The Rational Consumer Myth: EU Law and Digital Vulnerability

3 NOVEMBER 2026

Sara Frasnelli

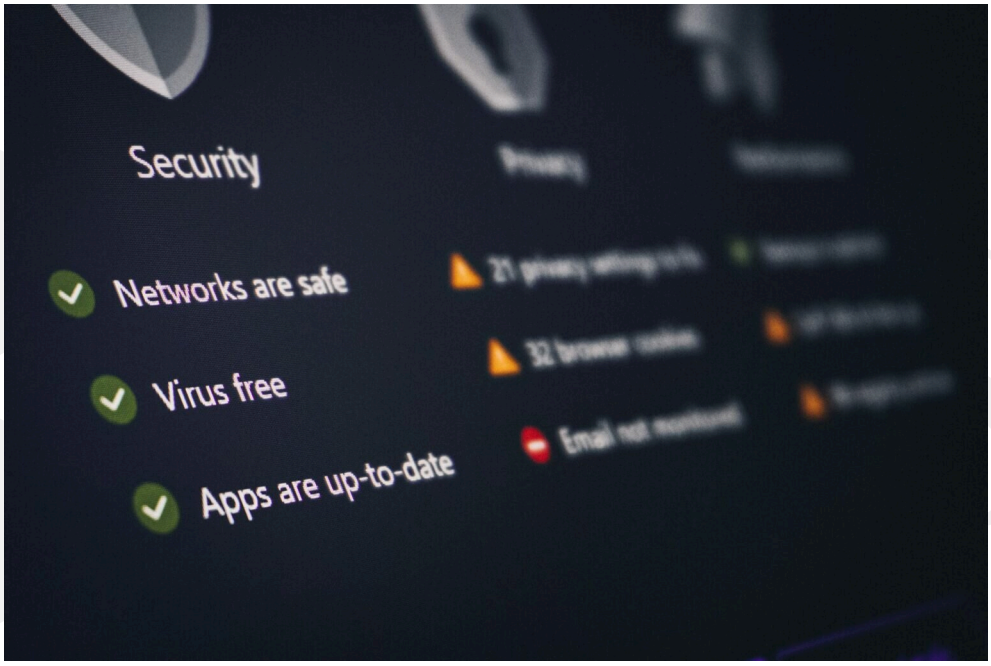


Photo by Zulfugar Karimov on Unsplash

From the Average Consumer to Digital Vulnerability

European consumer law has been built around a precise image of the subject to be protected: the average consumer, a normative benchmark referring to a person who is normally informed and reasonably circumspect, capable of making autonomous economic choices oriented towards the maximisation of their own welfare. This model, developed by the case law and incorporated into Directive 2005/29/EC on Unfair Commercial Practices (UCPD), represents a point of equilibrium between consumer protection and freedom of enterprise. Nevertheless, its capacity to ensure effective protection appears uncertain. A theoretical premise for discussing its limits is found in the critique of the full rationality of homo oeconomicus formulated by Herbert Simon in his essay "A Behavioral Model of Rational Choice" (1955): **human decision-making is conditioned by cognitive**

limits and by the characteristics of the external environment, and a greater quantity of information does not, on its own, guarantee fully rational choices. These limits are of particular significance in the contemporary digital economy.

Directive (EU) 2019/2161 updated and strengthened consumer law, including in digital markets, by also amending Directives 2005/29/EC and 2011/83/EU. Nevertheless, problems persist concerning the effectiveness of protection against the forms of conditioning exercised in the digital sphere, above all by large online platforms. The latter, indeed, do not merely offer goods and services: they design choice architectures, build algorithmic recommendation systems, track behaviour and infer psychological states, and modulate consumers' exposure to commercial stimuli on the basis of individual profiles drawn from the analysis of large quantities of data (*Resolution 2023/2043)*. An example of the adaptation of the offer to the individual user is price personalisation resulting from the automated processing of user data. The Directive does not prohibit differentiation outright, but requires that the consumer be notified when the price has been personalised. The problem lies in understanding which criteria are used, which data feed the system, and when the practice exceeds the existing instruments of protection, making a new regulatory intervention necessary. In this context, the rationality of the average consumer is not simply put to the test: it is systematically eroded.

The Fitness Check on digital fairness, published by the European Commission on 3 October 2024, estimates at no less than EUR 7.9 billion the annual financial detriment suffered by consumers in the digital environment.

The present contribution is situated precisely in this context, analysing the evolution of the concept of vulnerability in EU consumer law, the principal unfair commercial practices that exploit such vulnerability, and the prospects offered by the DFA proposal.

The Evolution and Dimensions of Digital Vulnerability

Directive 2005/29/EC adopts the benchmark of the average consumer as the reference point for assessing the unfairness of commercial practices. Pursuant to Article 5(2), "*a commercial practice shall be unfair if: (a) it is contrary to the requirements of professional diligence, and (b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers*." Moreover, paragraph 3 provides that practices likely to distort the economic behaviour of a group of vulnerable consumers, such as minors or the elderly, must be assessed from the perspective of the average member of that group. The wording evokes a vulnerability anchored to predetermined and stable characteristics of the

individual, rather than to the dynamics of the commercial environment in which they operate. Such a construction, as clarified by the Court of Justice in Orange Polska (C-628/17), proves not entirely adequate: as regards the assessment of the unfairness of a practice, "*full account should be taken of the context of the individual case concerned in applying that directive, which entails, in Article 8 thereof, an obligation to take account of all the features of the conduct of the trader in the factual context concerned*". This approach opens the way to the recognition of a situational vulnerability, induced not by the subjective characteristics of the consumer, but by the context in which the practice takes place.

A further clarification comes from the judgment in Compass Banca (C-646/22) of 14 November 2024. The Court confirms the reference to the consumer who is normally informed and reasonably observant and circumspect, but acknowledges that their decision-making capacity may be conditioned by cognitive biases. At paragraphs 53 and 57–59 it specifies that such conditioning must be taken into account where it is capable of materially distorting their behaviour, on the basis of the concrete circumstances. The mere possibility of a bias therefore does not automatically demonstrate the unfairness of the practice. The ruling confirms that it is possible to interpret the benchmark of the average consumer by taking into account the cognitive limits relevant in the decision-making context.

At the level of policy direction, a more explicit formulation emerges from European Parliament **Resolution 2023/2043** on "***Addictive design of online services and consumer protection in the EU single market***", where it is stated that "c*ertain technology companies use design and system functionalities to take advantage of users' and consumers' vulnerabilities in order to capture their attention and increase the amount of time they spend on digital platforms;...while some digital services work on data monetisation and time spent on the application in order to collect data and use it for advertising purposes, other digital services work in part or in full with subscription-based models that may or may not contain addictive design features*". Digital vulnerability is thus conceived as a potentially common condition, albeit with differing intensities and with a need for reinforced protection for certain groups.

For the purposes of this analysis, the elements that have emerged may be organised into **three dimensions of digital vulnerability**: cognitive, technological and structural. This is an interpretive framework proposed in the present contribution. The **cognitive dimension** concerns the informational asymmetry and the behavioural biases that platforms exploit: bounded rationality, information overload, FOMO, psychological vulnerabilities. The **technological dimension** concerns algorithmic opacity (an aspect addressed by the Digital Services Act through the transparency obligations on the main parameters of recommender systems in Article 27), profiling and personalisation, which enable, as recognised by the DSA, the adoption of targeting techniques that may be used to leverage individ-

ual interests and, potentially, the vulnerabilities of recipients. Finally, the **structural dimension** concerns, for example, the economic incentives of business models founded on the monetisation of data and attention.

The general clauses of Directive 2005/29/EC are technologically neutral in content and are applicable to online commercial practices. Nevertheless, the Fitness Check highlights difficulties in translating these principles into concrete guidance for digital design: "*the broadly worded legal provisions in the Directives might sometimes lack the necessary concreteness for their effective practical application to commercial practices and system architectures in the digital environment. It is difficult for traders to translate these general principles into concrete development decisions in design interfaces, software, hardware, infrastructure etc. Furthermore, general principles do not lend themselves easily to the use of technology in enforcement"*. The critical issue therefore concerns the concrete application of the UCPD to the more sophisticated dark patterns, to addictive design and to manipulative personalisation.

Existing Safeguards and Manipulative Digital Practices

An important turning point concerning consumer protection in the digital market came on 19 October 2022 with the adoption of the Digital Service Act (DSA). In particular, Article 25(1) prohibits deceptive or manipulative interfaces of online platforms, providing that "*providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions*". Paragraph 2 clarifies that this prohibition does not apply to practices covered by the UCPD or the GDPR: this provision makes coordination between the regimes central. Moreover, Article 38 requires providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs) that use recommender systems to ensure at least one option not based on profiling for each of their systems. The limits of the DSA are significant: for instance, the adoption of the risk-based approach to digital services, composed of risk assessment (Article 34) and risk mitigation (Article 35) obligations for VLOPs and VLOSEs, inevitably makes the DSA very vague.

In light of the current framework, the practices that may exploit online vulnerability can be grouped into three principal categories (*Directive 2005/29/EC*). The first category comprises **manipulative dark patterns**, including urgency patterns (deceptive countdown timers and artificial scarcity messages), confirm-shaming (guilt-inducing wording of the negative choice), the roach motel (cancellation made structurally more complex than subscription; *Regulation (EU) 2022/2065, Art. 25*) and drip pricing (late disclosure of mandatory costs, which hinders understanding of the total price). The second category concerns **behavioural design** (*Resolution*

2023/2043) that may encourage excessive or compulsive use of digital services, through features such as infinite scrolling, autoplay and notifications intended to draw the user's attention. The third category, finally, consists of **manipulative personalisation** (*Resolution 2023/2043, paragraph 8)*, which is difficult to recognise when the consumer is unaware of the criteria used to select the messages they receive.

The EDPB's Guidelines on "the targeting of social media users", in their final version of 13 April 2021, illustrate, in Example 8, the risks of targeting based on inferences relating to an individual's impulsivity and low income, with the offer of advertising for online betting: the example shows how inferred information may be used to direct commercial messages to persons exposed to specific vulnerabilities. The assessment of unfairness requires ascertaining how personalisation exploits such vulnerabilities and affects decision-making autonomy, also taking into account the protections provided in the field of personal data.

Towards a Digital Fairness Act

In this context, the DFA proposal aims to strengthen consumer protection and to improve the coherence of the existing framework. Its main purpose, as highlighted by the Commission, is to "***strengthen protection and digital fairness for consumers, while ensuring a level playing field and simplifying rules for businesses in the EU.***" For the reasoning developed here, three areas announced by the Commission are of particular importance: the countering of dark patterns, the design of digital products that induces addiction, and unfair personalisation practices. The precise content of the measures and their coordination with the UCPD, the DSA and the GDPR will have to be assessed on the basis of the forthcoming proposal.

The DFA thus aspires to build a coherent body of rules that fills the coordination gaps between the UCPD and the DSA, introducing a systematic approach to digital fairness founded not on the prohibition of individual practices, but on the regulation of the architectures of influence that platforms construct by exploiting their asymmetric knowledge of the consumer.

References:

A behavioral model of rational choice. (1955). https://www.rand.org/content/dam/rand/pubs/papers/2005/P365.pdf

EDPB Guidelines 8/2020. https://www.edpb.europa.eu/system/files/documents/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

Directive 2005/29/CE. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02005L0029-20260927

Husovec, M. (2024). The Digital Services Act's red line: what the Commission can and cannot do about disinformation. *Journal of Media Law*, *16*(1), 47–56. https://doi.org/10.1080/17577632.2024.2362483

Regulation 2022/2065. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065

Fitness Check 2024. https://commission.europa.eu/law/law-topic/consumer-protection-law/review-eu-consumer-law_en

Case C-628/17. Infocuria. https://infocuria.curia.europa.eu/tabs/document/C/2017/C-0628-17-00000000RP-01-P-01/ARRET/214885-EN-1-html

Case C-646/22. Infocuria. https://infocuria.curia.europa.eu/tabs/document/C/2022/C-0646-22-00000000RP-01-P-01/ARRET/292275-EN-1-html

What is the EU Digital Fairness Act (DFA)? Complete guide — Digital Fairness Act. Digital Fairness Act. https://digitalfairnessact.com/what-is-the-digital-fairness-act

Directive 2161/2019. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L2161

Resolution PE 2023/2043 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202404164

EPIS