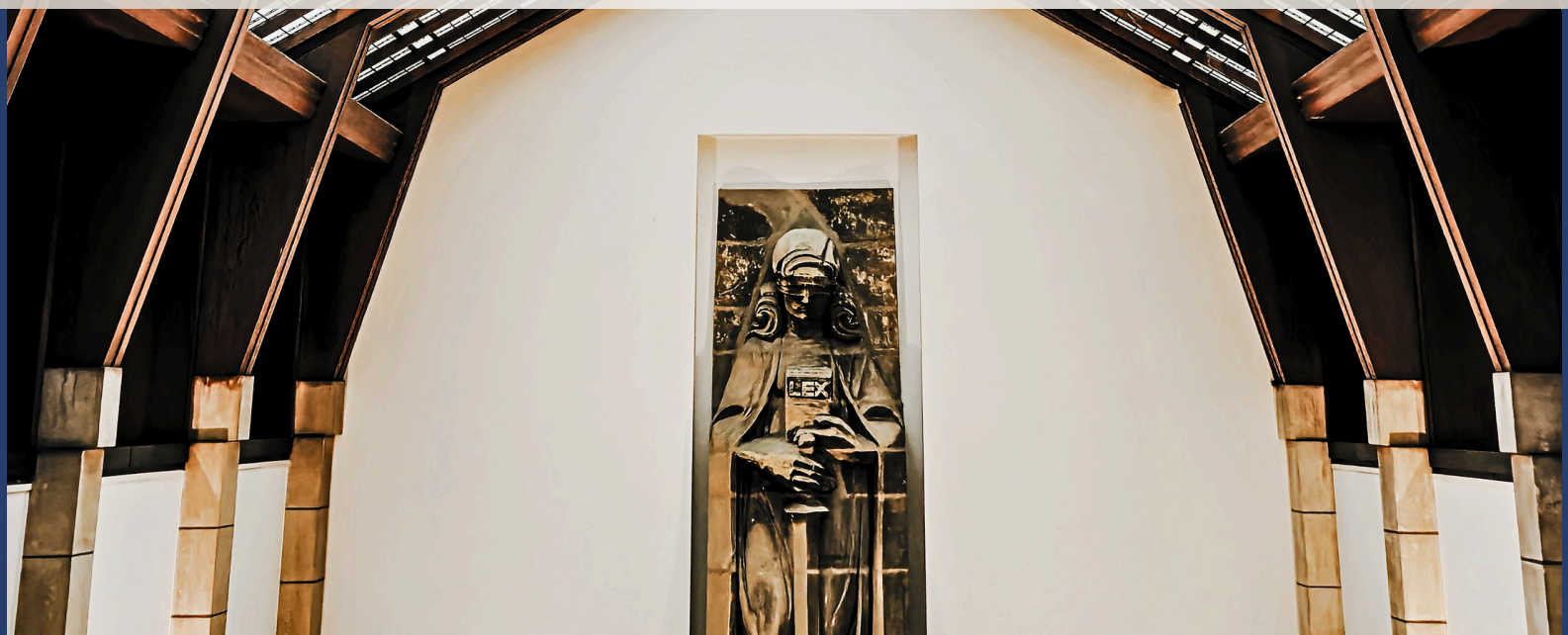
Maastricht University
Faculteit der Rechtsgeleerdheid

Maastricht Centre
for European Law

Autonomy in the Age of Transparency: Examining User Rights Through Conceptual Analysis Under the Digital Services Act

Majella Votta



MCEL Master's Thesis Series
No 2026/12

The MCEL Master's Thesis Series seeks to give excellent students the opportunity to publish their final Master's theses and to make their work accessible to a wide audience.

Those wishing to submit papers for consideration are invited to consult our website and to send their work to mcel@maastrichtuniversity.nl.

Published in Maastricht, March 2026

Faculty of Law
Maastricht University
Postbox 616
6200 MD
Maastricht
The Netherlands

This paper is to be cited as MCEL Master's Thesis Series 2026/12

Abstract

Can transparency in digital governance genuinely protect user autonomy in an online environment shaped by algorithmic influence and surveillance-based business models?

Adopting an interdisciplinary methodology, the thesis combines philosophical analysis of autonomy and transparency with insights from technology studies, psychology, consumer policy, communications research, and EU digital law. The first part develops a normative framework for understanding autonomy beyond mere freedom of choice, drawing in particular on Kantian conceptions of meaningful self-governance. The second part applies this framework to two case studies central to the Digital Services Act (DSA): recommender systems and dark patterns.

Through these case studies, the thesis demonstrates that although the DSA introduces significant transparency obligations, such as disclosure requirements for recommender systems and restrictions on manipulative interface design, these measures do not sufficiently address deeper structural asymmetries of informational and design power between platforms and users. Transparency risks overburdening users with information while leaving intact the underlying choice architectures that enable subtle forms of manipulation.

Accordingly, the thesis argues that transparency, while necessary for accountability, cannot by itself secure meaningful autonomy in digital environments shaped by surveillance-based incentives and behavioural influence. Beyond disclosure, the thesis probes the growing concentration of platform power and the implications of private corporations functioning as de facto rights adjudicators and arbiters of online speech, visibility, and participation. By embedding transparency within a framework that leaves core design and governance structures largely intact, the DSA risks legitimising this privatised model of internet governance rather than fundamentally recalibrating it.

Table of Contents

1. Introduction

At a time where every scroll and click can be subtly manipulated, the notion of free will is increasingly at risk, as unseen algorithms craft insecurities and dictate desires in ways we scarcely understand. The internet does not just connect us — it can quietly shape who we are, and sometimes, who we think we should be. The pervasive influence of digital technologies permeates nearly every facet of ordinary life. These technologies' relationship with individuals' autonomy can be observed to have a detrimental effect or pose a threat to self-governance and freedom of choice.[1] By way of example, algorithmic-driven targeted advertising has the capacity to exploit emotional vulnerability or insecurity in young women.[2] Indeed, they can even be said to fabricate such insecurities, by propagating a particular (often unrealistic) beauty standard on social media. Consequently, a young woman may internalise these standards, feeling pressure to conform by purchasing cosmetic products advertised to her, thereby exploiting her vulnerability. This manipulates her autonomy by shaping her choices and consumption behaviours without conscious awareness, ultimately contributing to the erosion of her self-worth and self-esteem. Thus, her actions may be viewed as lacking authentic autonomy, as they are driven by manufactured societal pressures rather than genuine preference.[3]

The EU's regulatory model is described as human-centric and rights-driven, encompassing a balance between free speech with other rights like data privacy, dignity and non-discrimination.[4] This contrasts other systems such as the United States' laissez-faire model which prioritises free speech as the fundamental right implicated by digital transformation, or China's state-driven model prioritising the political power of the government.[5] The European approach encompasses regulatory intervention, embedding its digital economy vision within laws enforced by democratic institutions, firmly anchored in the rule of law.[6] In the European Union, the Digital Services Act (DSA) belongs to a plethora of new legislative initiatives which aim to combat the deleterious effects of online platforms, with a focus on user safety and fundamental rights protection.[7] The DSA's chief aims target the protection of users' fundamental rights, the reduction of illegal or harmful online content, the allocation of liabilities for third-party

[1] Siavosh Sahebi and Paul Formosa, 'Social Media and its Negative Impact on Autonomy' (2022) 35 Philosophy & Technology 14.
[2] *ibid* 16.
[3] Sahebi and Formosa (n 1).
[4] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023) 105.
[5] *ibid* 106.
[6] Bradford (n 4) 109.
[7] Peter Church and Ceyhun Necati Pehlivan, 'The DSA: A New Era for Online Harms and Intermediary Liability' (2023) 4 Global Privacy Law Review 53.

content to online intermediaries, and to reconcile information asymmetries between services, their users and society.[8] Evidently, there is an emphasis on safeguarding individuals — their online experience, their data, and their fundamental rights. This attention to the increasing impact of digital transformation acknowledges issues regarding the highly fragmented digital landscape across the Union,[9] and issues emanating from the increasingly outdated e-Commerce Directive (ECD). 'Legal distance' caused by disparate transpositions of the ECD's measures in national legal systems has upset the efficacy of the legislation, causing barriers to trade.[10] This work contributes to ongoing discourse on digital transparency and the impact of surveillance-based business models of platforms on user autonomy. It does so by offering an original methodological approach to understanding the interplay between autonomy and transparency, in the context of recommender systems and dark patterns.

1.1. Research Question

The counterbalance between autonomy and transparency online is the central focus of this thesis, by which I aim to investigate whether increased transparency on platforms genuinely enhances users' ability to exercise meaningful choice and self-determination or if it merely provides superficial disclosures that do not address deeper issues of control and manipulation. For our purposes, autonomy, as elaborated upon later, concerns the individual autonomy of the humans engaging with platforms - the users. Our understanding of 'user' is broad, as this includes the everyday individual user, also NGOs and businesses that rely on the internet for their work etc. The conceptual analysis of transparency is focused on the platforms, amid the discourse sparked by the advent of the DSA. A concern arises regarding the transparency measures intended to ensure fairness in content moderation and information dissemination, regulating platform power, and whether this power should be vested in platforms in the first place.[11] Cauffman and Goanta caution against the implications emanating from this 'privatisation of internet governance,' particularly from a fundamental rights perspective.[12]

My core argument is that while the DSA aims to enhance user autonomy and transparency in digital governance by embedding them in its framework, it ultimately

[8] Aina Turillazi et al., 'The DSA: An Analysis of its Ethical, Legal, and Social Implications' (2023) 15 Law, Innovation and Technology 88.
[9] *ibid* 85.
[10] Teresa Rodríguez de las Heras Ballell, 'The Background of the Digital Services Act: Looking Towards a Platform Economy' (2021) 22 ERA Forum: Journal of the Academy of European Law 77.
[11] Marta Maroni, 'Mediated Transparency': The Digital Services Act and the Legitimisation of Platform Power' [2023] University of Helsinki Faculty of Law Legal Studies Research Paper Series No. 77, 4.
[12] Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12 European Journal of Risk Regulation 768.

struggles to overcome the challenges posed by surveillance-based business models that prioritise profit over user experience. Through an examination of ethical concerns regarding user autonomy and current transparency measures, the thesis assesses the DSA's ability to balance user protection with the operational realities of dominant online platforms. Central to this argument is that while the DSA incorporates transparency measures aimed at protecting user rights, it does not sufficiently address the deeper issues of control and manipulation inherent in digital platforms — transparency is a necessary but ultimately insufficient condition to achieving user autonomy. What I seek to contribute to the literature in this area is an original, methodologically-novel approach to understanding the interplay between autonomy and transparency in internet governance. My goal is to stimulate discussion on the issue of reforming internet governance to align with the vision of a responsible internet, to address the challenges of opaque digital systems and weak user control.[13] My conclusions on the DSA's efficacy aim to contribute to an ameliorated understanding of how to improve internet governance in a way that is more responsible and user-centric. I offer a novel perspective on how to align regulatory frameworks with ethical principles. I chose to examine recommender systems and the DSA's rules governing their operation to demonstrate the practical implications of transparency in algorithmic processes and to gauge whether genuine user empowerment can prosper. Dark patterns are assessed to provide insight into the conflict between private motives and user experience and safety, as these manipulative tactics can exploit cognitive biases and vulnerability, thus eroding autonomy.

1.2 Methodology

The substantive discussion of this thesis is divided into two main sections. The first part (Chapters 2 and 3) provides a theoretical foundation and discussion on the concepts of transparency and autonomy, utilising an interdisciplinary lens grounded in philosophy. I also examine research from various fields including science and technology, psychology, digital culture, ethics, artificial intelligence, information and communication studies, and consumer policy. In this way, it follows the critical approach of Hillebrandt et al. on the concept and practice of transparency. The second part (Chapters 4 and 5) adopts a more normative and practical perspective, which incorporates the case studies of recommender systems (RSs) and dark patterns, and is informed by insights from the first section.

The novel nature of this thesis is rooted in its interdisciplinary lens, with a focus on philosophical conceptions of transparency and autonomy. Rather than conducting a

[13] Cristian Hesselman et al., 'A Responsible Internet to Increase Trust in the Digital World' (2020) 28 Journal of Network and Systems Management 884.

purely legal analysis of a new piece of EU legislation, I chose, and perhaps even felt it necessary to widen the scope of research into areas such as computer technology, ethics, consumer policy, and psychology. This approach endeavours to strengthen the findings and their relevance. The ramifications of the DSA will have extensive legal, ethical, and societal effects on a wide range of areas, including markets, consumer welfare, information dissemination, and the formation of our online and human identities in general. Therefore, it is imperative to conduct this conversation in a manner which recognises this. This ensures that discussions of what it means for the internet to be safe and the responsibility of online platforms are well-informed and holistic.

Examining scientific and technological literature aided me in understanding the digital tools themselves, such as recommender systems and dark patterns. This background allowed me to grasp the perspectives of scientists and technological experts on user autonomy and transparency, which enabled me to recognise the vulnerabilities inherent in algorithm-driven technology and how these technologies can potentially undermine or fail to promote autonomy. Relying on psychological research allowed me to access deeper insight into human behaviour, motivation and decision-making processes. Integrating this insight allowed me to better understand how users interact with platforms and the psychological mechanisms that shape their behaviour, especially in response to algorithmic-driven technologies and targeted advertising. I deemed it relevant to include research on consumer policy and law to acknowledge where the DSA fits in amongst the existing regulatory frameworks that govern digital platforms and protect rights. The interplay between market power, competition and consumer welfare are crucial to this conversation on a responsible internet, as it creates the profit-driven environments and dynamics we engage with daily. This helps in balancing the interests of consumers, businesses and regulators. Communications research furnishes us with insight into information flows and media dynamics, including issues related to misinformation and content moderation. Information studies then assists us in understanding how users interact with digital platforms, including their information-seeking behaviours and the ways they engage with content. Together, these fields inform both ethical and legal analyses of how online platforms can influence communication practices and cultural norms, which ensures that our analysis of the DSA is cognisant of information asymmetries between platforms and users, and tackles power imbalances in digital interactions.

I chose to carry out my research in this two-part approach for numerous reasons. Firstly, autonomy and transparency are incredibly complex and nebulous concepts. Unravelling their philosophical underpinnings and existence in other areas of academic literature helps set normative benchmarks for these concepts. Further, a philosophical approach prompts questions not only about the legal implications but also the ethical

implications of platform practices and the effectiveness of regulatory measures in safeguarding user rights. I aim to move beyond the surface level of analysis and address deeper issues of power, control, and ethics in digital governance. This dual method aligns well with my aims, and is ameliorated by incorporating philosophical analysis.

1.3 Thesis Structure

As such, this research is divided into 7 chapters, each addressing key aspects related to the theoretical underpinnings and practical implications of transparency and autonomy within the context of the DSA. Chapter 2 offers insight into the context of digital platform governance in the EU, highlighting the tension between the dominant control of platforms and the regulatory attempts to enhance transparency and user autonomy. Chapter 3 provides a theoretical conception of platform transparency and user autonomy, emphasising their significance in understanding the impact of DSA regulations. This part explores transparency and autonomy with an interdisciplinary lens rooted in philosophy to elucidate the conceptual basis for these concepts in digital platform governance.

Chapter 4 examines the impact of recommender systems on user experience and autonomy, investigating how transparency and user autonomy intersect with recommendation algorithms. Chapter 5 focuses on dark patterns, investigating the use of deceptive design techniques to manipulate user behaviour and its implications for autonomy and subsequent regulatory response.

Finally, the thesis will critically evaluate the DSA as a tenable piece of legislation, with Chapter 6 considering its strengths and limitations in achieving its stated objectives. This analysis will produce findings that draw upon insights from the preceding sections to assess the overall impact and effectiveness of the DSA in regulating digital platforms and safeguarding user rights in the evolving digital landscape.

Of course, delivering an interdisciplinary approach with the aim of providing a rich and multifaceted perspective on this facet of digital governance also presents inherent limitations. By integrating perspectives from philosophy, psychology and technology and other fields, the challenge lies in balancing these insights in order to deliver a coherent argument. This may inadvertently lead to a limited depth of analysis within each individual discipline, potentially generalising the nuances of how transparency and autonomy are interpreted and function across different fields. Further, the status of the DSA as a relatively new instrument means there is limited judicial precedent and analytical studies to draw upon. Combined with the constantly evolving nature of digital platforms and technologies, there is a risk that relevance of the findings herein may diminish more quickly than in other academic fields.

2. Background

Our central concern involves the interplay between user autonomy and transparency in the online realm, utilising the DSA as a lens to showcase problems arising therein. Questions related to user autonomy, commonly referred to as 'user empowerment' by stakeholders, relate to broader structural issues such as platforms' business models, which incentivise profit-making over improved user experience.[14] Platforms are said to operate with a 'surveillance-based'[15] advertising-driven business model which monetises the personal data from users' interactions and relations on the internet.[16] For the largest online platforms, or gatekeepers of the internet, targeted advertising forms the core basis of their income.[17] The attention of users is the product being sold,[18] thus questions surrounding addictive design choices and the systems used to recommend content must be probed.

The concern for user autonomy arises because, as Domurath notes, this surveillance surpasses personalised advertisements to deliberate modification of human behaviour. Platforms now aim to shape consumer behaviour for commercial goals, not merely predict it. This involves manipulating consumers' inner motivations and emotions to achieve desired behavioural outcomes that align with business strategies - this is concerning for free will.[19] Zuboff, a seminal voice on surveillance capitalism, warns that it demeans human dignity.[20] Cohen argues that this surveillance leads to the creation of 'tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories.'[21]

NGOs have expressed concern about the transparency of platform's content moderation practices, citing issues of bias, credibility and manipulation. Wong and Floridi noted that Facebook's Oversight Board, established to provide more transparency to the platform's content moderation, has the potential to clarify such decisions and processes, but the nature of its limited jurisdiction and precedent leave much to be

[14] Ilayda Karagoel and Dan Nathan-Roberts, 'Dark Patterns: Social Media, Gaming, and E-Commerce' (2021) 65 Proceedings of the Human Factors and Ergonomics Society Annual Meeting 755.
[15] Ilaria Buri and Joris van Hoboken, 'The Digital Services Act (DSA) Proposal: A Critical Overview' [2021] Institute for Information Law (IViR), University of Amsterdam Discussion Paper, 29.
[16] Maroni (n 11).
[17] Lex Zard and Alan M Sears, 'Targeted Advertising and Consumer Protection Law in the European Union' (2023) 56 Vanderbilt Journal of Transnational Law 799.
[18] Vikram R Bhargava and Manuel Velasquez, 'Ethics of the Attention Economy: The Problem of Social Media Addiction' (2020) 31 Business Ethics Quarterly 2.
[19] Irina Domurath, 'Platform Economy and Individual Autonomy' (2022) 30 European Review of Private Law 959.
[20] Shoshana Zuboff; 'Google as a Fortune Teller: The Secrets of Surveillance Capitalism' in *Frankfurter Allgemeine Zeitung* (Frankfurt, 3 May 2016) 9. <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html>.
[21] Julie E. Cohen, 'What privacy is for' (2013) 126 Harvard Law Review 1917.

desired.[22] The transparency of the Board's decision-making was criticised by NGO Monitor for insufficient independence, political bias and conflicts of interests, particularly after finding that Meta disproportionately removed Palestinian content during the May 2021 Israeli-Palestinian conflict.[23]

Although steps have been taken to improve transparency concerns for end users, such as introducing more substantial information obligations within the EU regulatory framework, Seizov et al. argue that these measures do not lead to genuine user empowerment.[24] Thus, core to this conversation are the transparency obligations placed on Very Large Online Platforms (VLOPs) in the DSA. A new system of complex oversight mechanisms are to be put in place as a response to the aforementioned surveillance issue, as well as the codification of existing self-regulatory mechanisms for platforms.[25] Regarding transparency, there exists the concern that private actors are the final arbiters in determining what content is permitted online, and who gets to see it. Greater transparency in platform governance must protect users' rights amid enforcement obligations, as risks of over-enforcement diminish the freedoms to information and expression, thus lessening the public's ability to partake in 'debate essential to democracy.'[26] With respect to user autonomy, the DSA endows users with innovative 'levers of control' such as having more choice on recommender systems, the capacity to contest content moderation decisions, be represented in disputes with platforms, and receive compensation in case of mistakes.[27] In line with the professed human-centric ethos of the DSA, authorities intend to implement rules on targeting deceptive design choices i.e. dark patterns, some examples include the 'roach motel' and 'preselection' models.

Though, with great power comes greater risks. The potential for large online platforms to abuse their dominant market power poses numerous challenges, such as the distortion of competition in the single market. Globally, the top seven online platforms collectively command nearly 70% of the platform economy market.[28] The dominance of these VLOPs can create obstacles which hinder smaller enterprises from expanding and scaling up. This economic background is further relevant to our

[22] David Wong and Luciano Floridi, 'Meta's Oversight Board: A Review and Critical Assessment' (2023) 33 Minds and Machines 281.
[23] NGO Monitor, The Influence of Political Advocacy NGOs on Meta's Human Rights Content Moderation Process: Gaza 2021 Case Study (2023).
[24] Ognyan Seizov et al. 'The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU' (2019) 42 Journal of Consumer Policy 149.
[25] Maroni (n 11) 6.
[26] Giancarlo Frosio and Christophe Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' (2023) 29 European Law Journal 36.
[27] Martin Husovec, 'Rising above liability: the DSA as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38 Berkeley Technology Law Journal 133.
[28] Turillazi et al. (n 8).

discussion as it is important to recognise that despite efforts to solve concerns via regulation, there are significant qualms about the consequences of entrusting issues such as free speech into private hands, and the subsequent effect this has on user autonomy. Also, it is imperative to recognise that many such enterprises rely on these large online intermediaries for their operations.[29] Consequently, user autonomy is impacted by limiting consumer choices and access to information online. Further, the authority to set terms and conditions, establish prices, and restrict access to alternative services may stifle competition and innovation. As will be elaborated upon, our conception of user autonomy emphasises meaningful choice free from manipulation. Delivering this requires going beyond combating attempts at manipulation but also certifying that platform design respects individual control.

The role platforms play in content moderation has broad implications for fundamental rights protection, balancing harm mitigation from illegal or harmful content, with the fundamental freedoms to information and expression. These concerns are exacerbated by the lack of sufficient supervision of online services,[30] which makes discussions centred on the business models of these services and their relationship with public entities relevant. Frosio and Geiger warn that the 'invisible handshake' between private and public entities elicits accountability concerns.[31] Decisions regarding enforcement taken by these private actors are imbued with public influences. Liability frameworks have afforded platforms considerable power over user-generated content, it is the accountability of this power, or lack thereof, which warrants attention from European legislators. Moreover, public actors lack the technological expertise held and controlled by platforms, to adequately address the complexities regarding illegal and harmful content — hence this externalisation of enforcement responsibilities. As private actors have de facto become the 'watchdogs' of enforcement online, autonomy concerns emerge. Users may face limitations in seeking redress or avenues for appeal, impacting their ability to contest decisions that impinge upon their freedom of speech. Further, the power exerted by platforms over user-generated content highlights autonomy issues as well, particularly when platforms lack sufficient accountability to safeguard users' right to freedom of expression. This is evidenced by opaque grievance processes and the absence of accessible and effective mechanisms for contesting content moderation decisions. These shortcomings in accountability can lead to arbitrary or biased enforcement of content policies, further diminishing users' ability to maintain control over their own speech, and to exercise other fundamental rights.

[29] *ibid* 90.
[30] *ibid*.
[31] Frosio and Geiger (n 26) 34.

3. Theoretical Conceptions of User Autonomy and Transparency in Digital Platform Governance

The purpose of this chapter is to probe the theoretical foundation of transparency and autonomy in the context of digital platforms. While conversations surrounding transparency online have intensified with the emergence of the DSA, and existing work has attempted to scope the meaning of transparency in the context of content moderation,[32] less attention has been paid to examining the purported impact on user autonomy from a philosophical and interdisciplinary perspective. Given the significance of autonomy as a moral concept and the prominent role of online platforms in modern life, a thorough exploration is essential. I offer a topical analysis in this regard, particularly in light of the human-centric ethos of the DSA and the EU's professed emphasis on user safety and the protection of fundamental rights.[33]

In the early days of the internet, a cyberlibertarian ethos dominated; a lack of government control and apparent freedom from content moderation practices provided an 'autonomous space' for internet users to wield substantial control over their activities.[34][35] As the European Commission has highlighted, the evolution of platforms into major players in markets and how their power is leveraged creates growing interest in scrutinising their influence.[36] It can be argued that this paradigm has undergone a reversal: while transparency measures have been established and ostensibly increased (with government and corporate entities operating online more transparently than before), autonomy has diminished. For example, this can be seen in platforms like TikTok being more transparent about its practices through publishing regular transparency reports. Husovec remarks that the focus of legislative predecessors to the DSA, like the ECD, tends to be more provider-centric rather than user-centric. As will be discussed, platforms can become more transparent, however the extent to which

[32] Maroni (n 11).
[33] European Commission, 'A Europe Fit for the Digital Age: The Digital Services Act Overview' <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en>.
[34] Angela Daly, 'The Internet, User Autonomy and EU Law' in Angela Daly, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart Publishing 2016) 3.
[35] In short, the internet has significantly changed the business world and impacted autonomy in several key ways. Firstly, the internet has opened a global market which has expanded consumer choices with a broader range of products, services and information. But this increased access is tempered by, in certain areas, a concentration of power in a few dominant platforms, which can limit the genuine diversity of options. Secondly, the rise of big data has allowed businesses to collect personal information about consumers to tailor advertising. This both enhances consumer experience but raises concerns regarding loss of privacy and manipulation, particularly when this data is collected with users' full awareness or consent. Thirdly, undoubtedly the internet has revolutionised retail via e-commerce platforms, and has also established the gig economy, whereby individuals work through online platforms. However, issues of job security, benefits and working conditions signal concern about the true nature of autonomy in these new economic models.
[36] European Commission, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final (6 May 2015), 12.

users can truly exercise control over their digital experiences remains questionable.

Moreover, existing transparency measures insufficiently address the issue of user autonomy. Indeed, de Matos Alves observes that transparency reports can burden individuals by presuming information symmetries, and that measures like transparency reports are not accompanied by deeper engagement with user concerns.[37] It is essential to recognise that beyond the everyday individual, NGOs and governmental actors also serve as the end users of platforms, and the information in these reports serves different purposes for these distinct groups. Being transparent involves more than just providing more information or choices to users; such a narrow understanding of transparency is flawed. Thus, the notion of user autonomy, if it is indeed acknowledged by platforms, is less concerned with the actual freedom that individuals exercise on platforms, as this is governed by take-it-or-leave-it privacy policies, standard terms and conditions etc.[38]

Indeed, prior to the emergence of digital technologies, various legal, regulatory and cultural measures have belonged to systems of accountability that evaluated speech acts to determine their truthfulness and trustworthiness.[39] These measures typically took the form of newspaper editors for example, or legal standards like defamation law. However, the rise of digital technologies has disrupted this framework by facilitating rapid dissemination of content, bypassing traditional gatekeepers, and creating new ones. As a result, the origin or authority of digital communications have become difficult to discern. Digital technologies also pose public harms to democracy and culture, primarily driven by the business models of online platforms leveraging user data to influence and (mis)inform. Further, O'Neill submits that such business models can commonly neglect ethical principles and moral values.[40] This reinforces the significance of transparency and autonomy as critical concepts to analyse, given that it is evidenced that a lack of transparency in online communications can lead to mistrust and reliance on unreliable sources.[41] It is clear that without strict ethical standards, platforms will continue to undermine the core foundation of informed and democratic societies.

3.1. User Autonomy

Autonomy online can prove a 'vague and blurred' concept.[42] However, autonomy is considered a quintessential aspect of constitutionalism and contemporary Western

[37]Artur de Matos Alves, 'Platform Humanism and Internal Opacity: The Limits of Online Service Providers' Transparency Discourse' (2019) 4 Discourse Culture and Society 111.
[38] Domurath (n 19) 972.
[39] Onora O'Neill, 'Trust and Accountability in a Digital Age' (2020) 95 Philosophy 6.
[40] *ibid* 10.
[41] Ruijie Wang et al. 'Transparency in Persuasive Technology, Immersive Technology, and Online Marketing: Facilitating Users' Informed Decision Making and Practical Implications' (2023) 139 Computers in Human Behaviour 1.
[42] Marietjie Botes, 'Autonomy and the Social Dilemma of Online Manipulative Behaviour' (2023) 3 AI and Ethics 318.

thought.[43] This part introduces main conceptualisations of autonomy so as to be able to comprehensively examine the potential effects online platforms may have on it.

Autonomy derives from the ancient Greek autonomíā, meaning 'living by one's own laws,' the concept being traditionally used in the context of the self-governance of states.[44] But more modern interpretations have evolved the concept to include collective frameworks. For instance, Rousseau reframed autonomy as not merely freedom from interference on an individual basis, but as a higher form of freedom capable of being achieved only through participation in a collective moral and legal framework — moving beyond one's own private interests and viewing social membership as essential to one's identity.[45]

O'Neill highlights a difference between Immanuel Kant's conception of autonomy as the 'supreme principle of morality',[46] and how autonomy is commonly understood today. Modern ideations of autonomy tend to emphasise individual choice and expression, whereas Kant's view of autonomy extended beyond personal freedom, and more so adherence to moral principles that should apply universally to all individuals.[47] To illustrate this, Kant employs a comparison between moral legislation and political legislation; similar to how citizens within a state must consent to laws for them to be considered just, individuals must align their actions in a manner that could be universally accepted in order for them to be morally permissible.[48] A turn away from individualistic understandings of autonomy, which hold 'limited moral weight',[49] offers an enhanced framework of governance that prioritises dignity and autonomy of all, leading to a more inclusive and fair society.

This shift towards collective understandings of autonomy is relevant when discussing platform power because the platform economy increasingly challenges this collective dimension of autonomy. Domurath's three conditions for autonomy, intention and privacy, understanding and information, and freedom from coercion—are systematically eroded in the digital economy.[50] Platform surveillance, and more broadly surveillance capitalism, breeds distorted decision-making, leading users to outcomes that benefit advertisers more than users, ultimately overpowering the European Union's

[43] Autonomy in Moral and Political Philosophy, Stanford Encyclopedia of Philosophy. <https://plato.stanford.edu/entries/autonomy-moral/>.
[44] Lucas Swaine, 'The Origins of Autonomy' (2016) 37 History of Political Thought 217.
[45] Frederick Neuhouser, 'Rousseau and the Origins of Autonomy' (2011) 54 Inquiry: An Interdisciplinary Journal of Philosophy 478.
[46] Kleingeld, 'The Principle of Autonomy in Kant's Moral Philosophy: Its Rise and Fall' in Eric Watkins (ed), *Kant on Persons and Agency* (Cambridge University Press 2018) 61.
[47] O'Neill (n 39) 3.
[48] Kleingeld (n 46) 62.
[49] O'Neill (n 39).
[50] Domurath, (n 19) 951.

legal attempts to protect user autonomy.[51] This is alarming and warrants concern for the broader democratic implications of weakened collective autonomy, as the foundational principles of self-governance and participatory democracy are threatened.

Botes asserts autonomy as a vital principle in assessing the ethics of persuasive technologies.[52] Core to maintaining user autonomy is in the management of control — individual control over personal data, and control over content consumption.[53] Further, system transparency and facilitating users' comprehension of system design are critical for users to control these technologies.[54] Expanding on Raz's framework, user autonomy involves the notion of 'meaningful choice,' which entails being free from coercion and manipulation, with the state playing a role in facilitating these conditions.[55] Digital media platforms are considered to be highly manipulative, for example through addictive design features, algorithmic manipulation, or through targeted advertising, as previously touched on. Manipulation on social media platforms in particular undermines the self-determination element of autonomy, as users are directed towards choices which benefit the companies and their clients rather than reflecting on their own preferences and control over their lives.[56]

Manipulation ostensibly poses a central threat to user autonomy. Where once persuasive online technologies were designed to personalise advertising to influence users' purchasing decisions, now ethical concerns arise amid the risks posed by these technologies' ability to manipulate, to spread misinformation and to undermine democratic values.[57] Manipulative technologies can undermine individuals' ability to make decisions based on their values and beliefs and identify with the motives of their choices, thereby compromising their autonomy and sense of authorship.[58] Targeted advertising is an example which can cause concern for user autonomy, as Sahebi and Formosa assert that its centre of gravity is to serve the interests of advertisers, and may instrumentalise complex algorithms to influence users' attention and insecurities without their full awareness.[59] Similarly, Lessig's 'code is law' principle asserts that control over code equates to control over behaviour online — autonomy is interlinked with the values embedded in the code of cyberspace, so design choices prove pivotal

[51] *ibid.*
[52] Botes (n 42) 316.
[53] Leyla Dogruel et al., 'I'm Still the Master of the Machine.' Internet Users' Awareness of Algorithmic Decision-making and Their Perception of its Effect on Their Autonomy' (2022) 25 Information, Communication & Society 1315.
[54] Wang et al. (n 41) 5.
[55] Daly (n 33) 11.
[56] Sahebi and Formosa (n 1) 18.
[57] Botes (n 42) 315.
[58] Anastasia Kozyreva et al., 'Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools' (2020) 21 Psychological Science in the Public Interest 112.
[59] Sahebi and Formosa (n 1) 13.

for effective user autonomy.[60]

The Kantian understanding that violating autonomy entails using others as mere means without considering their intrinsic human value and respecting their rights and choices, is difficult to conceptualise in the online sphere. An issue requiring address is the extent to which manipulative techniques impinge on this autonomy and users' individual control over their own lives. This stresses the importance of assessing digital platform transparency alongside user autonomy. The following section will thus survey how platform transparency, or lack thereof, affects user autonomy and the ethical implications of this relationship.

3.2. Platform Transparency

Transparency of online platforms is multifaceted. While a more in-depth enquiry can be done, I am limiting the scope of this analysis to discussing transparency in terms of how it empowers users or grants agency to individuals. Bentham observed, in a political context, transparency or publicity as a means of moralising power, with the idea that public scrutiny can promote integrity and deter corruption and misconduct[61] — 'the more strictly we are watched, the better we behave.'[62] Modern scholarship indicates that with more transparency comes added legitimacy and public support, and importantly, control.[63] Yet, Mokrosinska points out that such assertions of this correlation lack conclusive empirical evidence. Indeed, de Fine Licht links transparency with decreased legitimacy in situations of information overload, or particularly complex matters.[64] Thus, rather than viewing transparency as a cure for the evils of secrecy and democratic deficits, a nuanced appreciation of modern transparency is crucial for examining its role in online platforms. I posit that transparency is a necessary but ultimately insufficient condition to achieving user autonomy. I will first present and analyse transparency as a condition, followed by a critique of its inherent limitations.

De Matos Alves observes the 'kaleidoscopic' nature of definitions of transparency across information technology, political science, sociology and communication studies literature. This part does not attempt to solve the conundrum of transparency in content moderation, but rather the aim is to illustrate components of online transparency. This

[60] Lawrence Lessig, 'Code is Law: On Liberty in Cyberspace' Cartorios, 3. <https://cartorios.org/wp-content/uploads/2020/11/LESSIG._Lawrence_Code_is_law.pdf>.
[61] Dorota Mokrosinska, 'Government Transparency: Dispelling the Myth' in Maarten Hillebrandt, Paivi Leino-Sandberg and Ida Koivisto (eds) *(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice* (Routledge 2023), 172.
[62] Jeremy Bentham, Stanford Encyclopedia of Philosophy. <https://plato.stanford.edu/entries/bentham/>.
[63] Mokrosinska (n 61) 174.
[64] Jenny de Fine Licht, 'The Janus Face of Transparency: Balancing Openness and Secrecy in Democratic Decision-making' in Dorota Mokrosinska (ed), *Transparency and Secrecy in European democracies: Contested trade-offs* (Routledge 2020), 22.

will help to better understand and discuss the transparency measures enshrined in the DSA – which aims to implement improved safeguards for users online and to rebalance the relationship between users, platforms and public authorities.

Conceptualising personal transparency is a complex task, existing scholarship notes its lack of clear definition.[65] Further, transparency has evolved as Turilli and Floridi conceptualise transparency as a factor that either facilitates an adherence to ethical practices and principles or hinders their operation within organisations. They frame transparency not merely as an ethical principle in itself, but rather as a 'pro-ethical' condition that enables ethical conduct to flourish within organisations.[66] The ethical nature of information transparency is important to accentuate the relationship between intermediaries, users, stakeholders, and other partners. In practice, this entails providing users with disclosures regarding data collection practices, processes like personalisation, and data sharing with third parties.[67] Wang et al. relate transparency to explainability and interpretability i.e. the comprehensibility of decisions within online systems, which can originate from algorithms or human agents and have potential implications for consumers or end users.[68]

Platform transparency practices can be identified as, inter alia, encompassing transparency reports - documents provided by companies with the aim to shed light on their internal operations and particularly, how they interact with governmental bodies in the context of content moderation.[69] Ad transparency has expanded with platforms now offering users insight into why they were targeted with specific ads, and disclosing the identities of the advertisers behind them, for example, Facebook's 'Why am I seeing this?' button.[70]

The challenges encountered with transparency and its effective implementation stem from its operationalisation. Perhaps this is grounded in the fact that transparency seems to orientate more around knowledge as opposed to action. Current measures may lack effect and are said to be opaque due to the absence of clear oversight and allocation of responsibility. A superficial performance of transparency forms resulting in

[65] Claire M Segijn et al., 'A Literature Review of Personalisation Transparency and Control: Introducing the Transparency-Awareness-Control Framework' (2021) 9 Algorithmic Systems in the Digital Society 121.
[66] Matteo Turilli and Luciano Floridi, 'The Ethics of Information Transparency' (2009) *11* Ethics and Information Technology 110.
[67] Segijn et al. (n 65) 122.
[68] Wang et al. (n 41) 2.
[69] Aleksandra Urman and Mykola Makhortykh, 'How Transparent are Transparency Reports? Comparative Analysis of Transparency Reporting Across Online Platforms' (2023) 47 Telecommunications Policy 2.
[70] Athanasios Andreou et al.,'Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations' (Network and Distributed System Security Symposium, San Diego, February 2018) 6.

an approach which likens transparency to a commodity as opposed to a sincere commitment to ethical standards or provision of genuine insight into algorithmic or surveillance practices.[71] Further, platforms' business models remain central in assessing transparency. Online platforms are purportedly asserting their transparency commitments by co-opting social responsibility rhetoric, yet this potentially obfuscates larger questions concerning business practices and internal decisions made related to the commercialisation and monetisation of user data.[72] Information asymmetries also present a significant challenge for transparency, the two being 'integrally connected'.[73] An information asymmetry refers to the substantial differences in information available to data-driven companies, such as Google and Facebook, compared to consumers and platform users. This imbalance may leave users in a vulnerable position where they may struggle to make well-informed decisions about their data usage or to exercise their rights effectively.[74] A systemic imbalance between the information that data controllers and users have access to can hinder the latter's ability to address concerns or rights violations. The issue of data control leads to considerations of autonomy in online spaces, where, echoing de Fine Licht above, research has shown that increased transparency does not necessarily result in increased control.[75] Indeed, critical transparency studies reveal that the long presumed belief, derived from traditional governance studies, that more information inherently leads to improved accountability and efficiency is no longer in vogue.[76] The preoccupation with solving the algorithmic transparency conundrum is misguided and narrow-minded as greater attention should be directed towards the socio-technical dynamics at play i.e. the algorithm is not the only device which shapes outcomes and user experience and decision making; the social context of usage, or 'the people around the black box' also plays a crucial role which regulation often overlooks.[77] Leerssen presents a more nuanced and updated perspective, suggesting that transparency regulations perhaps ultimately act as a pretext for dodging more strenuous duties.[78] Platforms may cling to transparency obligations like a life vest, claiming that their efforts are sufficient. This becomes problematic if we determine that transparency, as an anchor for regulation, is not effective.

Evidently, the examination of transparency and autonomy in the context of

[71] de Matos Alves (n 37).
[72] *ibid* 108.
[73] Peter van de Waerdt,'Information Asymmetries: Recognising the Limits of the GDPR on the Data-driven Market' (2020) 38 Computer Law & Security Review 2.
[74] *ibid*.
[75] de Fine Licht (n 64).
[76] Paddy Leerssen, 'Outside the Black Box: From Algorithmic Transparency to Platform Observability in the Digital Services Act' (2024) 4 Weizenbaum Journal of the Digital Society 2.
[77] *ibid* 8.
[78] *ibid* 4.

online platforms reveals a complex landscape shaped by shifting societal norms and the interplay between individual rights and corporate interests. Questions persist about the independence and efficacy of existing transparency mechanisms. While they are essential for holding platforms accountable, they must go beyond mere disclosure to empower users with meaningful insights into platform operations and decision-making processes. Similarly, autonomy online requires more than the illusion of choice; it demands robust safeguards against manipulation and coercion, ensuring that individuals can exercise genuine control over their digital experiences. Grounding the analysis of regulatory measures like the DSA in an interdisciplinary philosophical framework allows us to evaluate how well modern notions of transparency and autonomy align with their foundational principles. Further, in my view we should be wary of embracing transparency as a framework for regulation. Regulatory efforts to enhance transparency are not categorically incorrect, but we must be cautious in preventing transparency from becoming a superficial fix that acts as a veneer for deeper systemic issues. Over-reliance on transparency as a regulatory strategy risks lulling users and lawmakers alike into a false sense of security whereby they believe that they are autonomous and informed in as much as possible about their digital choices and lives, yet still are subject to subtle forms of influence and control. In my view, a regulatory framework centred on transparency alone is not radical enough to achieve genuine autonomy, if we define autonomy, based on the above analysis, as freedom from manipulation and meaningful control over personal data and content consumption, and participation in a collective framework which upholds the dignity and rights of all individuals.

4. Analysis of Recommender Systems

Recommendation systems are automated tools that support decision-making by suggesting items tailored to users' preferences, significantly shaping their digital experiences. RSs aim to guide choices, acting as a form of digital nudging by modifying users' digital choice architecture.[79] They play a key role in digital platform governance by filtering vast amounts of information and presenting content deemed relevant to users.

However, RSs lack transparency in their rationale,[80] which can affect users' practical reasoning and autonomy by subtly influencing their choices and perceptions of available options - acting as 'sticky traps.'[81] The influence of RSs extends beyond individual decision-making to societal impacts, such as polarisation, equality, and democracy. Concerns about the manipulative potential of RSs, particularly their ability to steer user attention and create filter bubbles, have sparked debates about their ethical implications on user autonomy.[82] The DSA addresses some of these concerns by requiring transparency and user control over RSs parameters, but challenges remain in guaranteeing that these measures are effective and accessible.

Technically, RSs use algorithms to predict and suggest items based on user data, but their proprietary nature and privacy issues complicate independent assessment of the structure and functioning of RSs utilised by online platforms.[83] Ethical concerns include privacy breaches, behaviour manipulation, and exposure to harmful content. User-centred solutions, while promoting transparency, can unfairly shift the responsibility onto users, who may lack the expertise to manage their privacy and preferences effectively.[84] Genuine user autonomy requires not just information but also the ability to understand and act on that information effectively. If users cannot manage their settings well, their autonomy is more theoretical than practical.

Analysing recommender systems in the context of user autonomy and transparency under the DSA is crucial. They have the potential to both enhance and undermine user autonomy. Their design and implementation require careful ethical

---

[79] Karina Grisse, 'Recommender Systems, Manipulation and Private Autonomy: How European Civil Law Regulates and Should Regulate Recommender Systems for the Benefit of Private Autonomy' in Sergio Genovesi, Katharina Kaesling and Scott Robbins (eds) *Recommender Systems: Legal and Ethical Issues* (Springer, 2023) 137.
[80] *ibid.*
[81] Silvia Milano et al,. 'Recommender Systems and Their Ethical Challenges' (2020) 35 AI & Society 962.
[82] Matteo Fabbri, 'Self-determination Through Explanation: An Ethical Perspective on the Implementation of the Transparency Requirements For Recommender Systems Set By the Digital Services Act of the European Union' (AAAI/ACM Conference on AI, Ethics, and Society, Montreal, August 2023) 654.
[83] *ibid.*
[84] Milano (n 81) 961.

consideration, balancing commercial objectives with the need to protect users' rights and foster trust. The effectiveness of regulatory measures like the DSA will depend on the extent to which users understand and can influence how RSs function, ensuring these systems serve their best interests without compromising autonomy. It is crucial we can recognise our choices as our own to avoid the risk of self-alienation and to make autonomous decisions.[85]

Undoubtedly, recommender systems profoundly affect user autonomy and the decisions users make by structuring the environment in which these decisions occur.[86] The conception of user autonomy on online platforms that I utilise emphasises individual control and meaningful choice, ensuring freedom from coercion and manipulation, and respecting users' rights and intrinsic human value within platforms. This concept entails managing the control over personal data and content consumption, necessitating system transparency and user comprehension of design to facilitate genuine self-determination and moral governance.

A fundamental requirement for recommender systems to support autonomous decision-making lies in users' ability to discern the underlying rationale behind recommendations. Algorithms, complex mathematical formulas and processes embedded within software systems, govern the selection, prioritisation, categorisation, and presentation of information and interactions online. Algorithms can appear as black boxes to users of online platforms, highlighting a need for transparency in interacting with these systems.[87] The opaque nature of algorithms can lead to situations where users feel their choices are influenced or constrained without their full understanding or consent.[88] Fabbri states that this opacity exacerbates the problem of epistemic fragmentation, where personalised content isolates users from shared experiences and common knowledge.[89] This can be seen in particular in targeted advertising, where algorithms may prioritise commercial interests over user preferences. Users, nudged by algorithms, may make purchases they might not have instinctively approved of otherwise – autonomy is thus routinely sacrificed on the altar of profit. When recommender systems are used manipulatively, they bypass rational deliberation and subvert the capacity for conscious decision-making.[90] Sunstein's criterion that influence counts as manipulative when it does not engage the capacity for reflection and

[85] Marius Bartmann, 'Reasoning with Recommender Systems? Practical Reasoning, Digital Nudging, and Autonomy' in Sergio Genovesi, Katharina Kaesling and Scott Robbins (eds) *Recommender Systems: Legal and Ethical Issues* (Springer, 2023) 143.
[86] *ibid* 134.
[87] Dogruel et al. (n 53) 1313.
[88] Fabbri (n 82).
[89] *ibid.*
[90] Grisse (n 79) 108.

deliberation is particularly relevant here.[91]

The inherent complexity of algorithms, coupled with the technical skills required to comprehend their code, exacerbates the challenge for users to exert meaningful control over their online experiences. Providers often cite reasons of corporate secrecy or technical complexity in withholding algorithmic details from users, further perpetuating the opacity that undermines user autonomy. However, efforts to enhance transparency in algorithmic decision-making, while desirable in principle, face practical limitations. Complete transparency may not always be feasible due to the dynamic and context-specific nature of algorithmic operations. Moreover, overly transparent algorithms can be vulnerable to exploitation or manipulation, potentially leading to biased outcomes or unintended consequences.[92] Thus, the critical question arises: where should we establish boundaries to ensure that user autonomy is respected and maintains its integrity under the current digital landscape dominated by recommender systems? I am first interested in assessing philosophical conceptions of the relationship between recommender systems and autonomy, before getting into an analysis of the DSA's provisions regarding recommender systems.

According to de Vries, personal identity is mediated by the categories assigned by recommender systems.[93] These systems do not track a pre-established identity but rather create user identities dynamically based on collective actions. This ongoing reconfiguration can disconnect users from their self-identity, as the algorithmic labels may not align with recognisable or meaningful attributes.[94] The notion that identity is fluid and constantly shaped by external influences aligns with Foucault's concept of 'techniques of the self.'[95] Recommender systems, through their algorithmic processes, function as an 'active membrane' that adjusts and redefines user profiles.[96] This perspective suggests that user profiles are not static representations but are continually evolving outputs influenced by both individual behaviours and collective data.[97] Stiegler's idea that tools and technologies mediate our identity formation further underscores this point.[98] Modern profiling algorithms, akin to traditional technological influences like supermarket layouts, shape consumer behaviour and identity formation. However, the speed and complexity of modern algorithms create highly dynamic and

[91] Cass R Sunstein, 'Fifty Shades of Manipulation' (2016) The Haravard John M. Olin Discussion Paper Series 01/2016, 6.
[92] Dogruel et al. (n 53) 1313-1314.
[93] Katja de Vries, 'Identity, Profiling Algorithms and a World of Ambient Intelligence' (2010) 12 Ethics and Information Technology 82.
[94] *ibid* 81.
[95] Tyler Reigeluth, 'Recommender Systems as Techniques of the Self?' (2017) Genealogy+Critique <https://www.genealogy-critique.net/article/id/7054/#>.
[96] *ibid.*
[97] *ibid.*
[98] de Vries (n 93) 80.

detailed profiles, constantly adapting to individual preferences in real time.

4.1. DSA Implications

To mitigate the risks posed to personal autonomy, transparency in algorithmic processes is crucial. Users need to understand why certain recommendations are made to integrate them meaningfully into their decision-making processes.[99] By dissecting the DSA's approach and potential implications on user autonomy and transparency, I aim to provide an improved understanding of its approach to empowering users, and the extent to which it holds platforms accountable.

The DSA defines a recommender system as:

> a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed.[100]

Article 27 DSA obliges online platforms employing RSs to disclose the 'main parameters' utilised in their algorithms. This requirement extends to all online platforms, not just those facilitating transactions between users, reflecting a thorough approach to algorithmic transparency. Article 27(2) DSA further stipulates that platforms must provide explanations for the relative importance of these parameters, in 'plain and intelligible language.'[101] Thus, this approach to transparency extends beyond merely informing users but to enhance public accountability of algorithmic decision making. What remains troubling about this obligation, however, is that platforms are entitled to hide these disclosures within their often lengthy terms and conditions. Busch points out that this suggests an underlying scepticism on behalf of legislators regarding the likelihood that users will meaningfully engage with or understand these disclosures, thereby limiting the impact of this transparency effort.[102] Stray et al. indicate that what constitutes a 'main parameter' remains ambiguous.[103] Thus, the effectiveness of these provisions is undermined by their indirect accessibility, effectual transparency ought to be directly integrated into the recommendation interface.[104]

---

[99] Reigeluth (n 95).
[100] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Article 3. Hereinafter called 'Digital Services Act.'
[101] Article 27, Digital Services Act.
[102] Busch, 'From Algorithmic Transparency to Algorithmic Choice: European Perspectives on Recommender Systems and Platform Regulation' in Sergio Genovesi, Katharina Kaeslingand Scott Robbins (eds) *Recommender Systems: Legal and Ethical Issues* (Springer, 2023), 47.
[103] Jonathan Stray et al, 'Building Human Values into Recommender Systems: An Interdisciplinary Synthesis' (2024) 2 ACM Transactions on Recommender Systems 29.
[104] Grisse (n 79) 120.

User autonomy is heightened with the DSA's 'tentative step' towards algorithmic choice.[105] Article 27(3) DSA requires all online platforms to inform users about options available to modify their recommendation parameters, and to do so with 'easily accessible' functionality.[106] Article 38 DSA further requires VLOPs and VLOSEs to include at least one option which is not based on profiling.[107] The efficacy of the implementation of these choices will depend greatly on the user interface design on platforms, and the willingness of platforms to provide meaningful options. These provisions undoubtedly present a model shift towards greater user agency and autonomy, but arguably an incremental one. In my view, limiting the profiling-free option to VLOPs and VLOSEs reflects a reluctance to fundamentally alter the underlying structures of algorithmic recommendation systems and perpetuates discrepancies in user autonomy protection.

In the context of algorithmic advertising targeting consumers, Article 26 DSA perhaps makes a more robust attempt at getting under the hood of the underlying practices determining what advertisements users engage with. The fourth subsection expands source transparency to parameter transparency by obligating the identification of who is responsible for a message, to providing information as to why a particular user, based on elements like their behaviour, preferences and profile, was shown a particular advertisement.[108] Further, while the DSA restricts the use of sensitive data for profiling and prohibits targeting advertisements based on such data, it stops short of a comprehensive ban on emotionally manipulative or fear-inducing recommendations. Although minors are shielded from targeted advertising based on profiling, broader protections against emotional manipulation are lacking, particularly concerning the use of inferred sensitive data not explicitly covered by the GDPR (Art. 26(3)).

VLOPs and VLOSEs are required under Article 34 DSA to undertake an annual systemic risk assessment. They must have regard for risks emanating from illegal content, negative effects on fundamental rights, and on areas such as public health, minors, and electoral processes. Recommender systems must be adapted if harm is found. Anchoring the regulatory approach in risks arguably disproportionately focuses on potential harms and not actual ones.[109] Again, this provision obscures the necessity of a deeper approach: privileging protection should be inherent in the design of a system and determining its guiding principles, rather than being an afterthought for regulation to address.

---

[105] Busch (n 102) 46.
[106] Article 27(3), Digital Services Act.
[107] Article 38, Digital Services Act.
[108] Elena Izyumenko et al, 'Online Behavioural Advertising, Consumer Empowerment and Fair Competition: Are the DSA Transparency Obligations the Right Answer?' (2024) 14. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4729118>.
[109] Stray et al. (n 103) 27.

In sum, recommender systems' role in shaping user autonomy and decision making is pivotal on online platforms. Their opacity presents autonomy concerns and while the DSA tries to quell them, I believe due to their complexity and proprietary nature, the provisions leave something to be desired as they do not significantly disrupt the dominant position of online platforms, particularly VLOPs. There must be a balance between increased transparency and preventing unintended biases and exploitation. Corporate interests largely remain unphased by these regulations, as the DSA's measures, while promoting transparency and user choice, do not fundamentally challenge the business models of these powerful entities.

5. Examination of Dark Patterns

First coined by Brignull, 'dark patterns' are sophisticated user interface design strategies employed within digital systems to manipulate users into behaviours that benefit the designer, often at the expense of the user's autonomy and best interests.[110] These tactics, which are 'increasingly ubiquitous', subtly or overtly steer users towards actions they might not have taken otherwise, exploiting consumer vulnerabilities and undermining informed decision-making regarding personal data, privacy permissions, contractual agreements, and other critical choices.[111] Dark patterns pervade a wide range of digital products, including websites, mobile applications, computer software, and operating systems, thereby contributing to an inequitable digital environment.[112] Lupiáñez-Villanueva et al. found that at least one dark pattern was utilised by 97% of the most widely used websites and apps among EU consumers.[113]

Examples of dark patterns that exploit users' attention include autoplay features and design that enables infinite scrolling. The patterns most concerning for user autonomy include forced registration and 'privacy zuckering'[114] where users are tricked into thinking registration is necessary or coaxed into sharing more personal data than intended. 'Preselection' manipulates interfaces by pre-selecting company-friendly defaults or hiding crucial information. This causes users to make decisions that favour the designer without full awareness of the consequences. The 'roach motel' model is a dark design which makes sign-ups easy and over-complicates opt-outs or cancellations.[115] Recently, the Commission formed the view that the social media platform X is in breach of the DSA's prohibition of dark patterns for, inter alia, allowing any user to purchase a 'blue checkmark' that was previously only available to notable figures. The Commission outlined that this practice deceives users and their ability to make free and informed decisions about who they interact with and the authenticity of accounts. If this preliminary view is confirmed, X could face a fine of up to six percent

[110] Harry Brignull, 'Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff' (90 Percent of Everything, July 8, 2010) <https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/index.html>.
[111] Colin M Gray et al. 'Mapping the Landscape of Dark Patterns Scholarship: A Systematic Literature Review' (In Designing Interactive Systems Conference, Pittsburgh, July 2023), 188.
[112] Fabiana di Porto and Alexander Egberts, 'The Collective Welfare Dimension of Dark Patterns Regulation' (2023) 29 European Law Journal 2.
[113] European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment - Dark patterns and manipulative personalisation - Final report (Publications Office the European Union 2022), 120 <https://data.europa.eu/doi/10.2838/859030>.
[114] Tim Jones, 'Facebook's 'Evil Interfaces' (Electronic Frontier Foundation, April 29, 2010) <https://www.eff.org/de/deeplinks/2010/04/facebooks-evil-interfaces>.
[115] Szymon Osmola, 'Neither Rules nor Standards: How to Regulate Dark Patterns' (2023), 6. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4515963#:~:text=Szymon%20Osmola,-The%20Edmond%20J&text=The%20article%20demonstrates%20that%20the,personalised%20online%20interface%20more%20generally>.

of its worldwide turnover.[116]

Different facets of autonomy are impacted by different types of dark patterns.[117] Control as an element of autonomy, for example, is eroded when users are deprived of the ability to make decisions relevant to them, such as when software updates occur automatically or when users are burdened with the responsibility of opting out of implied consent mechanisms. Users' independence is exploited by 'FoMo-centric designs' prevalent on social media, as they intentionally limit users' self-control by providing momentary sensations of gratification, encouraging a reliance on technology and compulsive and addictive engagement.[118] Westin et al. discovered that with FoMo-centric designs, presenting users with a choice between social benefits and privacy does not provide them with a genuinely fair option.[119]

Just as different types of dark patterns impact various facets of autonomy, so too must these elements be safeguarded by tailored regulatory responses. Ahuja and Kumar advise that while autonomy as control can be safeguarded through detailed legal rights such as those in the GDPR, it does not adequately address the concept of autonomy as agency – the capacity for individuals to make informed decisions. This can be observed with the prevalence of click-wrap consent agreements, as users often accept terms without fully understanding them.[120] Further, autonomy as independence poses a greater regulatory challenge, as protective measures may be viewed as paternalistic, particularly in contexts involving restrictions on social media or gaming.

Evidently, analysing dark patterns and their impact on user autonomy alongside the DSA's approach to addressing these challenges is critical. Brignull's initial definition of dark patterns is inherently concerned with the issue of autonomy, as he defined them as 'tricks that make you do things you didn't mean to.'[121] The legal justification behind regulating dark patterns at the European level is rooted in Article 7 of the Charter, the right to respect for private and family life.[122] This article supports the protection of individual autonomy and the ability to act in accordance with one's true preferences.[123]

---

[116] European Commission, Press Release 'Commission sends preliminary findings to X for breach of the Digital Services Act' (12 July 2024) <https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3761>.
[117]Sanju Ahuja and Jyoti Kumar, 'Conceptualizations of User Autonomy Within the Normative Evaluation of Dark Patterns' (2022) 24 Ethics and Information Technology 2.
[118] Fiona Westin and Sonia Chiasson, '"It's So Difficult to Sever that Connection": The Role of FoMO in Users' Reluctant Privacy Behaviours. In CHI Conference on Human Factors in Computing Systems' (Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, May 2021).
[119] Karagoel and Nathan-Roberts (n 14) 753.
[120] Ahuja and Kumar (n 117) 13.
[121] Brignull (n 110).
[122] Charter of Fundamental Rights of the European Union, Article 7.
[123] Thomas Akhurst et al, How Should the European Union Regulate Dark Patterns? (2023) SciencesPo Digital, Governance and Sovereignty Chair, 4.

Beyond the normative critique of dark patterns manipulating user choices and exploiting cognitive biases, there is a strong argument for regulation. Compared to the designers of dark patterns, average users of online platforms lack incentive and resources for legal representation due to the minimal individual harm a dark pattern may produce. Further, users must be cognisant of these practices to begin with, Osmola writes that the high-frequency and low-value nature of dark patterns makes users hesitant to exercise their rights.[124]

5.1. DSA Implications

Perhaps this is why the European regulatory response to dark patterns, most recently seen with the DSA (and DMA) focuses on their collective impact on the digital economy, rather than harm at the individual level. This is because both instruments represent market-oriented responses aimed at addressing the broader impact of dark patterns on, *inter alia*, fundamental rights, consumer trust and fair competition.[125] This emphasis on the cumulative impact of dark patterns still aligns with our previously outlined definition of autonomy within the context of online platforms. It is a collective effect on the decision-making capabilities and trust of the user community, or in a certain understanding, collective user autonomy. Importantly, Di Porto and Egberts advise that solving autonomy issues stemming from dark patterns at the individual level does not solve the issues caused by the immense scale of dark patterns' impact.[126]

Recital 67, the first legal definition of dark patterns in the EU regulatory landscape, provides that 'dark patterns on online interfaces of online platforms are practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions.'[127] Article 25 DSA prohibits providers of online platforms from designing, organising, or operating their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.[128]

Article 25 DSA joins the pre-existing frameworks of the Unfair Commercial Practices Directive (UCPD) and the General Data Protection Regulation (GDPR) to enhance consumer protection and address manipulative practices in online platforms. Before assessing the weaknesses, it may first be apt to evaluate the strengths of the DSA in maintaining user autonomy and ensuring transparency regarding dark patterns.

As a preliminary point, the DSA's status as a regulation is, in my view, a strength.

[124] Osmola (n 115) 19.
[125] di Porto and Egberts (n 112) 5.
[126] *ibid* 6.
[127] Recital 67, Digital Services Act.
[128] Article 25(1), Digital Services Act.

Having uniform binding legal force and direct effect throughout the entire Union is more preferable than the flexibility a directive affords. This is particularly important in the field of online safety and the transnational impact that online harms can have. This approach strengthens user autonomy online by ensuring consistent protection across member states. Secondly, the DSA provides an unequivocal prohibition of dark patterns. While the GDPR provides protection against dark patterns in the context of processing of personal data, and the UCPD protects consumers from misleading or aggressive practices that distort their economic behaviour, the DSA purports to take a broader approach, though the efficacy of this will be contested. However it is beneficial that the DSA moves protection beyond the direct relationships between data controller and subject, and trader and consumer.[129]

Further, the intention of the operator is absent from the DSA's determination of whether a practice constitutes a dark pattern. An emphasis on the real impact a design choice has on users and their decision-making enhances user autonomy and aids user-centric digital environments. This disregard for intention also means that even unintentional manipulative designs can be scrutinised and addressed, thereby protecting users from being subtly coerced into undesired behaviours.

The opportunity for independent vetted researchers to request data from VLOPs and VLOSEs under Article 40 is a welcome development. The provision allows for greater transparency and public oversight of VLOPs' and VLOSEs' practices, and would fill the lacuna of research currently available. By identifying systemic risks, researchers can study harmful activities such as the spread of illegal content and misinformation, thereby promoting user autonomy and risk mitigation. However, VLOPs and VLOSEs may not eagerly embrace this provision due to the aforementioned information asymmetries between platforms and users and the tension between corporate interests and individual rights. While Article 40 acknowledges the interests of VLOPs and VLOSEs in protecting their security and trade secrets, it is imperative that in practice, this does not water down the efficacy of the provision. The Commission must make certain that researchers must not only be given access to data, but that the conditions of this must be effectual. For example, researchers must not be 'dumped', so to speak, with vast amounts of indiscernible data.[130] Or as another example, in the aforementioned preliminary decision of the Commission, X's conditions granting researchers access to its programming interface allegedly breaches the DSA for imposing a disproportionately

[129] Inge Graef, The EU regulator patchwork for dark patterns: an illustration of an inframarginal revolution in European law? (2023) Tilburg Law and Economics Center (TILEC) Discussion Paper 2023-07, 10.
[130] Akhurst et al (n 123) 25.

high fee, discouraging researchers from conducting their projects.[131]

My criticism of the DSA's approach to addressing dark patterns derives from the text itself, and in its enforcement. What constitutes a material distortion or impairment of behaviour as per the first paragraph of Article 25 DSA is too vague to discern currently and is in need of interpretation. The DSA might adopt the framework of the UCPD, which includes both actual and potential deceptive practices.[132] In order for the DSA to apply, it must be confirmed that a particular dark pattern does not breach the UCPD, though decisions delineating this are not in abundance. Thus, clarification of Article 25(1) DSA is required on an ex-post case-by-case basis so it is clear how to address specific dark patterns.[133]

Evidently, another core difficulty is the interplay between the parallel frameworks of the DSA, the GDPR and the UCPD, while aiming to be complementary, may create legal uncertainty concerning the applicable regulations for various dark patterns as the DSA evolves. Article 25(2) DSA reduces the prohibition of dark patterns to instances not covered by the GDPR or the UCPD. The scope of this provision and its trigger(s) remains unclear, however making the DSA prohibition dependent on its counterparts arguably makes it too narrow and hinders the instrument's efficacy compared to the GDPR and UCPD.[134] If this provision is interpreted broadly, whereby it does not apply to any practice falling under the broad and principle-based protections in the GDPR and UCPD,[135] its scope is limited. Otherwise, a narrow interpretation requiring that the DSA cannot be applied before it is established that a certain practice is not illegal under the GDPR or UCPD, ultimately gives precedence to these two instruments. This is concerning for user autonomy because the fragmented nature of these regulations creates a misalignment in triggers for protecting the actual harm caused by dark patterns.[136] Instead of the nature of the harm suffered, the protection mechanisms and scope of these three instruments are based on legal definitions and their framework. Instead of filling in the protection gaps of the existing regulation, the DSA may inadvertently introduce gaps of its own. While I am not yet convinced by Osmola's contention that the DSA pays mere 'lip service' and does not provide users with substantial protection,[137] I believe Article 25(2) DSA could have been a valuable opportunity for a more harmonised

[131] Commission, Press Release: 'Commission sends preliminary findings to X for breach of the Digital Services Act' 12 July 2024 <https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3761>.
[132] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive').
[133] Osmola (n 115) 40.
[134] Graef (n 129) 18.
[135] *ibid.*
[136] *ibid.*
[137] Osmola (n 115) 41.

European approach to dark patterns.

Article 25(3) DSA grants the Commission authority to issue guidelines on the application of the ban on dark patterns.[138] This can be seen in both a positive and negative light. The interpretation and enforcement of such guidelines within a single body can be seen as a strength allowing for a more consistent approach across member states. However, guidelines are non-binding and may not be sufficiently specific to effectively tackle dark patterns. Further, the Commission has not yet issued such guidelines since the enactment of the DSA. This slow pace, coupled with the ambiguous scope analysed above, undermines the potential protection that could be afforded to users from dark patterns.

The annual systemic risk assessments required of VLOPs and VLOSEs with over 45 million users under Articles 34 and 35 DSA can be cautiously welcomed as a step to better protect users from harmful dark patterns. The presence and effect of dark patterns must be monitored and evaluated. VLOPs are required to implement strategies to neutralise dark patterns, which can include redesigning interfaces to prevent user manipulation, especially protecting vulnerable groups like children. What is strong about this obligation is that borderline design choices that loophole the Article 25 DSA requirement and are not explicitly illegal can still be assessed and their effect mitigated. However, it is concerning that employing dark patterns is immensely profitable for platforms,[139] which in my view, creates an inevitable conflict with the obligation to mitigate them. Given that these platforms possess complete access and knowledge of the intricacies of their practices, design choices and user data, they are best positioned to tackle this task. But it rightfully creates suspicion as to the commitment to fulfilling this obligation.

Overall, the challenge dark patterns present to transparency and user autonomy is significant. While the DSA's approach to mitigating these issues is both ambitious and necessary, its success will depend on the rigorous enforcement of these regulations and the genuine commitment of platforms to uphold user autonomy and transparency. It will also depend on the effort to centralise its enforcement, through cooperation between nationally-appointed Digital Services Coordinators (DSCs). Article 60 DSA obliges DSCs to assist one another and coordinate joint investigations, and Article 85 DSA establishes a 'reliable and secure' information sharing system.[140] The European Board for Digital Services, as per Article 61, is the advisory body in charge of these centralisation efforts. I cautiously approve of the DSA measures but am persuaded by Leiser and Santos'

[138] Art 25(3), Digital Services Act.
[139] Osmola (n 115) 42.
[140] Art 85, Digital Services Act.

assertion that we need to be going beyond the final arena of users' decision making – the online interface of platforms that they interact with.[141] To truly ensure dark patterns do not undermine user autonomy, it is essential to address the underlying mechanisms that make platforms' interfaces so personalised and engaging. By focusing solely on the interface, the DSA tackles only the tip of the iceberg. I contend that the DSA's provisions skirt around the fundamental fact that platforms are powerful by virtue of being the ultimate controllers of their own infrastructure and data. The bulwark that is their market dominance is not sufficiently challenged by Articles 25, 34 and 35 DSA.

[141] Mark Leiser and Cristiana Santos, 'Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface' (2024) 15 European Journal of Law and Technology 29.

6. Substantial Reform or Superficial Fix? A Discussion

Based on the above analyses of recommender systems and dark patterns under the DSA, it is evident that we are still in a speculative phase regarding its precise effectiveness. Much remains to be seen and much of the regulation's success is reliant on political will, institutional and infrastructural investment at both the European and national levels. While acknowledging these uncertainties is important, it should not prevent us from looking beyond the letter of the law. This thesis has aimed to provide a more holistic socio-legal view of the current state of affairs.

In this writer's view, the DSA demonstrates a needed step away from self-regulation in digital policy towards stronger public interventionism.[142] While this progression is undeniably essential, following Maroni's perspective, there are concerns that the DSA legitimises and entrenches platform power within the regulatory framework.[143] I concur with this, and as evidenced above, believe that the overall impact the regulation has on creating a more responsible internet (if we are to understand responsible as meaning a space which is thoughtfully designed as safe and accountable), is menial. Vapid transparency measures fail to confront the deeper structural problems which solidify platform power.

Specifically, a core contention of mine is that if EU regulation on internet safety is truly human-centric as it proclaims, designing legislation with the goal of achieving transparency for transparency's sake is a futile exercise if the broader aim is to genuinely empower users and provide them with autonomy. As evidenced above, disclosures and more information alone are surface level attempts at giving power back to users. But this type of transparency serves as a distraction, and produces a false sense of accountability.[144] Geng and Mokrosinska cite a lack of evidence that enhanced transparency curbs irresponsible behaviour on behalf of platforms.[145]

Of course, it would be remiss to say that the DSA is a completely wasted foray into enhancing internet protection within the Union, as regulation in this field is no longer optional. Overall, providing transparency about targeted advertising and increasing regulation around dark patterns for examples are all positive steps forward. However, from the perspective of user autonomy, as we have defined it through our interdisciplinary approach, I determine that the DSA misses the core issue. Specifically, in the case of recommender systems, that transparency should be viewed as a tool to

[142] Sebastian Heidebrecht, 'From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance' (2023) 62 Journal of Common Market Studies 216.
[143] Maroni (n 11) 2.
[144] Leerssen (n 76) 28.
[145] Mokrosinska (n 61) 172. Yinuo Geng, 'Transparency For What Purpose?: Designing Outcomes-Focused Transparency Tactics for Digital Platforms' (2023) 16 Policy & Internet 3.

complement the main goal of user protection, and for dark patterns true autonomy originates in the system design itself, well before end users interact with it.

In respect of recommender systems, informing users of how recommendations are generated, the parameters involved, their importance, and providing the option to modify such parameters under Article 27 DSA may help bridge information asymmetries to some extent. But in the larger picture, I am sceptical of their greater impact, which may do little more than disproportionately burden users with information.[146] The obligation for VLOPs and VLOSEs under Article 34 to carry out an annual systemic risk assessment has its own strengths and weaknesses as a mechanism in of itself, analysed above. However again, when considering the broader picture, I am sceptical of the overall impact of this. Periodic auditing may only provide a 'snapshot logic' of what is going on behind the scenes,[147] reinforcing the notion that platforms remain in control in a sense. The lack of legal guidance and the vague language of the provision risks overreach into things like freedom of expression, for example.[148]

The question then arises, what makes transparency of recommender systems meaningful? How can platforms employ transparency in a way which creates a responsible internet for users?

User-centric transparency is key; going beyond merely making information accessible but making it actionable. For example, instead of attempting to achieve the potentially Sisyphean task of explaining complex algorithms to users, user autonomy can be enhanced by allowing users to customise the parameters of their recommendation algorithms, thereby influencing the content they see. However, the DSA does not require platforms to offer more than one option to modify or influence these parameters, it only mandates that where such multiple options are given, platforms must provide a functionality that easily allows users to select and modify their preferred option. However, platforms have little incentive to part ways with the control over algorithmic decisions which is central to their business models. Interoperability options were proposed and supported by the European Data Protection Supervisor, which would enable personalised RSs to work across multiple platforms. This could help reduce the dominance of and concentration of power held by major online platforms, by facilitating competition and enabling smaller players to offer more personalised services, potentially swinging the pendulum in favour of greater user control in digital

[146] Geng (n 145) 13.
[147] Leerssen (n 76) 9.
[148] July Baltus, 'How will the framework for risk management in the Digital Services Act manage the tension between curbing disinformation and protecting freedom of expression' Studievereniging voor Informatierecht (Amsterdam, 18 March 2024) <https://svir.nl/how-will-the-framework-for-risk-management-in-the-digital-services-act-manage-the-tension-between-curbing-disinformation-and-protecting-freedom-of-expression/>.

environments.[149] Given these considerations, the DSA provisions on recommender systems utilise algorithmic transparency that falls short of addressing deeper structural issues.

In respect of dark patterns, all subsections of Article 25 DSA require definition and elaboration to properly gauge its effect on user autonomy. My primary concern with the DSA's handling of dark patterns is that, similar to recommender systems, deeper questions and issues are obscured by the regulation's approach. The nature of the DSA's position in the panoply of internet rights protection in the Union (including the GDPR, UCPD, and DMA) is a subsidiary one. Leiser and Santos warn that common patterns such as infinite scrolling and autoplay can slip between the cracks of these frameworks.[150] Implementing more user-centric system design is a method that can mitigate the seemingly pervasive presence of dark patterns. Caragay et al. propose a new design approach which encourages the development of designs that align with user needs and ethical standards, which may nip dark patterns in the bud, so to speak.[151] Documenting standard versions of software concepts and their variants, and moving towards a model which defines acceptable designs through the perspective of positive patterns is a means of achieving this. Regulators then possess an ameliorated and structured framework for articulating best practices in design.[152] What makes effective regulation in this field more difficult is the pace of development. A marrying of technical expertise taken from computer science etc. and legal oversight mechanisms should occur so that regulation keeps pace with the trends of user interface (UI) design and user experience (UX) design, preventing the DSA from being outdated quickly.[153]

What then makes dark pattern regulation effective for user autonomy? The key to answering this lies in amending the power imbalance issue between users and platforms – an asymmetry of both information and design power. The adage 'design is power'[154] refers to the patterns that platforms design which gather user and consumer behaviour and enhance the dark patterns which can exploit consumers in commercial transactions. Platforms hold the power as 'choice architects,'[155] creating the framework within which user autonomy and user decision-making exists. Thus, I concur with Leiser

[149] Kasia Soderlund et al, 'Regulating High-Reach AI: On Transparency Directions in the Digital Services Act' (2024) 13 Internet Policy Review 20.
[150] Leiser and Santos (n 141) 23.
[151] Evan Caragay et al, 'Beyond Dark Patterns: A Concept-Based Framework for Ethical Software Design' (Proceedings of the CHI Conference on Human Factors in Computing Systems, Honolulu, May 2024) 14.
[152] *ibid* 6.
[153] Leiser and Santos (n 141) 30.
[154] Alison Hung, 'Keeping Consumers in the Dark: Addressing 'Nagging Concerns and Injury' (2021) 121 Columbia Law Review 2486.
[155] Weiwei Yi and Zihao Li, 'Mapping the Scholarship of Dark Pattern Regulation: A Systematic Review of Concepts, Regulatory Paradigms, and Solutions from an Interdisciplinary Perspective' (2024), 14. <https://www.arxiv.org/abs/2407.10340>.

and Santos that effective regulation must tackle the entire architecture so that regulating dark patterns is not akin to putting a bandaid on a bullet wound. Osmola's proposal to outright ban algorithms which capitalise on users' cognitive limitations is an interesting one but perhaps is too unrealistic.[156] Regardless of the specific approach, for regulation to be responsible it must toe the line between the legitimate business practices which can be persuasive in nature, and practices which manipulate users. Albeit a tricky distinction, in my view, the ambiguity within Article 25 DSA does not offer a clear path forward for addressing this problem.

To return to our discussion on autonomy, as conceptualised using philosophy and other disciplines, and its translation of this to the online world, what does the DSA signify in this context? Our conception of autonomy, particularly in the Kantian sense, is not merely freedom of choice but about meaningful control. We have established that the DSA's fixation on transparency, without mandating more profound changes in platform design, does little to truly aid users and dismantle the power asymmetries between platforms and users, thereby failing to fully address the nuances of autonomy.

Going forward, what can then be done to genuinely strengthen user autonomy? The findings in this thesis align with Faraoni's argument that existing frameworks insufficiently protect against the 'unprecedented abilities of AI-driven manipulative technologies.'[157] Gartner has identified a shift in autonomy from being a meta-principle underlying rights like privacy and data protection, to explicit recognition in EU regulatory framework,[158] indicating a more aggressive stance towards protecting individual autonomy in the digital sphere.

The DSA entrenches transparency as the leitmotif of the EU's digital strategy. Thus, critiquing transparency as an insufficient regulatory framework for user autonomy is one thing, suggesting where to go from here is quite another. My findings indicate that the focus on algorithmic transparency is often narrow and overlooks broader socio-technical dynamics that can influence users' experiences and decision-making. But as stated previously, transparency is a necessary, yet insufficient means of achieving user autonomy. Perhaps in this context the word inevitable is more appropriate. Therein lies an observation about transparency and autonomy interacting with societal norms and the corporate interests of platforms. Transparency regulations, for what they are worth, do contribute to accountability, their presence is preferable to their absence. But what has become apparent is that true autonomy involves informed choice and protection

[156] Osmola (n 115) 50.
[157] Stefano Faraoni, 'Persuasive Technology and Computational Manipulation: 'Hypernudging out of Mental Self-Determination' (2023) 6 Frontiers in Artificial Intelligence 1.
[158] Maximilian Gartner, 'Regulatory Acknowledgement of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act' (2022) 8 European Data Protection Law Review 462.

from subtle forms of influence and manipulation within a framework that upholds fundamental rights and dignity; transparency, while valuable, cannot serve as the panacea for these issues.

7. Conclusion

Drawing upon a bevy of expertise and insights from law, philosophy, science and technology, communications literature and more, I have sought to address the issues stemming from platform control. My focus has been on particularly examining the relationship and ethical obligations arising between individuals, platforms, and governments, all while considering the urgency of protecting the autonomy of users. While escaping this power may not be possible, the way we intentionally respond to it is.

Overall, this thesis argues that the DSA represents an important but incomplete step in fostering a safer online environment for platform users. By analysing the practical implications of the DSA's provisions as well as combining philosophical, technical, and ethical insights, the thesis identifies the limitations of transparency; it alone does not tackle the systemic issues of control and manipulation. From the conceptual analysis of autonomy, it is evident that in an online context it is often complex and misunderstood, this thesis supports the view that meaningful user autonomy requires more than transparency; it demands a rethinking of the regulatory approach to prioritise user control and the ethical design of digital systems. The DSA's rules on recommender systems and dark patterns open up space for greater user agency, however the root causes of the ethical issues they pose – manipulation, exploitation and unintended biases for example, are bypassed.

Ultimately, this thesis contributes to the ongoing discourse on internet governance by challenging the effectiveness of the DSA in its current form and advocating for a more user-centric, ethically informed regulatory framework. By doing so, I offer a novel perspective on the interplay between autonomy and transparency, with the aim of fostering a more responsible and equitable digital environment.

List of References

EU Sources

Legal or Policy Documents

European Commission, 'A Digital Single Market Strategy for Europe' COM(2015) 192 final (6 May 2015) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192>

European Commission: Directorate-General for Justice and Consumers, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report (Publications Office of the European Union 2022) <https://data.europa.eu/doi/10.2838/859030>

European Commission, 'A Europe Fit for the Digital Age: The Digital Services Act Overview' <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en>

European Commission, Press Release 'Commission sends preliminary findings to X for breach of the Digital Services Act' (12 July 2024) <https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3761>

Legal Sources

European Union Law

Charter of Fundamental Rights of the European Union, 2000/C 364/01, European Union, 18 December 2000

Consolidated version of the Treaty on European Union, 2008/C 115/01, European Union, 13 December 2007

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) [2005] OJ L149/22

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1

Academic Sources

Books

Bradford A, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023)

Daly A, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart Publishing 2016)

Genovesi S, Kaesling K, and Robbins S (eds), *Recommender Systems: Legal and Ethical Issues* (Springer 2023)

Mokrosinska D (ed), *Transparency and Secrecy in European democracies: Contested trade-offs* (Routledge 2020)

Watkins E (ed), *Kant on Persons and Agency* (Cambridge University Press 2018)

Hillebrandt M, Leino-Sandberg P and Koivisto I (eds), *(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice* (Routledge 2023)

Journal Articles

Ahuja S and Kumar J, 'Conceptualizations of User Autonomy Within the Normative Evaluation of Dark Patterns' (2022) 24 Ethics and Information Technology

Akhurst T and others, 'How should the European Union regulate dark patterns?' [2023] SciencesPo – Chair Digital, Governance and Sovereignty <www.sciencespo.fr/public/chaire-numerique/wpcontent/uploads/2023/09/Dark-Patterns.pdf>

Bharghava VR and Velasquez M, 'Ethics of the Attention Economy: The Problem of Social Media Addiction' (2020) 31 Business Ethics Quarterly

Botes M, 'Autonomy and the Social Dilemma of Online Manipulative Behaviour' (2023) 3 AI and Ethics

Buri I and van Hoboken J, 'The Digital Services Act (DSA) Proposal: A Critical Overview [2021] Institute for Information Law (IViR), University of Amsterdam Discussion Paper

Cauffman C and Goanta C, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12 European Journal of Risk Regulation

Church P and Pehlivan CP, 'The DSA: A New Era for Online Harms and Intermediary Liability' (2023) 4 Global Privacy Law Review

Cohen JE, 'What is privacy for' (2013) 126 Harvard Law Review

Dogruel L and others, '"I'm Still the Master of the Machine." Internet Users' Awareness of Algorithmic Decision-making and Their Perception of its Effect on Their Autonomy' (2022) 25 Information, Communication & Society

Domurath I, 'Platform Economy and Individual Autonomy' (2022) 30 European Review of Private Law

Faraoni S, 'Persuasive Technology and Computational Manipulation: Hypernudging out of Mental Self-Determination' (2023) 6 Frontiers in Artificial Intelligence

Frosio G and Geiger C, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime (2023) 29 European Law Journal

Gartner M, 'Regulatory Acknowledgement of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act (2022) 8 European Data Protection Law Review

Geng Y, 'Transparency For What Purpose?: Designing Outcomes-Focused Transparency Tactics for Digital Platforms' 16 (2023) Policy & Internet

Graef I, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' [2023] <http://dx.doi.org/10.2139/ssrn.4411537>

Heidebrecht S, 'From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance' (2023) 62 Journal of Common Market Studies

Hesselman C and others, 'A Responsible Internet to Increase Trust in the Digital World' (2020) 28 Journal of Network and Systems Management

Husovec M, 'Rising Above Liability: The DSA as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38 Berkeley Technology Law Journal

Hung A, 'Keeping Consumers in the Dark: Addressing 'Nagging Concerns and Injury' (2021) 121 Columbia Law Review

Izyumenko E and others, 'Online Behavioural Advertising, Consumer Empowerment and Fair Competition: Are the DSA Transparency Obligations the Right Answer?' [2024] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4729118>

Karagoel I and Nathan-Roberts D, 'Dark Patterns: Social Media, Gaming, and E-Commerce' (2021) 65 Proceedings of the Human Factors and Ergonomics Society Annual Meeting

Kozyreva A, Lewandowsky S, Hertwig R, 'Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools' (2020) 21 Psychological Science in the Public Interest

Leerssen P, 'Outside the Black Box: From Algorithmic Transparency to Platform Observability in the Digital Services Act' (2024) 4 Weizenbaum Journal of the Digital Society

Leiser M and Santos C, 'Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface' (2024) 15 European Journal of Law and Technology

Maroni M, '"Mediated Transparency": The Digital Services Act and the Legitimisation of Platform Power' [2023] University of Helsinki Faculty of Law Legal Studies Research Paper Series No. 77

de Matos Alves A, 'Platform Humanism and Internal Opacity: The Limits of Online Service Providers' Transparency Discourse' (2019) 4 Digital Culture and Society

Milano S, Taddeo M and Floridi L, 'Recommender Systems and Their Ethical Challenges' (2020) 35 AI & Society

Neuhouser F, 'Rousseau and the Origins of Autonomy' (2011) 54 Inquiry: An Interdisciplinary Journal of Philosophy

O'Neill O, 'Trust and Accountability in a Digital Age' (2020) 95 Philosophy

Osmola S, 'Neither Rules nor Standards: How to Regulate Dark Patterns' [2023] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4515963>

di Porto F and Egberts A, 'The Collective Welfare Dimension of Dark Patterns Regulation' (2023) 29 European Law Journal

Reigeluth T, 'Recommender Systems as Techniques of the Self?' [2017] *Genealogy+Critique*

Rodríguez de las Heras Ballell T, 'The Background of the Digital Services Act: Looking Towards a Platform Economy' (2021) 22 ERA Forum: Journal of the Academy of European Law

Sahebi S and Formosa P, 'Social Media and its Negative Impact on Autonomy' (2022) 35 Philosophy & Technology

Segijn CM and others, 'A Literature Review of Personalisation Transparency and Control: Introducing the Transparency-Awareness-Control Framework' (2021) 9 Algorithmic Systems in the Digital Society

Seizov O and others, 'The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU' (2019) 42 Journal of Consumer Policy

Soderlund K and others, 'Regulating High-Reach AI: On Transparency Directions in the Digital Services Act' (2024) 13 Internet Policy Review

Stray J and others, 'Building Human Values into Recommender Systems: An Interdisciplinary Synthesis' (2024) 2 Association for Computing Machinery Transactions on Recommender Systems

Sunstein CR, 'Fifty Shades of Manipulation' [2016] The Haravard John M. Olin Discussion Paper Series 01/2016

Swaine L, 'The Origins of Autonomy' (2016) 37 History of Political Thought

Turillazi A and others, 'The DSA: An Analysis of its Ethical, Legal, and Social Implications' (2023) 15 Law, Innovation and Technology

Turilli M and Floridi L, 'The Ethics of Information Transparency' (2009) 11 Ethics and Information Technology

Urman A and Makhortykh M, 'How Transparent are Transparency Reports? Comparative Analysis of Transparency Reporting Across Online Platforms' (2023) 47 Telecommunications Policy

de Vries K, 'Identity, Profiling Algorithms and a World of Ambient Intelligence' (2010) 12 Ethics and Information Technology

Wang R and others, 'Transparency in Persuasive Technology, Immersive Technology, and Online Marketing: Facilitating Users' Informed Decision Making and Practical Implications' (2023) 139 Computers in Human Behaviour

van de Waerdt PJ, 'Information Asymmetries: Recognising the Limits of the GDPR on the Data-driven Market' (2020) 38 Computer Law & Security Review

Wong D and Floridi L, 'Meta's Oversight Board: A Review and Critical Assessment' (2023) 33 Minds and Machines

Yi W and Li Z, 'Mapping the Scholarship of Dark Pattern Regulation: A Systematic Review of Concepts, Regulatory Paradigms, and Solutions from an Interdisciplinary Perspective' [2024] CREATe <https://arxiv.org/pdf/2407.10340>

Zard L and Sears AM, 'Targeted Advertising and Consumer Protection Law in the European Union' (2023) 56 Vanderbilt Journal of Transnational Law

Conference Papers

Andreou A and others, 'Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations' (Network and Distributed System Security Symposium, San Diego, February 2018)

Caragay E and others, 'Beyond Dark Patterns: A Concept-Based Framework for Ethical Software Design' (Proceedings of the CHI Conference on Human Factors in Computing Systems, Honolulu, May 2024)

Gray CM and others, 'Mapping the Landscape of Dark Patterns Scholarship: A Systematic Literature Review' (In Designing Interactive Systems Conference, Pittsburgh, July 2023)

Westin F and Chiasson S, '"It's So Difficult to Sever that Connection": The Role of FoMO in Users' Reluctant Privacy Behaviours. In CHI Conference on Human Factors in Computing Systems' (Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, May 2021)

Non-Academic Sources

Autonomy in Moral and Political Philosophy, Stanford Encyclopedia of Philosophy <https://plato.stanford.edu/entries/autonomy-moral/>

Baltus J, 'How Will The Framework For Risk Management in the Digital Services Act Manage the Tension Between Curbing Disinformation and Protecting Freedom of Expression' (Studievereniging voor Informatierecht, 2024) <https://svir.nl/how-will-the-framework-for-risk-management-in-the-digital-services-act-manage-the-tension-between-curbing-disinformation-and-protecting-freedom-of-expression/>

Brignull H, 'Dark Patterns: Dirty Tricks Designers Use to Make People Do Stuff' (90 Percent of Everything, July 8, 2010) <https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/>

Jones T, 'Facebook's "Evil Interfaces"' (Electronic Frontier Foundation, April 29, 2010) <https://www.eff.org/de/deeplinks/2010/04/facebooks-evil-interfaces>

Lessig L, 'Code is Law: On Liberty in Cyberspace' Cartorios <https://cartorios.org/wp-content/uploads/2020/11/LESSIG._Lawrence_Code_is_law.pdf>

NGO Monitor, The Influence of Political Advocacy NGOs on Meta's Human Rights Content Moderation Process: Gaza 2021 Case Study (2023) <https://www.ngo-monitor.org/reports/the-influence-of-ngos-on-meta-facebook/>

Tech Policy Press, Policy Tracker, Digital Services Act <https://www.techpolicy.press/tracker/digital-services-act/>

Zuboff S, 'Google as a Fortune Teller: The Secrets of Surveillance Capitalism' *Frankfurter Allgemeine Zeitung* (Frankfurt, 3 May 2016) <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html>