Towards Digital Fairness

Hans-W. Micklitz, Natali Helberger, Betül Kas, Monika Namysłowska, Laurens Naudts, Peter Rott, Marijn Sax, Michael Veale[1]

Cite as: Hans-W. Micklitz and others, 'Towards Digital Fairness' (2024) 13 Journal of European Consumer and Market Law 24.
https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/13.2/EuCML2024004

I. Framing the Context

The EU Digital Policy Legislation, which is given form in several new legislative initiatives under the *von der Leyen* Commission,[2] is by and large based on the premise that the existing consumer law acquis suffices to cover potential risks to health and safety as well as to the economic interests of consumers. Over the past years, European institutions have worked intensively on a new EU Digital Policy Framework that must address new regulatory challenges from digitisation, changing market dynamics and the role of powerful technology providers. The Digital Services Act[3] (DSA), the Digital Markets Act[4] (DMA), the proposed Artificial Intelligence Act[5] (AIA), the proposed Data Act[6] (DA), the proposed Platform Workers Directive[7] and other ground-breaking regulations must address these challenges and create the conditions for effective oversight, public accountability and the protection and realisation of shared values and fundamental rights. In this new framework, consumers' interests are also addressed,

[1] Natali Helberger, Distinguished University Professor Law & Digital Technology, with a special focus on AI; University of Amsterdam, Netherlands; Hans-W. Micklitz, Professor of Economic Law, European University Institute, Florence, Italy; Monika Namysłowska, Professor, Faculty of Law and Administration, University of Lodz; Poland (The research was partly supported by the National Science Centre (Narodowe Centrum Nauki) in Poland under decision No. 2018/31/B/HS5/01169); Laurens Naudts, Postdoctoral Researcher at AI, Media & Democracy Lab - Institute for Information Law, University of Amsterdam, Netherlands; Affiliated Senior Researcher at KU Leuven Centre for IT & IP Law, Belgium; Peter Rott, Professor of Civil Law, Commercial Law and Information Law, Carl von Ossietzky University of Oldenburg, Germany; Marijn Sax, assistant professor at the Institute for Information Law with a background in Political Science, Philosophy, and Law, Netherlands; Michael Veale, Associate professor in law, University College London, United Kingdom.

[2] Overview <https://www.bruegel.org/sites/default/files/2023-11/Bruegel_factsheet.pdf> (accessed 16 January 2024).

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

[4] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

[5] Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), COM(2021) 206 final.

[6] Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final.

[7] Proposal for a Directive of the European Parliament and the Council on improving working conditions in platform work, COM(2021) 762 final.

albeit in a somewhat erratic and little systematic way. The underlying premise of the new EU Digital Policy Framework seems to be that the existing consumer law *acquis* (including, for example, the Unfair Commercial Practice Directive[8] (UCPD), the Consumer Rights Directive[9] and the Unfair Consumer Terms Directive[10]) is by and large still sufficient to protect the legitimate interests of consumers in the digital market space.

The EU Consumer Protection 2.0 study, commissioned by *Bureau européen des unions de consommateurs (BEUC)*,[11] provided a first comprehensive account of the potential deficit and proposed a possible remedy to rethink the existing consumer acquis in light of 'structural, architectural and universal vulnerability', to be translated into the legal concept of 'digital asymmetry'.

In reaction to the widely voiced critique of potential consumer protection deficits in the EU Digital Policy Legislation, the European Commission launched the '*Digital Fairness – Fitness Check*' in May 2022.[12] This fitness check '*will look at the following pieces of EU consumer protection legislation to determine whether they ensure a high level of protection in the digital environment: the Unfair Commercial Practices Directive 2005/29/EC, the Consumer Rights Directive 2011/83/EU, the Unfair Contract Terms Directive 93/13/EEC.*' It has to be applauded that the European Commission is ready to take up the challenge and to initiate a debate on 'digital fairness'. However, limiting digital fairness to three pieces of EU legislation is too narrow, which threatens to constrain and limit the discussion and, in turn, the protection EU law could and should afford. The EU Digital Policy Legislation cuts across the consumer law *acquis* as a whole and would require, in theory, to evaluate every piece of the consumer law acquis. The question to be studied is whether the European consumer law, which dates back to the famous *Kennedy* Declaration of 1962 and was developed under a political agenda and a different industrial economy, can handle the risks and problems consumers might face in the exponentially developing digital economy, which reaches beyond the linear thinking of humankind.

BEUC understood the EU initiative as a mandate to initiate a debate on what digital fairness should comprise. The DSA and the then AIA-Proposal served as a common background for existing and upcoming consumer problems. At the time of writing, the trilogue on the AIA was in full swing. We start from the premise that the finally adopted version will not change the baseline of our arguments. The authors, together with

---

[8] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market ('Unfair Commercial Practices Directive') [2005] OJ L149/22.

[9] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [2011] OJ L304/64.

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.

[11] N Helberger, O Lynskey, H-W Micklitz, P Rott, M Sax and J Strycharz, *EU Consumer Protection 2.0: Structural symmetries in digital consumer markets*, March 2021, <https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf> (accessed 16 January 2024); partly condensed into N Helberger, M Sax, J Strycharz and H-W Micklitz, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) 45 JCP 175

[12] <https://ec.europa.eu/.info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> (accessed 16 January 2024).

Kasper Drazewski and *Ursula Pachl* from *BEUC*, decided jointly to focus on six building blocks of relevance to consumers:

1. Digital Vulnerability and Manipulation in the Emerging Digital Framework, by *Natali Helberger and Marijn Sax*;
2. Toward Constructive Optimisation: Aligning the Recommender Stack under European Law, by *Laurens Naudts*, *Natali Helberger*, *Marijn Sax and Michael Veale*;
3. Dissolution of EU Consumer Law through Fragmentation and Privatisation, by *Hans-W. Micklitz*;
4. Ensuring Digital Fairness in EU Consumer Law through Fundamental Rights: is the EU Charter Fit for Purpose, by *Betül Kas*;
5. Future-Proofing the Unfairness Test, by *Monika Namysłowska*;
6. Burden of Proof, by *Peter Rott*.

The six building blocks reveal tendencies, which demonstrate that there is indeed a kind of rupture[13] taking place in the digital economy, which shatters established wisdom in the design and understanding of consumer law. The full text of the analysis is available via the *BEUC* website.[14]

The *first* tendency is the vanishing line between the consumer and the citizen.

The *second* is the privatisation of consumer law through the space given to the AI industry to develop a design whose complexity can only be revealed by breaking up the different stacks behind the design. This space is framed by a broad set of due diligence obligations, broadly worded in the EU digital policy legislation and concretised through EU-driven private regulation.

The *third* is the lack of a value-based guidance despite all the rhetoric on '*human-centric, secure, ethical and trustworthy AI*'.[15] The EU Digital Policy Legislation claims to fill the gap through extensive reference to the EU Charter on Fundamental Rights.[16] However, it turns out that fundamental rights serve as a generic, catch-all placeholder of limited use under the existing state of the case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). The fairness test enshrined in Art 5 UCPD, on the other hand, lacks the necessary concreteness of legal requirements, which could deal with digital vulnerability or the stacks behind the recommender system.

The *fourth* is the total neglect of the knowledge gap between the consumer/citizen and the provider of an AI system on the digital architecture, which renders the prosecution of consumer rights under the existing *acquis* difficult, if not impossible. The classical

---

[13] C. Twigg-Flesner, 'Disruptive Technology - Disrupted Law? How the digital revolution affects (Contract) law' in A De Franceschi (ed), *European Contract Law and the Digital Single Market* (Intersentia, 2016), Available at SSRN: <https://ssrn.com/abstract=3039952> (accessed 16 January 2024).

[14] The report will be published on the website of BEUC in due course. It will contain the full text of the six parts, listed above.

[15] For a deeper analysis H.-W. Micklitz, The Role of Technical Standards in Future EU Digital Policy Legislation, 2023, pp. 98-153, with particular emphasis on the Digital Services Act, the Artificial Intelligence Act and Cyber Resilience Act
https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf

[16] [2012] OJ C326/391.

distribution of the burden of proof between the consumer and the trader, relied on in the industrial economy, except product liability and anti-discrimination, has to be questioned in the digital economy.

The authors propose discussing the findings' possible implications to develop a 'Digital Fairness Act'. While the authors assert to address at least the most critical policy fields and consumer problems, they do not contend to exhaust the strive for 'digital fairness'. This is true not only for the substance, which would mean analysing all the EU consumer directives and regulations one by one and evaluating their suitability, in light of all the different regulations which come under the EU Digital Policy Framework, but in particular for the enforcement of the consumer acquis in the digital economy. Enforcement is the elephant in the room. There is evidence that the current enforcement structure, set up by General Data Protection Regulation[17] (GDPR), the DMA and the DSA and transplanted into the pending EU proposals, especially the AIA, is hardly apt to cope with burning political problems, such as the protection of children against all sorts of problematic practices offered by the online platforms.[18]

The following proposals demonstrate that the limits that govern the *Digital Fairness - Fitness Check* must be overcome. They reach beyond the UCPD, which is at the centre of attention, including suggestions to revise the existing consumer law acquis and the EU Digital Policy Framework. The European Commission promised to publish a report on *Digital Fairness* in the second quarter of 2024, until the end of June 2024. This report might, in a certain way, determine the political debate that will continue after the European Parliament's elections and the European Commission's re-establishment. The proposals should be understood as the first building block in an ongoing process to find appropriate answers not only for consumer protection but also for society at large.

II. Proposals

1. A Right to Constructive Optimisation

Recitals

(1) In various public and private domains, recommender systems are increasingly relied upon to structure people's access to various social and economic affordances, including but not limited to, advertisements and commercial product offerings, audio-visual entertainment, news media, personal connections, and professional opportunities. For citizens and consumers, recommender systems perform an active, yet often invisible, mediating role in their navigation of the digital society.

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[18] M Cantero Gamito and H-W Micklitz, *Too much or too little? Assessing the Consumer Protection Cooperation (CPC) Network in the protection of consumers and children on TikTok* (BEUC, 2023) <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf> (accessed 16 January 2024).

(2) Having become an integral part of the infrastructure of the digital public and private sphere, recommender systems hold an important societal dimension. The uptake of recommender systems in the internal market should therefore be accompanied by a high level of protection of public interests and fundamental rights.

(3) People have a legitimate right for recommender systems to be designed, operated, and evaluated in a way that is reflective of and accommodates, rather than interferes with, their true considered interests, including democratic and societal values, fundamental rights, and freedoms. In this context, it is necessary to build a robust and consistent regulatory framework that aligns the development and deployment of recommender systems toward an active protection and realisation of these interests.

(4) More specifically, recommender systems should be designed, operated, and evaluated to promote, rather than undermine, people's ability to live a fuller life and become (better) democratic subjects. Recommender systems should enable people to understand, develop, and explore their (different) preferences, commitments, and (life) projects, to engage and communicate with others, in settings where their experiences, views, and opinions are heard and recognised, rather than rendered unheard and invisible. Moreover, to enable people to have and maintain an active and autonomous say over the conditions that govern their lives in an information society, they should also be allowed to contest, as well as exercise agency and control over the goals pursued by, and reflected in recommender systems.[19]

(5) Recommenders are not a single piece of software but a collection of layers of different technical and organisational components, which together form a stack. Such layers include the Business-to-Consumer Interface (Software and Hardware); the Functionality level, which includes the tasks that computing systems are designed to achieve; the Engine level designed to fulfil optimisation logic, drawing on the personal and data input layers; the Business-to-Business Interface; the Connectivity Infrastructure; Operations and Management as the organisational layer in the company; and the Organisational Interface with accountability groups, advertisers, individual users, and communities. When regulating recommender systems, it is important to always consider how every layer of the stack, and the operators associated with those layers, inform and contribute to the design, operation, and evaluation of the recommender system.

(6) The realisation of constructive optimisation in recommender settings mandates accountability across the stack. Stack operators should be able to justify and defend the normative choices they have made and demonstrate the measures they took to ensure the protection and realisation of the true considered interests of people and society. Stack operators should also offer end-users, civil society groups, regulators, and others the ability to participate in the processes through which those choices are made. They should make publicly available documentation that enables others to scrutinise and contest the choices made across the recommender stack.

---

[19] Recital 4 is modelled to reflect (and protect) the values of self-development and self-determination as introduced and defined by Young in I M Young, *Justice and the Politics of Difference* (Princeton, New Jersey: Princeton University Press, 1990); id, *Inclusion and Democracy* (Oxford University Press, 2002), <https://doi.org/10.1093/0198297556.001.0001> (accessed 16 January 2024).

(7) Transparency requirements should thus be combined with substantive, mandatory, and enforceable accountability mechanisms.

(8) Accountability mechanisms cannot constitute a one-off inspection and evaluation of (layers of) the stack. Instead, in their responsibility to maintain accountability, stack operators should duly consider the dynamicity of the recommender ecosystem. Because recommender systems are typically designed, operated, and evaluated in a continuous iterative process, at different levels of and across levels of the stack, any fulfilment of accountability must be based on a philosophy of periodic monitoring and tracking. This is the only way to ensure that the consequences and impact of iterative design, operation, and evaluation processes can be anticipated and any harm to the true considered interests of people and society avoided.

(9) For recommender systems to be able to perform their societally important function in a manner that respects and promotes the flourishing and autonomy of *all* citizens, the responsible recommender system stack operators should ensure the presence of meaningful opportunities for the consultation and participation of (possibly affected) historically disadvantaged and marginalised individuals and groups. Without the active involvement of these groups, the responsible recommender system stack operators cannot properly anticipate and cater to the needs of the entire population using their services.

(10) The right to constructive optimisation informs what the requirements of professional diligence are when recommender systems are used in a (commercial) digital context, such as a social media or e-commerce platform. Designing, operating, and evaluating a recommender system in a manner that solely aims to optimise for metrics that serve the interests of the developer or deployer of the recommender system is not in conformity with professional duties. If doing so also materially distorts the economic behaviour of a consumer, or impedes upon the fundamental interests of individuals, social groups, or society at large, this constitutes a prohibited unfair commercial practice.

Recommendations

> **Art 1 – A right to constructive optimisation**
>
> 1. The design, operation, and evaluation of the recommender stack must be organised in a way that takes into account the legitimate interests of users - including marginalised and/or individuals rendered vulnerable - and social groups, in the protection and realisation of their fundamental rights, including the right to privacy, autonomy, equality and non-discrimination, and freedom of expression.
>
> 2. The burden of proof that this obligation has been complied with is on the economic developer and professional deployer as defined in the AIA. The scope and reach of the burden of proof follows Article 12 UCPD (see below under II. 4).
>
> 3. Responsible recommender stack operators must document and make public information on choices made during the ideation, design, and

development process to enable third parties, including affected end-users, civil society organisations, and the regulator, to assess whether a system is sufficiently aligned with democratic and societal values.

Explanation: This right is modelled after Art 3 of the proposed European Media Freedom Act,[20] which is less of an enforceable right and more of a legitimate expectation. The value of this legitimate expectation could be that it informs the interpretation of professional duties and concrete legal requirements, such as Articles 27 and 34 DSA (see below). This way, the right to constructive optimisation could be realised within existing rules – rather than proposing the (at this point) unrealistic amendment of the DSA. It could potentially also inform the interpretation of professional diligence obligations in Art 5 (2)(a) Unfair Commercial Practices Directive.

Concrete recommendations

The right to constructive optimisation along the optimisation stack influences the interpretation of existing norms, in particular:

1) **Article 27 DSA**

"Recommender system transparency

b. Providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters."

Interpretative guidance

"Main parameters used in their recommender systems" should be interpreted in the sense of the main economic and/or societal goals that the recommender system has been optimised for, and how, in doing so, the legitimate interests of users have been taken into account in the training and development of the model, the training and expertise of the staff involved in the development, as well as the initiatives from management to steer towards such constructive optimisation.

2) **Art 34 DSA**

"Providers of very large online platforms and very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.

[20] European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act), COM(2022) 457 final.

They shall carry out the risk assessments by the date of application referred to in Article 33(6), second subparagraph, and at least once every year thereafter, and in any event before deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks: ...

(b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non- discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high level of consumer protection enshrined in Article 38 of the Charter."

Interpretative guidance

When conducting risk assessments in the sense of Art 34(1) and (2) DSA and the obligation to undertake risk mitigation measures in Art 35 DSA, taking into account 'the design of their recommender systems and any other relevant algorithmic system' must be understood broadly. It should pertain not only to the concrete development and training of the model but also the levels of Operations and Management, and the way the legitimate interests of users have been operationalised and taken into account in the management decisions that preceded and govern recommender design. The company must be able to explicate how different groups of relevant stakeholders (internal and external), individuals, and communities have been actively heard and involved in the process. A failure to be able to do so creates a presumption of a systemic risk/is a strong indicator of a systemic risk in the sense of Art 34(1)(b).

Similarly, the failure to offer users a choice in the sense of Art 27 (3) DSA is a strong indicator of a systemic risk. In line with the proposed interpretation of Art 27, 34, and 35 of the DSA (see above).

Finally, such a right to constructive optimisation can also inform the interpretation of Art 5(2)(a) UCPD.

3) Art 5(2)(a) Unfair Commercial Practice Directive

"1. Unfair commercial practices shall be prohibited.

2. A commercial practice shall be unfair if:

(a) if it is contrary to the requirements of professional diligence,

(b) it materially distorts or is likely to materially distort the behaviour about 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."

Interpretative guidance

The right to constructive optimisation informs what the requirements of professional diligence are when recommender systems are used in a (commercial) digital context, such as a social media or e-commerce platform. Designing, operating, and evaluating a recommender system in a manner that solely aims to optimise for metrics that serve the interests of the developer or deployer of the recommender system is not in conformity with professional duties. If doing so also materially distorts the economic behaviour of a consumer, or impedes upon the fundamental interests of individuals, social groups, or society at large, this constitutes a prohibited unfair commercial practice.

2. Future-Proofing the Unfairness Test

Recitals

(1) The rapid advancement of digital technologies has transformed the consumer landscape. The commercial practices of traders towards consumers have adapted to the digital era. Their distinctive characteristics justify their classification as unfair digital commercial practices. Directive 2005/29/EC includes provisions designed to protect consumers, applicable to new unfair business-to-consumer (B2C) commercial practices. However, the existing regulations do not sufficiently account for the unique characteristics, scale, and resulting consumer harm associated with new forms of commercial practices. Recognising the inadequacy of the current legal framework in effectively safeguarding consumer interests, there is a necessity for adapting consumer protection measures to address emerging challenges and mitigate the harm caused to consumers by unfair digital commercial practices.

(2) The amendments, therefore, approximate the laws of the Member States on unfair digital commercial practices. The new, common general prohibition covers unfair digital commercial practices, which are contrary to the requirements of digital professional diligence and/or the law, and materially distort consumers' autonomous decision-making in such a way that it causes or is likely to cause harm. In line with the principle of proportionality, the amendments protect consumers from the consequences of such unfair digital commercial practices where they are material but recognise that, in some cases, the impact on consumers may be negligible. The amendments enact a paradigm shift in consumer protection based on innovative concepts tailored to address prevailing phenomena in the digital environment.

(3) The current definition of commercial practices does not allow the classification of all traders' activities within the digital sphere, such as addictive designs. Therefore, it is appropriate to adjust the definition to the digital environment. The new definition

of digital commercial practices incorporates some elements from the current definition of commercial practices in Article 2(d) of Directive 2005/29/EC. To tailor the definition to the digital environment, new forms of digital commercial practices are added, such as design choices and architectural features. Additionally, the product does not have to be provided for remuneration, and the practices do not have to be directly connected with the promotion, sale, or supply of a product to consumers.

(4) Since the digital environment creates new professional duties and obligations, it is necessary to introduce a new standard of digital professional diligence. The definition of digital professional diligence means not exploiting digital asymmetry and/or digital vulnerability by a trader towards consumers, which are fundamental characteristics of digital B2C relationships. 'Not exploiting digital asymmetry and/or digital vulnerability' echoes the same traditional values as 'being contrary to honest market practices and/or good faith' in the definition of professional diligence in Article 2(h) of Directive 2005/29/EC. The new definition weaves traditional values with contemporary challenges, establishing a solid foundation for safeguarding digital fairness.

(5) Digital asymmetry conveys the inherent power imbalances between traders and consumers in the knowledge and understanding of the functioning of a digital commercial practice (informational asymmetry), imbalance in the commercial relationship that a digital environment creates and maintains (relational asymmetry), structural differences in power to influence the process of autonomous decision making of the other party as a result of the control over data and/or a digital choice environment (structural asymmetry).

(6) Digital vulnerability refers to a universal state of susceptibility to the exploitation of differences in power in the trader-consumer relationship that result from internal and/or external factors beyond the consumer's control. 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.

(7) The amendments address commercial practices which distort consumer's autonomous decision-making. The concept of autonomy of consumer choice is central to EU consumer law. Therefore, adopting this concept in the new general clause confirms its importance for achieving a high level of consumer protection. The provision includes an additional criterion related to the necessity of causing harm which implies a causal link between the distortion of behaviour or autonomous decision-making and the resulting harm. This requirement ensures taking full account of the distinctive nature of consumer harm within the digital environment. The current lens of the distortion of economic behaviour is too narrow to achieve a high level of consumer protection in the digital environment.

(8) To close regulatory gaps resulting from the fragmentation of protection measures in the new digital law, the lack of legislation, or inadequate legislation, it is desirable to incorporate the concept of a 'breach of law' into the general clause. The use of 'and/or' implies that a digital commercial practice can breach either the digital professional diligence standard, the legal provisions, or both. This underscores that the legal framework embodies the shared standard of digital professional diligence.

Recommendations

Article 5a UCPD

1. Unfair digital commercial practices shall be prohibited.
2. A digital commercial practice shall be unfair if it
    a) is contrary to the requirements of digital professional diligence and/or the law, and
    b) it materially distorts or is likely to materially distort a consumer's autonomous decision-making in such a way that it causes or is likely to cause harm.

Article 2 UCPD (definitions)

'Digital commercial practices' means any act, omission, design choice, architectural feature or change, course of conduct or representation, commercial communication including advertising and marketing, by a trader, relating to a digital environment directly or indirectly connected with the promotion, sale or supply of a product to consumers, whether or not that product is provided for remuneration.

'Digital professional diligence' means not exploiting digital asymmetry and/or digital vulnerability by a trader towards consumers.

'Digital vulnerability' refers to a universal state of susceptibility to the exploitation of differences in power in the trader-consumer relationship that result from internal and/or external factors beyond the consumer's control.

'Digital asymmetry' refers to a situation of imbalance between traders and consumers in the knowledge and understanding of the functioning of a digital commercial practice (informational asymmetry), imbalance in the commercial relationship that a digital environment creates and maintains (relational asymmetry), structural differences in power to influence the process of autonomous decision making of the other party as a result of the control over data and/or a digital choice environment (structural asymmetry).

Explanation

The above proposals are based on the assumption of the need to adjust the UCPD to the digital environment and shield consumers from digital unfairness.

The proposed amendments require a new set of definitions:

- 'digital commercial practices' – the current definition of commercial practice is extensive but not endless. The classification of numerous traders' activities remains unclear within the digital sphere;
- 'digital professional diligence' – the digital environment creates new professional duties and obligations – digital professional diligence, which means not exploiting digital asymmetry and/or digital vulnerability by a trader towards consumers. The reference to these notions emphasises the paradigm shift required in the digital environment;
- 'digital asymmetry' and 'digital vulnerability', which are the fundamental characteristics of digital B2C relationships, were explored in the '*EU Consumer Protection 2.0*' study. These terms immediately convey the inherent power imbalances and potential areas of exploitation in digital B2C relations.

The basic idea is to introduce new Art 5a UCPD, analogous to Art 5 UCPD, which is composed of two paragraphs: a general prohibition of unfair digital commercial practices and a new general clause. The general clause addresses various consumer harms caused by unfair digital commercial practices. The current lens of the distortion of economic behaviour is too narrow and is replaced with the distortion of autonomous decision-making. Moreover, the concept of a breach of law is introduced into the general clause to strengthen its role as a horizontal safety net in the digital environment.

3. Redress of the Trader

Recital

Traders may use data for the building of advertising they have bought on the market where they cannot use any control over the data and/or the technical and organisation infrastructure behind their collection and processing. This is particularly true for small and medium-sized companies that do not have the resources to collect and process the data themselves. These traders liable under the UCPD should be granted a right of redress against the company from which they bought the data. The right of redress presupposes that a trader acted in good faith and does not know or could not have known of the unlawfulness of the data. As traders, who are acting in good faith, find themselves in comparable difficulties in providing evidence of the unlawful character of the data bought, they shall benefit from the regulation of the burden proof in Art 12 UCPD.

Recommendations

Proposal for a new provision amending the UCPD

(1) Where the trader is liable for an infringement of his obligations or for anyone acting in his name or on his behalf, and where the infringement results from unlawful data or the infrastructure behind the collection and processing of data over which neither he nor anyone acting on his behalf has control, the trader shall be entitled to pursue remedies against the person or persons liable for the supply of the data, provided he did not know or could not have known the unlawfulness of the data. The person against whom the trader may pursue remedies, and the relevant actions and conditions of exercise, shall be determined by national law.

(2) The rules on the burden of proof in Article 12 UCPD apply to the benefit of the trader, who does not know or should not have known of the unlawfulness of the data.

Explanation

The UCPD does not deal with the problem that the misleading effects of a commercial practice may result from the use of data and/or the use of the technical infrastructure behind the data, that the trader has bought and over which he has no control. This is true for the bulk of small and medium enterprise (SME) providers, who can afford the collection and processing of the data needed to build an advertising campaign. The proposed ruling is borrowed from Art 20 Directive 2019/770/EU.

There is one difficulty, which has to be taken into consideration. Whilst the SME might not have control over the data and the infrastructure behind the collection and processing of the data, it might have due diligence obligations to check the data. It seems appropriate to tie the due diligence obligations to knowledge. There must be a corresponding obligation on the side of the developer to provide the necessary information and where needed, assistance.

4. Burden of Proof

Recital

The burden of proof has been identified as a major obstacle in the fight against digital unfairness. Unfair commercial practices may be hidden in the architecture of a website. Therefore, effective remedies against unfair commercial practices require alleviation of the burden of proof where there is an indication of an unfair commercial practice. Thus, it should be on the trader to provide a meaningful explanation for a phenomenon that indicates an unfair commercial practice and to disclose relevant evidence. If the trader fails to do so, the practice shall be considered unfair and harm suffered by the consumer shall be presumed to have been caused by that practice if the harm is consistent with the practice.

Recommendations

Art 12 UCPD: Burden of Proof

(1) Member States shall ensure that in proceedings for the cessation of an unfair commercial practice or for claiming compensation for damage caused by an unfair commercial practice, at the request of a claimant who has presented facts and evidence sufficient to support the plausibility of an unfair commercial practice, national courts shall order the defendant to provide a meaningful explanation of the commercial practice and, where necessary, to disclose relevant evidence, subject to the conditions set out in this Article.

(2) The unfairness of a commercial practice shall be presumed if the trader has failed to comply with an obligation to provide a meaningful explanation or to disclose relevant evidence pursuant to paragraph 1.

(3) For the purposes of Article 11a, the causal link between an unfair commercial practice and harm suffered by a consumer shall be presumed,

where the harm is of a kind that is typically consistent with the unfair commercial practice.

(4) Member States shall ensure that, where a defendant is ordered to disclose meaningful information that is a trade secret or an alleged trade secret, national courts take the measures necessary to preserve the confidentiality of that information when it is used or referred to in the course of the legal proceedings.

Explanation

Art 12 UCPD is largely borrowed from the proposed Product Liability Directive[21] but has been adapted to the situation of digital asymmetry.

As the related recital indicates, the threshold of plausibility in the terms of Art 12(1) UCPD should not be high. The notion of meaningful explanation is borrowed from Arts 13(2)(f) and 14(2)(g) GDPR. Ordering the defendant to provide a meaningful explanation should not be at the discretion of the court but there should be legal certainty for the claimant consumer, consumer organisation, or public authority, that the trader has to provide a meaningful explanation. In line with the interpretation that is commonly given to these provisions, in the context of the Unfair Commercial Practices Directive the trader would not necessarily have to lay open the algorithm as such but explain (in plain and intelligible language) how the algorithm functions and why it has produced the observed phenomenon.

The upcoming rules in the Artificial Intelligence Act on 'technical documentation' to be specified by a delegated act should be taken into account, to highlight what is meant by meaningful.[22] There is a need in particular for local AI providers – rather than for large tech companies – to get to know common standards or common principles on what might be understood by meaningful explanation. If doubts remain, the court should have the power to order disclosure of evidence and evidence should not be limited to evidence at the trader's disposal. Thus, if the trader uses infrastructure that is provided by a third party, he must ensure that he can explain its function and provide related evidence, or that the third party does so on his behalf.

Art 12(2) UCPD is borrowed from the proposed Product Liability Directive and adapted to unfair commercial practices law.

Art 12(3) UCPD contains a rebuttable presumption that a consumer has acted in a particular manner because of the unfair commercial practice in question if that action is consistent with the unfair commercial practice.

Art 12(4) UCPD takes the protection of trade secrets into account – not as a defence that would allow the trader to reject an explanation without being sanctioned, but procedurally in terms of disclosure only in a protected manner. This is also in line with Art 64 (2) of the forthcoming Artificial Intelligence Act which foresees disclosure of the source code not to the public at large but only to public enforcement authorities.

[21] Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.
[22] Art 11 AIA in combination with Annex IV.