The Consumer Voice in Europe

EU CONSUMER PROTECTION 2.0

Protecting fairness and consumer choice in a digital economy

Contact: Kasper Drazewski – consumerrights@beuc.eu

BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2022-015 – 10/02/2022

Contents

Why it matters to consumers

The imbalance of power between consumers and data-powered traders who control digital environments creates a foundation for unfair practices – and the consumer can do very little to prevent it. Detailed insights and inferences about personal histories, convictions, biases and weakness of consumers are used in real time to maximise profit – be it from sale of products or simply from keeping the consumer clicking through and directing to specific content. When consumer choice suffers, damage happens to markets and societies alike. In the coming years, with the proliferation of AI systems and biometric technologies, the position of the consumer can only be expected to become ever weaker in the face of automated systems perfected for making money on human weaknesses and vulnerabilities. Consumer law as the horizontal framework protecting consumer agency is currently not fit for purpose to address many of these challenges and therefore must be urgently updated and upgraded.

Introduction[1]

(1) One of the most severe challenges for modern-day consumers is protecting their own choice in a data-driven environment. Throughout their online experience, consumers encounter personalisation of the environments they navigate that is near-inescapable.[2] Information on products and services is tailored to maximise conversion, anonymous shopping is becoming a thing of the past and the offered selection of news gets tailored to induce the strongest emotional responses. An unfiltered and objective view of the market (and of the world at large) becomes a rare commodity – with a long-term devastating effect on trust in markets and democratic societies in general.

(2) From the nature of the relationship consumers have with digital services, through the profound (and growing) power imbalance in the markets between data-empowered traders and consumers, here dubbed digital asymmetry, to the ease with which behavioural insights combined with biometric information in real-life commercial environments may further disempower consumers and affect freedom of choice.

[1] This paper is a product of BEUC's *EU Consumer Protection 2.0* project. The project was launched in late 2019 as a research and advocacy effort to address the issues that plague the digital consumers of today and undermine the digital society as a whole, with particular focus on behavioural manipulation, exploitation of vulnerabilities both pre-existing and engineered in real time, omnipresent personalisation affecting freedom of choice, as well as the rise of digital platforms which have become an essential element in the modern society, yet without any responsibilities that would reflect this position. For the research published under the project, see Micklitz, Helberger et al., (2021) EU Consumer Protection 2.0: Structural asymmetries in consumer markets, https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf and Micklitz, Helberger et al. (2021) The Regulatory Gap: Consumer Protection in the Digital Economy, https://www.beuc.eu/publications/beuc-x-2021-116_the_regulatory_gap-consumer_protection_in_the_digital_economy.pdf.

[2] On personalisation, individualisation and the false promises in the language layer, see Lynskey O, Micklitz HW, Rott P, Personalised Pricing and Personalised Commercial Practices (in) Micklitz, Helberger et al. (2021) EU Consumer Protection 2.0: Structural asymmetries in consumer markets. https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf, p. 94.

(3) This paper seeks to demonstrate that EU consumer law, despite being one of the most developed areas of EU law, it is not yet up to the challenge to effectively protect consumers in a digitalised economy – despite the principle of ensuring a high level of consumer protection of Article 12 of the TFEU. With the revision of the guidance document to the Unfair Commercial Practices Directive (UCPD), the European Commission has begun to explore how the UCPD can be interpreted to ensure a stronger protection of consumer agency and choice in the digital economy. However, further-reaching actions are needed. This paper, based on the research carried out by BEUC in the past years, seeks to provide concrete recommendations about how to update and upgrade EU consumer law.

(4) Matters of law enforcement are deserving of special attention. While European consumer law increasingly enables integrated enforcement solutions,[3] it is still suffering from inefficiencies which prevent it from fully harnessing the potential of a complimentary relationship between public and private enforcement. This issue will be tackled in a separate paper forthcoming from BEUC in early 2022.

1. What is digital asymmetry and why is it a problem?

1.1. In a digitalised environment, the consumer must be better protected

(5) **Digital asymmetry** is a term to describe how modern data-driven services put consumers at an unprecedented disadvantage. As they go online, they are faced with environments where traders control both the information that is presented and the entire choice architecture. Nearly every service they encounter in the digital environment benefits from insights formed by detailed knowledge of their life, choices, online searches, correspondence, personal biases and weaknesses. Even if consumers realise their online experience is personalised, they may never know the extent or mechanics of this personalisation, or the distortion it introduces into their view of the market or the world at large, and the choices they make as a result.

(6) Access to detailed insights about every consumer further sways the balance in favour of the trader who controls the digital choice environment and is capable of adapting it in real time to increase monetisation of each user. Benefiting from knowledge of individual pressure points and ongoing monitoring of behaviour, the algorithmic choice architecture is continuously optimised in real time to maximise conversion rates, while consumer choice becomes ever more illusory.

(7) The short history of the Internet provides strong examples of data-based personalisation leading to algorithmic exclusion of some consumers from seeing certain attractive offers. Knowing individual pressure points and real-time fluctuation of emotional states[4] renders it just as easy to manipulate consumers into making purchase decisions as it is to deny them access to certain products or services when they do not meet the desired race or gender profile. [5]

(8) In systems producing revenue from user attention and engagement, often reinforced by behavioural inferences, personalisation may take the form of offering clickbait content that the profiled individual is most likely to respond to, with

[3] This is evidenced in the insertion of Article 11a on proportionate and effective remedies through civil law courts into Directive 2005/29/EC by Directive (EU) 2019/2161 (the 'Omnibus Directive').
[4] Google (2016) The basics of micro-moments https://www.thinkwithgoogle.com/consumer-insights/consumer-journey/micro-moments-understand-new-consumer-behavior/
[5] Facebook has prevented consumers of an undesirable racial extraction from seeing certain housing ads. https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html. see also Julia Carpenter, Google's algorithm shows prestigious job ads to men, but not to women, The Independent 07 July 2015, https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-s-algorithm-shows-prestigious-job-ads-men-not-women-10372166.html

negative emotions like fear or anger being the most useful commercially and the easiest to invoke.[6] Evidence shows that sophisticated traders are aware about such psychological biases that can get exploited by ranking algorithms but typically choose to monetise them instead of counteracting them, with devastating effects on individuals and societies.[7]

(9) The consumer has very little choice on whether to enter this arrangement and rarely is informed about its nature and extent. No disclosure is currently mandated on the extent to which the offered view of the market (and the world at large) is filtered through algorithmic goggles.[8] But **even a detailed disclosure would not help** due to the complexity of the underlying system. Where the consumer is prompted to agree to the terms and conditions or a privacy policy, they are typically feigning an informed decision on the basis of a policy disclosure that is impossible to read. Otherwise, the only real option is to go to a different provider – if only there were anywhere to go. Studies show consumers – bombarded with meaningless disclosures and nagging consent requests - feel powerless about the practices of the online ecosystem and do not feel like they have a realistic alternative.[9]

(10) To summarise, digital asymmetry has three dimensions:

- **architectural / structural**, rooted in control of the choice architecture of the service and access to data (and the related difficulty of verifying compliant use of data in the supply chain)[10];
- **relational**, since the bargaining power of the consumer is low – they may either accept or leave, with very limited alternatives;
- **knowledge-based**, as the trader benefits from detailed insights about the consumer while the consumer often knows (or understands) very little of how the trader and the service operate.

(11) Digital asymmetry is not an unfair practice in itself. It is, however, a permanent characteristic of an environment that is highly favourable to distortion of consumer choice, reflected in actual purchases or simply in interacting with services.

(12) **These interactions are often extended in time and do not always allow for the pinpointing of single 'transaction' moments in such a relationship between a consumer and e.g., an online platform. Accordingly, this characteristic makes it difficult to establish a momentary 'direct interference' with the decision-making process of the consumer**.

---

[6] Hill K (2014) Facebook Manipulated 689,003 Users' Emotions For Science, Forbes.com https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/?sh=390b7938197c; Dorison et al. (2020) Sadness, but not all negative emotions, heightens addictive substance use, Proceedings of the National Academy of Sciences Jan 2020, 117 (2) 943-949; DOI: 10.1073/pnas.1909888116 https://www.pnas.org/content/117/2/943; see also Lanier J (2019) Ten Arguments for Deleting Your Social Media Accounts Right Now. Random House UK.

[7] Pelley S (2021) Whistleblower: Facebook is misleading the public on progress against hate speech, violence, misinformation https://www.cbsnews.com/news/facebook-whistleblower-frances-haugen-misinformation-public-60-minutes-2021-10-03/ Dwoskin E (2021) Misinformation on Facebook got six times more clicks than factual news during the 2020 election, study says, https://www.washingtonpost.com/technology/2021/09/03/facebook-misinformation-nyu-study/; Wells, Horwitz, Seetharaman (2021) Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show, The Wall Street Journal 2021 https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 .

[8] From May 2022, algorithmic personalised pricing will be subject to mandatory disclosure. However, evidence exists it will be of little help due to consumer resignation and disengagement. See section 1.4.

[9] Consumer attitudes are discussed in section 1.4 below.

[10] Which (2018) Control, Alt or Delete? The future of consumer data (report), available via https://www.which.co.uk/policy/digital/2659/control-alt-or-delete-the-future-of-consumer-data-main-report p. 42.

(13) Digital asymmetry cannot be overcome by simply providing the consumer with even more information. Consumers are already overburdened by the volume of often useless information - because not clear and intelligible - they are presented with in terms of service, public disclaimers, cookie policies and privacy policies which they all are expected to approve. Disclosure is often used as a mechanism by companies to justify their practices and shield themselves against enforcement actions. However, in a digitalised economy characterised by information overload ultimately limiting the cognitive ability of consumers to process and understand such information, even without the possibility to do anything against it except for not engaging with the service provider, further disclosure would be counterproductive.

(14) Under conditions of digital asymmetry, the consumer is particularly susceptible to practices which exploit the differences in power to the detriment of the consumer. This resulting universal state of vulnerability, referred to here as **digital vulnerability**, applies to virtually all[11] consumers who participate in the data economy and undermines their autonomy of choice.

1.2. Digital asymmetry extends beyond the online setting

(15) With the growth of the Internet of Things (IoT), the division between the online and the offline environments becomes increasingly blurred. With behavioural data siphoned by every service, app and connected device and then shared widely among traders, consumers have ever fewer ways of shielding themselves from the reach of the data collection ecosystem.

(16) The proliferation of AI systems and biometric technologies can be expected to create further opportunities to strengthen the position of traders vis-à-vis the consumer. In a brick-and-mortar commercial setting, behavioural insights and information about personal biases of the consumer may be extremely useful to traders in many industries. Similarly, inferences about the consumer's emotional states, if performed accurately, may be extremely useful in identifying moments of weakness.

1.3. Digital asymmetry and disruption of choice

(17) In a personalised environment, under conditions of digital asymmetry, choice becomes disrupted:

- in its *strictly transactional sense,* where the consumer is continuously exposed to personalised persuasion mechanisms offering content, products and services which are the most certain to evoke a response and maximise monetisation, and
- in the sense of individual autonomy, self-determination, privacy and human dignity: the consumer has no say about being included in the behavioural data ecosystem. A variety of measures including specially designed interfaces and choice architectures are deployed to ensure that remaining outside the system remains a purely theoretical option.

[11] Opting out of data collection is practically impossible. Experiments have shown that all it takes it to click 'I agree' once to allow that our personal data collected by the website or service be used to de-anonymise of other data which is collected without our consent. See e.g.); Frederike Kaltheuner (2018) I asked an online tracking company for all of my data and here's what I found, Privacy International, https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found. On the mechanics of cross-referencing of data and de-anonymisation, see also NCC (2020).

(18) Although personalisation and individual data increase efficiency of manipulation,[12] they are not necessary factors in choice disruption. Control over interfaces means control over the digital environment, including the way the consumer is presented with choices. Generalised inferences about cognitive and behavioural biases are used in design of dark patterns in the goods and services context (such as nagging, forced action, interface interference, subscription traps, etc.),[13] as well as through clickbait in attention-based markets.

1.4. Consumers' reactions to online tracking

a. Negative (but resigned) attitudes towards tracking

(19) Most consumers do not appreciate being tracked online. A December 2021 poll commissioned by MEP Patrick Breyer (Greens, Germany) asked 10,064 EU citizens whether Internet users should be given the right to use digital services **without any personal data being collected**. 64% of respondents were in favour of such a right (with 21% opposed).[14] An earlier YouGov study conducted on a sample of 2,000 French and German consumers, 83% rejected being tracked on the basis of personal data they shared with the social media company and 80% disapproved of making predictions based on third party data.[15]

(20) A 2021 Norwegian study by BEUC member organisation Forbrukerrådet showed that **two out of three** consumers felt negatively about commercial actors collecting personal information about them online, while only **one out of five** felt that using personal information to personalise advertising is acceptable. At the same time, **six out of ten** believed they had no other choice but to share this information.[16] This is in line with earlier findings of a 2020 survey conducted by Ghostery.com where 78% of respondents rejected the idea of giving companies their personal information even if it resulted in a product that's personalised just for them.[17]

(21) Although consumers feel concerned or anxious about the use of their data, they also feel powerless to change it – a feeling reinforced further when dealing with a dominant platform. A 2018 study by our UK member Which? showed that consumers do not feel they have realistic alternatives; e.g., 24% polled Facebook users said they considered leaving the site following the Cambridge Analytica revelations but did not and only 6% actually deactivated or deleted their account.[18]

---

[12] Lynskey, Micklitz, Rott (2021) p. 110 et seq.

[13] See e.g., OECD (2020) Roundtable on Dark Commercial Patterns Online, Summary of discussion, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2020)23/FINAL&docLanguage=En

[14] https://www.patrick-breyer.de/en/survey-on-the-digital-services-act-eu-citizens-want-the-right-to-use-digital-services-anonymously/. Concerns about being tracked online are not limited to Europe and similar sentiments were expressed in a 2022 US study by NordVPN: https://betanews.com/2022/01/11/almost-three-quarters-americans-worry-about-online-tracking/. An earlier Eurobarometer report showed that 74% consumers think it is unacceptable to pay in order not to be monitored when using a website, while 64% reject having their online activities monitored in exchange for unrestricted access to a certain website. Eurobarometer on e-Privacy (Dec 2016) https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=59394. Apple's 2021 changing their tracking choice architecture to opt-in resulted in extremely small consent rate of 4% in the US. https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

[15] https://www.globalwitness.org/en/blog/do-people-really-want-personalised-ads-online/

[16] Norwegian Consumer Council (2021) consumer attitudes to surveillance-based advertising. https://fil.forbrukerradet.no/wp-content/uploads/2021/06/consumer-attitudes-to-surveillance-based-advertising.pdf

[17] https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users

[18] Which? (2018), p. 43-45.

(22) The reasons UK consumers gave for this perceived powerlessness included:

- A lack of knowledge of what to do in order to take action, without disconnecting from technology.
- They found it hard to understand the impact of the data ecosystem on their lives.
- They felt it is already too late, as organisations already had their data.[19]

b. Personalised pricing and futility of resistance

(23) Algorithmic price personalisation based on behavioural data can be used as an example of how consumer preferences can be easily circumvented to obtain consent. Consumers reject personalised pricing and they see it as unfair, even if they stand to gain from it.[20] A 2021 behavioural study commissioned by the OECD reaffirms the negative sentiment – but it also shows how consumer consent to personalised pricing can be obtained nonetheless.

(24) According to the findings, online disclosures have only a limited effect on consumers' ability to identify and comprehend online personalised pricing. Disclosures (like cookie policies) did not significantly affect participants' purchasing behaviour – even though, on average, consumers did consider personalised pricing as an unfair practice that should be prohibited.[21]

(25) Although the disclosure of algorithmic price personalisation under the Omnibus Directive will become mandatory from 28 May 2022, the described observations put into question the actual value of such a measure, particularly if alternative providers in the market also end up using price personalisation.[22] This supports the conclusion about digital asymmetry being resistant to remedies based on information.

c. Consumers' understanding of tracking is limited

(26) Consumers might generally understand that they are being tracked online. However, the inner workings of the data collection ecosystem which involves harvesting, cross-referencing, de-anonymising and combining of data into persuasion profiles[23] are difficult for consumers to understand.

(27) In a 2021 study by Which? (n=1729), acceptance of tracking fell from 52% to 37% after consumers interacted with their tracking preferences on Facebook.[24] While 92% of users were aware (to some extent) that the platform collected first-party

[19] Id.
[20] In a UK study, 84% of respondents said they felt uncomfortable with personalised pricing in essential service markets and 3 in 4 said that if they encountered personalised pricing, they wouldn't trust their provider (Citizens Advice (2018) 'A Price of One's Own. An investigation into personalized pricing in essential markets' https://www.citizensadvice.org.uk/a-price-of-ones-own-an-investigation-into-personalised-pricing-in-essential-markets/). See also Rott P (2019) A Consumer Perspective on Algorithms. In: de Almeida L, Cantero Gamito M, Durovic M and Purnhagen KP (eds) The Transformation of Economic Law. Essays in Honour of Hans-W. Micklitz. Hart 2019.
[21] OECD (2021) The effects of online disclosure about personalised pricing on consumers. ISSN: 20716826 (online) https://doi.org/10.1787/20716826. https://www.oecd-ilibrary.org/science-and-technology/the-effects-of-online-disclosure-about-personalised-pricing-on-consumers_1ce1de63-en. Accessed on 24 Nov 2021.
[22] Lynskey, Micklitz, Rott (2021) p. 121 et seq.
[23] Norwegian Consumer Council (2020) Out of control. How consumers are exploited by the online advertising industry. 14.01.2020. https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf
[24] Which? (2021) Are you still following me? https://www.which.co.uk/policy/digital/8104/are-you-still-following-me

(on-site) data in order to inform targeted advertising, the majority of users had little knowledge about the extent of third-party tracking which is taking place:

- 79% had not realised Facebook was matching their profiles to data from other companies.
- 53% thought it was not acceptable for their profile to be matched to a customer list in any circumstances.
- 58% felt that all third-party website and app tracking was unacceptable.
- Once informed about how the system works and having engaged with privacy settings on Facebook, 28% of those who initially chose targeted adverts changed their preference to receiving generic ads. The proportion of users preferring targeted ads thus fell from 52% to 37%.

2. BEUC recommendations

In this section, we provide recommendations about how EU law, in particular the Unfair Commercial Practices Directive, should be amended in order to better respond to new market realities and ensure consumers are sufficiently protected.

2.1. Revision of the Unfair Commercial Practices Directive

(28) This section offers an overview of how the fabric of the Unfair Commercial Practices Directive needs to be updated to account for the dynamics created by the digital sphere.

a. New concepts of digital asymmetry and digital vulnerability

(29) Digital vulnerability should be introduced in the recitals to the Directive as a general description of a **universal state of susceptibility** to the exploitation of differences in power in the trader-consumer relationship resulting from internal and external factors beyond the control of the consumer. Such internal factors can include insufficient digital literacy, personal biases, limited cognitive capacity or plain information overload. External factors may include the digitally mediated relationship, the digital choice environments, the knowledge gap, limited control over data through user interfaces, the design of digital consumer environments, the lack of interoperability, the way default settings are configured, etc.

(30) The recitals should also indicate digital asymmetry as resulting from:

- structural differences in the power to influence the process of autonomous decision making of the other party, as a result of the control over data and/or the architecture of the digital choice environment (structural / architectural asymmetry), or
- imbalances in the (ongoing) commercial relationship that a digital consumer environment creates and maintains (relational asymmetry), or

- from a situation of imbalance in relation to the knowledge and understanding of the functioning and impact of a digital commercial practice (informational asymmetry).

b. Digital fairness and material distortion of behaviour

(31) The Directive should recognise that material distortion of the consumer's autonomous decision-making may result from the trader's practices using digital asymmetry to gain further advantage over the consumer, as well as from failing to prevent algorithmic exploitation of natural decision-making biases, to the detriment of the consumer. Such practices should be treated as unfair.

(32) Under conditions of digital asymmetry, the trader should have a duty of care to ensure that the consumer's decision autonomy is not impacted by its commercial practice, in particular the design and operation of the interface. This must include, as a minimum:

- enabling consumers to see, understand, and exercise their capacity for making different choices, which includes the manner of presentation of information;
- prevention of identifiable decision-making biases as well as mitigation of the imbalances in the relationship with the consumer;
- lack of direct and indirect interference with the decision-making process.

(33) Such a regime of safeguarding the consumer's decision-making autonomy should apply to all cases where digital asymmetry increases the risk of material distortion of behaviour. This must include:

- algorithmic personalisation of choice architectures;
- behavioural profiling for commercial purposes;
- recommender environments, particularly where a bias or vulnerability may be likely identified, amplified or created.

c. Burden of argumentation and burden of proof

(34) The Directive must reflect that digital asymmetry also affects enforcers, particularly in its knowledge dimension. In this context, the trader holds an advantage partly founded on the quick evolution of systems, the obscurity of algorithmic processes and the resulting difficulty to establish compliance of data-driven services throughout the supply chain.[25] Pinpointing unlawful behaviour is also made more difficult due to the time-extended nature of the relationships built with consumers which do not always allow authorities to identify single transactional moments that could be examined.

(35) In consequence, digital asymmetry also means that resources needed to effectively enforce the law are disproportionately high compared to the relative ease with which the data-driven commercial practice may be deployed or modified. Policing cases of unlawful influence on consumers necessitates lengthy and resource-consuming investigations, very difficult from an evidence perspective and likely to dwell on versions and variants of a service which have long been discontinued or displaced.[26]

[25] Which? (2018), p. 42.

[26] This was evidenced in the BEUC coordinated action against Google, where the interface designs the complaints pertained to were changed over the course of the investigation. For a writeup on the action, see BEUC (2020) The long and winding road: Two years of the GDPR: A cross-border data protection enforcement case from a

(36) In the case of a legal proceeding, the Directive should therefore require the trader to come forward with conclusive evidence on the details of the employed practice that will allow authorities to establish whether the practice establishes digital asymmetries which are used to materially distort the choices of the consumer. Failing to provide such evidence must result in a legal presumption in the affirmative.

(37) The burden of argumentation should also require that, in the case of the trader passively participating in an online marketplace and benefiting from its algorithmic environment, the provider of this environment could be required to provide the required evidence to prove that the digital asymmetry, if present, is not used to materially distort the decision-making autonomy of the consumer.

d. Economic behaviour and transactional decisions

(38) It is important to extend the understanding of economic behaviour and transactional decision of the consumer to include situations where no monetary payment is made and transactional value is built on the user's engagement with the digital choice environment. The trader's revenue is then generated on the basis of the length and level of activity of the consumer's engagement and will vary depending on whether the consumer should choose to passively scroll through the newsfeed for a second or longer, or whether they choose to interact with it by liking or sharing the content.

(39) The Directive's concept of 'transactional decision' should thus be broadened to reflect all cases where the behaviour of the consumer is connected to the revenue-earning model of the trader. In other words, if the business model is that of providing unpaid access to a social media platform, where various types of interaction of the consumer with the platform (e.g., clicking on ads and other content, scrolling the newsfeed, sharing, liking) are monetised, engaging in such types of interaction should be treated as transactional decisions on the part of the consumer.

(40) In discussing the meaning of 'economic behaviour' in this context, it is important to note that such exchanges are not free: the consumer pays with their attention, engagement, activity and behavioural data. In exchange, they are offered access to the service and its functionalities. Consequently, commercial practices which distort the consumer's decision-making in this context (e.g., providing misleading content masqueraded as news) should be treated as a material distortion of economic behaviour and this be seen as an unfair practice under the Directive.

e. Aggressive commercial practices

(41) The Directive's framework of aggressive commercial practices looks for harassment, coercion, or undue influence that is likely to significantly impair the conduct of the consumer causing a transactional decision that they would not have taken otherwise.

(42) To account for the realities of digital asymmetry, this construct should be updated accordingly to account for aggression that is rooted in the elements that form the foundation of the trader's advantage under the digital asymmetry, such as the choice architecture, the technical infrastructure, or the knowledge asymmetry. Practical application of this provision should be explained further in a future revision of the guidance document.

---

consumer perspective https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf

(43) It should also take note that aggression may not be limited to a single transactional moment (which may not always be possible to define) but one that is of external (or structural) nature and permeates the consumer's relationship with the data-driven service.

(44) The Directive's definition of an aggressive practice should therefore make clear that, in establishing whether a practice '*significantly impairs or is likely to significantly impair the conduct of the consumer'*, causing them to '*take a transactional decision that* [they] *would not have taken otherwise*', structural features and circumstances such as the digital choice environments, the technical infrastructure, and the degree of informational asymmetries must also be examined.

(45) The Directive should also offer an updated view of what constitutes harassment, coercion and undue influence (including structural influence). To this end, the test of Article 9 should include:

- the extent to which the digital consumer environment is personalised;
- the transparency or covertness of the practice;
- whether the practice is informed by insights resulting from analysis of consumer behaviour or individual characteristics;
- the extent to which the given service is interoperable with other services;
- the level of competition and ease with which consumers can switch to other digital choice platforms.

f. New black-list items

(46) With a view to the quick changes occurring in the digital environment, the revised Directive should not place undue focus on circumscribed prohibitions of specific practices. While the regulatory practice of establishing black-lists facilitates the application of the regime by providing examples of practices which are always unfair, it may also lead to the creation of legislation that is quickly outdated as new practices emerge.

(47) To tackle this issue, the envisaged discussion on regulatory governance in the context of revising the Directive and Annex 1 should include consideration of future futureproofing measures to allow regulation to react more quickly.

(48) The below items should be included in the list of unconditional prohibitions given the level of harm they carry, the incentives for unfair commercial behaviour they provide and consumers' difficulty to avoid them, despite negative sentiments expressed in opinion polls.

(49) Practices including behavioural (algorithmic) pricing, as well as those involving personalised pressure, performed based on detailed profiles mapping a person's personality, biases and vulnerabilities (psychographic profiles) should always be deemed as unfair.

(50) Similarly, digital commercial practices should be prohibited where they are using data which may reasonably be suspected to have been obtained in breach of data protection laws.

(51) In summary, the black-list in Annex 1 to the Directive should prohibit:

- use of psychographic profiles or similar approaches to exercise emotional or psychological pressure;
- use of psychographic profiles or similar approaches to personalise prices;
- use of personal data which the trader knows or should reasonably know was obtained unlawfully for any digital commercial practice.

2.2. Interplay with other legislation and prevention of pre-emption

(52) At the time of writing this paper, proposals for four new instruments have been put forward by the European Commission: the Digital Services Act (DSA),[27] the Digital Markets Act (DMA),[28] the Digital Governance Act (DGA)[29] and the Artificial Intelligence Act (AIA).[30] All four bills are relevant to the digital market of the EU and all aim at maximum harmonisation.

(53) Although none of the four proposals integrates consumer protection as a standalone objective in a systematic manner, it is also true that all of them are doubtlessly relevant to the achievement of goals of ensuring a high-level of consumer protection in the digital market and may contribute to them indirectly.[31] It is therefore a valid concern whether, by virtue of the occupied field doctrine,[32] the proposals do not preclude any further updates to consumer acquis in the digital sphere.

(54) If this is not the desired result, in order to avoid a preclusive effect, all four regulations should explicitly state that they are complementary to, and without prejudice to other consumer protection instruments.

2.3. The increasingly important role of technical standards

(55) The AIA proposal with its delegation of requirements of conformity of algorithms to standardisation bodies has triggered a discussion of whether the development such standards (extending product liability to matters of psychological harm and fundamental rights) is technologically and legally possible.

(56) This notwithstanding, the importance of standards in the building and operation of a fair digital future for Europe cannot be overstated, both from the perspective of developing reliable pathways for the development of algorithms and to facilitate demonstration of compliance by traders operating in the conditions of digital asymmetry.

---

[27] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final, 15.12.2020, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN

[28] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final, 15.12.2020 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

[29] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final, 25.11.2020 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[30] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts COM/2021/206 final, 21.4.2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[31] On AIA's definition of user, see BEUC (2021) Regulating AI to protect the consumer. BEUC-X-2021-088 - 07/10/2021 https://www.beuc.eu/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf

[32] Veale, Michael and Zuiderveen Borgesius, Frederik, Demystifying the Draft EU Artificial Intelligence Act (July 31, 2021). Computer Law Review International (2021) 22(4), Available at SSRN: https://ssrn.com/abstract=3896852; see also Weatherill (2020) The Fundamental Question of Minimum or Maximum Harmonisation https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3660372.

(57) However, a framework for the development of such standards would need to ensure that they are not produced exclusively by industry bodies and thus outside of democratic control. Considerations should be made of a new instrument to regulate the pathways for standard-making ensuring due role of civil society organisations in the process and a supervisory function of the European Parliament and thus ensure a desired level of democratisation in the digital economy.

END

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2021-2027).