection and socializing; in many cases, internet platforms have become essential for social connection and work, making avoidance nearly impossible.

This is further amplified by the phenomenon of the fear of missing out (FOMO), a psychological drive to stay connected for fear of missing updates, which leads to frequent device checking and detracts from real-life interactions. FOMO manifests in various forms related to online interactions and social networking. It includes fears of missing important information due to information overload, not connecting as desired, or missing timely or popular interactions leading to a constant need to engage, respond, and participate in digital spaces (Alutaybi et al., 2019).

Combined, all these strategies used by digital platforms to capture and sustain user attention, often undermine autonomy and digital well-being. Predominantly driven by advertising models, platforms employ tools like targeted advertising, adaptive algorithms, and attention-capture dark patterns to maximize user engagement. These practices, coupled with psychological triggers like intermittent rewards and FOMO, collectively, create an environment where users find it increasingly challenging to manage their attention, potentially leading to negative impacts on mental health and overall well-being. The constant demands on users' attention can result in feelings of anxiety, stress, and overwhelming digital fatigue. Building on this, in the next section I will discuss in more detail how adaptive algorithms shape user experiences, exploring both their functionality and the harms stemming from exposure to undesired social media content.

**Adaptive algorithms and harmful social media content**

To fully understand what digital well-being entails, it is essential to examine not only the amount of time users spend online but also the nature of the content they encounter. Beyond simply losing track of time, users might also experience a diminished sense of control over their digital environment, as algorithms increasingly determine the content they see. These algorithms, optimized for maximizing engagement, often prioritize attention-capturing content at the expense of user well-being, further complicating efforts to foster balanced and intentional digital media use.

The societal and well-being harms arising from adaptive algorithms are widely discussed in the literature. For example, scholars argue that personalization algorithms, central to social media feeds, are designed to keep users on the platform by leveraging behavioural data to suggest content (Mujica et al., 2022), even if it leads to harmful outcomes like "doomscrolling traps" or exposure to distressing material. Platforms' engagement-driven approach often reinforces echo chambers, amplifying ideologically similar content, and stifles exposure to diverse viewpoints (Risco & Lleonart-Anguix, 2024). This raises concerns about the broader societal impacts of current personalization practices, especially as they affect institutions like journalism, science, and public health. These institutions are typically governed by values such as fairness, accuracy, and quality, but social media algorithms disregard these principles, prioritizing content that maximizes engagement rather than content that meets high standards (Narayanan, 2023).

The detrimental effect on public discourse is particularly evident in social media campaigns, especially in the political sphere, where "affective and dissonant" communication strategies have gained prominence. These strategies, which exploit negative emotions, dramatization, and populist content, are designed to provoke strong emotional responses rather than foster rational debate. Studies show that negative campaigning generates more reactions, shares, and comments, increasing its visibility and circulation on platforms like Facebook. This shift towards emotionally-driven content reflects not just natural user behavior but the

incentives embedded in platform algorithms, which prioritize content that triggers anger or strong reactions (Klinger et al., 2022).

Further studies reveal that returning to reverse-chronological feeds could reduce user activity and diminish the echo-chamber effect, highlighting the misalignment between platforms' profit-driven incentives and users' broader social interests (Risco & Lleonart-Anguix, 2024). The widespread adoption of recommender algorithms on social media platforms is a relatively recent phenomenon. Just a few years ago, platforms like Facebook used the network model, where users were primarily influenced by content from their connections—posts from people they followed or subscribed to.

The shift from network-based to algorithmic content delivery was initially popularized by platforms like TikTok, which relies heavily on its "For You Page," and YouTube, which blends algorithms with subscriptions. In 2022, Instagram and Facebook adopted similar models in an effort to mimic TikTok. These platforms now track users' moment-to-moment actions to predict which posts are most likely to capture their attention. Algorithms must balance several factors, such as diversifying content to avoid overwhelming users with repetitive posts from a single source, while also considering context like location and prior interactions. The goal is to enhance the user experience by recommending content that is not only familiar but also introduces new and engaging posts, thereby maintaining users' attention (Narayanan, 2023).

Despite their sophistication, these algorithms are a double-edged sword, constantly evolving as platforms strive to retain user interest and maximize ad revenue (Narayanan, 2023). Engagement metrics increasingly take precedence over user preferences, with platforms weighting behavioural signals more heavily in their algorithms. This creates feedback loops that funnel users into narrow, often harmful content categories. Combined with ineffective user control tools, these practices often leave users defaulting to the platform's settings, perpetuating cycles of engagement-driven harm and reinforcing the platforms' business models (Głowacka et al., 2023).

Similarly, a survey by Zhang et al. (2022) found that Twitter users often feel a loss of control due to content-related issues such as the authenticity, emotional tone, or appropriateness of posts in their feeds. Interface design problems, like unresponsiveness and

confusing navigation, further exacerbate frustration by making it difficult for users to manage settings or interactions effectively. Platform recommendations—such as suggested accounts, trending topics, or personalized "for you" sections—can feel overly prescriptive, steering users toward content they did not choose and amplifying the sense of being manipulated by unseen forces. Ads and promoted posts inserted into timelines can also seem intrusive, distracting users from the content they actually want to engage with (Zhang et al., 2022).

This creates a paradox of personalization: while algorithms are designed to tailor content to users' preferences, they simultaneously limit agency by pre-determining what content users see based on past behaviours and predictive analytics. As a result, users may find themselves trapped in echo chambers or exposed to content that reinforces addictive patterns, intensifies negative emotions, or undermines meaningful engagement. This interplay between time, content, and control illustrates the complex ways in which digital environments influence our mental and emotional well-being.

Given the numerous ways digital platforms exploit user attention, the question of who should regulate this exploitation and how it should be done becomes ever more pressing. As dominant tech giants continue to consolidate power in an oligopolistic digital market (Giraldo-Luque et al., 2020), it is essential to address the ethical implications of these practices to protect user well-being. In the following subchapter, I will further argue for the necessity of targeted regulatory interventions to prevent practices that strip users of their agency.

**The case for integrating digital well-being into platform regulation**

As I discussed in the previous sections, attention-driven business models present a direct conflict with user well-being, often prioritizing engagement over mental health and autonomy. This raises critical questions about accountability: How do we ensure that technological advancements serve genuine human interests, enhancing well-being rather than exploiting it? And who bears responsibility for safeguarding users—individuals themselves, tech companies, or regulatory bodies? (Annemans & Dennis, 2024).

According to scholars, the responsibility so far is placed primarily on the users, who must become increasingly digitally competent while managing their online time and presence

effectively (e.g. taking care of privacy, staying focused and productive and protecting minors) (Syvertsen, 2020, Al-Mansoori et al., 2022). Syvertsen (2020) uses the term “responsibilisation” to describe the shift towards digital and media literacy as a solution that ultimately enhances personal responsibility, instead of stricker or prohibitive regulatory approaches.

Wu (2019) discusses extensively the challenges related to platform regulation by mentioning two main legal problems, antitrust regulation, and consumer protection. First, the antitrust authorities failed to define attention economy markets and allowed mergers, even though those acquisitions aimed at eliminating competition (Facebook/Instagram, Facebook/WhatsApp and Google/YouTube mergers being the most prominent examples). As a result, we see that digital markets are concentrated and oligopolistic (Giraldo-Luque et al., 2020). By eliminating competition, tech giants can raise the prices without risk of losing users to competitors. Not only advertisement placement costs more but also the attention required by the users is higher as sponsored content is increased compared to organic content (Wu, 2019).

Secondly, Wu (2019) argues that “regulators (...) don't have a paradigm for thinking about consumer harms that are not deceptive or involve physical or financial harm, but rather arise from the seizure of attention and consequential cognitive impairments” (p. 778). He highlights the failure of regulation to protect “captive audiences”, referring to situations where the user doesn’t have the option to avoid exposure to advertising (“non-consensual and entirely uncompensated transfers of attentional resources” (p. 803)).

An additional aspect of these issues is that the effects of the attention economy on well-being are not uniform; disparities often emerge based on social, economic, and technological access. Scholars mention that this is another dimension of digital divide since the less educated and lower-income individuals may consume more digital communication and thus experience heightened challenges in managing attention and achieving digital well-being (Syvertsen, 2020, Gui et al., 2017, Nguyen, 2021). Those groups might also not have the skills, resources, and capacity to regulate their digital media consumption time on their own. In this regard, disconnecting becomes a form of privilege and fuels pre-existing social inequalities (Syvertsen, 2020).

Al-Mansoori et al. (2022) suggests that there are different levels of responsibility, shared amongst designers, tech companies, the users and societies as a whole. One approach to managing the conflict between tech innovation and well-being is to apply regulations and risk assessments across all tech companies, preventing competitive disadvantages for those who adopt such measures (Al-Mansoori et al., 2022). Wu (2019) proposes that regulators consider "attentional theft" as a form of harm, advocating for policies that protect users from non-consensual transfers of attention, especially in unavoidable digital environments (p. 803). However, Bhargava and Velasquez (2020) caution that strict regulations may not always be effective; instead, they suggest that platforms be required to design more accessible “opt-out” features to empower user choice without overly restrictive mandates.

The EU policies have historically encouraged minimal intervention for online platforms to foster innovation, relying on self-regulation instead of the stricter oversight applied to traditional media publishers. This approach began to shift in 2018 when the Audiovisual Media Services Directive (AVMSD) was extended to include video-on-demand and sharing platforms, effectively blurring the lines between traditional and digital media (Syvertsen, 2020). Additionally, ambitious regulations such as the General Data Protection Regulation (GDPR) and the most recent Digital Markets Act and the Digital Services Act aim to enhance accountability and transparency for online platforms, addressing issues related to consumer protection and harmful content.

However, these regulations still grapple with significant challenges in addressing digital well-being concerns, especially when it comes to effectiveness and enforcement. As part of the 2020 New Consumer Agenda, the Fitness Check of EU Consumer Law, launched in 2022, evaluated whether existing frameworks adequately protect consumers in the digital environment. While the report acknowledges that current laws provide regulatory certainty and foster trust in digital markets, it finds them insufficient for addressing emerging issues like addictive platform design and exploitation of sensitive data. Importantly, the report ties consumer detriment to well-being, encompassing both financial and nonfinancial harms like mental health impacts, time loss, and environmental effects. Practices like addictive design and algorithmic profiling are linked to outcomes such as anxiety, depression, compulsive buying, and physical harms from sleep deprivation and sedentary behavior. It also warns that advancements

in AI could undermine user autonomy, challenging the EU's definition of the "reasonably rational and observant" consumer. The digital environment magnifies user vulnerabilities like information overload and low bargaining power, necessitating a rethinking of the current consumer standard (European Commission, 2024c).

Notably, the report distinguishes between problematic practices and the related technologies or business models that aren't considered inherently harmful, such as targeted advertising, which is not harmful, as opposed to the exploitation of sensitive personal data for user profiling. While users are often expected to manage their digital habits, this "responsibilisation" approach neglects structural issues like monopolistic markets and the lack of protection against cognitive harms from excessive attention capture. In additional, regulatory gaps exacerbate inequalities, as less privileged groups face greater challenges in achieving digital well-being.

In the next chapter, I will explore the current approaches to platform regulation within the EU as they pertain to digital well-being. Rather than providing an exhaustive review, this analysis will focus on identifying the rationale and principles of the regulatory approaches. By critically evaluating these regulations, we can better understand their implications for digital well-being and determine whether they effectively address the needs of users in a rapidly evolving digital environment.

## Current EU regulatory approaches and digital well-being

### General remarks

In the EU, digital platform regulation seeks to balance citizens' rights with market competition and innovation (European Commission, n.d.-b). To evaluate whether this approach sufficiently safeguards digital well-being, this analysis will focus on three core regulatory areas: consumer protection, privacy, and platform regulation. These fields form the foundation of the EU's strategy to address the risks posed by digital platforms. Examining these frameworks will help assess their role in protecting users and lay the groundwork for evaluating their effectiveness in promoting digital well-being.

Key regulations in consumer protection include the Unfair Commercial Practices Directive (Directive 2005/29/EC) (UCPD) and the Consumer Rights Directive (Directive 2011/83/EU) (CRD). The UCPD establishes standards to protect consumers against misleading information, hidden costs, and unfair terms in digital services. It prohibits practices that deceive or are likely to deceive consumers, ensuring that advertising and marketing communications are clear and truthful. The CRD complements this by setting out rules for consumer contracts, particularly in online transactions, requiring that terms and conditions be presented in a transparent and accessible manner. These directives mandate that online platforms provide clear information about products and services, enabling consumers to make informed choices and seek redress in cases of unfair treatment

Privacy is another foundational element of the EU's regulatory framework for digital platforms. The GDPR, enacted in 2018, sets rules for the collection, storage, processing, and transfer of personal data. It establishes individual rights such as access, correction, deletion, and data portability, empowering users to control their personal information. The GDPR requires companies to obtain explicit and informed consent from users before processing personal data and mandates that data protection measures be integrated into all stages of data handling ("data protection by design and by default"). Lawful data processing under GDPR must meet one of six legal bases, including consent, contractual necessity, compliance with legal obligations, vital interests, public interest, or legitimate interests, ensuring that data is handled transparently and

responsibly. Non-compliance with GDPR can result in significant fines, up to 4% of a company's global revenue, making it one of the most comprehensive privacy regulations worldwide.

Complementing the GDPR, the ePrivacy Directive (Directive 2002/58/EC)—commonly referred to as the "Cookie Law"—governs privacy and confidentiality specifically within electronic communications. It includes requirements for obtaining consent before placing cookies or similar tracking technologies on users' devices. The directive applies to data processing in electronic communications, including messaging apps and email services, aiming to protect users from intrusive monitoring while promoting transparency regarding the tracking and collection of personal data. The EU is currently in the process of updating the ePrivacy Directive with the proposed ePrivacy Regulation (COM/2017/010), which seeks to modernize and expand its provisions, aligning it more closely with GDPR standards. Together, these frameworks intend to ensure that users retain control over their personal information and are protected from unauthorized data usage.

While prior internet regulations addressed data protection and privacy, the DSA and the DMA, enacted in 2022, aim to establish clearer rules and obligations specifically for online platforms, Together, the DSA and DMA are designed to address distinct but interrelated issues: the DSA primarily regulates content and user protections, while the DMA addresses market power and fair competition. This regulatory framework is intended to address a broad spectrum of concerns associated with digital services, such as illegal content, harmful online activity, monopolistic practices, and transparency.

The DSA applies broadly to digital services, including social media networks, e-commerce platforms, search engines, and other intermediaries that host, distribute, or facilitate access to digital content within the EU. Specific rules are defined for different categories of platforms, with additional obligations placed on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). VLOPs and VLOSEs are defined as platforms or search engines with over 45 million users in the EU (approximately 10% of the EU population). This threshold reflects the scale at which these platforms are considered to have a significant societal impact, including on matters of public debate and user safety (Article 33, DSA). VLOPs and VLOSEs are required to carry out yearly risk assessments to identify potential impacts on user rights, public health, safety,

and societal well-being. They must also provide detailed transparency reports and grant access to their data to regulators and researchers for compliance verification (Article 40, DSA).

The DMA complements the DSA by targeting competition issues within digital markets. It focuses on large platforms that act as "gatekeepers" in essential digital markets, such as search engines, social networks, and online marketplaces. Gatekeepers are defined based on criteria including revenue, market size, and user base, and must meet specific thresholds that classify them as critical players in the digital economy. Platforms designated as gatekeepers are subject to additional regulations to prevent anti-competitive practices and ensure fair access for smaller businesses and consumers. Key measures introduced by the DMA include interoperability requirements, data portability, prohibition on self-preferencing, ad transparency, and bans on pre-installation and default settings. These measures aim to create a level playing field, promote competitive fairness, and enhance consumer choice within the digital marketplace (DMA, 2022).

Both the DSA and DMA are accompanied by a structured compliance framework. The European Commission, in collaboration with Digital Services Coordinators (DSCs) and national regulatory bodies, monitors and enforces these regulations. Fines for non-compliance can be substantial: the DSA and DMA allow fines of up to 6% and 10% of a company’s global turnover, respectively, for severe breaches of the rules. Additionally, the Commission has the authority to conduct investigations and impose corrective measures if platforms fail to comply with the obligations set forth.

Finally, the AI Act introduces a regulatory framework aimed at ensuring the safe, transparent, and ethical development and use of AI technologies. It classifies AI systems based on the level of risk they pose, with high-risk systems, such as those impacting safety or fundamental rights, subject to strict oversight and assessment. The Act bans AI systems with unacceptable risks, like cognitive manipulation or social scoring, and mandates transparency for generative AI models. The Act is set to be fully implemented by 2026, with certain rules taking effect sooner.

Given the broad scope and impact of these regulatory responses, some overlap across multiple fields, particularly in areas such as consumer protection and privacy. Recognizing this, I

will structure my analysis under broader thematic categories to avoid redundancy and improve clarity. This chapter is organized into three sections.

First, I will examine the regulations specifically targeting online platforms under the scope of the DSA, the UCPD, and other relevant regulatory tools. In particular, I will analyze three key themes identified in the literature: addictive platform design and dark patterns, illegal and harmful content moderation, and disclosure requirements and user control tools. The DSA provisions for risk assessments will be addressed in a separate subchapter due to their applicability across all these themes. Second, I will explore digital advertising, considering its central role in the attention economy and its connection to consumer protection, data protection, as well as platform regulation. Finally, the last section will focus on the broader concept of the 'right to disconnect.' This examination will provide the foundation for an evaluation of the specific measures implemented under the current regulatory framework and their implications for safeguarding users' digital well-being that I will discuss in Chapter 5.

**Platform regulation and consumer protection**

**Addictive platform design and dark patterns.** Aggressive and manipulative platform design has been explicitly acknowledged by regulators in the EU as one of the harms associated with digital platforms and social media use. However, despite this recognition, there is considerable debate among scholars and regulators about the adequacy of the existing framework, including the recently enacted DSA, in protecting users from the impacts of addictive platform design.

The 2024 Fitness Check of EU Consumer Law Annex VI specifically addresses and analyzes the area of addictive design and gaming. The reasoning the analysis applies is supported by the literature regarding attention-capture dark patterns and the fact that platforms' interests contradict consumer well-being. However, the report concludes that the EU's regulatory approach to addictive design and attention-capture dark patterns remains limited, with no dedicated legislative framework directly targeting these practices. In particular, while EU

consumer law technically covers all transactional exchanges[2] between consumers and digital platforms—including time spent on platforms and exposure to advertising (Zardiashvili and Sears, 2023)—problematic areas like addictive design and the exploitation of consumer vulnerabilities for commercial gain are identified as the least effectively addressed issues, according to the review's survey data. Although some of the risks associated with addictive design have been recognized in the UCPD, these issues are generally treated on a case-by-case basis rather than through a comprehensive regulatory response and target mostly addictive features in gaming (e.g. loot boxes, slot machine design). This approach leaves considerable gaps, as key features like autoplay, infinite scroll, and gamification, which encourage prolonged engagement, are not uniformly addressed under current EU consumer protection law (European Commission, 2024c).

On the contrary, Esposito and Ferreira (2024) argue that the practices defined as "hyper-engaging dark patterns", should be considered unlawful under the UCPD. Articles 8 and 9 of the UCPD (prohibition of aggressive and unfair practices) categorize aggressive practices as those that involve undue influence, coercion, or harassment, significantly impairing consumers' freedom of choice and autonomy. These practices fit within this framework because they manipulate users by exploiting behavioural vulnerabilities, leading to decisions about platform usage—such as frequency and duration—that they might not have made otherwise. Beyond aggressive practices, they can also be deemed unfair under Article 5(2) of the UCPD. Even if not explicitly aggressive, these practices breach professional diligence and distort consumers'

[2]According to 2021/C 526/01, *Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market,* "A commercial practice may be considered unfair not only if it is likely to cause the average consumer to purchase or not to purchase a product, but also if it is likely to cause the consumer to, for example: enter a shop; spend more time on the internet engaged in a booking process; decide not to switch to another service provider or product; click on a link or advertisement online; continue using the service by browsing or scrolling. The UCPD does not require to demonstrate whether the consumer's economic behaviour (i.e. its transactional decision) has actually been distorted. It allows an assessment as to whether a commercial practice is 'likely' (i.e. capable) to have such an impact on the average consumer. National enforcement authorities should therefore investigate the facts and circumstances of the individual case (i.e. in concreto), but assess also the 'likelihood' of the impact of that practice on the transactional decision of the average consumer (i.e. in abstracto)" (p. 32).

economic behavior, such as influencing how much time they spend on a platform (Esposito & Ferreira, 2024).

According to the authors, the DSA and the AI Act rather complement the UCPD in this type of dark patterns. More specifically, platform regulation under the DSA introduces some prohibitions on manipulative interface designs. Article 25(1) of the DSA specifically bans practices that distort users' ability to make autonomous and informed decisions, defining “dark patterns” as manipulative design choices that limit user autonomy by nudging them toward unwanted actions. However, whether attention-capture elements fall under this prohibition remains unclear, leaving a gap for addictive design features that may not be overtly deceptive but still exploit psychological vulnerabilities. Also, while the DSA obligates platforms to evaluate and mitigate risks from such patterns, it explicitly defers to the UCPD for defining unfair practices. The AI Act, meanwhile, introduces provisions addressing manipulative AI systems that exploit cognitive vulnerabilities, potentially classifying “hyper-engaging dark patterns” as unacceptable risks under its framework (ibid.)

The most direct response to the risks posed by addictive platform design has been put forward by the European Parliament’s Committee on the Internal Market and Consumer Protection in October 2023 (2023/2043(INI). The Committee also recognized the DSA as insufficient and proposed more concrete measures to address addictive design, emphasizing that techniques like infinite scrolling and autoplay, which effectively monetize prolonged user engagement, should be more rigorously regulated under the UCPD. The proposal includes introducing a “right not to be disturbed” by digital platforms and setting ethical design guidelines, such as limiting notifications, allowing for grayscale viewing, and implementing chronological feeds to reduce screen time. These recommendations place particular emphasis on protecting minors, who are more susceptible to the psychological effects of prolonged platform engagement, with concerns over long-term consequences such as stress, cognitive decline, and burnout. Nevertheless, interventions similar to those in place for industries like food, alcohol, and tobacco haven’t been adopted yet.

Overall, the EU’s current regulatory framework addresses certain aspects of addictive design and dark patterns through the DSA and UCPD, but significant gaps remain. The existing

frameworks primarily focus on overtly deceptive practices and minor-specific protections, leaving addictive features like autoplay and infinite scroll in a gray area of illicit commercial practices. Without a unified approach and concrete definitions, regulators may continue to rely on lengthy, case-by-case proceedings to address these practices in online platforms.

**Illegal and harmful content moderation.** Content moderation requirements for VLOPs is one of the main pillars of the DSA. Effective content moderation reduces users' exposure to harmful material, distressing imagery, and illegal content online. Recognizing the risk posed by unregulated content to society at large, the recent digital platforms regulation imposes greater responsibilities on intermediaries to moderate content and protect vulnerable groups, particularly minors.

The DSA redefined platform responsibilities, building on and addressing the limitations of the earlier E-Commerce Directive (Directive 2000/31/EC). The E-Commerce Directive had introduced the "safe harbor" principle, which exempted platforms from liability for illegal content, provided they acted as neutral intermediaries and removed such content expeditiously once notified. It also shielded "mere conduit" and "caching" services from liability and prohibited imposing general monitoring obligations on platforms. However, as the digital landscape evolved, these provisions proved insufficient to address the challenges posed by large online platforms, such as the dissemination of harmful content and the systemic risks linked to their operations. The DSA retains some aspects of the liability exemptions and the prohibition of monitoring obligations but expands platform responsibilities, especially when it comes to transparency obligations, accessible notice mechanisms and justifications for content removal (Galli et al., 2023).

Under DSA Article 16, platforms are required to implement systems that allow users to report illegal content efficiently. Once flagged, platforms must act swiftly to address the reported material, ensuring harmful content is removed or restricted in a timely manner. The DSA encourages collaboration with trusted flaggers—experts or organizations proficient in identifying illegal or harmful content. These entities assist platforms in swiftly and accurately moderating problematic material (Article 22, DSA). In addition, platforms are encouraged to adopt voluntary codes of conduct, raising their moderation standards beyond the DSA's minimum requirements

(Article 45, DSA) and are required to adopt enhanced moderation measures to counter the spread of disinformation and harmful content in times of crisis (Article 48, DSA). Various other measures are also established to ensure transparency and fairness, such as obligation to inform the affected user (Article 17, DSA), offering options to appeal a content moderation decision (Article 20, DSA) and safeguarding the reporting systems against abuse (Article 23, DSA).

Complimentary to this approach is the updated AVMSD, which was originally designed to regulate traditional television broadcasting. It was extended in 2018 to include video-on-demand and video-sharing platforms as part of a broader effort to address the evolving digital landscape. This expansion, formalized through amendments to the directive, ensures that platforms like YouTube, Netflix, and other online video services are subject to similar rules and regulations as traditional broadcasters. The AVMSD now covers a wider range of audiovisual content, including user-generated content, to ensure a consistent approach to issues such as the protection of minors, and the prevention of harmful content (like hate speech and disinformation). By bringing these platforms under the same regulatory umbrella, the EU aims to create a more level playing field and enhance user protection across both traditional and digital media services.

Yet, scholars identify several gray areas in the content moderation obligations for VLOPs related to the lack of concrete definitions for hate speech and disinformation. While the DSA outlines illegal content broadly, including hate speech, it does not provide specific guidance on what constitutes hate speech, leaving platforms with limited clarity on how to comply with its provisions. The absence of a uniform definition means that platforms may rely on their own interpretations or existing frameworks, such as the Code of Conduct on Countering Illegal Hate Speech, which itself is based on previous EU legal instruments. This ambiguity can lead to inconsistent application of content moderation policies, with platforms potentially over-moderating content to avoid liability, which could infringe on freedom of expression (Enarsson, 2024). A similar challenge is posed in the moderation of disinformation as so far efforts to counter disinformation have relied on platforms self-regulation (Fahy et al., 2022).

In compliance with the DSA, the content moderation decisions of VLOPs are now public and available to researchers. Some early empirical findings support the above-mentioned reservations. For instance, a study by Drolsbach and Pröllochs (2024) highlights significant

disparities in content moderation practices across major social media platforms, with TikTok performing far more moderation actions per user than platforms like X. While all platforms consistently address violent and pornographic content, their focus on other rule-breaking content, such as illegal speech and misinformation, varies.

Additionally, platforms differ in their responses to violations, with some prioritizing content removal and others reducing its visibility, as well as, in the use of automation. While most platforms rely on automated systems to detect and process violations, platforms like TikTok predominantly use automation, while X relies entirely on manual methods despite moderating less content overall. This variation underscores the challenges of scaling moderation efforts to meet the DSA's requirements, suggesting that some degree of automation may be essential for compliance across the EU (Drolsbach & Pröllochs, 2024). These inconsistencies reflect varied interpretations of the DSA, which could undermine its goal of establishing uniform moderation standards.

Considering that all platforms identified as VLOPs under the DSA, already have notice, content moderation mechanisms and community standards in place, it can be argued that the DSA doesn’t bring significant novelty in this field. The emphasis on transparency and fairness mandated in these provisions, especially in the DSA, highlights the power these platforms hold to decide which voices are heard online and which are restricted (by e.g. shadow banning). Rather than imposing specific rules and requirements on content moderation practices, the DSA aims to ensure that content moderation does not disproportionately affect certain users or unjustly suppress lawful content, limiting fundamental rights like the freedom of expression and freedom of the media.

**User control tools and disclosure requirements.** Considering the level of personalization of recommender algorithms and vast information asymmetries between platforms and users in the digital economy, user empowerment is another area addressed by the platform regulation in the EU. Content disclosure requirements and user control tools are strategies aiming at ensuring transparency and empowering users and consumers online. The DSA, and the AI Act establish obligations for platforms to disclose information about advertisements, algorithmic decision-making, and AI-generated content and provide alternatives that are not based on profiling.

The DSA introduces provisions aimed at enhancing user control over recommender systems, particularly under Articles 27 and 38, which focus on transparency and non-profiling-based alternatives. Article 27 requires platforms to clearly explain, in accessible language, the main parameters of their recommender systems, including how users can modify or influence these parameters. Article 38 mandates that VLOPs and VLOSEs offer at least one option for recommendations that is not based on user profiling. In addition, under Article 26 of the DSA, platforms are required to provide clear and accessible disclosures for all digital advertisements. Users should be able to easily recognize when content is a paid advertisement, identify the sponsor, and understand why it was targeted to them. This transparency prevents covert advertising practices that often manipulate user behavior, especially among vulnerable groups such as minors. Similarly, the AVMSD extends disclosure obligations to video-sharing platforms, requiring them to inform users about sponsored or harmful content and implement mechanisms to protect minors from exposure to unregulated media.

Moreover, the AI Act underscores the importance of transparency in AI systems, particularly those generating content. Article 50 mandates that users be informed when they interact with AI-created or significantly altered content, unless the nature of the content makes it self-evident. This provision seeks to counteract the risks associated with deceptive AI-driven practices, such as deepfakes or algorithmically optimized content designed to elicit emotional reactions. Disclosure of AI-generated material could help users critically evaluate the authenticity of what they encounter online, reducing susceptibility to manipulated or unrealistic representations.

In an effort to reduce the lock-in effects of dominant platforms, the DMA introduces several provisions designed to enhance consumer control over their data and ensure fair practices by gatekeepers. Article 5(2) specifically prohibits gatekeepers from processing or combining personal data for online advertising without explicit consumer consent, addressing privacy concerns. Additionally, the DMA mandates data portability, allowing users to transfer their data easily between platforms, and enforces interoperability, preventing gatekeepers from blocking third-party applications. It also bans self-preferencing in rankings, ensuring consumers receive fair access to services. Articles 6 and 7 further promote consumer choice by mandating

fair access to business data and ensuring interoperability between messaging services. Finally, Article 15 restricts the use and combination of personal data across services without consumer consent, protecting privacy and preventing misuse for targeted advertising.

However, critics argue that the implementation of these requirements has so far focused only on transparency rather than true user empowerment. While platforms like Facebook, Instagram, and TikTok now provide non-personalized feed options, such offerings often lack meaningful customization features. A genuinely user-centered approach would go beyond these basic functionalities to include dynamic controls, enabling users to adjust the degree of personalization, choose recommendation parameters, and provide explicit feedback on their preferences. Additionally, advanced features like personalization resets or multiple user profiles could help mitigate filter bubbles and encourage diverse content exposure. Despite these possibilities, platforms may resist granting full user control, given the potential impact on their business models. Consequently, while the DSA provides a foundation for greater user agency, its practical success depends on enforcing and expanding these requirements in ways that balance regulatory objectives with platform constraints (Reviglio & Fabbri, 2024).

So far, some limited empirical studies indicate that the user control functionality doesn't work in a way that really protects users from exposure to unwanted content. The Panoptykon Foundation's case study, *Algorithms of Trauma #2* (2023), examined Facebook's recommender system and evaluated the effectiveness of its explicit feedback tool designed to give users control over their feed. The research focused on a user who reported frequent exposure to distressing content, including posts on health issues, accidents, and deaths, in the "Suggested for You" section. Alarmingly, the number of distressing posts slightly increased following the user's feedback. The study raises concerns about whether such ineffective feedback mechanisms align with the obligations under the DSA, particularly Articles 27(3), 25, and 35, which mandate adequate mitigation measures and user empowerment tools for VLOPs.

Another study on TikTok's algorithmic transparency concludes that the platform is not fully compliant with the obligations outlined in the DSA. While the DSA emphasizes the need for platforms to disclose the most important criteria behind content recommendations and the reasons for their significance, TikTok's explanations remain largely generic. The platform does

not adequately clarify the factors influencing recommendations or their relative importance. This gap highlights the necessity of greater collaboration between social media platforms, regulators, and users to ensure that recommendation systems are explained in a way that aligns with regulatory requirements and is accessible to users (Mousavi et al., 2024).

To summarize, the EU's regulatory efforts, including the DSA, AI Act, and DMA, aim to enhance transparency and user empowerment in digital platforms through disclosure requirements and control tools. By mandating clear explanations of recommender systems, non-profiling-based alternatives, and transparent advertisement disclosures, these frameworks seek to bridge the significant information asymmetries between users and platforms. Provisions like interoperability, data portability, and restrictions on personal data misuse further aim to strengthen consumer autonomy while addressing privacy concerns.

However, critics highlight that existing tools, such as non-personalized feeds or feedback mechanisms, often fall short of providing meaningful control, leaving users exposed to unwanted or distressing content. Reviglio and Fabbri (2024) argue that "unless users can meaningfully shape their online experiences, the DSA risks falling short of its objective of making recommendations transparent and controllable for users." Nevertheless, implementing such features poses challenges to the financial incentives underpinning current social media platforms, which could hinder the enforcement of these provisions.

**Risk assessments.** As noted earlier, the DSA establishes an extensive framework for addressing systemic risks posed by VLOPs, acknowledging the substantial impact these platforms have on the broader societal well-being. Article 34 mandates that VLOPs perform detailed risk assessments to identify and address systemic risks linked to their operations. These assessments must consider practices that may lead to 1) the dissemination of illegal content, such as hate speech or misinformation, 2) adverse effects on fundamental rights, including privacy and freedom of expression, 3) wider societal risks, such as threats to public health or democratic processes, and 4) harmful consequences for individuals' physical and mental health.

According to scholars, the new approach to risk assessments in the DSA represents a shift from individual rights-based remedies to a broader, systemic approach to regulating online platforms. Unlike the traditional focus on individual complaints and remedies, systemic risk

assessments require platforms to evaluate and mitigate the wider societal harms of their content moderation practices, such as the amplification of harmful content, the design of recommender systems, and their impact on areas like civic discourse, public health, and democratic processes. This approach acknowledges that many harms extend beyond individual rights violations and affect the public at large, including non-users of platforms. By shifting responsibility from individuals to the state, the DSA aims to hold platforms accountable for systemic risks in a manner similar to how governments regulate other industries for public safety. However, uncertainty remains about how these assessments will be enforced and whether they will be effective, as the details of the implementation process are still unfolding, with the first reports expected in late 2024[3] (Eder, 2024).

Currently, the European Commission has issued formal requests for information to Meta, Temu, YouTube, Snapchat, and TikTok to gather details on the operation and design of their recommender systems. YouTube and Snapchat were specifically asked about the parameters used by their algorithms to recommend content, including their potential to induce addictive behaviours or amplify harmful content, as well as measures to address risks for minors (European Commission, 2024b). Even though digital well-being is not clearly defined in the DSA provisions, the Commission's formal requests indicate that addictive design is addressed as a serious harm. Following the risk assessment, Article 35 requires VLOPs to implement risk mitigation measures tailored to the identified harms. For digital well-being, this might include reducing addictive design features and adjustments to content recommendation algorithms.

However, researchers have identified several limitations in the DSA's risk assessment framework that could undermine its effectiveness. The enforcement of these assessments is seen as critical yet challenging. While the DSA encourages a coalition of experts to enhance scrutiny and accountability, platforms retain considerable influence in framing systemic risks and shaping benchmarks for assessments as they can set the agenda and drive the conversation around features that don't threaten their business model. Additionally, there are concerns that the publicly accessible reports will be overly generalized or heavily redacted under DSA Article 42(5) confidentiality provisions, limiting meaningful analysis by researchers and civil society (Jóźwiak,

[3] The risk assessments have not been published yet at the time of writing this essay.

2024).

For instance, Fahy et al. (2022) discuss the case of systemic risks related to the dissemination of disinformation. Under Article 26, platforms are required to identify and mitigate risks arising from their algorithms and operations. Disinformation can be classified as a systemic risk in cases where it violates national laws, undermines fundamental rights such as human dignity, or disrupts civic discourse, electoral integrity, or public security. Despite these provisions, enforcement poses challenges. Platforms are tasked with conducting their own risk assessments and implementing mitigation measures under Article 27. However, proving that disinformation has tangible negative effects often falls to auditors and the European Board for Digital Services, which face difficulties in establishing clear metrics for such impacts. This leaves significant room for interpretation, potentially allowing platforms to resist robust intervention against disinformation.

In conclusion, the DSA's risk assessment framework represents a shift towards addressing systemic risks posed by dominant digital platforms, focusing on broader societal harms rather than just individual rights violations. By mandating platforms to evaluate risks such as disinformation, algorithmic amplification of harmful content, the framework aims to promote accountability and safeguard public well-being. However, its effectiveness depends on rigorous enforcement, which faces challenges like platform influence, limited transparency, and difficulties in defining and measuring harm. While the approach sets a strong foundation for mitigating systemic risks, its success will depend on overcoming these implementation hurdles.

## Digital advertising regulation

**Consumer and data protection.** Digital advertising is a cornerstone of the online economy, yet it raises significant regulatory challenges due to its reliance on extensive data collection and its potential to exploit consumer vulnerabilities (Cappello, 2022). The EU, so far, attempted to address these concerns through a dual regulatory approach, encompassing consumer protection and data protection frameworks, both of which aim to balance economic innovation with the safeguarding of individual rights. At the same time, NGOs and advocacy groups call for stricter regulation of the advertising-based business model of digital platforms. As Nathalie Maréchal (2022) remarked, “We can’t govern the internet without governing online advertising”.

The European Court of Human Rights addresses advertising through the lens of Article 10 on freedom of expression, permitting limitations when necessary to protect consumers, minors, public health, or democratic processes (Fahy, 2022). In EU law, the consumer is considered to be a weaker party that requires special protection from unfair practices but legislators make the assumption that consumers who are informed will make informed choices. The UCPD specifically targets business-to-consumer relationships, prohibiting practices that distort consumers' economic behavior. Article 5(2) of the UCPD defines unfair practices as those that violate professional diligence standards and materially mislead or influence the average consumer's economic decisions. This includes both "misleading" and "aggressive" practices, which can deceive or pressure consumers into making decisions that are not in their best interests (Zardiashvili & Sears, 2023). Additionally, sector-specific rules in AVMSD bans advertising of alcohol, tobacco and medical products and imposes disclosure of sponsorships and product placement (Fahy, 2022).

Targeted advertising in particular is regulated under both consumer law, which governs advertising as a commercial activity, and data protection laws, such as the GDPR, due to the personal data involved in creating user profiles. However, as Zardiashvili and Sears (2023) note, while both frameworks theoretically carry equal weight, in practice, privacy rights are easier to enforce than consumer protection rights, which remain largely “aspirational”. The ePrivacy Directive complements the GDPR by focusing on data collected through user devices, such as

cookies and tracking technologies, requiring explicit consent before data collection, and regulating direct marketing communications like emails and automated calls.

The GDPR is designed to protect personal data and addresses several risks tied to targeted advertising, such as algorithmic discrimination and lack of transparency. With its principles of "privacy by design and by default," the GDPR mandates that data processing prioritize user privacy. Any data processing, including consumer profiling and automated decision-making for advertising, must be lawful—either based on user consent, a necessity or legal obligation, or the "legitimate interests" of the data controller, provided it doesn't infringe upon the fundamental rights of individuals. GDPR's guidelines on "legitimate interests" create a nuanced framework; although a company may argue that personalization and targeted advertising serve legitimate economic interests, these activities require user consent if they involve automated profiling. Consent under GDPR must be informed, specific, and offer the user the right to refuse without negative consequences (Tzoulia, 2021).

Despite being in force for eight years, the GDPR is often considered insufficient in addressing user autonomy concerns, as highlighted in the Consumer Law Fitness Check. The review found that users consider monetization not to be fair, as well as, not feeling "fully in control of the decisions they make or the content they are shown online" (p. 21-22), underscoring a significant limitation in consumer autonomy.

One limitation of the GDPR is its reliance on the notice-and-consent model, assuming users are informed and capable of making deliberate privacy decisions. This assumption is challenged by information overload and lengthy, complex privacy policies that discourage scrutiny. Instead, users tend to prioritize convenience over privacy concerns, often accepting terms without fully understanding the implications (Galli, 2022). Moreover, Galli (2022) argues that declining consent often feels impractical or impossible for users. In many cases, refusing to agree to data collection means foregoing essential online services, effectively rendering consent a formality rather than a genuine choice. This dynamic is exacerbated in environments dominated by quasi-monopolistic platforms or widespread reliance on invasive data practices. As a result, the notice-and-consent mechanism has evolved into a transactional model where privacy becomes a commodified trade-off for accessing digital services. Rather than curbing surveillance,

this model perpetuates and normalizes the exploitation of personal data, leaving consumers in a precarious state of digital vulnerability.

Further complicating the issue is the lack of a legal requirement for platforms to disclose the value derived from users' personal data. While the UCPD states that "free" services should not involve data exchange, the European Commission acknowledges that even actions like scrolling a feed can represent a transactional choice, further highlighting the inherent exchange involved in data-based services (Zardiashvili & Sears, 2023). Paradoxically, under current consumer protection law, the exchange of personal data for services is tied to unfair commercial practices, though data itself is not legally considered a commodity. The Digital Services Directive supports this by framing personal data sharing as transactional, unless required for contract fulfillment or legal obligations. However, the GDPR emphasizes that data provision for targeted advertising should never be a prerequisite for accessing digital services or content. Van De Waerdt (2020) argues that the reality of the data-driven business models overturns the good intentions of data protection law, so the question of adequate consumer protection in an environment characterized by vast information asymmetries still remains.

The UCPD could also play a role in addressing aggressive advertising practices, particularly in the context of unsolicited commercial communications. The directive considers persistent advertising that disregards consumer opposition as *per se* unfair under Annex I, point 26. This is especially relevant in the context of freemium services, where the volume and repetition of ads may overwhelm consumers, infringing on their "right to be let alone" as emphasized by the ePrivacy Directive (2002/58/EC). Such practices are deemed aggressive if they disturb the consumer to a degree that influences their transactional decisions—such as opting for paid versions of services simply to escape constant disruptions. Even when practices do not meet the *per se* threshold, they may still violate Articles 8 and 9 of the UCPD if the sheer volume or timing of communications unduly pressures consumers, undermining their economic autonomy (Tzoulia, 2021).

However, the absence of a concrete regulation addressing the frequency and aggressiveness of digital advertising could be attributed to the complexities of the online advertising ecosystem, where programmatic advertising systems dynamically adapt to user

behavior in real time, making uniform frequency caps challenging to implement. Additionally, unintended side effects could arise from these limitations. Platforms might respond by increasing the intrusiveness or length of individual ads to compensate for reduced frequency, potentially worsening user experience, in the absence of strong competition (Henriques, 2020). Alternatively, subscription-based models might become more prevalent, creating financial barriers to accessing digital content, especially for users who cannot afford such options.

The EU's approach to consumer and data protection in digital advertising seeks to balance economic innovation with safeguarding individual rights, but significant challenges remain. Consumer protection laws like the UCPD and data protection frameworks such as the GDPR aim to mitigate the risks of targeted advertising, including unfair practices, privacy violations, and algorithmic discrimination. However, enforcement disparities, information asymmetries, and the limitations of the notice-and-consent model hinder user autonomy. The commodification of privacy and the transactional nature of personal data exchange highlight the inadequacy of existing regulations in addressing aggressive advertising practices and protecting consumers from digital exploitation. Despite progress, achieving genuine consumer empowerment requires addressing these systemic shortcomings.

**Digital advertising in platform regulation.** The DSA introduces some additional provisions related to digital advertising; Recital 68 of the DSA specifically recognises risks related to online advertising such as the promotion of illegal content or activities and discrimination of consumers and citizens. The DSA thus introduces additional transparency obligations. Platforms should provide to users clear and accessible information whenever an advertisement is presented about 1) the identity of the advertiser, 2) the criteria used to target the ad, including whether profiling was used and, if so, the basis of such profiling (e.g., behavioural or contextual targeting) and the option to opt-out of personalized advertising, enabling users to switch to more neutral forms of advertising. Additionally, the DSA prohibits the use of sensitive personal data for profiling and targeted advertising. This includes data revealing racial or ethnic origin, political opinions, religious beliefs, or sexual orientation, aligning with GDPR's principles on sensitive data (Article 26, DSA).

VLOPs, given their outsized impact on the digital ecosystem, are subject to heightened

responsibilities. Under Article 39 of the DSA, VLOPs must maintain and publish a repository of all advertisements displayed on their platforms. This repository should include information about the content of the ads, the targeting parameters used, and the duration of their display. Such transparency facilitates independent risk assessments and studies, enabling regulators and researchers to identify potential systemic risks, such as the amplification of harmful content or patterns of discriminatory ad distribution Finally, VLOPs should assess the systemic risks stemming from their advertising system under Article 34(2).

The DSA regulation on advertising is complemented by DMA and AI Act provision on targeted advertising. Article 5(2) of the DMA prohibits gatekeepers from processing user data for advertising purposes across third-party services without explicit consent and bans the combining and cross-referencing of data from different services unless consent is obtained. The AI Act further complements these efforts by addressing the manipulative potential of advertising practices driven by AI algorithms. Article 5(1)(a) of the AI Act considers behavioural advertising that exploits consumers' decision-making vulnerabilities as potentially harmful, emphasizing its role in manipulating economic decisions against consumers' best interests. Zardiashvili and Sears (2023) note that these measures, alongside the DSA's restrictions and the judgment in *C-184/20* regarding sensitive inferences, could lead to heightened scrutiny of behavioural advertising practices as a whole, but overall, there is no hard ban of targeted advertising introduced in platform regulation.

According to Buri (2022), the regulation of internet advertising has been a controversial topic during the DSA negotiations and the DSA stops short of adopting stricter measures proposed during the legislative process. The European Parliament had expressed significant concerns about the societal risks associated with behavioural advertising and micro-targeting, which rely on pervasive user tracking. These practices, often linked to the business models of major online platforms, were criticized for contributing to societal issues such as disinformation and discrimination. The Parliament advocated for more stringent regulations, including a phased ban on behavioural advertising in favor of less intrusive contextual advertising. However, these proposals were ultimately not adopted in the final text of the DSA (Zardiashvili & Sears, 2023).

Moreover, the European Commission's choice to focus on transparency rather than

imposing stricter restrictions on advertising systems has been questioned by scholars. As Buri (2022) notes, the Commission did not provide a detailed justification for why transparency alone was deemed the most effective tool to address the harms of online advertising, despite acknowledging these harms in various provisions and recitals. One possible explanation is that the Commission believed such issues would be better addressed through existing frameworks like the GDPR or the forthcoming ePrivacy Regulation. Another consideration may have been the potential economic impact on small and medium-sized enterprises, which depend on targeted advertising systems for their outreach and operation (Corporate Europe Observatory, 2022).

Another limitation highlighted by Goanta (2022) is the DSA's scope, as it doesn't address the evolving landscape of social commerce, and it doesn't fully account for platforms that combine social networking and marketplace functions, such as Instagram. The DSA's scope excludes key transparency and compliance obligations for platforms facilitating consumer transactions, leaving influencers—who act as traders under European consumer laws—subject to fragmented national enforcement rather than a cohesive EU framework. Furthermore, the DSA narrowly defines advertising to include only platform-mediated remuneration, excluding off-platform influencer marketing. This regulatory gap prevents the DSA from effectively addressing many challenges of influencer-driven commerce, while also placing the burden of compliance on individual influencers rather than the platforms that facilitate these transactions (Goanta, 2022).

In practice, the response of platforms to the new restrictions are somewhat controversial. The most prominent example is Meta's decision to introduce a subscription fee in exchange for ad-free services in Europe from November 2023. The European Data Protection Board (EDPB) has, as a response, expressed strong reservations about "consent or pay" models used by large online platforms. It considers that these models generally fail to meet the GDPR's requirements for valid consent when users are forced to choose between consenting to data processing for behavioural advertising or paying a fee.

According to the EDPB, offering only a paid alternative should not be the default approach. Instead, platforms should explore offering a free option that does not rely on behavioural advertising, such as forms of advertising that use minimal or no personal data. Platforms must avoid creating scenarios where individuals feel compelled to consent due to high

fees, negative consequences, or imbalances of power. These imbalances can be particularly significant given the market dominance of large platforms and users' reliance on their services. The EDPB underscores that the right to data protection should not be commodified, and users must fully understand the implications of their choices (European Data Protection Board, 2024). One year later (November 2024) Meta announced a lower subscription fee and an additional option for the users to use Meta's services without personalized ads that will be, however, unskippable (Meta, 2024). These developments highlight that the DSA obligations are still being fine-tuned and the big players try to bypass their obligations.

The DSA introduces important provisions for digital advertising, emphasizing transparency and user control. It requires platforms to disclose key information about ads and prohibits the use of sensitive personal data for advertising purposes. However, the DSA stops short of adopting stricter regulations, such as a ban on behavioural advertising, despite concerns over societal risks like disinformation and discrimination. The focus on transparency, rather than stricter bans, has been critiqued, and gaps in regulation, especially regarding influencer marketing and social commerce, might limit the DSA's effectiveness.

**The right to disconnect**

The right to disconnect has emerged as a necessary safeguard due to the increasing intrusion of work into employees' personal time, facilitated by constant connectivity through electronic communication. In the past, it was rare for employees to be contacted outside working hours, but today, many are routinely expected to respond to emails and calls after work, on weekends, and during holidays. This shift is partly driven by the pressure for prompt responses, which is often linked to higher productivity and career advancement. As teleworking has become more common, especially following the COVID-19 pandemic, the lines between professional and private lives have blurred, making the right to disconnect crucial for maintaining a healthy work-life balance and protecting employees from overwork (European Law Institute, 2023).

The challenge of blurred boundaries arises from the ways digital technologies merge work, home, leisure, and travel domains. This overlap can lead to privacy breaches, reduced quality of life, online harassment, and strained social relationships as work increasingly

encroaches on personal time. Public policy could play a key role in addressing these risks. For instance, France's 2017 "right to disconnect" law requires larger companies to establish policies that limit work-related communications outside office hours. Although these legal measures aim to alleviate the effects of constant connectivity, their enforcement remains difficult. Complementary strategies, such as voluntary codes of conduct, anti-harassment policies, and support for workers facing internet addiction, are necessary to address the broader implications of work-related internet use (Brey et al., 2016).

Recognizing these challenges, the European Parliament adopted a resolution in January 2021 (European Parliament, 2021a) urging the European Commission to propose legislation ensuring the right to disconnect. Defined as the ability of workers to disengage from digital tools outside working hours without repercussions, this right aims to address health risks, disruptions to work-life balance, and unpaid overtime caused by constant connectivity. The resolution called for measures to protect workers, implement complaint mechanisms, and ensure remote training is appropriately compensated. Applying to both public and private sectors, the proposed directive would require employers to uphold and communicate these rights. In response, the European Commission launched a consultation with social partners in April 2024 to explore further actions on telework and the right to disconnect, informed by recent studies and ongoing digitalization trends (European Commission, 2024a).

As telework continues to grow, its flexibility comes with challenges, like the "always-on" culture that erodes the boundaries between work and personal life. As Syvertsen (2020) points out, these platforms often blur the line between professional and private time, making it even harder to maintain a clear separation. This highlights the need for coordinated action at the EU level, especially since regulating non-work digital platforms adds another layer of complexity.

## Discussion

### Assessing the framework: strengths and limitations of digital well-being regulation

As highlighted in the literature, digital well-being is inherently subjective, shaped by the diverse preferences and experiences individuals have with technology. What one person finds beneficial or fulfilling, another might perceive as harmful or distracting. This variability, combined with the lack of empirical consensus on broader social media harms, makes regulating digital well-being particularly challenging. However, the literature converges on a common principle: enhancing user autonomy and control. By empowering users with tools to shape their digital experiences, a sense of well-being can be fostered without imposing restrictive measures that could infringe on basic human rights, such as freedom of expression.

To evaluate the strengths and limitations of the current EU regulatory framework in safeguarding users' digital well-being, I will examine the two dimensions of control outlined in Section 2.1: 1) control over the time spent online, and 2) control over the content encountered. Through this lens, I will analyze how the regulatory responses discussed in Chapter 3 address these specific digital well-being challenges, with a particular emphasis on empowering users to manage their digital experiences effectively.

**User control over the time spent online.** The concept of "time displacement," as defined by Vanden Abeele et al. (2024), refers to how digital platforms affect users' time allocation, often reducing time for activities like studying, socializing, or sleeping. This is closely linked to "addictive by design" platforms that use attention-capturing dark patterns such as endless scrolling, autoplay, and tailored recommendations to prolong user engagement. These features often lead to extended platform use beyond users' intentions, resulting in feelings of guilt or frustration over "wasted time." Regulatory efforts addressing addictive design, dark patterns, and risk assessments under the DSA, and the UCPD are relevant to tackling time displacement.

Although addictive design and dark patterns are recognized in legal texts, current regulations like the DSA and UCPD mainly focus on overtly deceptive practices, leaving gaps in protecting users from subtle features like autoplay and infinite scroll, which contribute to prolonged time spent online. While the EU acknowledges the harms, including effects on well-

being, the regulatory response is fragmented. The DSA's prohibition on manipulative designs and the UCPD's focus on aggressive practices don't fully address the subtle manipulation that drives time displacement. Additionally, despite recognizing the need to protect vulnerable groups like minors, no comprehensive approach exists to address addictive design across platforms for the general population.

Risk assessments under the DSA could also address this problem by identifying and mitigating the risks associated with addictive platform design, provided the impact on mental health, social interactions, and productivity is considered a broader societal harm. However, the lack of clear, enforceable guidelines could result in insufficient mitigation of time displacement-related harms. Early analyses suggest platforms have significant influence over how risks are framed, raising concerns that they may downplay risks tied to features like autoplay and infinite scroll, which foster prolonged engagement. The European Commission's requests for information on recommender systems, including addictive behaviors and impacts on minors, indicate a focus on these risks, but concerns over transparency and the limited scope of current measures may hinder progress. With the DSA still unfolding, and the first reports expected in late 2024, it remains uncertain how effectively it will address addictive design.

Another dimension of diminished control over time is "boundary blurring" (Vanden Abeele et al., 2024) a harm stemming from constant digital connectivity. Digital media enable individuals to simultaneously manage multiple roles—such as being a parent, worker, and friend—leading to conflicting demands and challenges in maintaining a healthy work-life balance. The expectation to be "always on" often creates pressure to respond immediately, especially to work-related messages, exacerbating stress and reducing personal time. While strategies such as disabling work email notifications can help mitigate these pressures, some roles require continuous availability, making boundary blurring a complex issue to address. Initiatives like the "right to disconnect" may offer a potential solution by setting clear boundaries at least when it comes to work-related communication and helping individuals reclaim their personal time.

In particular, the right to disconnect can help address boundary blurring by providing employees with a legal safeguard against the encroachment of work into their personal time. As digital connectivity increasingly enables constant communication, workers face mounting

expectations to respond to emails, calls, and messages outside traditional working hours, further blurring the lines between work and personal life. By allowing employees to disengage from work-related digital tools without fear of reprisal, the right to disconnect aims to prevent overwork, reduce stress, and safeguard personal time.

The European Parliament's 2021 resolution and the Commission's 2024 response highlight the need for comprehensive measures to address boundary blurring, particularly with the rise of telework and workplace digitalization. However, as discussions continue, there is no clear indication of how the right to disconnect will be enforced or its potential scope, if implemented at all. Overall, due to its subjective nature, boundary blurring—especially between other roles, such as parent and professional—may not be suitable for universal regulation at all. Nevertheless, the meaningful implementation of other user control and autonomy measures discussed in this chapter could potentially help users better separate different spheres of their lives by reducing distractions and limiting their time on digital platforms according to their needs and preferences.

Overall, clear, standardized measures—such as limits on engagement features and tighter regulation of recommendation algorithms—will be crucial for ensuring meaningful interventions. The European Parliament’s 2023 proposal to regulate techniques like infinite scrolling and autoplay is a step forward, but without a unified framework, addictive platform design so far is still largely discussed rather than effectively addressed. Despite some positive developments, the current EU framework does not fully enable user control in this area yet.

**User control over the content encountered online.** Social media platforms, while fostering connectivity and self-expression, also expose users to significant mental and emotional challenges. These include social comparison, which can diminish self-esteem; cyberbullying, linked to stress, anxiety, and depression; and technostress, arising from the constant pressure to stay engaged online. Additionally, digital distraction is a pervasive issue, with the relentless flow of notifications, advertisements, and algorithmically amplified content disrupting focus and causing cognitive overload. To protect their well-being, users often employ strategies like unfollowing harmful accounts, curating content, or deleting platforms entirely—though these actions may inadvertently lead to social isolation (Vanden Abeele et al., 2024).

Content moderation practices play a crucial role in addressing exposure to harmful content, particularly by reducing users' exposure to distressing material that can negatively affect their mental and emotional well-being, as well as, the dissemination of illegal content. User control tools and transparency provisions could also help empower users to manage their exposure to undesirable content. Under the DSA, platforms must implement systems for reporting illegal and harmful content, ensuring prompt action is taken. The DSA also encourages collaboration with trusted flaggers and adoption of voluntary codes of conduct to raise moderation standards, reducing harmful content like hate speech and disinformation.

When it comes to regulating digital distraction, regulatory interventions in privacy, advertising and user control tools are particularly relevant. Privacy frameworks such as the GDPR and the ePrivacy Directive aim to limit data-driven profiling and targeted advertising by restricting the collection and use of personal data. Additionally, they enhance user control, requiring platforms to implement transparent consent mechanisms and provide users with tools to manage their data and, more recently, their social media feeds. Consumer protection regulations complement these efforts by addressing the placement, and transparency of ads. The DSA brings some novelty in this field, by requiring platforms to disclose the parameters of recommender systems (Article 27 of the DSA), offer non-profiling-based recommendation options (Article 38), and clearly label advertisements so users can identify paid content and understand why it was targeted to them (Article 26).

However, despite this progress, several challenges remain. The lack of clear definitions for terms like hate speech and disinformation in the DSA creates ambiguity, leaving platforms to interpret these terms on their own. Additionally, while platforms offer some control, such as non-personalized feeds, these features often lack meaningful customization, limiting their effectiveness. These limitations indicate that while transparency and control tools are steps toward protecting freedom of speech and fundamental rights, they currently fail to provide users with significant customization options. To truly empower users, these tools need to be more dynamic, with better customization and feedback mechanisms. While large platforms already have content moderation systems in place, the DSA's primary innovation lies in enhancing the transparency in content moderation practices, rather than expanding user control over online

content.

On the other hand, the risk assessments of VLOPs and VLOSEs mark a shift toward proactively identifying and addressing the root causes of harmful content dissemination, such as the design of recommender systems. Through these assessments, platforms are required to evaluate how their algorithms may contribute to physical and mental health issues, and to take corrective actions when systemic risks are identified. For instance, platforms may be required to adjust their algorithms or remove features that exacerbate addiction or amplify harmful content. This approach directly addresses the risks associated with prolonged exposure to distressing or toxic content, potentially providing users with a safer, more supportive online environment.

The effectiveness of risk assessments in reducing exposure to harmful content largely depends on their enforcement and the quality of the assessments themselves. While the DSA requires platforms to assess and mitigate these risks, platforms have significant discretion in framing and evaluating systemic risks, which may allow them to downplay harmful practices that could threaten their business models. Additionally, concerns about the transparency and accessibility of risk assessment reports—such as excessive redactions or overly generalized findings—could limit the public's ability to hold platforms accountable for their impact on digital well-being. This raises doubts about whether the DSA will lead to meaningful changes in how platforms manage harmful content and protect users' mental and emotional health. With the first risk assessment reports due in late 2024 and further clarification on systemic risks expected by February 2025, it remains uncertain whether the DSA's provisions will effectively address the challenges related to digital well-being and the lack of user autonomy.

A key criticism of current regulations is their heavy reliance on transparency and consent mechanisms rather than imposing specific restrictions on manipulative targeting practices. While the DSA requires platforms to disclose key parameters of their recommender and ad-targeting systems, it does not prohibit or significantly limit the use of sensitive behavioural insights to influence user decisions. Although some protections exist for categories like political opinions or mental health information, the widespread use of detailed consumer data to drive engagement remains largely unchecked. This leaves consumers burdened with navigating complex consent processes while still vulnerable to subtle, algorithm-driven manipulation (Fahy, 2022). Moreover,

the "transparency paradigm" can overwhelm users with excessive or overly complex data. Transparency measures often fail to present information in a manner that is accessible, engaging, or capable of influencing consumer behaviour, reducing their practical effectiveness (Zardiashvili & Sears, 2023).

The EU's approach to digital advertising, focusing primarily on transparency and consent, has been also criticized for failing to address the systemic power imbalance between users and platforms. Even with increased transparency, consumers are frequently subjected to targeting techniques that undermine their autonomy by subtly influencing decisions and behaviours. To effectively safeguard consumer interests, a stronger regulatory framework may be needed—one that directly addresses platform power dynamics and the behavioural impacts of data-driven targeting (Fahy, 2022). Persistent and intrusive advertising, particularly in freemium models, exacerbates distraction by overwhelming users with constant disruptions. These practices, though could potentially be addressed under the UCPD as aggressive, lack robust enforcement mechanisms or explicit regulations on frequency and intrusiveness, allowing platforms to push boundaries with programmatic ad systems.

Ultimately, while transparency and consent tools provide some degree of user control over online content, they are insufficient to address the pervasive interference caused by digital platforms, particularly in the realm of digital advertising. Meaningful customization options remain largely absent, limiting users' ability to effectively manage their experiences in digital platforms.

**Alternative approaches to internet and platform regulation**

As a final contribution in this analysis, I will explore alternative approaches to internet and platform regulation aimed at fostering digital well-being and creating healthier online environments. Existing regulations, such as the GDPR, AVMSD, UCPD, and the newly introduced DSA, take steps to address issues like addictive design, online profiling, and manipulative practices. However, as already discussed, some gaps remain. Current frameworks focus on transparency and consent but fall short of addressing exploitative behavioural targeting or the amplification of harmful content by algorithms. Additionally, manipulative practices, including

the commodification of user data and persistent advertising, continue to undermine user autonomy. Bridging these gaps requires a more nuanced approach that balances platform power dynamics and ensures technological innovation does not compromise individual well-being.

A significant challenge in regulatory efforts is the ambiguity in defining terms like "addictive design" or "manipulative practices," which lack clear legal definitions. This makes it difficult for platforms to comply with regulations and for regulators to enforce them consistently, creating risks of uneven enforcement or regulatory capture by powerful platforms exploiting vague language. Furthermore, the scale and complexity of platform operations present major obstacles for regulators, who may lack the resources and expertise to effectively monitor or address violations, particularly with large global tech companies. The principle-based approach in frameworks like the DSA, while flexible, often fails to provide specific guidelines, which weakens accountability and leaves room for subjective interpretation. This makes it harder to tackle systemic issues like algorithmic manipulation or exploitative advertising.

In particular, according to Becker and Penfrat (2022), while the DSA is carefully designed to uphold digital rights in the EU, it focuses narrowly on content moderation and overlooks critical structural issues, such as the pervasive surveillance-based business models of large tech firms that drive harmful content's proliferation. Additionally, the DSA fails to address the root causes of content spread, including the role of platform algorithms in amplifying harmful content and the commercial incentives that shape these systems, leaving fundamental questions about platform accountability and the ethics of algorithmic design unaddressed (Becker & Penfrat, 2022).

Moreover, transparency obligations currently focus on disclosing advertising practices and profiling methods but often omit critical insights, such as the actual cost of services to users, particularly in terms of data monetization. Providing clearer information about how platforms monetize user data could foster greater accountability and understanding of digital markets. Finally, the reliance on transparency as a primary regulatory tool does not guarantee fairness. Ensuring fairness requires more proactive measures, such as limiting exploitative practices and addressing structural power imbalances between platforms and users, which are not fully addressed by the current framework. These limitations highlight the need for further refinement

to create a truly equitable and user-centric regulatory environment (Zardiashvili & Sears, 2023).

The existing digital advertising regulation doesn't consider at all questions, such as how much advertising is too much, and how much user attention can be consumed by advertisers before it becomes unsustainable or harmful. To address digital distractions, particularly in online advertising, a regulatory approach akin to the AVMSD's provisions for traditional television broadcasts could be insightful. The AVMSD allows member states to regulate the volume and placement of ads, recognizing the potential of such measures to enhance viewer engagement while protecting content integrity. For example, it limits ads to 20% per clock hour and sets guidelines to minimize disruptions to specific content types like films and children's programming (Articles 20 & 23, AVMSD). Translating this model to digital platforms, regulators could consider introducing frequency caps or time-based restrictions for ads, ensuring that users are not overwhelmed by excessive interruptions.

Currently, the EU faces the challenge of fostering innovation without compromising consumer protection, creating a regulatory environment that allows for technological advancements while safeguarding users' physical, mental, and emotional health. In this complex environment, considering the realities of the digital environment is also crucial. For example, recommender systems are designed to help users navigate the vast amount of content available online, addressing the issue of information overload. While the DSA suggests chronological feeds as an alternative to adaptive algorithms and the lack of transparency in recommender systems, purely chronological systems are not optimal in today's digital environment.

As noted by Narayanan (2023), ranking algorithms have become necessary due to the sheer volume of content, making chronological feeds unfeasible for mainstream platforms. One potential alternative is horizontal interoperability, which would require platforms to support cross-platform connectivity. This approach could shift competition from platform size to the quality of algorithms, encouraging platforms to develop user-centric algorithms that improve digital well-being and reduce issues like FOMO. Innovations such as the "breaking echo chambers" algorithm, which aims to promote healthier online interactions, show promise. While interoperability presents challenges, it aligns with regulatory goals of reducing monopolistic practices and prioritizing user welfare (Risco & Lleonart-Anguix, 2024).

The systemic risk assessment approach in the DSA faces several similar challenges that could limit its effectiveness. One key issue is its reliance on human rights frameworks, which offer broad principles but lack specific guidance on moderating content or addressing systemic risks like misinformation and harmful content amplification, let alone more nuanced harms. While human rights provide a foundation, they don't fully address the complexities of content moderation. Additionally, the institutions involved, such as platforms, the European Commission, and the Board for Digital Services, are not well-equipped to manage these tasks. Platforms may lack credibility in self-assessments due to their profit-driven focus, which could conflict with the public interest (Eder, 2024).

According to Eder (2024), there are suggestions to involve auditors, civil society organizations, and national courts in the risk assessment process. However, auditors, often large consultancy firms, may lack the expertise and public trust needed to hold platforms accountable. On the other hand, civil society involvement, while aiming to increase transparency and accountability, faces challenges due to its voluntary nature, which gives platforms too much discretion. Additionally, the diverse interests of civil society groups may make it difficult to reach implementable solutions, and marginalized groups may be underrepresented. Still, the Commission could strengthen civil society's role by empowering these organizations in developing platform guidelines, creating a more balanced and accountable system for content moderation (Eder, 2024).

Regarding privacy, scholars argue that a more comprehensive data privacy framework is needed, one that protects user privacy while ensuring freedom of expression and information security. Key elements would include banning online behavioural advertising, which exploits user data for targeted ads, and enforcing data minimization to ensure companies only collect necessary information. Additionally, the law should outlaw pay-for-privacy schemes, ensuring privacy is not a privilege for the wealthy, and prevent deceptive user interfaces that manipulate consent (McSherry et al., 2023).

The tension between user autonomy and platform responsibility is another central issue in protecting digital well-being as the different definitions would call for different kinds and degrees of intervention. If digital well-being is discussed in the context of internet addiction,

there is a call for regulatory approaches similar to those for addictive substances, suggesting that platforms bear a significant responsibility for the harm caused by addictive behaviors. The EU Parliament's proposal, which draws parallels between internet addiction and substance abuse, signals such a stance on addressing these issues, though internet addiction still remains a controversial topic in scientific research (Bhargava & Velasquez, 2020).

On the other hand, if the concern is more about daily digital nuances as suggested by Vanden Abeele (2020), such as how users manage their online time and presence, then the responsibility may shift more toward individual mindfulness and digital detox practices. Technology solutions like screen time controls and digital detox apps have emerged as responses, but they often place the burden of self-regulation on the user, with some tools requiring payment or offering suboptimal alternatives. In addition, social media companies frequently use tools like time-tracking features to shift the responsibility for harmful digital environments onto users, rather than addressing the platform design issues that contribute to these harms (Montag & Elhai, 2023).

Similarly, increasing digital literacy places additional pressures on individuals to not only become digitally competent but also to manage their digital lives effectively, balancing productivity with privacy concerns (Syvertsen, 2020). This raises important questions about user autonomy, as individuals should have the freedom to choose how they engage online without constantly being pressured to optimize their digital presence. Moreover, there is a tension between initiatives aimed at closing the digital divide and ensuring digital well-being. While citizens must be online to participate in the digital society and access public services, they are often required to sacrifice privacy and personal data to private companies in the process. Alternative models, such as public domains or platforms funded by public resources or subscriptions, are proposed as solutions that could prioritize user well-being over profit, offering healthier alternatives to the current system dominated by data-driven platforms (Montag & Elhai, 2023).

The current regulatory framework in the EU fails to challenge the dominant business model of digital platforms, with alternative approaches, such as public domains, remaining largely unexplored. Ad-based models have allowed platforms to maintain the perception of a

"free" internet; however, as long as these platforms operate within an oligopolistic and profit-driven framework, genuine user autonomy will remain out of reach. I argue that, if digital platforms wish to be perceived as trusted institutions (Balkin, 2019), they should be held to standards comparable to those applied to traditional media. Although social media initially revolutionized communication by offering interactivity and user independence, the growing dominance of algorithms in content creation, curation, and moderation increasingly undermines user autonomy, turning social media into a more passive means of content consumption. This shift prompts critical questions about the nature of digital platforms: can we move toward a model where users regain control over their content preferences, and feeds, rather than being subjected to intrusive, low-quality recommendations designed solely to maximize screen time?

# Conclusion

## Summary of key findings

Digital well-being is inherently subjective, shaped by individual preferences and experiences with technology. This variability, combined with a lack of consensus on the specific harms of social media, makes regulation challenging. However, there is broad agreement in the literature that enhancing user autonomy and control can improve well-being without infringing on fundamental rights like freedom of expression.

While the EU has not formally recognized "digital well-being" as a distinct concept, it has increasingly addressed related issues such as the attention economy, attention-capture dark patterns, dissemination of harmful content and addictive platform design in legal texts. These references reflect growing concern about the impact of digital platforms on users' mental health. Although recent regulations like the DSA address significant aspects of digital well-being, there remain critical gaps in user protection. For instance, only the largest platforms are required to reduce addictive features, and there is no general ban on such practices. While transparency measures, risk assessments, and consent-based controls represent positive steps, these solutions fall short of fundamentally changing the way platforms operate.

The most explored area of digital well-being regulation is the exposure to harmful content. The DSA represents progress in holding platforms more accountable for content moderation, especially with transparency requirements. However, despite targeting issues like hate speech and disinformation, the lack of clear definitions for these terms creates enforcement challenges. Additionally, current content moderation systems lack the flexibility to give users full control over their online experiences. Though the DSA includes transparency provisions, it does not provide users with the necessary tools to personalize their content feeds. There is a clear need for more dynamic, customizable tools to offer users genuine control over their content exposure.

Addictive design features also remain a prominent concern. While regulators acknowledge the harms of such practices, the DSA does not impose a strict ban, except for protecting minors. Risk assessments are a positive step, but they focus primarily on the largest

platforms, leaving room for these platforms to assess their own practices. While the DSA encourages transparency and offers non-personalized feed options, these measures are insufficient to address the underlying issues driving addictive design.

Boundary blurring, particularly in the context of work-life balance, is another challenge exacerbated by constant connectivity on digital platforms. The "right to disconnect," currently under discussion in the EU, aims to give workers more control over when they are expected to be online. However, this issue is complex and intertwined with other digital well-being concerns, making it difficult to address through regulation alone. While the right to disconnect could help, cultural shifts are also needed to alleviate the pressure of being "always on".

Finally, the business models of digital platforms present systemic challenges by prioritizing profit through data-driven targeting and algorithmic amplification, often at the expense of user well-being. Regulations like the DSA and GDPR focus on transparency but fail to address the root causes of manipulative practices tied to surveillance capitalism and behavioural advertising. Stronger interventions are needed, including bans on intrusive ads, limitations on data collection, and more robust regulation of harmful content amplification. A shift toward more user-centric control features is needed to allow individuals to better tailor their digital experiences and protect their autonomy and mental health. Overall, there is a need to explore alternative models that prioritize user control and hold platforms to higher social responsibility standards.

**Limitations of the study**

One limitation of this research is that it focuses solely on EU law, and there may be differences in how digital well-being is regulated in other jurisdictions. Additionally, the DSA and the DMA are still in their early stages, making it difficult to assess its full impact and enforcement. Future studies will need to evaluate the long-term effectiveness of these frameworks, particularly in addressing issues such as harmful content and addictive design features. Furthermore, digital well-being is inherently subjective, shaped by individual experiences, which complicates the development of universal regulations. The current regulatory focus on larger platforms leaves other sectors, like mobile apps and online gambling, underexplored. Finally, the systemic

challenges posed by business models that prioritize data targeting and algorithmic amplification highlight the need for further research into alternative models that prioritize user well-being over profit, as well as the potential impact of cultural shifts in addressing issues like the "right to disconnect".

## References


Al-Mansoori, R. S., Al-Thani, D., & Ali, R. (2022). Digital Wellbeing: Designers' Perspectives on Where the Responsibility Lies. In *2022 9th International Conference on Behavioural and Social Computing (BESC), Matsuyama, Japan* (Vol. 9, pp. 1–6). https://doi.org/10.1109 /besc57393.2022.9995236

Alutaybi, A., Arden-Close, E., McAlaney, J., Stefanidis, A., Phalp, K., & Ali, R. (2019). How Can Social Networks Design Trigger Fear of Missing Out? *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 3758–3765. https://doi.org/10.1109 /smc.2019.8914672

Annemans, D., & Dennis, M. (Eds.). (2024). *Reimagining Digital Well-Being 2024: Report for Designers & Policymakers*. https://ris.utwente.nl/ws/portalfiles/portal/459263241/Reim agining Digital Well-Being Report 2024.pdf

Balkin, J. M. (2019). How to Regulate (and Not Regulate) Social Media. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3484114

Becker, S., & Penfrat, J. (2022). The DSA Fails to Reign in the Most Harmful Digital Platform Businesses – But It Is Still Useful. In J. Van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri, & M. Straub (Eds.), *Putting the DSA into Practice: Enforcement, access to justice and global implications* (pp. 51–62). Verfassungsbooks.

Bhargava, V. R., & Velasquez, M. (2020). Ethics of the Attention Economy: The Problem of Social Media Addiction. *Business Ethics Quarterly*, *31*(3), 321–359. https://doi.org/10.1017/beq.2020.32

Brey, P., Gauttier, S., & Milam, P.-E. (2016). *Harmful internet use: Part II: Impact on culture and society, EPRS | European Parliamentary Research Service*. European Union. https://doi.o rg/10.2861/391152

Burr, C., Taddeo, M., & Floridi, L. (2020). The Ethics of Digital Well-Being: A Thematic Review. *Science and Engineering Ethics*, *26*, 2313–2343. https://doi.org/10.1007/s11948-02 0-00175-8

Cappello, M. (Ed.). (2022). *New actors and risks in online advertising: IRIS Special*. European Audiovisual Observatory. https://rm.coe.int/iris-special-1-2022en-online-advertising/168 0a744d7?c=199&traversed=1

Carpentier, C.-L. (Ed.). (2023). *Attention economy: New economics for sustainable development*. United Nations Economist Network. Retrieved November 1, 2024, from https://www .un.org/sites/un2.un.org/files/attention_economy_feb.pdf

*Commission opens formal proceedings against TikTok under the Digital Services Act*. (2024, February). [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926

*Commission sends requests for information to YouTube, Snapchat, and TikTok on recommender systems under the Digital Services Act*. (2024, October). [Press release]. https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-youtube-snapchat-and-tiktok-recommender-systems-under-digital

Drolsbach, C. P., & Pröllochs, N. (2024, May 12). Content Moderation on Social Media in the EU: Insights From the DSA Transparency Database. In *https://dl.acm.org/*. https://doi.or g/10.1145/3589335.3651482

Eder, N. (2024). Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation. *German Law Journal*, 1–22. https://doi.org/10.1017/glj.2024.24

EDPB. (2024, April 17). *EDPB: 'Consent or Pay' models should offer real choice* [Press release]. https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en

Enarsson, T. (2024). Navigating hate speech and content moderation under the DSA: insights from ECtHR case law. *Information & Communications Technology Law*, 1–18. https://doi.org/10.1080/13600834.2024.2395579

Esposito, F., & Ferreira, T. M. C. (2024). Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns. *European Journal of Risk Regulation*, 1–18. https://doi.org/10.1017/err.2024.8

*EU Digital Markets Act and Digital Services Act explained*. (2021, December). European Parliament. https://www.europarl.europa.eu/topics/en/article/20211209STO19124/eu-d igital-markets-act-and-digital-services-act-explained

European Commission. (2024, April 30). *Commission launches first-stage consultation of social partners on fair telework and the right to disconnect* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1363

European Commission: Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., & Liva, G. (n.d.). *Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation : final report*. Publications Office of the European Union. https://data.europa.eu/ doi/10.2838/859030

*European Digital Rights and Principles*. (n.d.). https://digital-strategy.ec.europa.eu/. Retrieved November 18, 2024, from https://digital-strategy.ec.europa.eu/en/policies/digital-princ iples

European Law Institute. (2023). *Guiding Principles on Implementing Workers' Right to Disconnect: Report of the European Law Institute*. https://europeanlawinstitute.eu/fil

eadmin/user_upload/p_eli/Publications/Guiding_Principles_Workers_Right_to_Disconnect.pdf

European Parliament. (2021). *The right to disconnect: European Parliament Resolution of 21 January 2021 with recommendations to the Commission on the Right to Disconnect (2019/2181(INL))*. European Union, 2021 - Source: European Parliament. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0021_EN.html#top

European Parliament. (2023). *2023/2043(INI) - 12/12/2023 - Addictive design of online services and consumer protection in the EU single market*. European Union, 2024 - Source: European Parliament. https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1769972&t=e&l=en

European Parliament, & Müller, K. (2020). *The right to disconnect: Briefing, European Added Value in Action, EPRS | European Parliamentary Research Service*. European Union. https://www.univiu.org/images/aauniviu2017/GP/co-curr/VeUMEU2021/The_Right_to_Disconnect.pdf

*Facebook and Instagram to Offer Subscription for No Ads in Europe*. (2024, November). [Press release]. https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscr iption-for-no-ads-in-europe/

Fahy, R., Appelman, N., & Helberger, N. (2022, August 5). *The EU's regulatory push against disinformation: What happens if platforms refuse to cooperate?* https://verfassungsblog.de/. Retrieved November 22, 2024, from https://verfassungsblog.de/voluntary-disinfo/

*Fitness Check of EU Consumer Law on Digital Fairness [Commission Staff Working Document): SWD(2024) 230 Final*. (2024). https://ec.europa.eu/info/law/better-regulation/have-y our-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

Galli, F. (2022). Algorithmic Marketing and EU Law on Unfair Commercial Practices. In *Law, governance and technology series*. https://doi.org/10.1007/978-3-031-13603-0

Galli, F., Loreggia, A., & Sartor, G. (2023). The Regulation of Content Moderation. In *Law, governance and technology series* (pp. 63–87). https://doi.org/10.1007/9_78-3-031-40516-7_5

Giraldo-Luque, S., Afanador, P. N. A., & Fernández-Rovira, C. (2020). The Struggle for Human Attention: Between the Abuse of Social Media and Digital Wellbeing. *Healthcare*, *8*(4), 497. https://doi.org/10.3390/healthcare8040497

Głowacka, D., Szymielewicz, K., & Sapieżyński, P. (2023). Algorithms of Trauma #2: Stuck in a "doomscrolling trap" on Facebook? The platform will not let you escape. In *en.panoptykon.org*. Panoptykon Foundation.

Goanta, C. (2022). Now What Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising. In J. Van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri, & M. Straub (Eds.), *Putting the DSA into Practice: Enforcement, access to justice and global implications* (pp. 135–150). Verfassungsbooks.

Gui, M., Fasoli, M., & Carradore, R. (2017). "Digital Well-Being". Developing a New Theoretical Tool For Media Literacy Research. *Italian Journal of Sociology of Education*, *9*(1), 155–173. https://doi.org/10.14658/pupj-ijse-2017-1-8

Henriques, D. (2020). Effects of TV airtime regulation on advertising quality and welfare. *Information Economics and Policy*, *55*, 100897. https://doi.org/10.1016/j.infoecopol.2020.100897

*How corporate lobbying undermined the EU's push to ban surveillance ads*. (2022, January 18). https://corporateeurope.org/. Retrieved November 20, 2024, from https://corporateeurope.org/en/2022/01/how-corporate-lobbying-undermined-eus-push-ban-surveillance-ads

Jóźwiak, M. (2024, November 22). *The wait is (almost) over! First risk assessment and audit reports – what will be published, when, and the way forward*. https://dsa-observatory.eu/ . Retrieved November 22, 2024, from https://dsa-observatory.eu/2024/11/22/the- wait-is-almost-over-first-risk-assessment-and-audit-reports-what-will-be-published-when-and-the-way-forward/

Kircher, T., & Foerderer, J. (2023). Ban Targeted Advertising? An Empirical Investigation of the Consequences for App Development. *Management Science*, *70*(2), 1070–1092. https://doi.org/10.1287/mnsc.2023.4726

Klingelhoefer, J., & Meier, A. (2023). Social media and well-being at work, at home, and in-between: A review (post-print version). *Edward Elgar Publishing eBooks*, 398–418. https://doi.org/10.4337/9781789906769.00032

Klinger, U., Koc-Michalska, K., & Russmann, U. (2022). Are Campaigns Getting Uglier, and Who Is to Blame? Negativity, Dramatization and Populism on Facebook in the 2014 and 2019 EP Election Campaigns. *Political Communication*, *40*(3), 263–282. https://doi.org/10.1080/10584609.2022.2133198

Lyngs, U. (2019). Putting self-control at the centre of digital wellbeing. In *2019 ACM CHI Conference on Human Factors in Computing Systems [Position paper])*. https://ulriklyngs.com/pdfs/2019-02-08_Lyngs_workshop_digi_wellbeing.pdf

Maréchal, N. (2022). *We can't govern the internet without governing online advertising. Here's how to do it.* https://rankingdigitalrights.org/. Retrieved November 3, 2024, from https://rankingdigitalrights.org/mini-report/we-must-govern-online-ads/

McSherry, C., Trujillo, M., Cohn, C., & Klosowski, T. (2023). *Privacy First: A Better Way to Address Online Harms*. Electronic Frontier Foundation. https://www.eff.org/document privacy-first-better-way-address-online-harms

Montag, C., & Elhai, J. D. (2023). On Social Media Design, (Online-)Time Well-spent and Addictive Behaviors in the Age of Surveillance Capitalism. *Current Addiction Reports*, *10*(3), 610–616. https://doi.org/10.1007/s40429-023-00494-3

Mousavi, S., Gummadi, K. P., & Zannettou, S. (2024). Auditing Algorithmic Explanations of Social Media Feeds: A Case Study of TikTok Video Explanations. *Proceedings of the International AAAI Conference on Web and Social Media*, *18*, 1110–1122. https://doi.org/10.1609/icwsm.v18i1.31376

Mujica, A., Crowell, C., Villano, M., & Uddin, K. (2022). ADDICTION BY DESIGN: Some Dimensions and Challenges of Excessive Social Media Use. *Medical Research Archives*, *10*(2). https://doi.org/10.18103/mra.v10i2.2677

Narayanan, A. (2023). *Understanding Social Media Recommendation Algorithms: Optimizing for what? Algorithmic amplification and society*. Knight First Amendment Institute, Columbia University. https://academiccommons.columbia.edu/doi/10.7916/khdk-m460

*New EU rules needed to make digital platforms less addictive*. (2023, October). https://www.europarl.europa.eu/news/en/press-room/20231023IPR08161/new-eu-rules-needed-to-make-digital-platforms-less-addictive

Nguyen, M. H. (2021). Managing Social Media Use in an "Always-On" Society: Exploring Digital Wellbeing Strategies That People Use to Disconnect. *Mass Communication & Society*, *24*(6), 795–817. https://doi.org/10.1080/15205436.2021.1979045

Reviglio, U., & Fabbri, M. (2024, November 22). *The Regulation of Recommender Systems Under the DSA: A Transition from Default to Multiple and Dynamic Controls?* https://dsa-observatory.eu/

Risco, M., & Lleonart-Anguix, M. (2024). *Feed for Good? on the effects of personalization algorithms in social platforms* (Discussion Paper Series – CRC TR 224; Discussion Paper No. 580). University of Bonn and University of Mannheim. https://www.wiwi.uni-bonn.de/bgsepapers/boncrc/CRCTR224_2024_580.pdf

Roffarello, A. M., & De Russis, L. (2022). Towards Understanding the Dark Patterns That Steal Our Attention. *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. https://doi.org/10.1145/3491101.3519829

Sala, A., Porcaro, L., & Gómez, E. (2024). Social Media Use and adolescents' mental health and well-being: An umbrella review. *Computers in Human Behavior Reports*, *14*, 100404. https://doi.org/10.1016/j.chbr.2024.100404

Saurwein, F., & Spencer-Smith, C. (2021). Automated Trouble: The Role of Algorithmic Selection in Harms on Social Media Platforms. *Media and Communication*, *9*(4), 222–233. https://doi.org/10.17645/mac.v9i4.4062

Syvertsen, T. (2020). You are the Problem! Everybody Online and Self-regulation. In *Digital Detox: The Politics of Disconnecting (Society Now)* (pp. 49–71). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78769-339-520201004

Tzoulia, E. (2021). Targeted Advertising in the Digital Era: Modern Challenges to Consumer Privacy and Economic Freedom: The Responses of the EU Legal Order. In *Springer eBooks* (pp. 447–477). https://doi.org/10.1007/978-3-030-69583-5_19

Van De Waerdt, P. J. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. *Computer Law & Security Review*, *38*, 105436. https://doi.org/10.1016/j.clsr.2020.105436

Vanden Abeele, M. M. P. (2020). Digital Wellbeing as a Dynamic Construct. *Communication Theory*, *31*(4), 932–955. https://doi.org/10.1093/ct/qtaa024

Vanden Abeele, M. M. P., Vandebosch, H., Koster, E. H. W., De Leyn, T., Van Gaeveren, K., De Segovia Vicente, D., Van Bruyssel, S., Van Timmeren, T., De Marez, L., Poels, K., DeSmet, A., De Wever, B., Verbruggen, M., & Baillien, E. (2024). Why, how, when, and for whom does digital disconnection work? A process-based framework of digital disconnection. *Communication Theory*, *34*(1), 3–17. https://doi.org/10.1093/ct/qtad016

Wu, T. (2019). Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal*, *82*, 771.
https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3030&context=faculty_scholarship

Zardiashvili, A., & Sears, A. M. (2023). Targeted Advertising and Consumer Protection Law in the EU. *Vanderbilt Journal of Transnational Law*, *56*(3). https://papers.ssrn.com/sol3/paper s.cfm?abstract_id=4249743

Zhang, M. R., Lukoff, K., Rao, R., Baughan, A., & Hiniker, A. (2022). Monitoring Screen Time or Redesigning It? *CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3491102.3517722