PART I
Digital Vulnerability as a Paradigm for Consumer Law

Consumer Protection and Digital Vulnerability: Common and Diverging Paths

Catalina Goanta, Giovanni de Gregorio, Jerry Spanakis

A. Introduction

The past years have seen a steep increase in scholarship, public policy and civil society in the concept of vulnerability, and particularly consumer vulnerabilities on digital markets. With targeted advertising relying on mass consumer surveillance and subsequently harmful profiling, 'digital vulnerability'[1] has been presented as a concept that challenges existing understandings of European consumer protection, such as the idealised and stereotyped consumer personas introduced by the Unfair Commercial Practices Directive.[2] At the core of the argument is the consideration that the "reasonably well-informed, reasonably observant and circumspect" average consumer benchmark,[3] as well as its 'vulnerable consumer' variant focusing on personal attributes and cognitive capacities,[4] are no longer a fit for the realities of digital markets, where structural asymmetries warrant an even higher level of protection. This is due to the increasingly important assumption that "(i)n digital marketplaces, most if not all consumers are potentially vulnerable".[5] In such digital environments, it no longer

1 Natali Helberger and others, 'Structural asymmetries in digital consumer markets' (*BEUC*, March 2021) < https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf> accessed 1 March 2024.

2 Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L-149/22 (UCPD).

3 Case C-210/96 *Gut Springenheide GmbH, Rudolf Tusky v Oberkreisdirektor des Kreises Steinfurt- Amt für Lebensmittelüberwachung and Another* [1998] ECR I-4657, para. 31. See also Rossella Incardona and Cristina Poncibò, 'The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) 30 Journal of Consumer Policy 21; Hanna Schebesta and Kai Purnhagen, 'Island or Ocean: Empirical Evidence on the Average Consumer Concept in the UCPD' (2020) 28 European Review of Private Law 293.

4 Christine Riefa, 'Protecting Vulnerable Consumers in the Digital Single Market' (2022) 33 European Business Law Review 607, 611.

5 Helberger and others (fn 1) at 5.

makes sense to single out very specific groups of consumers, and use more traditional means of typification that have been crystallised in European consumer law and policy during its life-span of around 50 years. This is because everyone participating in these environments as an individual is prone to be defenceless against manipulation and exploitation.

In many ways, digital vulnerability is an accurate depiction of the risks consumers face when transacting online. One of the most debated such risks, which has already led to a wave of policy and regulatory attention around the world, is that of dark patterns. Defined as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make",[6] dark patterns are currently seen as one the biggest dangers consumers are faced with when interacting with online marketplaces. So much so, that the European Commission even ran a sweep on such practices.[7] In a study of 399 online retail shops ranging from textiles to electronic goods, it was shown that 148 websites contained at least one of three dark patterns: fake countdown timers; online interfaces "designed to lead consumers to purchases, subscriptions or other choices"; and hidden information.[8] More specifically, 42 websites were found to include fake countdown timers, 54 websites either directed consumers towards more expensive goods or options for delivery, and 70 websites were found to hide relevant information from consumers either entirely or by making it less visible.[9] The sweep builds on an earlier study launched by the European Commission showing the interest of European lawmakers in

6 Arunesh Mathur and others, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1.

7 In the policy field of consumer protection in the European Union, sweeps are wide-ranging investigations taking place at the same time in a broad number of Member States, and coordinated by the European Commission through the Consumer Protection Cooperation Network. See for instance 'Consumer Protection Cooperation Network (CPC) | Single Market Scoreboard' <https://single-market-scoreboard.ec.europa.eu/governance-tools/consumer-protection-cooperation-network-cpc_en> accessed 1 March 2024.

8 'Manipulative Online Practices' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418> accessed 4 March 2024.

9 ibid.

taming the wild west of contemporary e-commerce.[10] This interest is shared by other regulators, such as the United States Federal Trade Commission (FTC), who published a report in 2022 showcasing how "companies are increasingly using sophisticated design practices known as "dark patterns" that can trick or manipulate consumers into buying products or services or giving up their privacy",[11] by "disguising ads to look like independent content, making it difficult for consumers to cancel subscriptions or charges, burying key terms or junk fees, and tricking consumers into sharing their data".[12]

In theory, a new conception of digital vulnerability makes sense. Yet for legal reform, as we go on to argue in this chapter, it still requires a lot of theoretical and practical unpacking, as proposed regulatory solutions building on new standards of consumer vulnerability currently do not account for the broad range of infrastructural problems that can give rise to new vulnerabilities in different online consumer environments. Our contribution focuses on contextualising and critically reflecting upon digital vulnerability in two ways. First, in a concrete and very practical technology case study drawing from computational social media research, and second, through a doctrinal exploration of the potential interpretation of digital vulnerability by courts. In doing so, we put forth the view that current iterations of digital vulnerability in legal doctrine do not fully address the complexity and diversity of problems connected to platform infrastructures, and that a system-level technological rethinking of European consumer protection is necessary.

This chapter is structured as follows. The first part offers a short description of digital vulnerability,[13] as well as some popular solutions currently proposed as policy recommendations for the implementation of the concept in European consumer law and practice. The second part presents our two-pronged critique. First, we explore a computational case study

10 European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F. et al., 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> accessed 1 March 2024.

11 'FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers' (*Federal Trade Commission*, 15 September 2022) <https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers> accessed 4 March 2024.

12 ibid.

13 Helberger and others (fn 1).

relating to vulnerability on social media, and discuss the ways in which digital vulnerability could be identified online to maximise consumer protection, albeit at the expense of other consumer rights. Second, we address the doctrinal implications of digital vulnerability vis-à-vis legal certainty by discussing the reliance of European consumer protection on judicial interpretation. The third part of the chapter synthesises the arguments under the umbrella of the critique that while conceptually fascinating, the proposed digital vulnerability notion is unsuitable to solve the problems of our current digital markets as it lacks system-level applicability, and should instead be further reframed in the light of this major limitation.

B. Digital vulnerability and structural asymmetry affecting European consumers

As briefly indicated in the introduction, the concept of digital vulnerability in consumer markets reflects a daring proposal for a paradigm shift in European consumer protection law and policy. This concept was most comprehensively articulated in a 2021 report of the European Consumer Organisation (BEUC).[14] With consumer harms arising at unprecedented pace and scale from business practices such as targeted advertising based on consumer profiles, price discrimination and dark patterns,[15] digital vulnerability is presented as a necessary answer to the growing concern that existing levels of consumer protection are insufficient in addressing these harms.

Consumer vulnerability has long been a topic of consumer research. A literature review looking at 25 years of post-modern practices in marketing across 859 published articles, revealed four major research themes on this topic: "marketing, fraud and consumers; consumer vulnerability and well-being; ethics and vulnerable consumers; and consumption, disability and gender".[16] The first theme was associated mostly with research on financial services, persuasion and low-income consumers. The second theme addressed children, poverty, subsistence marketplaces and effects on well-

14 ibid.

15 ibid at 6.

16 Rituparna Basu, Anil Kumar and Satish Kumar, 'Twenty-five Years of Consumer Vulnerability Research: Critical Insights and Future Directions' (2023) 57 Journal of Consumer Affairs 673.

being. The third cluster of publications generally dealt with corporate social responsibility, elderly consumers, sustainability and consumer behaviour. Lastly, the fourth research theme tackled consumer issues focused on disability, gender, identity and motherhood.[17] These thematic research clusters mirror the more traditional understanding of vulnerability as crystalised in existing legislation. For instance, as the BEUC report also highlights, according to the UCPD, consumers "can be considered vulnerable because of their personal characteristics, namely mental or physical infirmity, age or credulity",[18] leading to a "vantage point from which commercial practices can be assessed",[19] by identifying consumers or groups of consumers who may be more prone to manipulation and harm. The report discusses arguments from multidisciplinary vulnerability scholarship that distinguishes vulnerability from victimization and victimhood,[20] seen as "unnecessarily stigmatising, patronising and disconnected from social reality",[21] as consumer vulnerability "is a sometimes misunderstood or misused concept that is equated erroneously with demographic characteristics, stigmatization, consumer protection, unmet needs, discrimination, or disadvantage".[22] At the same time, the report also points to other opinions aiming to limit a more universal understanding of consumer vulnerability as being too all-encompassing, given the vast implications of diverse vulnerabilities at individual level.[23]

The report shapes the concept of digital vulnerability around a series of proposed characteristics. First, digital vulnerability must take into account the conceptual refinement of the notion of vulnerability itself, as we ought to differentiate between sources and states of vulnerability, where the former can be inherent (intrinsic to the human condition) and situational (arising in a particular context or situation), while the latter can be dispositional (potential) and occurrent (dispositional vulnerabilities that

17 ibid; See also Ronald Paul Hill and Eesha Sharma, 'Consumer Vulnerability' (2020) 30 Journal of Consumer Psychology 551.
18 Helberger and others (fn 1) at 9.
19 ibid.
20 Alyson Cole, 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique' (2016) 17 Critical Horizons 260.
21 Helberger and others (fn 1) at 10.
22 Stacey Menzel Baker, James W Gentry and Terri L Rittenburg, 'Building Understanding of the Domain of Consumer Vulnerability' (2005) 25 Journal of Macromarketing 128.
23 ibid at 11.

manifest themselves).[24] Second, seeing the data-driven nature of online markets, digital vulnerability is architectural and it reflects the properties of digital architectures.[25] Third, digital vulnerability is relational because of the way in which consumers interact with one another and with the influences of commercial parties.[26] Fourth, lack of privacy can be seen as a potential source of vulnerability, given the nature of "data-driven practices that promote exploitation of vulnerabilities".[27]

Some of the concrete recommendations made in the BEUC report reflect concrete proposals for regulatory reform, as "the law on unfair commercial practices has to be rethought in order to remain a useful tool in the fight against digital asymmetry".[28] Reform proposals include the anchoring of digital vulnerability and digital asymmetry in the UCPD (e.g. Articles 5, 8 and 9), the reversal of the burden of proof "as a necessary consequence of the way in which new technology is used to manipulate the consumer through all sorts of marketing strategies",[29] or the blacklisting of additional commercial practices as a self-standing category of digital practices.[30] Other recommendations propose regulatory co-design, such as concretising legal benchmarks in guidelines co-created by businesses, consumers and enforcement authorities.[31]

This brief overview of how digital vulnerability is proposed in the BEUC report aims to bring into discussion the very valuable and innovative conceptual framing presented in the study, with which the authors undoubtedly make significant contributions to existing scholarship. The characteristics of digital vulnerability presented therein reflect very persuasive arguments that warrant the reconsideration of whether the current legal understanding of vulnerability is socially, economically and also technologically decrepit. This reconfiguration, focused on the particular context of consumers who may be vulnerable in different ways at different moments throughout their lives, is reminiscent of theories of personalised law, which equally hold that the law should apply in a bespoke manner to individuals, as opposed to the standardisation and typification that legal systems around the world gener-

24 ibid at 16-17.
25 ibid at 18.
26 ibid at 20.
27 ibid at 23.
28 ibid at 76.
29 ibid.
30 ibid at 79.
31 ibid.

ally work with.[32] Yet just like personalised law, in spite of its conceptual attractivity, digital vulnerability does not come across as very practical, particularly when linked to policy recommendations that do not really rethink the nature of consumer protection, but merely continue the established tradition of troubleshooting and patchworking the European consumer *acquis*. In the next section, we explore to what extent the articulation of a new concept of consumer digital vulnerability in the real-world might deliver on its promised value.

C. The ever-expanding complexity of digital vulnerability

As the European Union explores regulatory reforms to develop strengthened protections for individuals on digital markets, the digital vulnerability framework has gained a lot of traction in both (legal) scholarship and policy-making circles. Whether such a framework will be embedded in, for instance, the expected reform of the UCPD following the Commission's Fairness Fitness Check, remains to be seen.[33] Between contracted studies,[34] public consultations[35] and the rising volume of consumer research on vulnerability, the Commission could make very sensible proposals as to why there should be additional changes to the UCPD even as early as five years after the upgrades introduced by the Modernisation Directive.[36] The public consultation on the Fitness Check, comprising 350 online responses to a questionnaire and 71 position papers, revealed some wide-spread consumer

32 Omri Ben-Shahar and Ariel Porat, 'Personalizing Mandatory Rules in Contract Law Symposium: Personalized Law' (2019) University of Chicago Law Review 255; Christoph Busch, 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law Symposium: Personalized Law' (2019) University of Chicago Law Review 309.

33 'European Commission - Have Your Say' (*European Commission - Have your say*, 14 June 2022) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 5 March 2024.

34 Lupiáñez-Villanueva and others (fn 10).

35 'European Commission - Have Your Say' (n 33).

36 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328 (Modernisation Directive).

issues around dark patterns in general, as well as subscription cancellation difficulties and a lack of disclosures of paid promotions in particular.[37]

It is noteworthy that the Fitness Check has a broader scope of reflection than most of the literature available on (digital) consumer vulnerability. Consumer protection is traditionally discussed in the context of marketplaces and e-commerce.[38] Yet other digital industries are equally embracing e-commerce in even more complex and opaque online architectures than the checkout interfaces of websites like Amazon or Shein. One of the core industries where this trend has been visible in the past years already is social media. Social commerce reflects the integration of e-commerce on social media.[39] This trend has been shaping social media in at least two ways.

On the one hand, new content monetisation products launched by social media platforms are proliferating contractual interactions between traders and consumers. An example in this respect is the TikTok Shop, launched in September 2023, offering users the opportunity to sell goods through designated e-commerce interfaces pertaining to TikTok, which are often linked to content production on LIVE shopping.[40] Put differently, platforms like TikTok are starting to offer new iterations of teleshopping services, where instead of calling a number to buy a pan seen on television, a consumer has to navigate a complex ecosystem of social media affordances (e.g. the Shop Tab, Product Showcase, In-Feed Video and Live Shopping, Shop Ads) and indirect interactions with other data brokers in the e-commerce supply chain (e.g. affiliate networks, commerce platform partners, multi-channel partners, dropshipping intermediaries) to buy a product.

On the other hand, products promoted on social media are not just merely listed on product pages, but also featured in commercial content that is generally underdisclosed as such.[41] The drivers of this new form

37 'European Commission - Have Your Say' (n 33).

38 Mathur and others (n 6).

39 Christine Riefa, 'Consumer Protection on Social Media Platforms: Tackling the Challenges of Social Commerce' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law in the Digital Era* (Springer International Publishing 2020) <https://link.springer.com/10.1007/978-3-030-25579-4_15> accessed 8 February 2023.

40 'Introducing TikTok Shop' (*Newsroom | TikTok*, 12 September 2023) <https://newsroom.tiktok.com/en-us/introducing-tiktok-shop> accessed 5 March 2024.

41 'Results of a Screening ("Sweep") of Social Media Posts' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_708> accessed 5 March 2024.

of native advertising are influencers and content creators, an emerging stakeholder group attracting and keeping audiences on social media. The connection developed between creators and their audiences, referred to as parasocial relationships,[42] are rooted in the familiarity, authenticity and relatability that content creators can offer to their online followers. Parasocial relationships are also full of emotions, leading followers to admire and defend the choices of their favourite Internet celebrities. These features nurture consumers' trust in the recommendation and review of products and services.[43] The content creation global market is expected to reach half a trillion dollars by 2027.[44] Given that it brings together the three most popular activities Internet users currently enjoy online, namely social networking, content streaming and shopping,[45] the content creation economy warrants much more attention in terms of consumer protection pitfalls. This should not be limited to questions of digital addiction,[46] but also include clarifying how consumer law applies to digital content and services shaped by the content monetisation strategies of social media platforms.[47]

The Fairness Check addresses some of the risks of undisclosed advertising by social media influencers, but does not fully acknowledge the

42 See for instance Amanda N Tolbert and Kristin L Drogos, 'Tweens' Wishful Identification and Parasocial Relationships With YouTubers' (2019) 10 Frontiers in Psychology 2781.

43 For a comprehensive overview on the influence of influencers see Frithjof Michaelsen et al, 'The impact of influencers on advertising and consumer protection in the Single Market' (Study requested by the IMCO committee, European Parliament, February 2022) <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703350/IPOL_STU(2022)703350_EN.pdf>. See also Marijke De Veirman, Liselot Hudders and Michelle R Nelson, 'What Is Influencer Marketing and How Does It Target Children? A Review and Direction for Future Research' (2019) 10 Frontiers in Psychology 2685.

44 'The Creator Economy Could Approach Half-a-Trillion Dollars by 2027' (*Goldman Sachs*, 29 February 2024) <https://www.goldmansachs.com/intelligence/pages/the-creator-economy-could-approach-half-a-trillion-dollars-by-2027.html> accessed 5 March 2024.

45 Vibhor Agarwal and Nishanth Sastry, '"Way Back Then": A Data-Driven View of 25+ Years of Web Evolution', *Proceedings of the ACM Web Conference 2022* (ACM 2022) <https://dl.acm.org/doi/10.1145/3485447.3512283> accessed 9 July 2022.

46 'New EU Rules Needed to Address Digital Addiction | News | European Parliament' (12 December 2023) <https://www.europarl.europa.eu/news/en/press-room/20231208IPR15767/new-eu-rules-needed-to-address-digital-addiction> accessed 5 March 2024.

47 Taylor Annabell, Catalina Goanta and Sophie Bishop, '"You and TikTok are, and will remain at all times, independent contractors": Classification of influencers and monetisation practices in TikTok documentation', forthcoming 2024.

fundamental business model shifts social media platforms are undergoing through the further development of monetisation.

These emerging ecosystems raise their own challenges for digital vulnerability, with far stretching implications that lead to further interpretation issues. How will the dark patterns discussion be extended to social media interface features? How should we distinguish between the impact of interface architectures and other manipulative influences such as parasocial relationships which rely on emotional manipulation? Should we distinguish between individual instances of vulnerability and clusters of practices that may enhance the severity of vulnerability? These are only a handful of questions unveiling the complexity of the topic.

So far, consumer literature on vulnerability has focused on making theoretical contributions to the understanding of this problem, aiming to conceptualise some of the notable shifts in what our legal understanding of consumer harms ought to be. In what follows, this chapter will complement existing analyses with two more applied perspectives: one focused on specific industry practices in the social media sector, and another focused on judicial practices around the interpretation of consumer protection in Europe.

I. Case study: monetising conspiracy theories on YouTube

To exemplify the complexities of digital markets, this subsection describes and discusses concrete instances and dimensions of vulnerability in relation to social media monetisation, by unpacking a 2022 study on the monetisation of YouTube conspiracy theories.[48]

1. A brief introduction to monetisation

Before delving into the study itself, it is important to first revisit the monetisation discussion and briefly set the scene around social media monetisation. Consumer markets where more traditional transactions have been moved to the online world (e.g. selling and buying consumer goods)

48 Cameron Ballard and others, 'Conspiracy Brokers: Understanding the Monetization of YouTube Conspiracy Theories', *Proceedings of the ACM Web Conference 2022* (ACM 2022) <https://dl.acm.org/doi/10.1145/3485447.3512142> accessed 4 March 2024.

have their own challenges and transformations, such as the rise of intermediation, opaque targeting, etc. However, as emerging transactional environments, social media platforms bring with them even more complexity. In this context, monetisation can be interpreted to refer to two types of economic practices. On the one hand, monetisation drives the development of new business models by social media platforms. For instance, the displaying of ads on YouTube channels – known as YouTube AdSense[49] - has been one of YouTube's most famous business model around user-generated content. In more recent years, YouTube has been diversifying its monetisation approaches by for instance partnering up with Shopify and enabling users to purchase goods and services while they are featured in videos.[50] Additional developments include for instance BrandConnect, the platform solution for the intermediation of influencer marketing.[51] These are examples of monetisation products developed by YouTube to diversify its revenue streams by tapping into and shaping new socio-cultural phenomena and consumer needs. On the other hand, monetisation also reveals the economic incentives of other stakeholders in digital supply chains. This includes legitimate economic actors such as creators, brands, advertising agencies, etc., but also illegitimate actors such as scammers and criminal organisations. Monetisation products made available by platforms can be bundled into what we can call as 'monetisation portfolios', namely a variety of business practices enabling these economic actors to produce revenue across a wide range of platforms and monetisation opportunities, making them more resilient to losing any one particular revenue stream.

2. Monetising conspiracy channels

Ballard et al. investigated the monetisation 'methods' of a specific category of YouTube channels, focused on conspiracy theories. In doing so, researchers collected information about the ads delivered on these channels, as well as any other information they could gather from the description of the videos. Starting with advertising, they identified three types of advertising

49 See Google FAQs <https://support.google.com/youtube/answer/11602441?hl=nl> accessed 4 March 2024.

50 'Sell to Customers on Google and YouTube' (*Shopify*) <https://www.shopify.com/google> accessed 1 April 2024.

51 'BrandConnect for Influencer Advertising - YouTube Advertising - YouTube Advertising' <https://www.youtube.com/ads/brandconnect/> accessed 1 April 2024.

on YouTube: video ads "served before or during a video"; "advertisements on the video sidebar"; and "banner ads in the middle of videos that do not interrupt viewing".[52] Researchers emphasise that these ads are part of YouTube's ad delivery system, which allows advertisers to "upload a combination of text, images and video" and "specify on which sites or apps the advertisement can be seen and how the ad should be targeted", in exchange for specifying "the amount of money they are willing to spend per interaction with an ad, referred to as a bid".[53] The research team also specifies that Google controls the process determining when and where the ads will be served, "through a combination of content restriction, bidding and personalisation", and that ad personalisation entails the targeting of audiences on the basis of "personal demographics or interests of the viewer", as well as "ad context, i.e. where the ad is shown".[54]

To investigate the advertising monetisation models, the study set up two different datasets: a conspiracy dataset focused on 818 YouTube channels, where 43,379 ad impressions were extracted from 93,443 videos; and a control dataset amassing 11,912 channels, 140,839 ad impressions and 47,847 videos. The conspiracy channel list was sourced in two ways. First, by relying on a labelled YouTube channel dataset from an earlier political study,[55] and second, by identifying further conspiracy channels based on shared subscribers.[56] The findings showed that certain types of ads are more common in the conspiracy dataset, such as self-improvement ads (e.g. advertising 'webinars, books or courses promising an easy route to financial independence'[57]), lifestyle and alternative health ads, as well as low-quality gadgets and beauty products. With an additional check of the domain names (URLs) associated with predatory ads, the research team found that "ads […] identified as deceptive or predatory accounted for 15% of all impressions in the conspiracy set, but only 1.4% of control impressions. Ad content ranged from get-rich-quick schemes, to promises of immortality through essential oils, to 5G-proof un- derwear".[58]

52 Ballard and others (n 48).
53 ibid.
54 ibid.
55 Mark Ledwich and Anna Zaitsev, 'Algorithmic Extremism: Examining YouTube's Rabbit Hole of Radicalization' [2020] First Monday <https://journals.uic.edu/ojs/index.php/fm/article/view/10419> accessed 1 April 2024.
56 Ballard and others (n 48).
57 ibid.
58 ibid.

The study also revealed other business models used by the owners of conspiracy channels on YouTube. Based on an analysis of the video descriptions of the collected videos, researchers were able to identify that monetisation models focused on requesting donations (e.g. Patreon, GoFundMe), selling merchandise directly to consumers, or directing consumers to additional websites with alternative monetised content (e.g. 'free speech' platforms such as Rumble) were also prevalent in the conspiracy dataset. This is evidence of the complexity of the 'monetisation portfolio' mentioned above, where economic operators (whether in good or bad faith) cluster a wide array of practices meant to bring them revenue.

3. Relevance for the digital vulnerability debate

The study referred to in this section is an important example of how consumer vulnerability is exploited in the practice of social media content monetisation, not only by bad faith actors, but also by platforms themselves. This happens in at least three layers of commercial activity. First, YouTube channels with specific content are set up – in this case conspiracy theories. Such theories can range across a wide amount of topics and may be more or less grounded in science, but what is most important is that they bring together a homogenous audience based on the interest of viewers in that specific content. Here, consumers are viewers. Second, YouTube channels are primarily monetised through advertising, and the ads shown on conspiracy channels target users based on demographic data and content interest. The channels displaying such ads earn advertising revenue through YouTube, and the companies buying targeted advertising are able to deliver fraudulent goods and services to audiences, as consumers become potential purchasers of these goods and services. Third, conspiracy channels themselves may re-direct viewers to additional websites promoting fraudulent product or service offers, turning viewers once more, into potential buyers or donors for specific causes. The second and third layers of commercial activity (monetisation through advertising; and monetisation through selling/donations) link the content of YouTube channels, which may be persuasive and very much based on extracting emotional reactions from audiences, to transactions that consumers may immediately engage in. For the sake of visualising how this works, imagine watching a conspiratorial video about vaccinations, aimed to instil fear and rally support against public policies related to vaccination, only for the video description to contain specific products recommended to replace vaccination, and which are

directly ready to purchase at the click of a few buttons. This transactional simplification showcases a dual vulnerability for consumers: noy only is the specific group of conspiracy-loving consumers easily identifiable as the audience of specific YouTube content, but it also becomes subsequently targeted (whether via YouTube's personalisation or the channel's monetisation itself) with additional harmful commercial practices.

4. Contextual vulnerability: technical solutions for complex social media consumer harms?

It is not the purpose of this section to delve into a comprehensive application of European consumer protection to the consumer harms scenarios arising out of the conspiracy study described and analysed above. Still, it can be reasonably argued that to the extent European consumers viewing conspiracy videos on YouTube channels would also be exposed to goods and products advertised using incorrect scientific and factual claims, they may generally be considered unfair under the UCPD. In principle, and depending on the procedural implementation of the UCPD in different Member States, consumers may have – among others – tort-based remedies to alleviate the damages suffered by engaging in snake oil transactions (e.g. fake medicinal products). Moreover, national authorities tasked with the enforcement of consumer protection may dispose administrative sanctions such as fines and injunctions to stop the proliferation of harmful practices. Yet in this case, the UCPD would very likely lead to the limitation that sanctions and remedies have not traditionally been targeted at platforms, but instead, at advertisers and sellers themselves. In this case, it would entail that consumers and authorities would have to identify and take legal action against the owners of channels, as well as advertisers who may engage in unlawful conspiratorial advertising and selling. This is due to the fact that the UCPD was not designed as a platform instrument, but has rather focused on more direct transactional relationships between traders and buyers. And while it is true that YouTube is itself a trader vis-à-vis European consumers, applying the UCPD in its current shape to the case study described above would only – at best – attract YouTube's liability with respect to this relationship between itself and consumers as viewers/users of the platform.

So how could YouTube actually take into account contextual consumer vulnerability? As a platform collecting every click and action taken by

users while engaging with its products, YouTube has the necessary data points to identify for instance when a specific user goes on a conspiracy binge, and when such a binge would be followed by engagement with third party websites. Particularly if consumers use in-app browsers (e.g. using YouTube on a mobile phone and clicking on external websites from there), YouTube would in principle also be able to collect shopping data about the consumer.[59] Assuming YouTube could detect and determine links between the consumption of emotional content and the purchasing of problematic goods or services, it could impose for instance limitations on monetisation by the channel owners or advertisers. Demonetisation, seen as removing the possibility of making revenue by YouTube channels, is an approach that YouTube is already using to limit problematic content. However, what exactly is problematic content? Even for authorities and courts, drawing the line between safe and unsafe products, or holistic medicine and snake oil is no easy task – and neither is determining when a consumer may be contextually vulnerable. As a result, while YouTube may have a lot of power and information about its users, identifying and proactively protecting vulnerable consumers entails setting private governance standards that may not always perfectly align with the law. Is placing the burden on YouTube to replace our judiciaries and public administration institutions on determining, on a case by case basis, what is a good product and what is a bad product, the way ahead? Or do we need to bring the focus back from the private governance by platforms to public governance through European harmonisation and judicial interpretation? The next section segues into this latter point.

II. Revisiting the harmonisation debate through judicial interpretations of European consumer protection

Traditionally, European consumer protection has heavily relied on judicial interpretation for the development of its core concepts. This is due to the fact that while it has a long standing history in European law and policy, consumer protection legislation has fuelled a lot of political and doctrinal

59 'iOS Privacy: Instagram and Facebook Can Track Anything You Do on Any Website in Their in-App Browser' (*Felix Krause*, 10 August 2022) <https://krausefx.com//blog/ios-privacy-instagram-and-facebook-can-track-anything-you-do-on-any-website-in-their-in-app-browser> accessed 1 April 2024.

disagreement in relation to its goals and practical implications. An example in this respect is the Unfair Contract Terms Directive and its 'irritating' effect on UK law, beautifully captured in Teubner's analysis from a few decades ago,[60] as one of the many discussions relating to how consumer harmonisation has not been without its own discontents at national and supranational level, in policy as well as in academia.[61]

The harmonising impact of consumer protection legislation must be once more revisited in the context of digital vulnerability: as the complexity of market practices and architectures grows exponentially, is it reasonable to rely on patchwork regulation to address transnational, complex platform systems with the goal of protecting against legally uncertain, contextual vulnerabilities? European consumer protection law remains inherently dependent on judicial interpretation for its effectiveness – a feature that not even the UCPD managed to change, in spite of its annex of prohibited commercial activities. This interpretation, in turn, remains bound by national preferences and practices, but most importantly – remains also case-specific. In other words, the scalability of judicial interpretation is modest at best, even when flowing from the European Union's highest court.

To shed some further light on interpretational issues, we draw on the empirical study conducted by Schebesta and Purnhagen on the concept of the average consumer.[62] This 2020 study, combining doctrinal and empirical methods, aimed to understand how the UCPD average consumer test is applied by the CJEU, by systematically analysing 12 relevant cases with a clear application of the average consumer concept, and finding that the "empirical analysis revealed the muddy nature of the Court's legal

60 Gunther Teubner, 'Legal Irritants: Good Faith in British Law or How Unifying Law Ends up in New Divergences' (1998) 61 The Modern Law Review 11.

61 Roger Van Den Bergh, 'The Uneasy Case for Harmonising Consumer Law' in Klaus Heine and Wolfgang Kerber, *Zentralität und Dezentralität von Regulierung in Europa* (De Gruyter 2007) <https://www.degruyter.com/document/doi/10.1515/9783110511260-009/html> accessed 1 April 2024; Marcus Klamert, 'What We Talk About When We Talk About Harmonisation' (2015) 17 Cambridge Yearbook of European Legal Studies 360; Onyeka K Osuji, 'Business-to-Consumer Harassment, Unfair Commercial Practices Directive and the UK—A Distorted Picture of Uniform Harmonization?' (2011) 34 Journal of Consumer Policy 437; Simon Whittaker, 'Unfair Contract Terms and Consumer Guarantees: The Proposal for a Directive on Consumer Rights and the Significance of "Full Harmonisation"' (2009) 5 European Review of Contract Law 223; Hans-W Micklitz, 'Minimum/Maximum Harmonisation and the Internal Market Clause', *European Fair Trading Law* (Routledge 2006).

62 Schebesta and Purnhagen (n 3).

reasoning about the average consumer benchmark".[63] What is more, the authors also posited that the average consumer test of the UCPD had led to an isolated interpretation when considering other areas of European law, and that it ultimately relies on the further interpretation of national courts.

This study is essential in understanding the slow and convoluted process of judicial interpretation in the context of supranational governance and harmonisation policies, even when addressing a rather popular instrument that has led to a lot of case law both at European and national level. Moreover, attention should also be paid to the fact that the judicial interpretation by the CJEU is deemed to be 'muddy' even in the context where one Court has had a little under 20 years to build on its understanding of a fundamental concept for the operation of the UCPD.

So what does this mean for new concepts of consumer vulnerability? In short, new substantive formulations of consumer vulnerability, such as contextual vulnerability, will not solve digital asymmetries – or at a minimum will not solve them fast enough – because of the shortcomings of judicial interpretation. This argument can be unpacked along two such limitations. First of all, contextualising vulnerability in the meaning that anyone can be vulnerable on the Internet[64] entails understanding the specific situations in which a consumer may find themselves vulnerable. The idea of breaking the boundaries of legal stereotypification (e.g. based on age or credulity as insufficient determinants of vulnerability) may have great theoretical value, but at the same time it may open the door to an overwhelming amount of individually personalised parameters and combinations of parameters which may be very specific to the circumstances of individual consumers. In this case, even with the CJEU guiding the abstract interpretation of novel concepts, the filling of these concepts by national courts could very well lead to a complete collapse of harmonisation as we know it. Second of all, even if more systematic approaches can be found to avoid the over-personalisation of vulnerability (e.g. by adding new, specific vulnerability determinants), judicial interpretation clarity only comes with high volumes of case law which would take a very long time to develop in legal practice. As a result, it is unclear to what extent such a solution would address the problems of legal uncertainty embedded in the application of a legislative instrument whose innate flexibility has already led to 'muddy' interpretations.

63 ibid at 308.

64 Helberger and others (fn 1) at 25.

Overall, given the reliance of European consumer protection on judicial interpretation, current legislation such as the UCPD simply does not lend itself to the scalability that is required when aiming to effectively solve consumer harms on a broad range of digital markets, even though the need for this scalability is arguably a part of the structural asymmetry discussion. Perhaps most importantly, to the extent that they are divorced from market knowledge about commercial practices across all relevant sectors, as exemplified in Section 3.1, novel frameworks of consumer vulnerability will not be sufficient to further patchwork European consumer protection legislation into more effective application.

Instead, a complete overhaul of the goals of European consumer protection legislation such as the UCPD might be necessary. Literature on platform governance – and particularly on content moderation – has been advancing the argument that the focus on individual cases and interpretations characterising today's jurisdictions in relation to unlawfulness in digital environments such as social media platforms is a 'mistake'.[65] The next and last section elaborates on this argument and applies it to digital vulnerability framework.

D. Synthesis and conclusion: digital vulnerability and the need for systems-thinking

In a recent paper on content moderation and US constitutional law, Douek forwards the argument that legal decision-making in the context of scaled, complex systems such as social media platforms ought to fundamentally shift from an individual case basis to 'mass speech administration'. This is due to the fact that "the vehicle of individual error correction" allowed for by judicial and doctrinal interpretations of constitutional legal standards in the US is no longer fit to deal with the "complex and dynamic system" of platform governance, and it should be replaced with what the paper calls "a second wave of regulatory thinking about content moderation institutional design that eschews comforting but illusory First Amendment–style analogies and instead adopts a systems thinking approach".[66] This argument builds on earlier iterations of critiques around the fitness of traditional legal

65 Evelyn Douek, 'Content Moderation as Systems Thinking' (2022) 136 Harvard Law Review 526, 532.

66 ibid.

systems in governing speech online, such as those proposed by Balkin and Langvardt, who drew attention to the process of administratively managing content moderation at unprecedented scale.[67]

This argument neatly applies to any interaction between traditional legal thinking and complex digital commercial ecosystems. So what would systems-thinking look like in the context of applying European consumer protection at scale? This chapter does not aim to provide a comprehensive analysis of this question, but rather exemplify a few directions this discussion could further take, particularly at the intersection of literature on platform governance and consumer protection. To open the appetite for such theoretical incursions, two points are briefly addressed: the need to develop cohesive platforms-as-systems obligations under the European consumer *acquis*; and the classification of consumer protections based on their potential technological operationalisation at scale.

In terms of the first point, even after the Modernisation Directive, the UCPD and its tests – including the existing conception of consumer vulnerability – have generally not focused on platforms as intermediaries. The few exceptions which can be observed in the updated Annex include obligations for search engines (point 11a),[68] as well as obligations for platforms displaying consumer reviews (points 23 b and c).[69] Although as such, platforms themselves may be traders, the UCPD does not explicitly acknowledge the role of platforms in collecting and intermediating information. For instance, while the application of the UCPD to influencer marketing practices around advertising disclosures has been unquestionably established, the discussion has generally focused on the obligation of influencers as traders in making such disclosures. However, it can be argued that platforms themselves, through interface design and architectures, make it difficult for disclosures to be properly made or displayed. Still, to date, the role of platforms in the policy process around the regulation of influencer marketing from a consumer perspective remains minimal. Particularly in

67 ibid.

68 Point 11a, UCPD Annex: "Providing search results in response to a consumer's online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of products within the search results."

69 Point 23b, UCPD Annex: "Stating that reviews of a product are submitted by consumers who have actually used or purchased the product without taking reasonable and proportionate steps to check that they originate from such consumers"; Point 23c, UCPD Annex: "Submitting or commissioning another legal or natural person to submit false consumer reviews or endorsements, or misrepresenting consumer reviews or social endorsements, in order to promote products."

the case of new frameworks around digital vulnerability, platforms should have a central role not only in reshaping the substance of legal standards, but also in terms of their procedural application. This discussion will have to also involve growing concerns relating to the cohesion of the European consumer *acquis*.

With the adoption of the Digital Services Act, which includes a lot of relevant provisions for consumers, and which is deemed a systems regulation, European law now faces the difficult task of aligning existing sectoral rules with the newly emerged digital *acquis*.[70] This does not only entail aligning interpretations across instruments, but also making sure that legal obligations do not conflict. Would imposing more consumer obligations on platforms be a permitted deviation from the liability exemptions platforms may enjoy under the DSA? If we consider consumer protection legislation as *lex specialis*, that should be indeed the case. In addition, the interpretation of 'illegal content' in the light of the consumer acquis is another aspect of this legislative interaction which ought to be clarified in the coming years.

However, while the notion of illegal content is left to the law of Member States, it is not the same for harmful content for consumers which, despite legal, are left in the decision-making process of online platforms. Proposing a certain diet or lifestyle is not illegal per se but it could lead to users' distress and addiction. Even influencing public opinion by relying on political speech to hide strategies of content monetisation does not qualify as an illegal conduct, but it can be harmful for democracy. This grey area for consumer law is left to online platforms which, in case of Very Large Online Platforms (VLOPs), can consider this issue as a system risk based on Article 34 DSA if considering that consumer protection is a fundamental right protected by the European Charter.

More broadly, the DSA can be conceived as the starting point of a regulatory 'administrativisation' of content moderation. The European reaction to platform governance has led to the introduction of procedural safeguards which aims to protect users in the process of content moderation. Nonetheless, the scale and quantity of the activity in content moderation has already underlined the potential limit of these safeguards, including transparency and disclosure for consumers, which now have access to billions of entries, just when referring to the obligation of statement of reason based on Article

70 Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) European Journal of Risk Regulation 1.

15 DSA. This framework leads to thinking more about the process of content moderation in a systematic way, and, therefore, requires enforcement authorities to think in the same direction.

This moves us to the second point regarding the operationalisation of consumer protection obligations at scale. A quick look at the DSA Transparency Database,[71] which also includes marketplaces and not only social media platforms in terms of compliance with the transparency requirements in Article 17 DSA (e.g. submitting content moderation decisions in a publicly available database), reveals that most content moderation decisions are actually made by marketplaces such as AliExpress. On marketplaces, content moderation often takes the form of policing unsafe and illicit products. While some interpretational issues may still exist around determining which products may be lawfully sold, product safety practices have led to the development of databases such as Safety Gate,[72] where national consumer authorities report unsafe products in an agile manner, which can be prone to further operationalisation by large online marketplaces, through, for instance, API implementation.[73] This is a concrete expression of the administrative dimension of systems-thinking such as that put forth by Douek. Furthering this perspective can entail classifying consumer protection obligations on the basis of whether they can be technically implemented or not. Information duties in the consumer *acquis*, trader registration are examples of obligations that can easily be implemented in the architectures of platforms, with the advantage of automating compliance checks as well. This is due to their administrative registration nature, which does not leave that much leeway for subjective interpretation. Whether consumer digital vulnerability can be automated at all, remains to be seen. Most likely, some aspects of it should be straight forward to platforms. For instance, YouTube should already restrict certain types of advertising on channels dedicated to children. A 'Safety Gate' for children advertising topics (including products), that could allow national authorities to set out constantly updating limitations would be another example of technically embedding legal standards on platforms at a systems level.

71 See <https://transparency.dsa.ec.europa.eu>.

72 See < https://ec.europa.eu/safety-gate-alerts/screen/webReport>.

73 Catalina Goanta, Thales Bertaglia and Adriana Iamnitchi, 'The Case for a Legal Compliance API for the Enforcement of the EU's Digital Services Act on Social Media Platforms', *2022 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2022) <https://dl.acm.org/doi/10.1145/3531146.3533190> accessed 1 April 2024.

Neither of the two ideas elaborated above are perfect solutions to the problem of complexity around consumer vulnerability on digital markets. However, what this chapter has aimed to achieve is a brief demonstration that without taking into account the system-level nature of transnational superplatforms, and adapting consumer protection accordingly, we are not sufficiently addressing the new world of digital markets. Although theoretically fascinating, digital asymmetries and contextual vulnerabilities will not be solved by exclusively increasing the standard of substantive consumer protection, or by adding new procedural safeguards in traditional judicial processes. Instead, focusing on the responsibility of platforms to adapt to and interact with European consumer protection standards at infrastructural level ought to be the focus of regulatory reforms that should technically rethink the role of consumer protection in the digital sphere.