European Journal of Risk Regulation (2026), 1–17
doi:10.1017/err.2026.10146

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Digital Fairness Act: Mapping the Expectations

Liubomir Nikiforov[1,2]

[1]EDHEC Augmented Law Institute, IPoP, France and [2]VUB, Belgium
Email: liubomir.nikiforov@edhec.edu

Abstract

This paper examines the emerging Digital Fairness Act (DFA) against the development of the EU consumer law safety net, the 2024 Fitness Check and the Consumer Agenda 2030. It explores how EU consumer law should address data-driven commercial practices that leverage digital asymmetries and vulnerabilities without adding to regulatory fragmentation and legal uncertainty. The key challenge is applying technology-neutral consumer rules effectively to modern choice architectures in a way that is sufficiently specific, coherent and, importantly, enforceable. This paper combines doctrinal analysis with insights from anonymised stakeholder discussions held throughout 2025 to outline the key institutional and legislative decisions about the DFA. It also draws on Helberger et al.'s study as a benchmark to assess potential substantive and procedural updates. The paper argues that the value of the DFA largely depends on three factors: its alignment with existing consumer and digital laws, the clarity of definitions such as manipulation, digital asymmetry and contextual vulnerability and, most importantly, the strength of its enforcement mechanisms.

Keywords: digital asymmetry; Digital Fairness Act; digital manipulation; digital professional diligence; digital vulnerability

1. Introduction

Are the best customers also the most stupid ones? This is what Schrage asks in a blog post for the Harvard Business Review 15 years ago.[1] He does so to highlight a classical informational asymmetry, described by Akerlof as a "market for lemons,"[2] whose consequences are a market where low-quality goods dominate.[3] This logic persists, raising the question of whether the most profitable customers are also the easiest to manipulate. Digital commerce has worsened this imbalance. Traders can tailor interfaces, personalise offers and leverage behavioural data to target cognitive biases or situational vulnerabilities, exerting an influence on consumers resulting in decisions, disclosures or subscriptions they might not choose otherwise. Thus, the key issue today is not a lack of sufficient information. Quite the opposite: a data-driven choice architecture that influences how consumers perceive and make decisions.

[1] M Schrage, "Should Your Best Customers Be Stupid?" Harvard Business Review (19 November 2010) <https://hbr.org/2010/11/should-your-customers-be-stupid>.

[2] G Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism" (1970) 84 The Quarterly Journal of Economics 488 <https://doi.org/10.2307/1879431>.

[3] Sellers know the true quality of their products, buyers cannot distinguish good product from a bad one, buyers settle for an average price leading to high-quality products and sellers exiting the market. This creates a market where low-quality products and sellers dominate due to informational asymmetry.

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/err.2026.10146

Against this background, the foundational principles of EU Consumer law rest on an ideal type: the informed, reasonably observant and circumspect average consumer, presumed capable of autonomous transactional choice when provided with clear and sufficient information. The contemporary digital economy challenges this presumption. The Court of Justice of the EU (CJEU) recognised the abstract fundamentals of the notion of "average consumer," based on the perfectly rational "homo economicus," but importantly recognised that human behaviour may be bounded by cognitive biases, impairing an individual's decision-making capacity.[4] Digital consumers, however, operate within environments characterised by continuous data collection, profiling, personalisation, information overload and behavioural targeting.

In this environment, and after an unprecedented adoption of multiple digital regulations,[5] a brand-new piece of legislation lies on the Brussels legislative conveyor belt. This happens amid ongoing discussions about the potential to optimise European red tape,[6] identified as a competitive handicap.[7] Handicapped or not, the Commission launched a concept testing in October 2025 for the newest product on the EU legislative market: a kit of new consumer fairness-based principles, rules and duties ahead of the official release of the proposal for the Digital Fairness Act (DFA) in the second half of 2026.

This paper provides a one-stop overview of current discussions, sheds light on the context with a focus on the UCPD, reviews key institutional stakeholders to the DFA and highlights potential hindrances. I argue that the DFA's value depends on three factors: its coherence with the existing digital legal framework, the definitions and implementation of vulnerability and manipulation and the strength of its enforcement mechanisms.

Dark patterns illustrate the three problems, especially the interaction between UCPD's standards, the DSA's sector bans and their enforcement. The paper does not analyse dark patterns as a standalone topic, nor does it define or categorise them. Notably, and somewhat unusually, this paper also compiles anonymised discussions with private-sector representatives, scholars, and EU officials conducted throughout 2025.[8] Any normative proposals in this paper are my own and do not reflect institutional positions.

The paper continues with Section 2, which situates the DFA within the evolution of the EU consumer law safety net and identifies the shortcomings exposed by data-driven commerce. Section 3 draws on anonymised stakeholder discussions to examine the main legislative choices confronting the initiative, including its legal form, scope and enforcement architecture. Section 4 analyses the reform model advanced by Helberger et al., with particular attention to digital asymmetry, contextual vulnerability, fairness by design and the proposed shift in evidentiary burdens. Section 5 then critically assesses the main risks facing the DFA, such as regulatory overlap and fragmentation, conceptual and operational uncertainty and weak enforcement, and proposes ways for addressing them. Section 6 concludes.

[4] *Judgment of 14 November 2024, Compass Banca SpA v Autorità Garante della Concorrenza e del Mercato (AGCM), Case C-646/22, ECLI:EU:C:2024:957*. Paras. 42–43 and 59.

[5] For example, Digital Services Act (Regulation 2022/2065), the Digital Markets Act (Regulation 2022/1925), Data Act (Regulation 2023/2854) and the Artificial Intelligence Act (Regulation 2024/1689).

[6] <https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation/simplification_en#omnibus-proposals>.

[7] Draghi's report: <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en>.

[8] This paper integrates insights based on two previous works of mine: L Nikiforov, "Digital Fairness Act: If and How?" [2024] Brussels Privacy Hub <https://doi.org/10.2139/ssrn.5025754>; Liubomir Nikiforov, "Are We Forcing Companies to Be 'Fair'?" <https://doi.org/http://dx.doi.org/10.2139/ssrn.5217982>.

https://doi.org/10.1017/err.2026.10146

2. The digital fairness check report

The consumer-law "safety-net" comprising the three Directives: UCTD, UCPD and CRD,[9] has been praised for breadth and technological neutrality, while adjacent and horizontal instruments such as the Digital Services Act (DSA), Digital Markets Act (DMA) and the AI Act, alongside the GDPR, have materially upgraded governance of platforms, data practices and algorithmic systems. The UCPD establishes, in its Annex I, a blacklist of specific business methods which are considered harmful and therefore banned in all circumstances. For all other particular cases, the UCPD provides a general clause prohibiting business practices such as those contrary to professional diligence, *potentially* distorting consumers' decision-making, misleading or aggressive (Arts. 5–9 UCPD). Importantly, and contrary to the provisions in Annex I, the burden of proof lies on the consumer, who should demonstrate that the practice has the potential to be detrimental to an average consumer, or that the same would not have occurred if the business method had not been applied.

The Consumer Rights Directive 2011/83/EU (CRD) focuses on ensuring that consumers receive proper precontractual information (Arts. 5–6 CRD), establishes formal requirements for the conclusion of a contract and grants consumers a 14-day withdrawal right (Arts. 13–14 CRD). Finally, the Unfair Contract Terms Directive 93/13/EEC (UCTD) protects consumers against the use by traders of not individually negotiated contract terms which, contrary to the requirement of good faith, create a significant imbalance in the parties' rights and obligations to the detriment of the consumer (Art. 3 UCTD), which are not binding in that case. It contains, in its Annex, a non-exhaustive list of terms that may be considered unfair, which aims to guide national authorities and courts in their case-by-case assessment of a contract term by listing some of the most common types of potentially unfair terms.

The EU consumer law does not exist in isolation from the evolving digital technologies and practices, as well as the latest EU digital acquis. The combination thereof raises specific challenges, analysed in the Digital Fitness Check Report (hereinafter, the Fitness Check),[10] commissioned in response to that evolving landscape.

2.1 The fitness checks: recurring protection and enforcement issues

Specifically, the Fitness Check examined how well existing EU consumer protection laws work, seeking to determine if the current legal framework, based on three core directives, still effectively safeguards consumers in a digital environment that has changed considerably since these laws were introduced.

Although the Directives apply equally online and offline, the Fitness Check reveals that, while still relevant, they were designed before the full-scale rise of digital markets. While they have been applied in the digital environment, the safety net lacks the specificity

[9] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95/29); 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") (OJ L 149/22); Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304/64).

[10] European Commission, "Commission Staff Working Document Fitness Check of EU Consumer Law on Digital Fairness (SWD(2024) 230 Final)" <https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en>.

https://doi.org/10.1017/err.2026.10146

needed to address some of the emerging issues that digitalisation has brought. Those challenges have two dimensions.

The first one relates to the new business models and practices. Annex VI of the Fitness Check identifies recurrent problematic practices such as dark patterns, addictive design and gaming, personalisation, social media commerce and influencer marketing, contract cancellations, subscriptions and contract terms. The challenge is not that these practices are not covered by consumer law, but that applying the Directives' net often depends on a case-by-case basis and can render the result evidentiary, difficult and, finally, legally uncertain.[11]

Take, for example, the term "dark patterns," designating practices commonly assessable under the UCPD and prominently pointed out as problematic in the Fitness Check. The Directive does not contain a dedicated concept. Instead, those practices may be challenged under the Directive as unfair commercial practices, depending on the case, as "misleading" (Arts. 6 and 7 UCPD) or "aggressive" (Art. 8 UCPD), and, in some instances, under Annex I. The UCPD is generally celebrated for its adaptability to evolving market strategies because of its principle- and horizontally based approach. Interestingly, a much more recent law clarifies "dark patterns" further. Recital 67 DSA establishes that those 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," and prohibits certain interface designs in Article 25 DSA. The result is that the DSA adds a sector-specific layer to an already complex consumer protection system, relying on substantial case-by-case assessment by enforcers and courts. Thus, the advantage of flexibility turns into a disadvantage of regulatory fragmentation. A core issue for consumers, as well as for digital law, such as manipulative designs, is scattered across legislation that, although intersecting in subject matter or objective, "differ(s) in scope and enforcement."[12] It is precisely enforcement that is the next dimension.

The second dimension of the challenges before consumer law involves the normative and enforcement response. The Fitness Check highlights persistent issues that undermine the initial purpose and effectiveness of the consumer protection measures designed at the beginning of the century. Using the same example as above, while design-level manipulation and opaque personalisation are regulated through a patchwork rather than a single, coherent regime, captured as unfair B2C practices, the DSA adds a sectoral prohibition of "dark patterns" of online platforms and additional safeguards for very large online platforms (VLOPs) or search engines (VLSEs). Beyond that specific context, the applicable laws (e.g., UCPD, CRD, GDPR) and the enforcement agencies (national consumer bodies or consumer protection cooperation, digital services coordinators or data protection authorities) differ.

Insufficient enforcement persists, despite improved cross-border coordination and new possibilities for collective redress.[13] The report points to continued constraints on the Consumer Protection Cooperation (CPC) Network's effectiveness in digital markets (including limited resources and procedural complexity). In addition, consumer awareness

[11] Ibid, p 148 "Only a limited number of dark patterns are directly prohibited in the UCPD blacklist, although none of the existing prohibitions refer specifically to digital interfaces and their application hinges upon a case-by case assessment ... the lack of legal certainty about the fairness or unfairness of specific types of dark patterns under the UCPD could undermine the effectiveness of its application."

[12] "Commission Communication, COM(2025) 708."

[13] European Commission, "Digital Fairness Check Report" (n 10). p 48 "The Fitness Check indicates that the effectiveness of the three Directives is undermined by suboptimal private and public enforcement, in line with findings from previous evaluations. During the evaluation period, there has not been a sufficient level of case law and enforcement actions applying the Directives to digital practices, especially to novel and data-driven practices. This problem is likely to worsen under the conditions of legal uncertainty, which has a chilling effect on enforcement and increases the risks that the litigant or authority has to bear in the face of uncertain outcomes."

https://doi.org/10.1017/err.2026.10146

of rights, necessary to trigger complaints and redress, remains insufficient and continues to undermine the effectiveness of EU consumer law in the digital environment.

These different levels of protection, complementary regulations and multiple enforcers give rise to inconsistent governance across the full spectrum of trader-to-consumer interactions, particularly beyond very large platforms and enforcement remains uneven across authorities and regimes.[14] The cumulative effect is fragmentation, legal uncertainty for traders and enforcers and persistent risks to consumer autonomy and fair dealing. The e-market transformation has not only commercial and technological dimensions but has also led to a shift in consumer behaviour. As digital transactions have grown, so have concerns about unfair practices and the exploitation of consumers online.

The Fitness Check highlights the need for further EU action to address those challenges and thus lays the tracks on which the new Digital Fairness Act proposal[15] would be railed, addressing gaps that have emerged over the last decades of the evolution of digital markets.

Unsurprisingly, for those who follow the topic closely, the idea is not new. Actually, neither the idea nor the exercise. A Fitness Check conducted in 2017 identified the need for an updated regulatory evaluation (hereinafter, the 2017 Fitness Check).[16] The European Commission's "New Consumer Agenda" (2020) emphasised the need for a review and, potentially, new legislation to address the specific challenges of the digital environment.[17] The Modernisation Directive 2019/2161,[18] which entered into force in 2022, is the product of that public effort and introduced new amendments to all three Directives in response to problems identified in the 2017 Fitness Check and the CRD evaluation.

The conclusions of the 2017 Fitness Check highlight the lack of "significant progress on traders' compliance with consumer protection rules," despite the "overall positive outcome" resulting from the study and the capability of the Directives to address consumer problems, including in the digital and online markets. Nevertheless, the 2017 Fitness Check underlines that the undermining factors for a better effectiveness of the Directives are insufficient enforcement, limited awareness of consumers' rights and deficiencies in redress mechanisms. The solutions envisaged are EU-wide rights to remedies (the UCPD, back then nor today, sets forth any direct rights for consumers to individual remedies), possible updating of the UCPD blacklist, introduction of a UCTD black or grey list of unfair terms, instead of a non-exhaustive one, as well as other changes to regulations, which are not covered by the 2024 Report. Overall, the 2017 Report is optimistic about Directives' effectiveness, complementarity, efficiency and continued relevance, given modern challenges and proper enforcement.[19]

Curiously, the 2024 Fitness Check of the consumer legislation not only builds on those studies and the 2017 Fitness Check, but restates the challenges and repeats the conclusions. In fact, the 2024 Report argues that the effectiveness of the three Directives is limited by a lack of traders' compliance, ineffective enforcement, legal uncertainty, regulatory fragmentation and a "changing regulatory landscape with the arrival of new legislation." Precisely, the latter factor is the focus of the 2024 Fitness Check, which stresses issues

[14] See also, F Esposito, C Santos et al. in this special issue.

[15] <https://digital-strategy.ec.europa.eu/en/consultations/commission-launches-open-consultation-forthcoming-digital-fairness-act>.

[16] Civic Consulting, "Study for the Fitness Check of EU Consumer and Marketing Law" <https://ec.europa.eu/newsroom/just/items/59332/en>.

[17] European Commission, "New Consumer Agenda – Strengthening Consumer Resilience for Sustainable Recovery" <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2069>.

[18] 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 (OJ L 328/7).

[19] Enforcement and also, awareness and knowledge improvement as well as simplification, where justified.

https://doi.org/10.1017/err.2026.10146

concerning consumers' data, transparency in advertising and pre-contractual information as well as digital addiction. The wave of new legislation is the trigger for the renewed assertion of the need to take steps to refurbish the consumer safety net. Along with this, old arguments persist, such as fragmentation, legal uncertainty and the evergreen enforcement problems. The document acknowledges two conceptual challenges vis-à-vis progress in digital technology.

2.2 *The conceptual mismatch: the average and vulnerable consumer*

The recurring issues of coverage, enforcement and regulatory coordination are linked to a fundamental conceptual challenge. EU consumer law benchmarks, designed to evaluate decision-making and vulnerability, were developed in a less data-driven commercial context. Consequently, a growing disconnect exists between the legal perceptions of consumers and the actual realities of digital decision-making.

First, the "growing mismatch" between the conceptualisation of the "average consumer," who is informed and rational and the reality of human behaviour, both online and offline. This is so because consumers rarely fully understand digital supply chains, data collection and algorithmic processes, as well as the logic behind any automated decisions and services, and their inherently limited bargaining power.[20] Second, the concept of "vulnerable consumer" traditionally refers to a set of *recognised* vulnerable consumers with fixed characteristics, which places them in an adverse situation compared to other consumers. This is particularly relevant in the context of children's use of internet services. The digital environment requires further adaptation and stronger inclusion[21] of the term in line with the present reality, which demands a context-dependent approach, beyond the non-binding UCPD Guidance,[22] "including socio-demographic characteristics but also personal or psychological characteristics, such as interests, preferences, psychological profile and mood."[23] Therefore, the concern here could be restated as one related to an emergent set of risks issuing from the use of personal data for personalisation and targeting. This leads to "limited or non-existent bargaining power, aggravated by insufficient digital literacy, cognitive biases, information overload, manipulative design of online choice architectures, a lack of interoperability between services, among other factors," according to the 2024 Report.

Taken together, the institutional and conceptual diagnosis explains why the Commission has reopened a consumer-law framework recently amended through the Modernisation Directive. As confirmed in November 2025, the Consumer Agenda 2030 identifies four key areas, with competition as the overarching priority, alongside sustainable consumption and enforcement initiatives. "Consumer protection and digital fairness" completes the Commission's list of priorities for the 2030 Agenda.[24] The Digital Fairness Act should address consumer vulnerability and manipulative digital design, such

[20] Expressly acknowledged recently in C-646/22, see above.

[21] Already mentioned in Art. 5(3) UCPD, Recital 19.

[22] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021) (OJ C 526/01).p 47. Reportedly several stakeholders consulted argued that the approach to "vulnerable consumers" is too unclear and too narrow, and therefore codifying the term in binding law is necessary. They also say it's uncertain whether vulnerability can arise from specific technologies or commercial practices, not just from personal characteristics. The definition is criticised for not adequately covering consumers vulnerable to discrimination, exclusion, harassment or targeting linked to protected characteristics. Business/trader respondents mostly consider the "average" and "vulnerable" consumer concepts adequate, while consumer organisations disagree.

[23] European Commission, "Digital Fairness Check Report" (n 10). p 47.

[24] "Communication 2030 Consumer Agenda COM(2025) 848 Final" <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2730>.

https://doi.org/10.1017/err.2026.10146

as dark patterns, addictive design, personalised pricing and advertising, online profiling and influencer marketing, by harmonising clearer rules and stronger enforcement mechanisms.[25] In line with the Commission's agenda, the DFA aims to simplify "consumer information requirements in specific types of contracts and in repetitive transactions with the same traders."

The objective is thus set. However, questions about the pertinence, timing, scope and terminology, as well as the interplay with other regulations, surface immediately. The next section draws on and encapsulates stakeholders' rationale to explore emerging queries.

3. Are we forcing companies to be fair?

3.1 Why another regulation?

It has been highlighted that the Modernisation Directive 2019/2161 recently introduced changes deemed necessary. Then, why is the European Commission taking the initiative to propose a new regulation? Part of the answer lies in the consumer legislation architecture itself, which still resists the current e-businesses' commercial and marketing practices, responding with broad principles that lack concrete, black-and-white rules for modern e-commerce practices. The resulting risk is twofold. On the one hand, confusion among e-businesses about existing concepts and the interpretation of rules; on the other, inaction by national enforcement authorities, reluctant to litigate in ambiguous territory.

Another part lies in the newly adopted digital legislation. Despite the new regulations, such as the DSA, still being relatively fresh, they do not systematically address manipulative designs or a wide range of unethical commercial practices across the entire digital marketplace. For example, the DSA addresses some of them in a sector-specific way. Article 25 DSA prohibits manipulative or materially distortive interface design by providers of online platforms. Article 26 imposes transparency duties on advertisements on online platforms, and Article 27 requires transparency regarding recommender systems. Yet vast swaths of online commerce are not necessarily platform-based. A direct-to-consumer brand (e.g., Zara), an e-shop (e.g., supermarkets) or a software provider selling through its own website (e.g., McAfee), falls outside the DSA's scope for dark patterns prohibitions.[26] The GDPR addresses the manipulative use of personal data, but only in certain contexts, because problematic practices do not always revolve around data collection; for example, they can involve interface design and choice architecture. Thus, consumers and enforcement authorities primarily rely on the three aforementioned Directives, which should be interpreted, applied and aligned with the latest stack of digital laws. In other words, the Commission seeks to bridge the gap between the existing *analogue* law and the current commercial and normative reality with a targeted tool.

The challenge is not limited to a specific concept or practice; some may be easier to define than others,[27] while others may be contested because they generate benefits while

[25] "Mission Letter Ursula von Der Leyen" <https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf>; European Commission, "Call for Evidence for an Impact Assessment. Digital Fairness Act" <https://ec.europa.eu/transparency/documents-register/detail?ref=Ares(2025)5829481&lang=en>.

[26] See further, F Esposito, C Santos et al. in this special issue.

[27] Despite best efforts from scholars to map and connect existing scholarship on the definition of "dark patterns" (e.g., camouflage design, fake countdown timers, impossible subscription-cancellation pages), they conclude that a "universally accepted definition" does not exist and propose one based on a systematic literature review. The authors propose the following definition: a dark pattern is the design of a digital choice environment, normally of commercial nature, that is capable of distorting user behaviour, often by exploiting heuristics and biases. In C Isola and F Esposito, "A Systematic Literature Review on Dark Patterns for the Legal Community: Definitional Clarity and a Legal Classification Based on the Unfair Commercial Practices Directive" (2025) 58 Computer Law & Security Review 106169 <https://doi.org/10.1016/j.clsr.2025.106169>.

https://doi.org/10.1017/err.2026.10146

also amplifying manipulation, opacity or exploitation of consumers' vulnerability risks.[28] This is why the policy debate in Brussels is so challenging. It involves not only clearly constraining harmful practices but also determining the extent to which the law should regulate or restrict commercially valuable yet potentially distortive techniques.

3.2 *The quantum legislation*

The DFA is in a *quantum*, undefined state where every outcome is possible. Two variables maintain this state. First, it is unknown whether the Act in the DFA is a replacement for regulation or a directive. The answer should determine the impact and consequences thereof. Second, and probably more importantly, whether the DFA would be a standalone piece of legislation or would turn out to be another update to the UCPD and other relevant directives. This choice is not superfluous. It will shape legal certainty and the coherence of the consumer and digital rulebooks, because further layering through partial amendments and cross-references can increase interpretative complexity and compliance concerns and can undervalue the coherence that EU legislative commitments and drafting guidance treat as central.

One of the anonymised discussions conducted in 2025 with an official from an EU public body[29] suggests that the initiative is not conceived as a freestanding online platforms regulation, despite the Digital Fairness Act label, but rather as targeted adjustments to existing instruments, notably the UCPD and the CRD. Despite that indication of institutional direction at that stage of the legislative process, the outcome of the Call for Evidence of the Impact Assessment[30] expected with the proposal of the DFA could be drastically different, especially once consultations begin, and stakeholders weigh in.

According to the same source, the Commission is not seeking an ethics-driven overhaul of industry practices. Rather, it aims to tighten the legal definitions of harmful or deceptive conduct and, plausibly, to adopt a negative list of manipulative "dark pattern" tactics so businesses know precisely what is off-limits, potentially alongside other measures to concretise and operationalise today's broadly framed safety-net rules.

One provocative question is how far the DFA would go in prohibiting manipulative design outright. The Commission may incorporate a new, or at least expanded, list of specific prohibited practices. Frequent examples include colour cues that steer users towards higher-priced subscriptions or pop-ups that obscure the "cancel" option. A further live issue is whether to articulate a broader "fairness by design" principle, inspired by the GDPR's Article 25, "data protection by design and by default," and as some civil society organisations propose.[31] Yet the boundary between a *friendly* and a manipulative nudge is highly blurry, and the conceptually problematic umbrella term "dark patterns" covers everything from mild persuasion to outright deception. The regulatory task, therefore, is to define prohibited practices with precision or require functionally equivalent alternatives so that the ban targets manipulative variants rather than entire feature classes.

[28] "... online personalisation in theory can benefit consumers if it matches them to products that best suit their needs, lowers prices and reduces their search costs. However, personalisation can negatively affect consumers if it is used to steer them towards the most expensive products that they are willing to pay for. In turn, personalisation may benefit consumers who actively shop around and are tech-savvy." Consumers, Health, Agriculture and Food Executive Agency. and others, *Consumer Market Study on Online Market Segmentation through Personalised Pricing/Offers in the European Union Final Report.* (Publications Office 2018) <https://data.europa.eu/doi/10.2818/990439>.

[29] At the request of the source, the person's name remains undisclosed.

[30] European Commission, "Call for Evidence for an Impact Assessment. Digital Fairness Act" (n 25).

[31] N Helberger and others, "Digital Fairness for Consumers" (BEUC, 18 November 2024) <https://doi.org/10.31219/osf.io/hqa4n>.

https://doi.org/10.1017/err.2026.10146

For example, under the DFA, would the Netflix autoplay be considered a dark pattern or a service feature? Experts and officials need to devote additional attention and scrutiny to the distinction between valuable and convenient features and "harmful manipulations," to avoid overregulation or tipping the balance towards excessive caution.

Equilibrium is a term with economic and legal connotations and is highly pertinent to the discussion of EU competitiveness. The sadly familiar remark that "while others innovate, Europe regulates" is often met by the counterargument that clearer rules can reduce cross-border compliance costs. Some argue that a definitive negative list of manipulative design patterns, for example, would save SMEs the expense of navigating twenty-seven divergent national interpretations. Taking other Regulations into account, while the DSA already addresses certain "dark patterns" on platforms (Art. 25 DSA), many apps, e-shops and services fall outside its scope. Similarly, the GDPR targets the processing of personal data rather than interface design. Therefore, the issue of regulating digital manipulation is navigating the different patches, each regulating certain aspects of e-deception and complementing the others. Thus, another horizontal instrument clarifying which manipulative practices are prohibited for all businesses could reduce fragmentation, in line with the Commission's logic.

Although companies frequently cite compliance costs as a barrier, the 2024 Fitness Check's insiders deny that this area is cost-intensive: obligations are principle-based, with no routine reporting, and primarily require abstention from misleading and aggressive practices. Importantly for consumers, however, whether any new rules would translate into higher consumer prices and remains an empirical question. The Fitness Check suggests that the regulatory burden is generally modest. Some of the surveyed traders (around 10–18%) report "high" compliance costs for the relevant activities. The Report also indicates a significant asymmetry in magnitude between estimated consumer detriment (around EUR 7.9 billion per year) and estimated annual compliance costs for traders (around EUR 511–737 million).[32] However, whether consumers pay more after regulatory tightening cannot be assessed solely by price. Traders can also compete (or discriminate) through personalised contract terms, shifting the relevant welfare question towards a price–quality (or price–terms) adjustment rather than simply on the nominal price.[33]

Another recurrent critique of EU consumer law is its weak enforcement. Although the CPC (Consumer Protection Cooperation) Network and Regulation[34] connect national authorities, the Commission, unlike under the DSA, for example, has no direct enforcement role in consumer cases and cannot impose fines because the control remains largely national. The Commission can coordinate joint positions in high-profile matters (for example, recent action concerning platform discounting practices).[35] Yet, concrete sanctions or compelled compliance take years. Therefore, the DFA proposers face a typical policy-related dilemma: whether to explore direct enforcement powers for large, cross-border consumer cases or to keep the current decentralised model. Securing agreement among

[32] The Fitness Check suggests that the regulatory burden is generally modest. Only a minority of surveyed traders (around 10–18%) report "high" compliance costs for the relevant activities. The Report also indicates a large asymmetry in magnitude between estimated consumer detriment (around EUR 7.9 billion per year) and estimated annual compliance costs for traders (around EUR 511–737 million). European Commission, "Digital Fairness Check Report" (n 10). p 86.

[33] A Davola, F Esposito and M Grochowski, "Price Personalization vs. Contract Terms Personalization: Mapping the Complexity" (2024) Cambridge Handbook on Price Personalization and the Law <https://ssrn.com/abstract=4791124>.

[34] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345/1).

[35] <https://ec.europa.eu/commission/presscorner/detail/fi/ip_24_5707>.

https://doi.org/10.1017/err.2026.10146

twenty-seven Member States would, however, be politically demanding and highly uncertain amid divergent political agendas, competitiveness concerns and stakeholder pressure.

One dimension of consumer protection is often overlooked or underestimated: the collective harm arising from personalisation and targeting. Observed or inferred preferences enable outreach to consumers whose data may never have been directly collected. The risk is not merely deception of an individual, but systematic steering of social or economic groups, including algorithmically designed ones.[36] Existing instruments partially acknowledge this concern, most notably the Representative Actions Directive,[37] whose practical effects are still early to observe. Complementary safeguards could be explored through the DSA's systemic-risk assessments (Arts. 34–37) and the GDPR's representative actions mechanism (Art. 80). If the DFA recognises collective harms expressly or engages with those mechanisms, beyond existing terms such as average/vulnerable consumer, it would constitute a significant shift.

The next section explores an influential consumers' organisation report released (March 2024) before the 2024 Fitness Check (published in October 2024), which clearly interacts therewith, if not inspires the 2024 Fitness Check's core taxonomy, conceptualisation, challenges identification and solutions.

4. Digital fairness for consumers

The mismatch between available legislation, consumer behaviour and commercial practices has been the focus of a series of studies[38] dating back to as early as 2021. Among the contributions to the emerging DFA debate, the 2024 report by Helberger et al. provides a specific examination because it develops one of the most comprehensive reform models for adapting EU consumer law to data-driven commerce. It is discussed here not as an indication of the Commission's eventual position, but as an analytical benchmark. The report connects the conceptual diagnosis of digital consumer vulnerability with concrete substantive, procedural and institutional reforms. It therefore provides a useful basis for assessing whether an ambitious DFA could address the shortcomings identified in the Fitness Check without reproducing the fragmentation, conceptual uncertainty and enforcement weaknesses already affecting the digital acquis.

In the first place, Helberger et al. modernise EU Consumer law conceptually by aligning it closer to the digital environment, where consumers' harms do not stem from pre-established and fixed features but are a dynamic product of a combination of factors leading to a state of digital asymmetry,[39] which leads to a digital

[36] F Esposito and M Grochowski, "Introduction: Algorithmic Price Personalization: From Laesio Enormis to Laesio Algorithmica?" *The Cambridge Handbook of Algorithmic Price Personalization and the Law* (Cambridge University Press 2025).

[37] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409/1).

[38] N Helberger and others, "EU Consumer Protection 2.0 Structural Asymmetries in Digital Consumer Markets" <https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf>; Helberger and others (n 31); Christoph Busch and Amelia Fletcher, "Shaping the Future of European Consumer Protection: Towards a Digital Fairness Act?" <https://cerre.eu/wp-content/uploads/2024/12/Shaping-the-Future-of-European-Consumer-Protection-Towards-A-Digital-Fairness-Act.pdf>; K Drazewski, "EU Consumer Protection 2.0 Protecting Fairness and Consumer Choice in a Digital Economy" <https://www.beuc.eu/position-papers/eu-consumer-protection-20-protecting-fairness-and-consumer-choice-digital-economy>; Steven Berger, "From Influence to Responsibility: Time to Regulate Influencer Marketing" <https://www.beuc.eu/position-papers/influence-responsibility-time-regulate-influencer-marketing>.

[39] Digital asymmetry has three components. The first element is structural, stemming from control over service architecture and data access. The asymmetry in digital space is relational, as consumers are disadvantaged, often reliant on providers due to lock-in, network effects and switching costs. Finally, digital

https://doi.org/10.1017/err.2026.10146

vulnerability[40] that consumers cannot readily detect or contest. Those circumstances provide grounds for potential consumer digital manipulation in the context of inadequate and uneven European legislation regarding modern business practices.[41] Those conceptual adaptations, however, need their procedural pathways.

This is why, in the second place, modern e-commerce reality requires tailored business duties that take into account the vulnerabilities and challenges consumers face. The authors of the study argue for the introduction of a digital fairness-by-design principle, drawing on the experience of privacy and data protection legislation, where it is already a well-established duty under Article 25 GDPR. This obligation embeds fairness requirements into systems, interfaces and processes from the outset, thus shifting the emphasis from ex-post verification, duties and potentially sanctions to ex-ante prevention.

Another key duty would be digital professional diligence, which entails an obligation not to exploit digital asymmetries or vulnerabilities. It recalibrates the traditional professional diligence for data-driven contexts and refocuses on exploitation of systemic imbalances, not merely "being contrary to honest market practices and/or good faith" (Art. 2 (h) UCPD).

In the third place, and in connection with the previous, those changes would require a paradigm shift, with the burden of proof reversed from the consumer (duty not to act unfairly) to the trader (duty to act fairly). This new approach would procedurally lower the bar for proving an infringement.[42] This mechanism is strengthened by a requirement to provide a "meaningful explanation" of the observed difference, where if a trader does not manage to do so, it would be presumed that the practice observed is unfair.

Those substantive and procedural changes aim to prevent the risks of mismatch between core concepts such as average consumer or vulnerable consumer and their digital expressions and, in so far, mitigate the claimed insufficient specificity of the principle-based legislation (UCPD, UCTD, and CRD). Moreover, the study authors argue that those changes would prevent further fragmentation not only across jurisdictions but also across recently adopted digital legislation.

For all those reasons, there are two proposed solutions. The first one, and most realistic as well as feasible, short-term solution is to recalibrate the "safety net" and translate the identified pitfalls into a set of targeted amendments. The second option is to adopt a new law, the Digital Fairness Act. Both solutions are not mutually exclusive. In reality, a reform of the UCPD could be the precursor of a future separate EU regulation.[43]

asymmetry is knowledge-based because traders know more about consumers and products, including through predictive profiling based on behavioural data. Those elements expose a mismatch between the benchmark established by the traditional term "average consumer," which presumes bargaining power, rationalism and attentiveness, and the digital environment, already acknowledged in case law in C-646/22. See further in Helberger and others (n 38).

[40] Digital vulnerability has similar elements (relational, structural and privacy erosion). First, consumer vulnerability is relational, linked not just to personal traits but also to the service's infrastructure and consumers' position. Second, the service architecture may exploit and reveal consumer weak points. Lastly, personal data sustains this by collecting and inferring consumers' behaviour. See in ibid.

[41] Digital manipulation is understood as an influence that targets and exploits (actual or presumed) vulnerabilities to steer people's behaviour, generally in a trader's interest. Helberger et al. acknowledge that the wide array of deception techniques makes it hard to define "manipulation" in positive law, stressing that laws such as the DSA (Art. 25 (1)) or the AI Act (Art. 5 (1)a and b) mention manipulation but do not define it.

[42] Helberger et al. give the following example: "In the case of unfair commercial practices law, it would thus be necessary to show some sort of anomaly that indicates the potential presence of a breach of law. For example, in case of the suspected personalisation of prices, indication of an infringement could simply consist of two screenshots taken at the same time concerning the same product with different prices."

[43] "Looking further into the future, one can envision a separate legal act: the Unfair Digital Commercial Practices Directive (the UDCPD), the Digital Fairness Act, or even a new regulatory framework – EU Fair Trading Law 2.0 . . ." Helberger and others (n 31).

https://doi.org/10.1017/err.2026.10146

The report thus crystallises the central question examined in the remainder of this paper: whether this conceptual and procedural recalibration can be translated into sufficiently precise, coherent and enforceable legal duties. Section 5 tests that reform model against the principal difficulties identified throughout the preceding analysis: the choice of legislative instrument, overlap with the existing digital acquis, the operationalisation of vulnerability and digital asymmetry, the design of fairness-by-design duties and the persistent weakness of consumer-law enforcement.

5. Concerns: a three-body problem

Reading the experts' report reviewed in the previous section, together with the ongoing public and private discussions in Brussels, the impression of a compromise among needs, concerns and objective reality is evident between the lines. The proposed solutions are a way to balance what is possible and what is desirable: the optimal and best solution is a new act, DFA,[44] directive or regulation. However, objectively, a more probable initial way forward is another amendment to the UCPD (its Annex I and the other Directives). Calibrating these three vectors, necessity, feasibility and institutional policy choice, is a true three body problem.[45]

Everything is possible. Nevertheless, quite recently, in 2019, a package of amendments to the "safety net" was adopted with the Modernisation Directive.[46] Thus, it is not only questionable to update the UCPD, but it is already clear that the Commission prefers to elaborate a new piece of law. I agree with the conceptual and technical recalibration proposed in Helberger et al. in general and in principle. However, a major concern, shared by all stakeholders along the line, remains: how would this reconceptualisation and paradigm shift be operationalised? And, even more importantly, would the enforcement improve? Several concerns regarding the Digital Fairness Act initiative and its optimal result follow:

1. Regulation, Directive or another update: The name Digital Fairness Act, from the experience with the *Acts* in the past couple of years adopted by the Parliament in the ambit of the digital legislation, gives the impression that the upcoming proposal is a Regulation: the utmost harmonisation instrument. That impression might be misleading.

   The Commission signals that the aim is not to build an entirely new law, despite the Digital Fairness Act's name, but to refine the existing acquis, notably the UCPD and the CRD. Caution is advised, since the scope may shift during consultations as stakeholders weigh in. Multiple private sources indicate that the objective is not an "ethical" supervision of corporate strategies but sharper legal definitions of harmful or deceptive conduct. In that vein, the Commission could introduce an Annex I-style blacklist of manipulative interface tactics so businesses know precisely which designs are banned or borderline, coupled with targeted measures that concretise and operationalise today's broad, safety-net rules.[47]

[44] "...an optimal solution would be the introduction of the Digital Fairness Act, emphasising the shift in perspective already in its name. Amendments to existing legislation, especially the UCPD, are not recommended." ibid.

[45] By "three-body problem" I refer to a physics problem and a TV show: a systems with three interacting forces where small changes can produce very different outcomes, making a single solution unlikely.

[46] 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 (OJ L 328/7) (n 18).

[47] Nikiforov, "Are We Forcing Companies to Be 'Fair'?" (n 8).

https://doi.org/10.1017/err.2026.10146

Then, how would the adoption of a new law be better than the potential consecutive amendment of the UCPD, for example? Unless the proposal is in the form of a Regulation, a separate Directive would be an amendment of the safety net, similarly to the very fresh one from 2019 without another modernisation act. The risk is that it will water down the momentum and produce a beautiful document that does not solve the core issues: implementation, enforcement and interplay with other norms.

2. Already complex picture: The Consumer law legislation is already highly complex, not only because of the intricate contemporary business transactions, existing EU regulations but also due to different Member States' case law and doctrines. In addition, it intersects with multiple sectoral laws, such as those on Competition or Digital.

   Therefore, there are critics in Brussels who question the need to adopt a new piece of legislation and by that adding another layer to an already overloaded normative picture. On the one hand, adopting a new Directive would add complexity and burden to traders, practitioners and enforcers in an environment where business-consumer rules are predominantly harmonised through Directives and thus broad, purpose-driven norms. This legal reality should be able to aptly and effectively match and interact with the digital legislation, bound by direct and immediate-effect regulations. The consequences thereof are already known and reported: divergent case law and interpretations regarding Consumer law among member states. The adoption of a DFA as a Directive risks further fueling the imbalance between the broadness of consumer norms and the immediate effect of digital legislation, while both should be as aligned as possible.

3. Another patch: The risk to sew a new patch to the net of norms currently in force is real. A new regulation would introduce a new set of concepts that are discussed extensively in academia. However, in a context where existing terms are judicially underdeveloped as the case of professional diligence, manipulation or vulnerability, despite years of application, in addition to a recent wave of new legislation, which is not only lacking case law but also continuous scholarly tradition, is an adventurous and arguably hasty solution. Moreover, this move practically contravenes the aim stated in the Commission's 2024 Fitness Check to provide legal certainty. How do traders gain certainty by introducing new concepts which need to be interpreted and, most importantly, proven in practice?
4. Overlap management and regulatory coherence: The DFA's core risk is not insufficient coverage but overlap. A horizontal "manipulation" rulebook will inevitably touch Article 25 DSA (design/interface prohibitions limited to platforms), the GDPR's risk- and accountability-oriented duties (especially Arts 5, 24, 25) and AI Act risk controls. Without clear ordering, the result could be an increased complexity with little added value and 1) duplicative obligations (two or more assessments for one design choice),[48] 2) unlikely but possible inconsistent definitions (for example, "manipulation," "profiling," "personalised pricing/advertising"), 3) forum-shopping in enforcement, where jurisdictions' interpretations is more favourable and 4) legal uncertainty for everyone. Thus, failing the

[48] Overlap also raises a constitutional enforcement constraint: where the same conduct is sanctioned through parallel administrative/criminal tracks, cumulative penalties may be limited by the *ne bis in idem* principle (EU Charter Art. 50), which increases the need for clear allocation of competence and coordination across regimes. Also, see for example, C-27/22 Volkswagen Group Italia EU:C:2023:463; CJEU, C-205/23 Energie România EU:C:2025:43 (both on the conditions for applying ne bis in idem and limits on cumulative sanctions).

https://doi.org/10.1017/err.2026.10146

main goal. A coherence clause should state DFA's relationship with existing norms, cross-reference existing definitions and if strictly needed, coining new ones, establish a single-process "equivalence" rule (for example, compliance with Article 25 GDPR documentation can satisfy DFA ex-ante documentation where scopes overlap) and finally mandate single or coordinated joint guidance among the Commission, CPC Network authorities and, where relevant, the EDPB/AI-Act Board. Absent these guardrails, the DFA risks becoming a fourth assessment layer for the very same interface decisions the DSA, GDPR and AI Act already touch.

5. Digital vulnerability: Moving from the UCPD flexible standards to court-enforceable duties may end up diluted in two ways. First, the duty may be watered down during the trilogue through a narrower scope or vague wording. Second, even if adopted, its open-to-interpretation concepts ("digital professional diligence," "autonomous decision-making," "digital asymmetry/vulnerability") may be judicially operationalised in a cautious, high-threshold manner, making the standard difficult to apply and to prove in litigation and therefore ineffective in practice. In Helberger et al., a "new Article 5a" UCPD is proposed, introducing a definition of "unfair commercial practices," which are unfair if 1) contrary to "digital professional diligence" and 2) they could potentially and harmfully distort a consumer's autonomous decision-making. Digital professional diligence means "not exploiting digital asymmetry and/or digital vulnerability." While digital asymmetry designates the imbalance based on unequal knowledge and position between the trader and the consumer, digital vulnerability refers to a "universal state of susceptibility" to exploitation in that imbalanced relation. Precisely at this point, the hypothesis underlying a potential digital vulnerability provision is at its weakest. The provision presupposes that everyone is constantly vulnerable due to "internal and/or external factors."[49] This risks putting every consumer's experience in the same basket, regardless of the specific vulnerabilities present. Given the interconnectedness with data protection, I think the work of Malgieri is useful to exemplify why this "universalistic" approach could be misleading.[50] If "everyone is vulnerable," the term risks inflation and protecting vulnerable consumers may demand, in fact, profiling by default. This is an undesired outcome in data protection,[51] but also in consumer law.[52] The opposite, where some people are *more vulnerable* than others, is neither a desirable solution because of the risk of labelling and missing the dynamic nature of the digital environment and its harms.

   Malgieri proposes, in the context of data protection, a layered approach to vulnerability that distinguishes between different sources and degrees of vulnerability in digital environments. This resembles the data protection variant of the famous Hands' formula, which seeks to regulate the private law concept of negligence.[53] The DFA could adapt it accordingly. Consumers may become situationally or contextually vulnerable, for example, a typically "average"

[49] "Internal factors refer to variations in digital capacities to deal with external factors. They may be situational, information or source-bound, including, for example, the lack of digital literacy or personal biases. External factors cover the digitally mediated relationship, the digital consumer environments/digital choice environments and the knowledge gap, and include, for example, control over personal data into the preferences and behaviour of consumers, the design of digital consumer environments, the lack of interoperability or the way of default settings configurations." In Helberger and others (n 38).

[50] G Malgieri, *Vulnerability and Data Protection Law* (First edition, Oxford University Press 2023).

[51] Here the data minimisation principle would explode because in order to ensure *everyone is not vulnerable* traders should collect more than the necessary data.

[52] The risk of frivolous claims and litigation, based on presumed vulnerability exploitation is envisageable.

[53] It states that an individual is liable for negligence if the burden of taking a precaution (B) is less than the probability of harm (P) multiplied by the magnitude of the harm/loss (L), B<PxL.

https://doi.org/10.1017/err.2026.10146

consumer could be *vulnerable* when confronted with certain personalised targeting or manipulative interface designs. This goes beyond the static view of vulnerability in the Directive. While the UCPD does account for vulnerable consumers to some extent, it considers vulnerable groups (such as those with mental or physical conditions, or those of certain ages) who are especially at risk. Thus, protection is limited to predefined categories and obvious imbalances. Malgieri's layered approach, by contrast, recognises that digital market power asymmetries and profiling techniques can create momentary or context-specific vulnerabilities even for consumers outside the traditionally vulnerable groups. In other words, any consumer might be at a disadvantage if a trader uses data-driven insights to exploit that person's specific weakness or decision-making bias at a particular time. The added value of a new DFA built on this insight lies in its potential to operationalise such protections in ways the current UCPD framework struggles to do.

The DFA could adapt accordingly, offering an operational, non-binary approach to tackling the contextual vulnerabilities created by profiling, personalisation and choice architecture, in contrast to the current one. For example, a trader is liable for exploiting vulnerabilities if the burden of precaution (costs, effort and the feasibility of implementing measures by the trader) is less than the layered probability that the consumer's autonomous decision-making will be harmfully distorted, determined by a combination of factors. The latter is multiplied by the loss of autonomy/severity of the harm. Therefore, the future DFA text would benefit if it bridges the two approaches (universalistic and particularistic) by adapting it to the dynamism of today's digital commerce, where a consumer may be vulnerable in different ways, at different times and in different situations, especially in an age of profiling, personalisation and inferred decision-making. In other words, the DFA would add value if it codifies and operationalises situational vulnerability for data-driven commerce, moving beyond Art. 5(3) UCPD's static categories by targeting profiling and design-based vulnerability triggers, while avoiding a regime that forces traders to treat consumers as "vulnerable" only through blanket profiling.

6. Digital asymmetry: Digital asymmetry is structural, relational and knowledge-based. It should be tackled from its structural side, mainly for the following reasons. First, relationally, there has been, and always will be, a dependence of the consumer on the trader for the provision of services or products. This is why competition is important, because consumers could eventually switch to better service and thus drive the traders to strive for the best product and adapt to consumers. Second, the knowledge-gap imbalance, also identified as problematic in the Commission's 2024 Fitness Check, is unsolvable. I think the idea of bringing the consumer's knowledge and the expert's understanding of the product together is utopian. This debate goes beyond the scope of this article, but it is hard to imagine that a person would understand the value of every product and service fully; also, I doubt it is needed at all. For example, does a patient need to have complete knowledge and understanding of medicine in order to evaluate a medical service or the quality of a pill? Of course, bioethics requires that a patient be informed of the medical procedure and its risks, but he does not need to know why this procedure is preferable to the other. Also, gaining this knowledge requires effort and investment (time, money) by the consumer, which I consider burdensome and impracticable. This is why, in Economics, there is a distinction between search (evaluation possible prior to consumption), experience (evaluation after consumption) and credence goods (difficult or impossible to evaluate even after consumption, for example, legal services or medical treatment). Perfect consumer knowledge (and thus preferences and reasoning prior to purchase) is an economic

https://doi.org/10.1017/err.2026.10146

fiction, constrained by transaction costs such as time, money and effort. Finally, the only way to tip the balance in favour of the consumer without pursuing utopic mirages or encroaching on others' rights (right to do business) is to focus on the structural element. This is to enhance consumer choice and ability to act through ensuring consumers' autonomy (freedom to decide) and the levers to contest unfair practices. In fact, this is in line with the proposed fairness-by-design approach (Section 4). This includes maximum competition, minimum transaction costs, access to redress and powerful enforcement authorities.

7. Fairness by design: It is a concept inspired by data protection (Art. 25 GDPR) where a data controller has to implement data protection principles, rules as well as appropriate technical and organisational measures ex ante in order to protect the rights of data subjects. This potentially new requirement would enhance consumer protection and would allow traders to prove their business practices are not unfair. However, this measure in the GDPR ensuing from the accountability principle (Art. 5 (2) GDPR) which establishes that the controller is responsible for the compliance of the rules and should be able to demonstrate it. Practically, this happens with documentation and impact assessment (Art. 35 GDPR). The Helberger et al. report envisages documentation duties and a "meaningful explanation" provision. However, there is no similar to data protection mechanism (impact assessment) proposed so far in the context of the issues analysed here, which casts doubts on the operationalisation of the mechanism if analogous to the one in data protection law.
8. Enforcement: The most important issue. For a legal norm to function as such, it is imperative that a sanction be foreseen. Otherwise it is a declaration. Moreover, norms not only punish but also have a deterrence effect. Based on those two factors, EU Consumer law faces the challenges discussed throughout the text rather dubiously. CPC enhanced, common EU enforcer are all on the table.[54] Take, for example, the proposed consumer law Hand's formula. It would not work if the burden of precaution, although low, is not met with adequate sanctions, because it would be cheaper for the trader to pay a one-time fine compared to the vast revenue margin he is extracting from an unfair commercial practice. In other words, without proper sanctions, it would be economically beneficial to be an infringer. Sanctions go hand in hand with enforcement. Currently, the enforcement of consumer rules is bound by the financial and political reality in Member States. This reality dictates the enforcement and protection of consumers' rights and broadens the gap between the protection EU citizens receive, despite the efforts for common solutions such as the Consumer Protection Cooperation (CPC) Regulation.[55] For example, the evaluation of the implementation of the CPC Regulation documented that the procedures in place are "long and cumbersome, thus not optimal for digitalised markets" and large, multinational traders have a strong impact on the overall level of compliance of entire economic sectors." The analysis confirms the conclusion here, by adding that the "effectiveness of the CPC Regulation is hampered by differences in the capacity of national authorities to deal with CPC cases, due to limited resources, diverging interpretations of the rules

[54] "Communication 2030 Consumer Agenda COM(2025) 848 Final" (n 24). In 2026 the Commission will propose a revision of the CPC Regulation, support coordinated enforcement actions of the CPC Network and "will assess the need for centralised investigation and enforcement powers at EU level in specific cases and how to further strengthen coordination among national authorities."

[55] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345/1) (n 34).

https://doi.org/10.1017/err.2026.10146

of the Regulation and of EU consumer rules and differences in the implementation of minimum investigation and enforcement powers," which limits its deterrent effect.[56] Therefore, it has little impact to amend old or adopt new rules if their deterrent effect or sanctioning power is limited, hampered and uneven across Europe. This is why any future fairness rules should be coupled with common EU-level enforcement rules and an enforcing authority, at least for the most severe and transborder infringements.

6. Conclusion

Addressing digital manipulation and data-driven unfairness is inherently complex and interdisciplinary. The Digital Fairness Act could strengthen consumer protection not only as a matter of consumer rights but also by reinforcing data protection as a fundamental right. Yet doubts about the DFA's suitability and potential provisions remain. EU interventions are often perceived as targeting non-EU "big tech" operating in Europe, while given the Union's economic structure and competition rules, the EU has few home-grown rivals to the very firms it regulates. It is widely observed that European companies either stay small or relocate to more favourable jurisdictions in search of a more flexible business environment. Consumers may be vulnerable and manipulable, but the legislation is more manipulable due to a lack of clarity, appropriateness, fragmentation and inefficient enforcement. The DFA would need to address these challenges and make a meaningful contribution to consumer law and the internal market project.

[56] European Commission, "Report from the Commission to the European Parliament and the Council on the Application of Regulation (EU) 2017/2394 of the European Parliament and of the Council on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Law (COM(2024) 311 Final)"; VVA., Tetra Tech. and IPSOS., *Information Gathering for Assisting the European Commission in Complying with Its Obligations under Article 40 ("Reporting") of Regulation (EU) 2017/2394 on Consumer Protection Cooperation: Final Report.* (Publications Office 2024) <https://data.europa.eu/doi/10.2838/569634>.

Cite this article: L Nikiforov, "Digital Fairness Act: Mapping the Expectations". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2026.10146

https://doi.org/10.1017/err.2026.10146