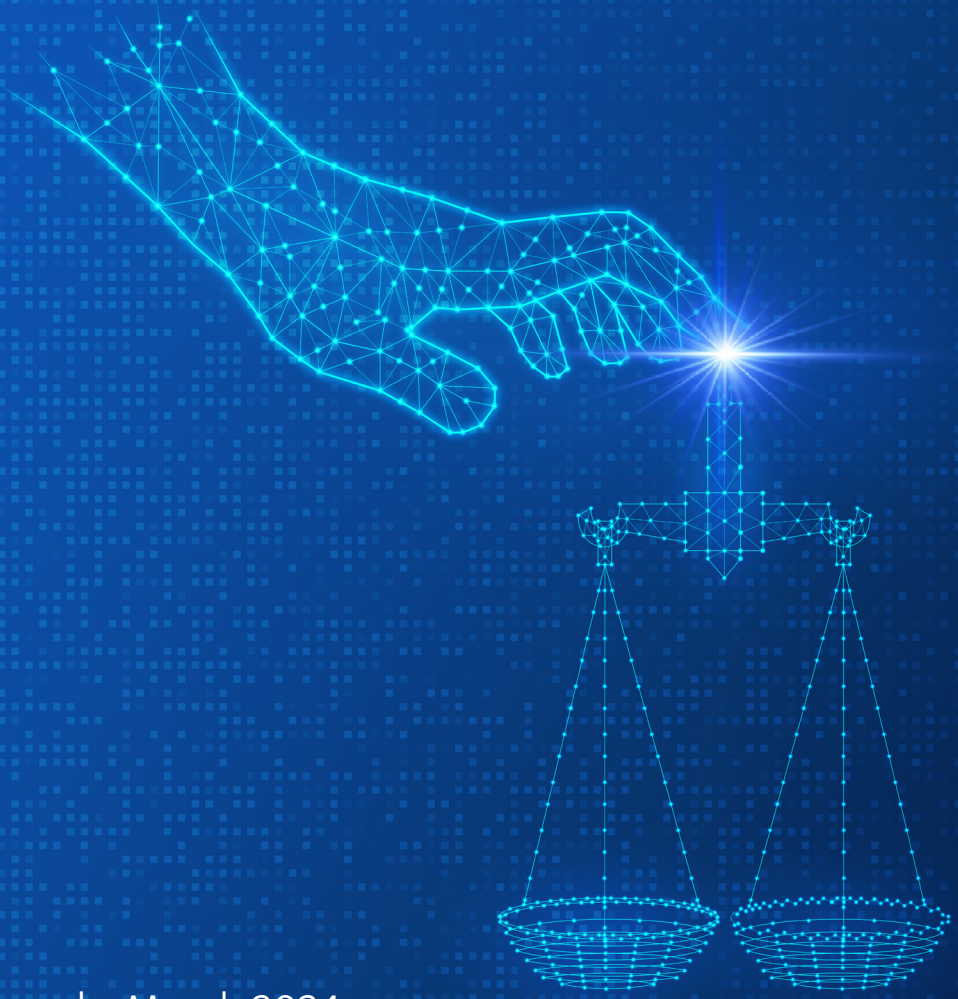
BEUC The European Consumer Organisation

Digital Fairness for Consumers

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



Brussels, March 2024

European University Institute, Robert Schuman Centre for Advanced Studies
IViR
Erasmus University Rotterdam
Faculty of Law and Administration, University of Lodz
Carl von Ossietzky Universität Oldenburg

Co-funded by
the European Union

The content of this publication represents the views of the authors only and it is their sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.

ADESSIUM FOUNDATION

Made possible with the support
of the Adessium Foundation

This publication only reflects the personal opinions of the authors and can neither be attributed to their respective research institutions nor to any other persons working for these institutions.

BEUC The European Consumer Organisation

Rue d'Arlon, 80 Bte 1
B – 1040 Brussels
Tel: +32 2 743 15 90

Digital Fairness for Consumers

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

Published in March 2024

Project information

The New Digital Fairness (NDF) project is a research and advocacy initiative launched by BEUC with support from the Adessium Foundation, seeking to address the challenges and potential harms caused to consumers, citizens and societies by the use of new technologies and business models in today's digital economy.

The present report arrives in direct succession of the EU Consumer Protection 2.0 (EUCP2.0) project and builds on the conceptual framework developed at that stage of the research, particularly in regard to the disempowerment of consumers due to asymmetries of knowledge and power, new categories of consumer vulnerability caused and aggravated by algorithmic environments as well as omnipresent surveillance and behavioural personalisation. This work takes the analysis further, identifying systemic processes gradually weakening the position of consumers in the digitalised markets. It also shows the way forward, by proposing a regulatory framework that would strengthen and safeguard consumers and provide a digital market that is safe and fair to them by design and by default.

The broad applicability and technological neutrality of horizontal consumer law render it a fitting vehicle for protecting the needs and safeguarding the rights of modern-day digital consumers. In the light of the ongoing, EU 'digital fairness' fitness check assessment of consumer law, this work proposes specific solutions and recommendations that could form the backbone of EU's regulatory response to the age of digital asymmetries that should be the Digital Fairness Act.

This publication constitutes independent research that was commissioned by BEUC, the European Consumer Organisation.

Contents

Study authors

Natali Helberger

Distinguished University Professor of Law and Digital Technology at the University of Amsterdam. Her interdisciplinary research bridges law with social and cultural science and focuses on artificial intelligence, information technology and social and economic conditions.

Betül Kas

Visiting Fellow at the Private Law Department of Erasmus School of Law, Rotterdam, author of publications on the influence of EU fundamental rights on private law, EU civil justice and litigation.

Hans-Wolfgang Micklitz

Professor for Economic Law, Robert Schuman Centre for Advanced Studies at the European University Institute in Florence, with a broad track record in European Private and Economic Law, National and European Consumer Law and Legal Theory.

Monika Namysłowska

Full Professor and Head of the Department of European Economic Law at the Faculty of Law and Administration of the University of Lodz, specializing in national and EU competition law, unfair commercial practices and advertising law in the context of new technologies.

Laurens Naudts

Postdoctoral Researcher at the AI, Media and Democracy Lab and Institute for Information Law, University of Amsterdam; Affiliated Senior Researcher KU Leuven CiTiP. Laurens' research focuses on the regulation of artificial intelligence and information technology, digital fundamental rights, and the emergence of (structural) social injustice in the data-driven society.

Peter Rott

Professor of Civil Law, Commercial Law and Information Law at Carl von Ossietzky University of Oldenburg, Germany, his research focusing on European and German consumer law, including litigation of consumer claims, regulation of algorithms and personalisation practices.

Marijn Sax

Assistant Professor at the Institute for Information Law, University of Amsterdam with a background in political science, philosophy and law, with a focus on researching the normative implications of behavioural influence in digital choice environments.

Michael Veale

Associate Professor and Vice-Dean (Education Innovation) in the Faculty of Laws, University College London, with a focus on human-computer interaction, computer science and technology law, data protection and emerging technologies including AI and encrypted data analysis.

I. Introduction

The EU Digital Policy Legislation, built around 12 different legislative acts,[1] 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. The various legal acts already adopted or in the process of being adopted are only occasionally and, if so, in a quite erratic way, dealing with consumer issues. The EU Consumer Protection 2.0 study, equally commissioned by BEUC and written by Helberger, Lynskey, Micklitz, Rott, Sax, Strycharz in 2021[2] provided for a first account of the potential deficit and proposed a potential 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 consumer protection deficits in EU Digital Policy Legislation, the European Commission launched the 'Digital Fairness – Fitness Check on EU Consumer Law' in May 2022.[3] This fitness check would *'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'. The here presented study on 'Digital Fairness for Consumers' has to be placed into the context of the EU digital fairness test, which will not come to an end in the van der Leyen Commission, but which will, in all probability, have to be continued after the next elections of the European Parliament.

The authors hope to initiate a broader discussion on what digital fairness might mean and how digital fairness can be anchored in the EU consumer law. Limiting digital fairness to three pieces of EU legislation is certainly not a promising avenue. The EU Digital Policy Legislation cuts across the consumer law acquis as a whole and would require to evaluate each and every piece of the consumer law acquis. The question to be studied is whether the European consumer law acquis, which was developed under a political agenda which dates back to the famous Kennedy Declaration 1962 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 human mankind. In that sense, the findings should be

1 The references provide for a comprehensive overview https://www.bruegel.org/sites/default/files/2023-07/Tables_Scott_Kai.pdf

2 N. Helberger/ O. Lynskey/ H.-W. Micklitz/ P. Rott/ M. Sax/ J. Strycharz, EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets, A joint report from research conducted under the EUCP2.0 project, BEUC, March 2021, 207 pages; https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

3 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en

understood as the first building block in an ongoing process to find appropriate answers not only for consumer protection but for society at large.

The regulatory background results from the analysis of the DSA and the AIA Proposal, which serves as a common background for existing and upcoming consumer problems, are to be elaborated. The authors, together with 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, Marijn Sax, Michael Veale;
2. TOWARD CONSTRUCTIVE OPTIMISATION: ALIGNING THE RECOMMENDER STACK UNDER EUROPEAN LAW, by Laurens Naudts, Natali Helberger, Marijn Sax, 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.

All six building blocks follow a comparable structure. The first step is to analyse the impact of the digital economy in light of the EU Digital Policy Legislation and the consumer acquis with regard to the identified six major policy issues: the impact on digital vulnerability (1), the impact on recommender systems (2), the impact on the notion of the consumer and the obligations imposed on the provider of AI systems (3), the impact on fundamental rights (4), the impact on the unfairness test in the Unfair Commercial Practices Directive (5) and last but not least the impact on the distribution of the burden of proof (6). The second step is to come up with conclusions, broader observations and concrete recommendations, aiming at providing guidance on the kind of action the European Commission should take.

The six building blocks reveal tendencies which demonstrate that there is indeed a rupture[4] taking place in the digital economy, which shatters established wisdoms in the design and understanding of consumer law. The *first* 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, a space which is framed by a broad set of due diligence obligations, broadly worded in EU Digital Policy Legislation and concretised through EU driven private regulation. The *third* is the lack of value-based guidance despite all the rhetoric on '*human-centric, secure, ethical and trustworthy AI*'. EU Digital Policy Legislation claims to fill the gap through extensive reference to the EU Charter on Fundamental Rights and more implicitly than explicitly through the unfairness test of the UCPD as a safety net. However, it turns out that fundamental rights are a placeholder for everything and nothing, of extremely limited use under the existing state of case-law of the CJEU and the ECtHR. The unfairness test enshrined in Art. 5 UCPD, on the other hand, lacks the necessary concreteness of legal requirements, which could deal

4 Twigg-Flesner, Christian, Disruptive Technology – Disrupted Law? How the Digital Revolution Affects (Contract) Law (May 26, 2016). C. Twigg-Flesner, "Disruptive Technology – Disrupted Law? How the digital revolution affects (Contract) law" in A. De Franceschi, European Contract Law and the Digital Single Market (Intersentia, 2016), Available at SSRN: https://ssrn.com/abstract=3039952.

with digital vulnerability or with 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 regarding the digital architecture, which renders the enforcement of consumer rights under the existing acquis difficult, if not impossible. The classical distribution of the burden of proof between the consumer, or consumer organisations, and the trader, relied on in the industrial economy, except for product liability and anti-discrimination, must be questioned in the digital economy.

The authors propose to discuss the possible implications of the findings with a view to developing a 'Digital Fairness Act'. While the authors claim to address at least the most important policy fields and consumer problems, they certainly do not claim to exhaust the strive for digital fairness. This is true not only with regard to substance, which would mean analysing all the Directives and EU Regulations one by one, and evaluating their suitability, but in particular with regard to 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 GDPR, the DMA, the DSA and transplanted into the pending EU proposals, in particular the AIA, is hardly suitable to cope with pressing political problems, such as the protection of children against all sorts of problematic practices offered by the online platforms.[5]

5 M. Cantero Gamito/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, 17-02-23) 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.

II. Digital Vulnerability and Manipulation in the Emerging Digital Framework

Marijn Sax & Natali Helberger[1]

1 Institute for Information Law, University of Amsterdam. Both authors contributed equally.

Introduction and recap: Digital vulnerability

The use of the term '*digital* vulnerability', as opposed to just 'vulnerability', highlights how our technological circumstances require us to adopt a more dynamic approach to vulnerability. It no longer suffices – if it ever did at all – to think in terms of stable, permanent characteristics or circumstances that render a person vulnerable. A *digital* vulnerability approach is based on the insight that not only fixed characteristics of a person can render her vulnerable, but that in the continuous interplay with one's (digital) environment one can – sometimes only momentarily, or only in specific contexts – move in and out of states of vulnerability. As a result, the classic distinction between the 'normal, non-vulnerable' versus 'the vulnerable' consumer is collapsed. Every consumer is potentially vulnerable, depending on the (digital) circumstances and environments she finds herself in. Vulnerability becomes the rule, rather than the exception.

With special attention for the ways in which vulnerability plays out in digital choice environments also increasingly comes attention for manipulative influences exert in and through digital choice environments. Manipulative influences are exerted precisely by the targeting and exploitation of known or presumed vulnerabilities in order to (try to) make manipulation targets serve the ends of the manipulator.[2] It therefore comes as no surprise that in the EU's recent digital technology legislative agenda manipulation and vulnerability are often mentioned and addressed in close connection to one another.

The thematisation of (digital) vulnerability and manipulation in close connection to one another is promising, but also comes with challenges. The main challenge is that precisely because vulnerability and manipulation are so closely related, it is especially important to both conceptually and definitionally highlight not only the similarities but also the differences. Both vulnerability and manipulation are complicated concepts in their own right. Their interrelation is even more complex. The aim of this piece is to provide a first exploration of how (digital) vulnerability and manipulation, as separate concerns but also increasingly as interrelated concerns, play a role in the emerging digital framework of the Digital Services Act (DSA), Digital Markets Act (DMA), draft AI Act (AIA), draft Political Advertising Regulation (PAR).

Elsewhere, we have defined digital vulnerability as "a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer-seller relations and the very architecture of digital marketplaces."[3] And we argued that digital vulnerability is related to the power or ability of commercial actors to affect the decisions, desires, and behaviour of the consumer in ways that the consumer, all things considered, does not condone, but are also not in a position to prevent. That this is so is the result of what Kaptein *et al.*[4] have referred to as an "adaptive persuasive system". In more concrete terms this means that to be able to evaluate commercial practices in terms of their fairness, it is not enough to evaluate the message; the systemic set-up and the way technology shapes the relationship between consumer and advertiser should also figure

2 Sax, M. (2021). *Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps*. Kluwer.

3 Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M., Strycharz, J. (2021). *EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets*, report for BEUC - The European Consumer Organisation; Helberger, N., Sax, M., Strycharz, J., & Micklitz, H.-W. (2022). Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. *Journal of Consumer Policy, 45*(2), 175–200.

4 Kaptein, M., Markopoulos, P., De Ruyter, B, & Aarts, E. (2015). Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles. *International Journal of Human-Computer Studies, 77*, 38–51.

prominently in such an analysis. We have therefore argued that addressing vulnerability and tackling systemic structures of commercial manipulative exploitation of those vulnerabilities is not just a question of consumer empowerment but of changing markets and addressing the digital asymmetries that enable those practices in the first place.

Definition of (digital) vulnerability across the emerging digital regulatory framework

Three elements, in particular, characterise the concept of digital vulnerability: its relational nature, its architectural nature, and the erosion of privacy. In the digital realm, consumer vulnerability can be the result of asymmetrical and potentially continuous power relationships where the productive force of those relationships can produce vulnerabilities. Vulnerability is thus inherently **relational**. As such, vulnerabilities can be not only the result of individual characteristics or the social or economic position of the consumer but also the result of the properties of a digital platform, app store or another form of digital choice architecture. Digital environments can be data-driven, dynamically adjustable and designed to infer or even create vulnerabilities. The **architectural** make-up of those digital environments – i.e., their entire technology stack – can thus be geared towards the production and exploitation of vulnerabilities. Finally, there is the element of extraction and use of exploitative data practices to segment, classify, profile and target individuals. Part of the design of digital choice architecture is finding ways to collect (more and more) data about consumers, data that can be used to target and personalise services. The interaction of consumers with these services generates new data that will flow into the system, help to adjust and optimise it, make it more responsive to the explicit or inferred signals from consumers, and ultimately the business goals that inform the overall design of the choice architecture. A structural disregard for consumer **privacy** is thus, again, an essential productive force for digital vulnerability. After having signalled the importance of understanding digital vulnerability and addressing digital vulnerability and manipulation (as an element and condition of digital asymmetry), the following section examines a) the extent to which the emerging digital framework accommodates and responds to such a more comprehensive understanding, b) gaps and inconsistencies, as well as c) possible need for improvement.

Broadening a traditional concept

The emerging digital framework (DSA, DMA, AIA, PAR) is divided. On the one hand, the traditional concept of vulnerability in the sense of a pre-defined group of consumers as an exception to the rule (average consumer) is still dominant. Particularly in the AI Act but also the DSA, there are numerous references to the elderly, minors and disabled as traditionally recognised groups of vulnerable consumers.[5] Having said so, several developments are noteworthy. First of all, the proposals for the AI Act from the Council, the European Commission and the European Parliament add new categories of vulnerable users, including migrants,[6] persons living in poverty, ethnic or religious minorities,[7] and people applying for or receiving public assistance, services or benefits.[8] Like the traditional concept of vulnerability in consumer law that singles

5 See, e.g., Art. 52a(3b) EP version: Information shall be accessible to vulnerable persons, including persons with disabilities or children.
6 Recital 16 of the AI Act in the draft version from 21/01/2024.
7 Ibid.
8 Recital 37 AIA in the draft version from 21/01/2024.

out members of particular groups in society, also the AI Act singles out particular groups of users and designates them as potentially vulnerable. Unlike the vulnerable consumer concept, however, vulnerability under the AI Act and the DSA can be found in commercial relationships as well as in consumers' relationships with public institutions (for example, as receivers of public benefits). The AI Act explicitly acknowledges that vulnerability can be the result of a dependency situation. Another and related direction in which the concept is broadened is that vulnerability implies that consumers are not only susceptible to the infringement of their rights as consumers (information, fair prices, choice, being free from harm), but also to the infringement of fundamental rights and their legitimate interests as citizens. In this context, one fundamental right in particular stands out, which is the right to non-discrimination. Both the DSA and the AI Act conceptualise consumer vulnerability repeatedly as susceptibility to undue discrimination or biases as the result of the use of digital technology.[9] And whereas consumer vulnerability has been typically referred to in the context of harm for individual consumers, in the emerging digital framework, vulnerability and the exploitation of vulnerabilities can also extend to harm to society. For example, in the draft PAR (EC version), the Commission first explains how digital technology can be used to segment individuals and exploit their characteristics or vulnerabilities to explain then that this can have detrimental effects on individual citizens' fundamental rights and freedoms (such as the right to data protection, to make political decisions and exercise voting rights), but that this can also negatively impact the overall democratic process "as it enables a fragmentation of the public debate about important societal issues, predatory voter analysis, selective outreach and, ultimately, the manipulation of the electorate", next to increasing the risk for disinformation and foreign electoral interference.[10] Recital 69 DSA reads: "In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example, by contributing to disinformation campaigns or by discriminating against certain groups. Online platforms are particularly sensitive environments for such practices and they present a higher societal risk." Put differently, a broader understanding of vulnerability emerges from the digital regulatory framework. Vulnerability is used to refer to the situation of users as consumers but also as citizens. Their freedoms and fundamental rights are at stake, as are the interests of society as a whole, when exploiting vulnerabilities results in collateral harm to societal values such as democracy or an inclusive society. This broader understanding of vulnerability reflects the reality of the digital environment and of platforms in particular, where it becomes increasingly difficult to draw a clear distinction between consumers and citizens. Platforms in particular serve as both economic marketplaces and privately controlled forums of public debate and engagement. Neither do their algorithms and ad auction systems distinguish between the citizen and the consumer.

Emerging new understandings of vulnerability

Next to a more traditional conception of vulnerability in the DSA the AI Act and the PAR (the DMA does not refer to vulnerability), a new approach to user vulnerability can be observed, too. This is most apparent in the proposals for an AI Act and here in Recital 16 and the corresponding Articles 5(1) a) and b). According to Recital 16 (EP version), "AI-enabled manipulative techniques can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making

9 E.g., recital 44 AIA, recital 69 DSA, Recital 47 PAR (EP version).
10 Recital 47 (EP version) PAR.

and free choices".[11] The draft law furthermore, acknowledges that such exploitation can have a temporal component by referring to harms that may be accumulated over time, thereby pointing towards a relational understanding of vulnerability in the sense of our definition of digital vulnerability. The proposed act also addresses the use of newer AI to *make* users vulnerable, in the form of using "machine-brain interfaces or virtual reality as they allow for a higher degree of control of what stimuli are presented to persons, insofar as they may be materially distorting their behaviour in a significantly harmful manner". Though the provision has a distinctive 'cyberpunk' feel to it, it does clearly acknowledge that vulnerability is not necessarily inherent to the consumer but can be optimised for. Finally, unlike in consumer law, the proposed AI Act (in the EP version) intends to protect users from economic and all kinds of harm (whereas the Council and EC version focus on physical or psychological harm).

The emerging digital framework also acknowledges that vulnerability can be the result of the design and deployment of AI systems or platforms. Even though an earlier proposal of the European Parliament to include an obligation for national supervisory authorites to investigate the design goals has not made it into the later version of the text of Article 65 AIA: "Where there is sufficient reason to consider that an AI system exploits the vulnerabilities of vulnerable groups or violates their rights intentionally or unintentionally, the national supervisory authority shall have the duty to investigate the design goals, data inputs, model selection, implementation and outcomes of the AI system." According to Recital 69 of the DSA, "Online platforms are particularly sensitive environments for such practices [targeting techniques optimised to match users interests and appeal to their vulnerabilities" and they present a higher societal risk."

Data, or the extraction and use of data, is also explicitly considered as a potential source of vulnerability. According to Recital 47 PAR (EC Version): "On the basis of the processing of personal data, in particular data considered sensitive under Regulation (EU) 2016/679 of the European Parliament and of the Council and Regulation (EU) 2018/1725 of the European Parliament and of the Council, different groups of voters or individuals can be segmented and their characteristics or vulnerabilities exploited for instance by disseminating the advertisements at specific moments and in specific places designed to take advantage of the instances where they would be sensitive to a certain kind of information/message." These examples signal that a process of rethinking of vulnerability has begun in the sense of a more relational, architectural and data-reliant conceptualisation of vulnerability.

Finally, and unlike in consumer law, where the concept of vulnerability is, in the first place, a benchmark or vantage point from which to assess a particular technology, the emerging digital framework has begun to attach legal consequences to the exploitation or causation of digital vulnerabilities (or the potential thereof). For example, the potential to cause or exploit vulnerabilities can be part of the assessment of whether an AI system is high risk or not,[12] digital vulnerability can trigger the need to undertake mitigation measures and improve systems design,[13] and can be central to the ban of particular uses of digital technology.[14]

---

11 Recital 16 (EP version) AIA.
12 Article 7f AIA.
13 Art. 29a AIA (EP version), Articles 34 and 35 DSA.
14 Art. 5 (1) AIA, Article 12 (1) PAR.

Definition of manipulation across the emerging digital regulatory framework

In recent years, the concept of manipulation has found its way into the European legislative agenda for the regulation of the digital economy. The increasing interest in manipulation as a regulatory concern is closely tied to the mission of protecting vulnerable consumers, since manipulation is typically predicated on the exploitation of vulnerabilities. So, in a digital landscape where many of consumers' interactions with commercial parties take place within digital choice environments – which are especially well suited to track, analyse, and influence behaviour – the risk of manipulation and concerns over digital vulnerability are two sides of the same coin. Legislative initiatives to address manipulation are thus also initiatives that have a direct impact on the legislative approach to vulnerability.

As the recent surge in philosophical literature on (digital) manipulation clear shows, manipulation is difficult to define.[15] These definitional challenges do, of course, carry over to the legal context. So much so that even though several recent legislative initiatives – e.g., the DSA and the AI Act – contain explicit manipulation clauses, none of these legal instruments contain a legal definition of manipulation. It thus remains unclear how manipulation should be interpreted as a *legal* concept in the EU's legislative agenda on the digital economy.

The lack of a proper definition in the DSA

Article 25(1) of the DSA contains a straightforward manipulation ban:

> "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".

Even though manipulation is explicitly mentioned, it remains unclear what it means in the context of Article 25(1). The structure of this article is best understood by starting at the end of the article. That which is ultimately safeguarded is people's ability "to make free and informed decisions". To that end, the article mentions two specific forms of influence – manipulation and deception – that can "distort or impair" free and informed decisions, while also acknowledging that there can be other "ways" in which people's free and informed decisions can be undermined. Lastly, there is the open-ended, very inclusive formulation of "shall not design, organise or operate their online interface in a way that deceives or manipulates". Clearly, the DSA aims to address the digital choice environments that betray a manipulative potential *in their entirety*.

With no definition of manipulation being mentioned elsewhere in the DSA, this specific manipulation clause does little to explicate what manipulation means in this context. It is clear that manipulation is understood as a form of influence that can impair free decision-making, but

15 Susser, D., Roessler, B., & Nissenbaum, H. (2019). Online Manipulation: Hidden Influences in a Digital World. *Georgetown Law Technology Review, 4*(1), 1–45; Sax, M. (2021). *Between Empowerment and Manipulation: The Ethics and Regulation of For-Profit Health Apps*. Kluwer; Jongepier, F., & Klenk, M. (Eds). (2022). *The Philosophy of Online Manipulation*. Routledge.

that can be said of many different forms of influence – coercion and blackmail also impair free decision-making but are clearly not cases of manipulation (or deception). So, the current framing of manipulation is too generic to be helpful. One could turn to Recital 67 which deals specifically with dark patterns. Dark patterns are not mentioned in any of the articles in the DSA, so the recital on dark patterns is the most plausible source of guidance for understanding manipulation in the DSA.

This recital, however, does little to explain how – conceptually speaking – influences such as deception, nudging, nagging, and manipulation are be understood and, importantly, differentiated from each other. The recital mentions these different forms of influence, seemingly as examples of dark patterns. It remains unclear, however, whether the concept of dark patterns is treated as just an umbrella term for several types of influences (deception, manipulation, nudging, nagging) that can somehow distort decision-making. Because no (approximations of) definitions of these forms of influences are provided, we only know that in the context of Recital 67 – and the DSA more generally? – these forms of influence are somewhat similar to each other because they are all collected under the umbrella of 'dark patterns'. What also doesn't help the reader is the fact that the DSA only contains vague gestures to what makes these different forms of influence undesirable. In Recital 67, deception, manipulation, nudging, and nagging are all described as forms of influence that impair/distort/unreasonably bias the decision-making of the consumer. If anything, this makes it even more unclear how one should differentiate between these forms of influence because they all seem to share the same wrong-making feature.

One is also kept wondering why Recital 67 is explicitly framed in terms of dark patterns, with deception, manipulation, nudging, and nagging seemingly being specific instances of dark patters, but why Article 25(1) is not framed in terms of dark patterns and *only* mentions manipulation and deception. Should deception and manipulation in Article 25(1) be read as incomplete short hands for dark patterns? If so, why aren't nudging and nagging included? If, however, manipulation and deception should not be read through the lens of the dark patterns recital, then where is one supposed to gather the interpretational resources to understand what is meant by these terms in Article 25(1)?

In sum, even though manipulation is explicitly mentioned in the DSA, it remains unclear how this challenging concept should be understood. And the DSA offers little 'interpretative materials' to work with in this regard.

AI Act: strong and limited harm focus

Manipulation is also mentioned explicitly in the AI Act. Article 5(1)(a) forbids

> "The placing on the market [or] putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques with the objective to or to the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or a group of persons significant harm."

The similarities with the DSA are clear. Again, manipulation is mentioned as form of influence that can distort someone's decision-making capabilities. In the AI Act, there is a harm requirement added to the article. This is especially interesting because, again, like the DSA, the AI Act does not define manipulation anywhere. So, without a definition of manipulation and, as a result, without guidance on what sets manipulation apart from deception and other forms of influence, it is also challenging to formulate what type of harm manipulation is or can result in.

The connection to (digital) vulnerability is made especially clear in Article 5(1)(b). This article repeats the language of Article 5(1)(a), but instead of mentioning "purposefully manipulative and deceptive techniques, the Article 5(1)(b) mentions

> "An AI system that exploits any of the vulnerabilities of a person or a specific group of persons, [...]".

From a digital vulnerability perspective, the phrasing of this article seems promising since it explicitly moves beyond the 'non-vulnerable average consumer *versus* the vulnerable consumer' framing. Explicit attention is paid to the ways in which not only (semi-)permanent characteristics, but also particular (temporary) situations can render people (temporarily) vulnerable. What is curious, however, is the decision to draft two separate articles, one on manipulative AI systems (5(1)(a)) and one on AI systems exploiting vulnerabilities (5(1)(b)). This raises the question how the relationship between manipulation and vulnerability is understood by the legislator. Most philosophical conceptualizations of manipulation emphasize how manipulation is predicated precisely on the deliberate exploitation of vulnerabilities in order to make targets serve the ends of the manipulator. Seen from this perspective, it would stand to reason to see the threat of manipulative AI systems and the threat of AI systems exploiting vulnerabilities as one and the same threat – whenever an AI system is manipulative, it will necessarily also (seek to) exploit vulnerabilities. The fact that the exploitation of vulnerability is explicitly mentioned in a separate article, raises the question how manipulation is understood by the legislator if manipulation is also seen as distinct from the exploitation of vulnerabilities?

With the harm requirement present in the AI Act, a further question raised is whether we should be (mainly) concerned with *manipulation itself* as a harm, or with harms that can be the result of manipulation. Because we lack an underlying theory of manipulation, it also remains unclear how the relationship between manipulation as an undesirable form of influence and harm should be understood.

Critical commentary

A common thread in both the DSA's and the AI Act's incorporation of manipulation and vulnerability language is the inability to provide conceptual clarity on not only the meaning of these concepts, but also their interrelation. The dominant philosophy seems to be that in order to regulate phenomenon X, one should explicitly mention that X is in fact forbidden. If that approach is adopted without doing the necessary underlying conceptual work, this seemingly straightforward approach is bound to fail. At a minimum, there should be some clarity on what it is about the phenomenon of manipulation that makes it manipulation. Because if it is not clear how manipulation differs from, e.g., persuasion, deception, or dark patterns, it also does not help to write the term manipulation into law as the term will not help us distinguish between phenomena.

The urge to mention manipulation explicitly in new legislation is understandable given the popularity of the term in popular critical discourse. However, precisely because of the conceptual and definitional unclarities around the term, it could be wiser to opt for an approach where manipulation is addressed indirectly. One can, for instance, address some of the possible (necessary) preconditions for manipulation without explicitly conceptualizing manipulation. Another option is to rely on existing legal concepts that can be used to 'capture' manipulation concerns.

The Unfair Commercial Practices Directive (UCPD) is an informative example. This Directive precedes the recent turn to manipulation as a dominant concern in the digital economy, so the directive doesn't thematise or even mention manipulation. Still, the Directive contains a lot of interpretational resources to address manipulation in the consumer-vendor relationship.[16] Put briefly, the core aim of the UCPD is to "keep and maintain the consumer's autonomy".[17] If there is one value that is clearly threatened by manipulation, it is personal autonomy. So, manipulation worries are very relevant in the UCPD framework. If we look at the specific articles of the UCPD, especially Articles 8 and 9 dealing with aggressive practices contain a lot of material to understand and capture manipulative commercial influences. For example, the concept of 'undue influence'[18] plays a key role, as does the circumstance of vendors using an asymmetrical power relation to apply to undue influence to exploit vulnerabilities or circumstances of consumers. The attentive reader will have already noticed that without ever mentioning the concept of manipulation, the UCPD approach to aggressive commercial practices already captures most of the elements of a manipulation relationship.

All of this is not to say that the DSA and the AI Act should have opted for the UCPD approach. The UCPD is merely meant to show that one does not have to explicitly mention manipulation to capture manipulation worries.

Challenges and Potential Shortcomings of the Current Approach

The digital vulnerability framework highlights the relational and architectural nature of vulnerabilities in the digital economy. This perspective adds a certain dynamism and fluidity to (the approach to) vulnerabilities. Consumers can move in and out of states of vulnerability, and different digital environments can either trigger or exploit vulnerabilities differently. This dynamism is mirrored in our thinking about manipulation. The design of manipulative influences through digital choice environments is greatly helped by the agile nature of those same choice environments, which allows for the constant explorative search and iterative testing of the most efficacious manipulation techniques.

The architectural nature of digital vulnerabilities – and their exploitation for manipulative influences – also implies the importance of critically analysing the organizations that enable digital

16 For an elaborate analysis along these lines, see Sax, M. (2021) *Between Empowerment and Manipulation*. Kluwer.
17 Micklitz, H.-W. (2006). The General Clause on Unfair Practices. In. G. Howells, H.-W. Micklitz & T. Wilhelmsson (Eds.), *European Fair Trading Law: The Unfair Commercial Practices Directive* (pp. 83–122), p. 104.
18 Defined in Art 2(j) UCPD.

vulnerability exploitation *in their entirety*. Put differently: throughout the *entire stack* of service providers that deal in digital vulnerabilities and manipulation points of intervention can and should be found. With "stack" we refer to the fact that a digital choice environment is the result of combining (or stacking) a number of inter-related technical or organisational processes at different levels within and outside a company or organisation, involving a multitude of actors that decide about select parts of the service architecture. The user will often only see the public-facing user interface, but the fact that the user is presented with a particular service or user interface is the result of diverse design decisions at the operational, development, business or infrastructure level, or the result of decisions of external actors, such as standardisation bodies. For example, optimization logics permeate the entire stack. Such logics are decided on by management, but can inform every part of the organization down the line. It informs the KPIs that structure business decisions. It informs which user data are to be collected, how models are trained by those (and other) data to be rendered productive towards the optimization logics. It informs how the user interface – with all its features – are not only designed but constantly redesigned. This also implies that the optimization logics inform which (often iterative) software design philosophy is embraced. The optimization logics which inform all of the above will even determine which people end up being hired to work on, again, all of the above. Put simply: every layer of the stack that makes up a digital service should be a potential target of regulatory intervention if one takes digital vulnerability and manipulation seriously.

The inherent fluidity of digital vulnerability, as well as the need for a full stack approach to the manipulative exploitation of digital vulnerabilities, does raise the question how these concerns can be operationalised in static legal provisions. To be fair, the realization that addressing digital vulnerability and manipulation requires a wide, stack-like approach seems – albeit partly and indirectly – to be present in Article 25 of the DSA. The Article mentions that "Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates". The "design, organise or operate" can indeed be read as an attempt to capture not just specific, isolated surface-level implementations, but also address the underlying organization. This broad reading is, however, directly limited again by only focusing on "online interface" which is just one part of the stack, and not typically the part in which decisive service design choices are made.

The phrasing of Article 25 DSA thus exemplifies the operationalisation challenge at hand. A vague and indirect gesture towards a stack-like approach is made, but the Commission ultimately fails to actually spell this approach out. In a more general sense, it would be beneficial if the legislator managed to tie piecemeal legislation that addresses different layers of the stack together in a wider, more coherent narrative. For example, data protection law addressing data practices and unfair commercial practices law addressing undue influences exerted on consumers both contain the legal resources to be part of a larger stack-like approach to manipulative digital consumer environments. Another example is the prohibition in Article 5 (2)(b) DMA to "combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper". Limiting the ability to combine data from different services also limits the possibility of making inferences which again contributes to an asymmetrical relationship in which a company has much more knowledge about the consumer than the consumer about the company (and what it knows about him). Yet another example is Article 6 (3) DMA according to which designated gatekeepers must enable consumers to easily change default settings in a virtual assistant that directs or steers end users to produce and services of that gatekeeper. This is an example of a provision that reaches further down the stack to the operational and development

level. In other words, sprinkled across the emerging regulatory framework are different behavioural, structural and design requirements that address different aspects or layers of a digital choice environment and, doing so, tackle some of the underlying digital asymmetries that enable manipulation and exploitation of digital vulnerability in the first place. But when only dealt with separately, dealing with separate sub issues in isolation and without a more coherent approach, it will remain difficult to get into focus how the stack *as a whole* enables the production and exploitation of digital vulnerability and manipulative designs, or how the law can play a role in remedying the underlying structural asymmetries.

The stack approach is also useful in thinking about monitoring compliance and enforcement of the provisions of regulations like the DSA. For example, in order to monitor compliance with Article 25, competent authorities would need to look further than the design of the user interface, and also require information about the underlying algorithmic models, business decisions regarding optimisation decisions, user testing, input data, etc. In this context it is striking that Articles 67–69 of the DSA do already give the European Commission far-reaching means to collect the relevant information regarding the general organisation of a service, the algorithmic level but also business and data handling practices of Very Large Online Platforms and Very Large Online Search Engines, but that the Commission's investigative powers are not mirrored in the entitlements for national competent authorities and Digital Services Coordinates under the DSA.[19]

The Looming Privatization of Consumer Protection

The emerging regulatory framework must provide regulators and various societal actors with the means to address situations of digital asymmetry and more generally, scrutinize private control over the digital infrastructure of our algorithmic society. At the same time, it also lays the foundations for a growing privatisation of digital consumer protection, putting private companies increasingly in a position to (try to) *make or break* consumer protection. Private ordering through contracts but also technology design is not a new phenomenon in consumer law and protection.[20] In parts, regulations such as the DSA and the DMA can be seen as attempts to subject private ordering to new levels of regulatory scrutiny.[21] At the same time, the emerging digital regulatory framework, and here in particular the DSA and the AI Act, also embrace and institutionalise the conditions for private companies to define and operationalise consumer protection in digital choice environments. Consider the following examples of how they lay the foundations for new levels of privatisation of consumer protection:

---

19 Compare Art. 49 – 51 DSA.

20 Bakos, Y., Marotta-Wurgler, F., & Trossen, D.R. (2014). Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts. *The Journal of Legal Studies, 43*(1), 1–35; Belli, L., & Venturini, J. (2016). Private Ordering and the Rise of Terms as Service as Cyber-Regulation. *Internet Policy Review, 5*(4); Reidenberg, J. (1997). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review, 76*(3), 553–594.

21 For example, as part of the systemic risk monitoring and mitigation obligations under Articles 34 and 35 specifically include an obligation to monitor terms and conditions upon their potential to create systemic risks, and where necessary, adjust those. Another example is Article 14(3) of the DSA, ordering providers to take into regard the rights and legitimate interests of users when enforcing their terms and conditions. Article 14 (3) DSA is, at the same time, also an example of how the DSA continues to leave acknowledge and even legitimate the use of contracts for private ordering by not submitting the terms and conditions themselves to regulatory scrutiny, see Quintais, J.P., Appelman, N., & Ó Fathaigh, R. (2023). Using Terms and Conditions to Apply Fundamental Rights to Content Moderation. *German Law Review, 24*, 881–911.

A first example are the systemic risk provisions in the DSA, and more generally the risked-based approach in the AI Act. Under Articles 34 and 35 in the DSA, it is an obligation of Very Large Online Platforms and Very Large Online Search Engines to 'diligently identify, analyse and assess' any systemic risks that are the result of the design or functioning of the digital choice environments they operate, including risks to a high level of consumer protection, and decide on the necessary mitigation measures. The DSA leaves it in the first place large discretion of VLOPS and VLOS to decide a) what risks to look into, b) interpret what a 'high level of consumer protection' entails, c) what metrics to use in testing their systems and d) what effective mitigation measures are.[22] Similarly, under the proposed AI Act it is the responsibility of the developers of high-risk AI systems to conduct a risk assessment. It is here that the problem of un(der) defined concepts such as vulnerability or manipulation become obvious: in the absence of a clear definition of what manipulation entails how will VLOPS or VLOS be able (or even attempt to) identify how their algorithmic systems engage in unethical or unlawful manipulation? Powerful commercial players in the digital economy will have to start engaging with increasingly important yet un(der)defined concepts such as (digital) vulnerability and manipulation.

The second example is the reliance on due diligence obligations and code of conducts (as the results of self- or co-regulation). One instrument in the DSA to "contribute to the proper application" of the regulation is voluntary codes of conduct, for example, in the area of systemic risks.[23] The Commission and the Board "shall aim to ensure that the codes of conduct clearly set out their specific objectives, contain key performance indicators to measure the achievement of those objects and take due account of the needs and interests of all interested parties, and in particular citizens, and in case of failure the Commission and board "may invite signatories to the codes of conduct to take the necessary action". In light of the interests and fundamental rights at stake, the phrasing of this paragraph signals polite resignation and reliance on the goodwill and expertise of technology providers. Even more striking is the approach under the AI Act where codes of conduct are the primary means of governance of all non-high risk AI systems (including most applications in the consumer sector).[24]

The third example is the prominent role of standardisation and adherence to (technical) standards as a form of demonstrating compliance with both, the DSA and the AI Act.[25] For example, according to the AI Act, high-risk AI systems that are in conformity with harmonised standards shall be presumed to be in conformity with the requirements of the AI Act.[26] The result is that (technical) standardisation bodies will play a critical role in interpreting and operationalising the regulatory framework, including the rules meant to protect vulnerable consumers against misleading or deceptive practices. The lack of necessary expertise in fundamental and

22 Leerssen, P.J. (2023). *Seeing What Others Are Seeing: Studies in the Regulation of Transparency for Social Media Recommender Systems*, PhD dissertation, University of Amsterdam; Leerssen, P.J. (2023). Counting the Days: What to Expect from Risk Assessments and Audits under the DSA – and When?. *DSA Observatory blog*, https://dsa-observatory.eu/2023/01/30/counting-the-days-what-to-expect-from-risk-assessments-and-audits-under-the-dsa-and-when/; Mantelero, A. (2022). Fundamental Rights Impact Assessments in the DSA: Human Rights and the Risk-Based Approach of the New EU Regulations on the Digital Society. *Verfassungsblog*, https://verfassungsblog.de/dsa-impact-assessment/.

23 Article 45 DSA.

24 Article 69 draft AI Act.

25 See for a comprehensive analyse the following excellent report: Micklitz, H.-W. (2023). *The Role of Standards in Future EU Digital Policy Legislation. A Consumer Perspective*. Report for BEUC (The European Consumer Organisation). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf

26 Article 40 draft AI Act (EC, EP and Council version).

human rights, and adequate representation of the interests of consumers has been flagged by academics and civil society as a serious concern.[27] Again, the failure to clearly define concepts such as vulnerability or manipulation can be instrumental in the failure of the regulatory framework to realise the values it seeks to protect.

The new playing field that emerges is one where we can expect the big commercial players that are the subject of regulation are also the ones that will proactively try to shape the interpretation and implementation of the un(der)defined concepts. The eventual definition and legal operationalisation of, e.g., 'manipulation' that will be settled on matters to the opportunities as well as constraints for online service providers. So absent guidance on how manipulation is supposed to be understood legally, one should expect the addressees of the new legislative agenda to volunteer interpretations that are especially business-friendly.

The privatization of consumer protection raises new challenges for consumer law and policy:

- new roles: with their rich expertise of consumer law and consumer concerns, consumer organisations will have an important role in issuing guidance for the concretisation of abstract terms such as vulnerability or manipulation by private organisations but it also can be necessary to consider new roles, for example representing the interests of consumers in standardisation efforts or the auditing of mandatory risk assessments from the perspective of consumer protection.
- new powers: One question around the privatisation of consumer protection is how far the authority and intervention rights of consumer organisations go, and if they are sufficient to monitor compliance of privatised acts of consumer protection. The question of powers and the reach of existing tools of consumer enforcement is particularly pertinent in situations in which no concrete consumer harm is materialised (yet) but the way private companies interpret and operationalise consumer protection does not take into account sufficiently the interests of consumers.
- new forms of cooperation: with the privatisation of consumer protection, new forms of alignment and cooperation between consumer authorities and private companies will emerge and be necessary. This creates new opportunities, for example for knowledge exchange and learning, but also new challenges for example of how to protect consumer authorities' independence.

The Consumer-Citizen: the Crumbling Distinction between the Consumer and the Citizen

The boundary between the consumer and the citizen is becoming increasingly porous. Today's digital marketplace is also the marketplace of ideas and podium of public discourse. The example of political microtargeting is useful to illustrate to what extent public and private functions, and consumers and citizens conflate. Commercial targeting practices are increasingly also

27 Micklitz, H.-W. (2023). *The Role of Standards in Future EU Digital Policy Legislation. A Consumer Perspective*. Report for BEUC (The European Consumer Organisation). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf; Ebers, M. (2022). Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act. In DiMatteo, L.A, Poncibò, C., & Cannarsa, M. (Eds.) (2022), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and* Ethics, (pp. 321–344) Cambridge University Press; Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach. *Computer Law Review International, 22*(4), 97–112.

used by political campaigns for political (micro)targeting,[28] relying on the same platforms (like Google and Facebook), even the same advertising auctioning system and the same data.[29] Political campaigns increasingly rely on the tools developed for commercial targeting practices and the same commercial parties (and here in particular the Google and Facebook duopoly) to spread their messages. The consequence is that political advertising is turning, at least from the perspective of platforms, into 'just another form of advertising', and it is becoming difficult to distinguish the citizen from the consumer. The blurring boundaries between the protection of consumers and citizens is also apparent in the way the AI Act is expanding the concept of vulnerability (see above) but also provisions like Article 25 DSA. According to Art. 25 (2) DSA, "[t]he prohibition in paragraph 1 shall not apply to practices covered by Directive 2005/29/EC or Regulation (EU) 2016/679". Effectively that leaves non-commercial forms of targeting as the main area of application of Art. 25 DSA. The crumbling distinction between citizen and consumer makes questions about the role and mission of consumer protection authorities and consumer law more pressing. Is it still realistic to distinguish between commercial and non-commercial communication? How far does the mandate of consumer protection authorities go? Do they increasingly also have a societal role, to not only consider the interests of consumers but also more collective and societal interests and fundamental rights? And what forms of cooperation are necessary between the different regulators?

Conclusion

The EU's new legislative agenda for the digital society is certainly ambitious. The package of the DSA, DMA, AI Act, and PAR is clearly aimed at addressing a wide range of issues and, moreover, tries to do so in a more structural manner. It is clear that the EU sees the exploitation of vulnerabilities and manipulative digital choice environments as serious systemic risks that warrant a systemic response. The laudable ambitions do, however, also result in a somewhat fragmented approach. In terms of vulnerability, the various legislative initiatives move between, on the one hand, a continuation of the 'average consumer versus the vulnerable consumer' approach, and, on the other hand, the first contours of a wider approach to *digital* vulnerability with more emphasize on the relational, architectural, and privacy-related nature of vulnerability. Manipulation, in turn, is making an appearance in the DSA, the AI Act, and the PAR. The appearance of manipulation of consumer and citizen behaviour as an explicit concern in legislation is unfortunately not yet accompanied by conceptual and/or definitional clarity. Nowhere is manipulation defined, and in the recitals and articles where it appears its relation to other problematic forms of influences (e.g., deception, dark patterns, nudging) remains unclear. The unclarities concerning the underlying legal theories and conceptualizations of (digital) vulnerability and manipulation are somewhat worrisome seen from the perspective of *private ordering*. The combination of 1) undertheorised and underdefined key concepts in combination with 2) an increased reliance on due diligence obligations and codes of conduct to give shape to these key concepts, potentially places quite some power in the hands of private companies to volunteer and propagate interpretations of (digital) vulnerability and manipulation that are above all commerce-friendly. These worries on private ordering in combination with vague concepts are, in turn, further exacerbated by the fact that the distinction

28 Dobber, T., Trilling, D., Helberger, N., & De Vreese, C.H. (2017). Two Crates of Beer and 40 Pizzas: The Adoption of Innovative Political Behavioural Targeting Techniques. *Internet Policy Review, 6*(4), 1–25.

29 Helberger, N., Dobber, T., & De Vreese, C.H. (2021). Towards Unfair Political Practices Law: Learning Lessons from the Regulation of Unfair Commercial Practices for Online Political Advertising. *JIPITEC, 12*, 273–296.

between the consumer under consumer law and the citizen as part of a democratic society is increasingly broken down. Take, for instance, the PAR. Political advertising on highly commercial platforms is both an issue of targeting consumers in commercial environments *and* an issue of targeting citizens involved in democratic processes. As digital choice environments increasingly break down contexts once conceived of as distinctive spheres, so do the recent legislative initiatives increasingly address people as citizen-consumers that play different roles in different context, all at the same time. The resulting conceptual messiness is understandable, but also leaves much room for improvement.

III. Toward Constructive Optimisation: a new perspective on the regulation of recommender systems and the rights of users and society

Laurens Naudts, Natali Helberger, Marijn Sax, Michael Veale[1]

1 For its conceptualization of self-development and self-determination as digital values, this study builds upon Naudts, Fair or Unfair Differentiation? Reconsidering the Concept of Equality for the Regulation of Algorithmically Guided Decision-Making (Doctoral Dissertation, KU Leuven: Leuven, 2023). In reference to: Iris Marion Young, Justice and the Politics of Difference (Princeton University Press 1990) and Iris Marion Young, Inclusion and Democracy (Oxford University Press 2002)

Introduction

How should we regulate systems designed to optimise digital environments and interactions?

One needs to develop at least two critical perspectives to answer such a question. First, relative to what normative standards should optimisation be held? Second, how should regulation understand the tools of optimisation, such as 'recommender systems'? This study develops an approach to both questions and integrates the corresponding perspectives into one answer.

The study is divided into three main parts. In **Part 1** a normative framework – centred around the values of self-development and self-determination – is elaborated as an interpretational resource to understand better how optimisation can be meaningful. When it comes to recommender systems, there is a need to move beyond naïve approaches, which implicitly assume that 'the recommender system' is an identifiable, discrete 'unit' that can be addressed and regulated as such. Instead, we propose to conceptualise and evaluate recommender systems through a so-called "stack approach". This is the purpose of **Part 2**. The envisaged "stack approach" embraces the insight that beyond the surface interface level, recommender services are the result of different interactions, operations and layers, that are both social and technical in nature — software, hardware, infrastructure, organisational, design principles, and so on. All these parts work in concert to, ultimately, create particular tools, interfaces, and functionalities. Finally, **Part 3** combines the normative framework of Part 1 and the stack approach of Part 2 for a critical analysis of the current approach to the regulation of recommender systems under the DSA, and for developing constructive suggestions of how to better account for the legitimate interests of users and society. Recommender systems should be regulated addressing *every layer of the stack*. Put simply, analysing and regulating the recommender system is not (only) about analysing and regulating the actual recommender engine, i.e., the software systems designed to fulfil optimisation logics, or the interface people interact with. The net should be cast wider. Optimisation goals determined by management, KPIs determined by business departments, performance reviews, hiring practices, data collection and analysis practices, iterative software design philosophies, UX/UI design choices, data training models, and so on, should all be incorporated into the bread and butter of recommender system regulation.

This study, then, combines a more realistic, helpful approach to recommender systems as socio-technical artefacts with an original theoretical perspective on the normative standards we should hold optimisation systems to. In this report, we formulate a set of overarching recommendations that could guide future regulatory amendments. In an upcoming update and annex to this report, we will take up this exercise ourselves, and demonstrate how our model can be translated into concrete regulatory provisions. At the same time, we offer the stack approach as a toolkit to the reader: a starting point for reflection toward a more healthy and fair digital eco-system. In this context, it should be noted from the outset that the more realistic stack approach can be as enlightening as it can be overwhelming. The benefit of the approach is that it allows for a very wide, structural approach that cuts across the *entire* recommender value-chain or stack to show how a wide range of EU legislation can be used to regulate various elements of this ecosystem. The resulting analysis can, at the same time, also lead to what feels like a rather fragmented story – at least in terms of presentation. To further add to this enlightening complexity, the stack approach allows one to address separate layers of the stack individually, but one can also show how several layers (can) interact with one

another in the regulatory context, or how 'whole stack provisions' address the entire stack. In short, the stack's *analytical* modularity allows for a very all-encompassing mosaic approach that can address several analytical levels at the same time. Its inherent complexity is a feature, not a bug. This should be kept in mind when reading this exploratory study.

A. Recommenders and Society

Physical and digital settings are increasingly subject to systems that attempt to optimise humans and their interactions.[2] In various public and private domains, systems affect the content people see, whether advertisements or commercial product offerings, audio-visual entertainment, news media, potential professional and personal connections, etc.[3] In short, recommender systems have become integral to structuring the digital society. In this function, they actively co-mediate people's social and economic affordances.[4] Their underpinning logic however, is one of 'capture' and 'traps', where through their interaction with these systems, individuals' behaviours are codified and computed, and their actions and attention are steered into certain business logics that can be difficult to escape from.[5] Given their ubiquity, recommender systems can, in theory, help with information overload — helping maximise user freedom, filtering content that is more catered to the needs and desires of the recipient, thereby reducing the time they would otherwise lose when confronted with cognitive overload.[6] This was the dream of early proponents of these systems, where 'adaptive hypermedia' would allow users to achieve their goals more easily.[7] On a societal level, recommender systems used by news websites can incorporate diversity metrics to promote voices that are otherwise left unseen and unheard. Yet, those same data-driven techniques can also be used in the opposite direction. Individuals and groups can find their social and economic practices captured and subject to manipulation.[8] Already marginalised groups can be rendered even more invisible.[9]

Recommender system's alignment with democratic norms and values, fundamental rights, freedoms and interests, greatly depends upon the optimisation strategies followed within them. Yet, as Kulynych and others warn, when they are "developed to capture and manipulate

---

2 Bogdan Kulynych and others, 'POTs: Protective Optimization Technologies', *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (ACM 2020) <http://dl.acm.org/doi/10.1145/3351095.3372853> accessed 29 January 2020.

3 Max van Drunen, Brahim Zarouali and Natali Helberger, 'Recommenders You Can Rely on: A Legal and Empirical Perspective on the Transparency and Control Individuals Require to Trust News Personalisation' (2022) 13 JIPITEC <https://www.jipitec.eu/issues/jipitec-13-3-2022/5562>. Paddy Leerssen, 'Seeing What Others Are Seeing: Studies in the Regulation of Transparency for Social Media Recommender Systems.' (2023).

4 Iason Gabriel, 'Towards a Theory of Justice for Artificial Intelligence' (2022) 151 Daedalus 12.

5 Nick Seaver, 'Captivating Algorithms: Recommender Systems as Traps' (2019) 24 Journal of Material Culture 421; Philip E Agre, 'Surveillance and Capture: Two Models of Privacy' (1994) 10 The Information Society 101.

6 See John Danaher, 'Freedom in an Age of Algocracy' in Shannon Vallor (ed), John Danaher, The Oxford Handbook of Philosophy of Technology (Oxford University Press 2022) <https://oxfordhandbooks.com/view/10.1093/oxfordhb/9780190851187.001.0001/oxfordhb-9780190851187-e-16> accessed 4 May 2022.

7 Peter Brusilovsky, 'Adaptive Hypermedia' (2001) 11 User Modeling and User-Adapted Interaction 87.

8 See for instance: Marijn Sax, *Between Empowerment and Manipulation: The Ethics and Regulation of for-Profit Health Apps* (2021) <https://dare.uva.nl/search?identifier=52225d37-e7e1-4883-9dab-a3f5d3a063d8> accessed 18 September 2023.

9 See for example: Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York University Press 2018) <http://www.degruyter.com/document/doi/10.18574/9781479833641/html> accessed 8 December 2021; Catherine D'Ignazio and Lauren F Klein, *Data Feminism* (The MIT Press 2020) <https://mitpress.mit.edu/books/data-feminism>; Sanne Vrijenhoek and others, 'Recommenders with a Mission: Assessing Diversity in News Recommendations', *Proceedings of the 2021 Conference on Human Information Interaction and Retrieval* (ACM 2021) <https://dl.acm.org/doi/10.1145/3406522.3446019> accessed 7 September 2023.

behaviour and environments for the extraction of value, [they introduce] broader risks and harms for users and environments beyond the outcome of a single algorithm within that system." [10] While these systems are commonly called 'personalised', this term is misleading. All too often, 'personalisation' masks self-serving optimisation. They rarely treat individuals as individuals, focussing on their contribution towards aggregate outcomes. They rarely allow users to set their own 'personal' goals. Likewise, the systemic threats recommenders pose to democratic and societal interests, interactions and structures are too often overlooked. Instead, the goals are those set by firms with decisional power over the implementation and control over the infrastructural, data and knowledge resources needed for their design. Sometimes, these firms are traditional economic actors, but often, they are intermediaries or 'platforms', where both sides of a transaction are relatively powerless compared to those setting and shaping the rules of engagement.[11]

The importance of socio-technical systems optimising people and environments means that they should be designed to align with the citizen-consumer and the democratic and social values the EU promotes, from the outset and from the cradle to the grave.[12] Such ambitions are also reflected in the European Declaration on Digital Rights and Principles, which promotes human-centricity and freedom of choice, solidarity, inclusion and participation in the democratic process as key commitments in the EU's digital transformation.[13]

B. Challenges in Realising Constructive Optimisation: Motivating our Approach.

To realise the lofty ambitions of a just digital future, several challenges must be overcome. First, among the various values we could choose from as leading technological advancements, which and whose to prioritise? This is why in Part 1 of this study; we offer a theoretical framework which serves as an indispensable background to navigating questions on values. The digital ecosystem is comprised of multiple actors and groups who each might pursue differing and competing interests and values. Our current information society is further characterised by significant asymmetries in power over (physical and digital) infrastructures, design choices, expertise, knowledge of consumers, and data creation processes. One of the main current tools of optimisation online, the recommender system, therefore, often operates behind a

10 Bogdan Kulynych e.a., 'POTs: Protective Optimization Technologies', in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (FAT* '20: Conference on Fairness, Accountability, and Transparency, Barcelona Spain: ACM, 2020), 177–88, https://doi.org/10.1145/3351095.3372853.moral, social, and political impact that digital systems have on populations through solutions that can be applied by service providers. Fairness frameworks do so, in part, by mapping these problems to a narrow definition and assuming the service providers can be trusted to deploy countermeasures. Not surprisingly, these decisions limit fairness frameworks' ability to capture a variety of harms caused by systems. We characterize fairness limitations using concepts from requirements engineering and from social sciences. We show that the focus on algorithms' inputs and outputs misses harms that arise from systems interacting with the world; that the focus on bias and discrimination omits broader harms on populations and their environments; and that relying on service providers excludes scenarios where they are not cooperative or intentionally adversarial. We propose Protective Optimization Technologies (POTs

11 Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

12 Natali Helberger, 'On the Democratic Role of News Recommenders' (2019) 7 Digital Journalism 993; Marijn Sax, 'Algorithmic News Diversity and Democratic Theory: Adding Agonism to the Mix' (2022) 10 Digital Journalism 1650.

13 European Declaration on Digital Rights and Principles for the Digital Decade, see also: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#digital-rights-and-principles; https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7683

veil of opacity.[14] Consequently, it has become increasingly difficult to assess whether these socio-technical systems pursue merely self-serving interests or comprehensively consider people's fundamental rights, democratic values and social well-being. It has been difficult even to understand the contribution of these systems to outcomes both online and offline.

Moreover, in choosing specific values over others, we must also consider the inherent trade-offs that often need to be made to safeguard the interests of the individual on the one hand and those of (social) collectives on the other. Maximising individual user preferences might come at the cost of content diversity.[15] In certain domains, like news provision, optimising for corporate goals might deny certain social groups the visibility needed to organise themselves politically. Likewise, pursuing short-term goals, like personal relevance-based metrics, might ultimately have a detrimental long-term impact. For example, it might diminish people's opportunity to encounter unexpected voices or perspectives and develop new interests. Likewise, if consumption is encouraged, what is the impact thereof on the environment? Tensions between interests will undoubtedly arise, and answers on how they can be resolved depend upon one's normative and political outlook. Still, when choosing the values we want to promote within the digital environment, we can take stock of these complexities. More specifically, we need values that enable us to capture, reflect on, and address these conflicts as they emerge; values that recognise how people's wellbeing is not determined in light of one particular preference, need or desire, but shaped by a multitude of interweaving factors. Only then will we be able to steer optimisation systems and recommender systems to work in favour of — or at least not to the significant detriment of — the broader health and welfare of the information ecosystem.

Second, to ensure a healthy digital environment, we must address its complexity. This is what Part 2 of the study is focused on. Optimisation systems have 'many hands' involved and are not as easy to steer and regulate as some other phenomena.[16] We need to understand how recommender systems interact with their surroundings to assess their possibilities and limitations, risks and benefits, the conditions under which they can do good, and the conditions that impede that goal. Optimisation systems are already soaked in EU regulation, but we have to ask whether these initiatives hit the right targets, work together in concert, and achieve their aims. Existing technology laws, such as the Digital Services Act or the GDPR, (should) exert influence on design, development and deployment, but in practice, may not be aligned or refined enough to do so. Opportunities that exist under existing law may not be taken full advantage of. In mapping how recommenders, and those who control their value-chain, interact with and affect their surroundings, we can assess whether current laws adequately capture the (systemic) risks these systems threaten to impose onto citizens, and in case of regulatory failure, propose legislative recommendations to mitigate future harm.

---

14 Naudts (n 1).

15 Helberger (n 12).

16 A Feder Cooper and others, 'Accountability in an Algorithmic Society: Relationality, Responsibility, and Robustness in Machine Learning', *2022 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2022) <https://dl.acm.org/doi/10.1145/3531146.3533150> accessed 23 June 2022; Helen Nissenbaum, 'Accountability in a Computerized Society' (1996) 2 Science and Engineering Ethics 25; Jennifer Cobbe, Michael Veale and Jatinder Singh, 'Understanding Accountability in Algorithmic Supply Chains', *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2023) <https://dl.acm.org/doi/10.1145/3593013.3594073> accessed 14 June 2023. Natali Helberger, Jo Pierson and Thomas Poell, 'Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34 The Information Society 1.

An important connection between Part 1 and Part 2 is the thematisation and capturing of *relational dynamics*. As one can see directly below, in Part 1 we formulate a theoretical framework which explicitly acknowledges the *relationality* inherent in our current technological predicament. Various stakeholders interact with each other, citizens interact with technology and do so differently in different contexts. Likewise, the values and principles we might want to see realised, can play out differently in each of these constellations. Part 2 also works with this relationality by introducing the stack approach which is aimed precisely at analytically disentangling the relationships that exist within and between the many layers of the stack. By laying bare these relational dynamics, the role the (constitution of) technology plays in societal relational dynamics can be better analysed. It's relationality all the way down.

This study addresses these challenges via the following strategy. In Part 1, we first argue that recommender systems can only be made sense of when viewed in light of society's structural, institutional and relational dynamics. Second, we posit self-development and self-determination as leading values that should inform recommender systems' development, integration and regulation. In Part 2 we lay out a framework to better understand the structural and social dynamics that give meaning to and are influenced by recommender systems. To this end, we propose visualising these socio-technical systems through a *stack* of interrelated decision-making moments, infrastructural capacities, steps and processes. In part III, we analyse the current regulatory approach to recommender systems through the lens of constructive, accountable and societally aligned optimisation across the entire stack. Throughout this analysis, we make recommendations for tweaks, initiatives and improvements.

PART 1: Normative Foundations

1.1. Relational Dynamics

For citizens and consumers, recommender systems perform an active mediating role in navigating the digital society. In attributing recommender systems as active co-mediators, we acknowledge a certain fluidity to their functioning. Their interventions are dynamic, and this dynamicity occurs alongside three broad dimensions.

First, recommender systems are informed by an interplay of interpersonal, institutional, and socio-technical relationships. For example, recommender systems operate on data collected from a wider population. Those data might reflect the prejudiced beliefs and stereotypes held by society's members. The norms and values held by individuals, communities, professions and industries, might equally inform the choices during the design, development and deployment of recommender systems. Certain industries and fields might be characterised by a vehement belief in techno solutionism as the answer to all of societies woes.[17] At the same time, recommender systems must comply with the EU legislator's principles, norms and rules. And within these broader structures, actors in recommender systems take a wide variety of roles and perspectives.[18]

---

17 Abeba Birhane, 'Algorithmic Injustice: A Relational Ethics Approach', *Patterns (New York, N.Y.)* 2, nr. 2 (12 February 2021): 100205, https://doi.org/10.1016/j.patter.2021.100205.{\\i{}Patterns (New York, N.Y.

18 For instance, as *data controllers* they are obliged to incorporate data protection by design standards. Likewise, recommender systems are rightfully expected not to act in discriminatory ways. As *providers of AI systems* (and depending on the nature of the final AI Act) they may be obliged to treat their systems as (high-)risk. As *contractual*

Second, and upon deployment, citizens and consumers interact with recommender systems. As recommendations are provided, they simultaneously adapt to their user's preferences. This also means that users, through their interaction and the data they provide, contribute to the performance and improvement of a recommender system.[19] Yet, dependent on the goals imbued within the system, the consumer is expected, or steered, to behave and act in specific ways. Individuals on the other side of optimisation systems give a lot, including the labour of navigating them and the externalities they create, but have little say in how they function, or mechanisms to have them aligned with their own interests.

Third, recommenders maintain an interactive relationship with the individual citizen consumer and draw from and co-shape the (social) position of consumers vis-à-vis other consumers. Citizens are grouped together and thus positioned in a relationship with each other based on their habits, preferences or other monitorable behaviours. Depending on the context and circumstances, the latter could impact, both positively and negatively, the social positioning of individuals and the groups they are a member of. For instance, the offering to young men of clothing embroidered with slogans affirming stereotyped gender patterns could damage women's social position. They mix the economic and the expressive and produce and reproduce socioeconomic structures. Regulating optimisation is a hazardous business because the potential goals are varied, contextual, dynamic and political. Yet to leave them insufficiently steered and regulated leaves these significant choices in solely private hands.

1.2 Self-Development and Self-Determination as Digital Values[20]

Drawing from Iris Marion Young's political philosophy, we put self-determination and self-development as the values a just society should promote to safeguard people's dignity and equal moral worth. Due to optimisation systems contribution to the structuring of society, these principles and values should be respected throughout the digital value chain if they are to be realised. From a regulatory perspective, the objective should be twofold. Positively, regulators should maximise people's capacity for self-development and self-determination. Negatively, regulators should remove social and institutional barriers that can negatively impact people's access to self-development and self-determination. Those regulatory efforts can take various forms and target different actors. They can comprise technical design strategies, organisational requirements, procedural contestation measures, impact assessments, data audits, etc. Importantly, however, there is no one-size-fits-all solution.

Before analysing the regulatory efforts to govern recommender systems across the stack, we first establish the interconnected notions of self-development and self-determination and

parties in the AI supply chain, they may have interconnected obligations with cloud and infrastructural providers. Yet as *intermediaries* under the Digital Services Act, they may have both platform-related obligations while benefiting from certain immunities for the actions they take or content they host.

19 Balázs Bodó and others, 'Interested in Diversity' (2019) 7 Digital Journalism 206; Masoud Mansoury and others, 'Feedback Loop and Bias Amplification in Recommender Systems' (arXiv, 25 July 2020) <http://arxiv.org/abs/2007.13019> accessed 28 July 2023.

20 Drawing from Young's politics of difference and democratic theory, the ideation and application of both notions within the digital environment used in this study were first introduced in Naudts, *Fair or Unfair Differentiation? Reconsidering the Concept of Equality for the Regulation of Algorithmically Guided Decision-Making (Doctoral Dissertation, KU Leuven: Leuven, 2023)*, Chapter. 6, Socio-Relational Conceptualisations of Equality and Algorithmically Guided Decision-Making. Iris Marion Young, Justice and the Politics of Difference (Princeton University Press 1990) and Iris Marion Young, Inclusion and Democracy (Oxford University Press 2002)

the social ambitions these values seek to realise. Second, we want to position these values as social rather than purely individual.

1.2.1 Self-determination

The value of self-determination concerns people's ability "to participate in determining one's action and the condition of one's action."[21] To exercise this type of control, people need access to social and material resources which enable them to exercise choice.[22] Conversely, people do not have self-determination when others can arbitrarily interfere with their exercise of choice. Where individuals and groups are subject to external optimisation strategies, these practices and the systems involved, are perhaps best understood as affecting the mental, physical, social and material resources people need access to in exercising choice and control over the conditions that govern their lives.[23]

If designed carefully, there are situations where recommender systems could positively complement people's ability to exercise choice. For one, Danaher notes, they can help citizens 'identify and select among options that might (or might not) be conducive to [their] goals' because they 'filter choices and reduce the feeling of being overwhelmed.'[24] Yet without appropriate governance mechanisms, recommender systems can turn the online environment into a space of arbitrary or unchecked control.[25]

Following a republican perspective, the current position held by operators might enable 'algorithmic domination'.[26] Drawing from citizens' data, behaviour or other monitorable actions, recommender systems limit, replace or create the options, content and goods people see and access in favour of the goals of the optimisation.[27] This control over choice is problematic because it is *outsourced* without the citizen-consumers' deliberative engagement. Indeed, citizens often have little to no say, influence, or insight into what most recommender systems have been optimised for. Instead, the operators of recommender systems have been placed in a position where they can control the choices offered to citizens under their sole discretion and according to their preferences.[28]

Regulatory efforts should attempt to make the digital environment more favourable, inclusive and participatory as to include the interests of citizens, social groups, and society at large. Those efforts can take two strategies. First, regulators should enhance and broaden citizens' resources to exercise deliberate control over recommender systems.[29] And, where consumers agree to have their choices curated by others, they should understand the rules of engagement.

---

21 Iris Marion Young, *Inclusion and Democracy* (Oxford University Press 2002) 32 <http://www.oxfordscholarship.com/view/10.1093/0198297556.001.0001/acprof-9780198297550> accessed 7 October 2020.

22 Philip Pettit, *On The People's Terms: A Republican Theory and Model of Democracy* (Cambridge University Press 2012) 45.

23 Naudts (n 1).

24 Danaher (n 6).

25 E Gräf, 'When Automated Profiling Threatens Our Freedom': (2017) 3 European Data Protection Law Review 441, 450.

26 Philip Pettit, *Republicanism: A Theory of Freedom and Government* (Oxford University Press 1999) <https://www.oxfordscholarship.com/view/10.1093/0198296428.001.0001/acprof-9780198296423> accessed 29 February 2020; Pettit (n 22); Gräf (n 25); ibid; Danaher (n 6).

27 Gräf (n 25) 450.

28 The notion of operators should be broadly understood, referring to a wide variety of actors within the technology stack, including those who provide the infrastructural resources needed to maintain and sustain their functioning.

29 See also: Gräf (n 25).

People must understand the conditions under which curation takes place, have the opportunity to contest certain decisions that impact their choices, and, where possible, they themselves or their representatives should be able to participate in the design of recommender systems. It does bear explicit mentioning that the ideation of citizens as deliberate actors should not be interpreted as favouring disclosure and consent as the chosen regulatory solution. Quite the opposite. Among others, and as we show below, recommender systems are opaque, not simply because they are technically arcane but because their outcomes are the result of distributed decisions across an entire technological stack. There is no easy transparency fix. Even if citizens have been given some degree of control over how they navigate their digitally mediated environment, their doing so is often conditional upon someone else's goodwill: infrastructural and knowledge asymmetries characterise people's digital living space, those with the power to determine how and when recommender systems will be designed and deployed often can unilaterally decide how and when people's choices will be interfered with. Given these external constraints, it has become increasingly difficult for citizens to understand exactly what they would consent to. That does not mean that disclosure and consent cannot be appropriate under certain circumstances. In (complex) digital environments however, they can be too easily abused by operators to reallocate the responsibility in the incurrence of injustice and harm back to the citizen.

A better interpretation of the notion of self-determination is to further democratise the regulation of recommender systems, rather than have the rules of, and goals pursued by, optimisation unilaterally decided upon and imposed onto them. In other words, citizens should be given the possibility to co-determine how their living sphere will be mediated through digital technologies, rather than opt-in, through consent, to an environment, the conditions of its structuring, has already been predetermined for them. The effective ability for citizens to determine their actions and the conditions of their actions, must therefore be realised through a wide range of measures, which moreover, must be interpreted in line with the below-mentioned value of self-development.

Second, regulators should minimise and constrain operators in their ability to (deliberately) undermine the interests of citizens in pursuit of self-serving ones. These two regulatory strategies could moreover be combined by promoting inclusivity and active participation as part of regulatory governance strategies, whether they pertain to the broader infrastructures and architectures in which systems are embedded, the technical design choices and parameters that guide a recommender system's optimisation goals or the law-making process, including its enforcement, itself. In this context, it is also valuable for citizens to have access to meaningful alternatives. Where the digital environment is dominated by a select few actors, people's ability to choose a different service provider that offers other conditions for content recommendations is limited, and their freedom to exercise choice becomes further reduced. Moreover, in doing so, we can maximise the positive externalities recommender systems provide, such as their ability to filter choice to limit informational glut.[30]

1.2.2 Self-development

The value of self-development can be interpreted as people's ability to 'learn and use satisfying and expansive skills in socially recognised settings, and enable them to play and communicate

30 Danaher (n 6).

with others or express their feelings and perspectives on social life in contexts where others can listen.'[31] This value has been linked to the capability approach.[32] Under this approach, capabilities are understood as the substantial freedoms or opportunities people have to achieve alternative beings and doings.[33] Though people vary in their conception of the good life, in a pluralist society, people should be free to pursue what they deem valuable. And people only have a real opportunity to pursue their goals when they have access to the appropriate emotional, psychological, social, institutional and material supportive mechanisms to do so. Though material resources are an important benefactor, people's capacity to convert their opportunities also depends on their cultural and social positioning and recognition as equals.[34]

Once again, socio-technical systems act as an external (environmental) condition that can either limit or enhance people's ability to flourish. These systems help structure who is offered what type of content and when, and therefore also what content will remain invisible to whom. For example, whereas a price differentiation system can determine who has access to certain goods at more favourable prices (material resources), news recommenders can determine whose voices will be heard, and whose will be silenced (cultural and social). In turn, the choices underlying recommender systems affect people's interpretation and navigation of the digital society.

For example, imagine a mass-used video-on-demand platform whose recommendations promote programming that reinforces gendered stereotypes of women. In perpetuating prejudiced and generalised assumptions regarding the social position of women, such a recommender system could actively undermine women's capacity to 'develop their personal abilities, pursue their professional careers and/or make choices about their lives.'[35] Likewise, if news recommender systems never offer news content related to the struggles faced by marginalised or vulnerable communities, the average citizen might remain insensitive to their needs. In the worst case, those communities are rendered invisible, and their members unable to express themselves in socially recognised settings, such as public political discourse.

Self-development is at stake both from the substance of optimisation but also is affected by the conditions under which this optimisation can be controlled. Where controls around these systems exist but are in practice unusable or opaque, those resources to contest undesirable decisions might as well not be there. Such conditions require a consideration of the entire optimisation process, from top to bottom, to ensure individual citizen consumers, as well as the social groups they are a member of, are recognised and heard.

---

31 Young (n 1) 31–32; Iris Marion Young, *Justice and the Politics of Difference* (Princeton University Press 1990).

32 Amartya Sen, 'Equality of What?' (1979); Amartya Sen, *The Idea of Justice* (Belknap Press: Harvard University Press 2009); Martha C Nussbaum, *Creating Capabilities: The Human Development Approach* (The Belknap Press of Harvard University Press 2011).

33 Sen (n 32); Nussbaum (n 32); Ingrid Robeyns, 'The Capability Approach' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Winter 2016, Metaphysics Research Lab, Stanford University 2016) <https://plato.stanford.edu/archives/win2016/entries/capability-approach/> accessed 18 December 2019.

34 Young (n 31); Nancy Fraser, 'From Redistribution to Recognition? Dilemmas of Justice in a "Post-Socialist" Age' [1995] New Left Review 68; Amy Allen, 'Power and the Politics of Difference: Oppression, Empowerment, and Transnational Justice' (2008) 23 Hypatia 156.

35 https://www.ohchr.org/en/women/gender-stereotyping

1.3 Self-Determination and Self-Development as Social, Egalitarian and Structural Values

Self-development and self-determination should not be viewed solely as individual values but as values that represent, and are informed by, collective, social, egalitarian, and structural dynamics.

As the above examples illustrate, recommender systems can mirror and reinforce the (historical) prejudice, stereotypes and stigma faced by marginalised or otherwise vulnerable communities and their members. These types of injustice act as social, economic and institutional barriers that limit people's ability to be seen, heard, and recognised (self-development), which, in turn, undermines their capacity to exercise deliberative choice over the conditions that govern their life (self-determination). However, tackling prejudiced recommenders cannot be resolved through individual or isolated interventions alone. For instance, when confronted with a biased recommender system, an individual right to opt-out from personalisation does little to address the problem at its core. Without structural interventions, the normalisation of prejudiced worldviews through technology persists. Because individuals can face disadvantages due to their membership in social groups, mechanisms should be available to enhance the collective ability of these groups to contest and evaluate recommender systems.

At the same time, recommender systems perform group-level operations under the guise of personalisation.[36] The information relied on is aggregated on a population level, and the targets optimised toward are similarly aggregated. Optimisation systems convey information about individuals as group members rather than individuals as individuals (e.g. *people* who watch x might like y).[37] Consequently, in structuring the world as we see it, recommender systems do not affect single individuals but groups of individuals. Moreover, as these groups are typically not stable enough to talk about as delineated collectives or for them to socialise and mobilise, it renders the negotiation, representation and dialogue of tech governance more difficult.

Of course, people receive content from various sources, and recommender systems continuously perform actions that might limit or impede people's self-development and self-determination. Hence, their influence might not seem as impactful when viewed in isolation. The point we make, however, is to acknowledge that these systems, due to their integration and widespread use, exert control over people's conditions to participate in social and economic life and that the origins of this influence might manifest itself on a collective level first, before ultimately harming individuals as members of these collectives. Hence, the realisation of individual self-development and self-determination, as well as the protection of group interests, needs to be performed through individual-, collective-, and societal-level interventions.[38]

In identifying these collective dynamics, we might also see tensions arise between individual and group-level interests. For instance, in specific contexts, such as news curation, it could

---

36 Salomé Viljoen, 'A Relational Theory of Data Governance' [2021] the Yale Law Journal 82.

37 See also: Anton Vedder, 'KDD: The Challenge to Individualism' (1999) 1 Ethics and Information Technology 275; Anton Vedder and Laurens Naudts, 'Accountability for the Use of Algorithms in a Big Data Environment' (2017) 31 International Review of Law, Computers & Technology 206; Viljoen (n 36).

38 Given the widespread interest in and popularity of foundation models, the problem of harm arising on a collective level will likely persist. Indeed, foundation models "are not built for a specific *context* or conditions of use, and their openness and ease of control allow for unprecedented *scale* of use." See also: Natali Helberger and Nicholas Diakopoulos, 'ChatGPT and the AI Act' (2023) 12 Internet Policy Review <https://policyreview.info/essay/chatgpt-and-ai-act> accessed 25 May 2023.

be beneficial to increase the visibility of marginalised groups, even if this would contradict the personal interests of individual users.

In trying to resolve such tensions, it is best to understand self-development and self-determination as egalitarian values. As observed by Young, these values "assume the equal moral worth of all persons, and thus justice requires their promotion for *everyone*."[39] Yet, in a society characterised by social and economic inequality, we should acknowledge that not every person currently has *equal* access to the means for self-development and self-determination. To assure self-development and self-determination for everyone, however, the regulation of recommender systems should be informed by the broader social and institutional infrastructures in which these systems are embedded and with which they interact. In this context, the structuring function of recommender systems is often informed by background conditions of injustice, as evidenced by examples in which they reinforce historical prejudice.[40] Regulators and operators should, therefore, show awareness of the disadvantage people might experience because of group membership, paying particular attention to the social and economic position held by marginalised or otherwise vulnerable communities. To positively contribute to a healthy digital living environment, recommender systems should be harnessed to dismantle, rather than perpetuate, structural inequalities.[41] This also means sufficient – and often more – corporate, procedural, cultural and institutional resources should be made available to ensure their interests are represented and prior injustice rectified. Though the social recognition and economic integration of marginalised communities can only be realised through concerted and society-wide efforts among them, technology regulation should be no exception. These efforts are needed to ensure every person is able to deliberate and participate on *equal footing* as individuals or community members, either alone or collectively through their representation via social interest groups, in creating (ex-ante) and evaluating (ex-post) recommender systems.

1.4 The Supportive Function of the EU Charter of Fundamental Rights

The effective enjoyment of fundamental rights is a necessary external institutional condition that enables EU citizens to exercise self-development and self-determination. At the same time, fundamental rights concern areas of life in which people should be seen and heard and be able to exercise control as to how they can enjoy these rights. In other words, whereas people require fundamental rights to effectuate self-development and self-determination, self-development and self-determination are needed to fully enjoy their fundamental freedoms. In sum, fundamental rights are an inviolable North Star in the recommender systems' design, deployment and evaluation. Still, as Kas notes in Chapter V of this anthology, the Charter's position as an institutional bulwark in the protection of citizen consumers can be further strengthened. Indeed, more efforts will be needed to realise the Charter's potential in realising citizen consumers' interests to be free from digitally generated harm and injustice through fundamental rights.[42]

---

39 *Justice and the Politics of Difference* (Princeton University Press 1990) 37.
40 Annette Zimmermann and Chad Lee-Stronach, 'Proceed with Caution' [2021] Canadian Journal of Philosophy 1.
41 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (Macmillan Publishers 2018).
42 Betül Kas, Ensuring Digital Fairness in EU Consumer Law through Fundamental Rights: Is the EU Charter Fit for Purpose?

PART 2: The Stack Approach

2.1 The need for Constructive optimisation

The logics of optimisation are so deeply entwined with the fabric of society, there will seemingly always be some role for them in digital society going forward. They are part of the infrastructure of the digital public sphere, and as such have an important societal dimension. Yet society has few mechanisms to hold them to account, and to align them so that their goals reflect a plurality of interests, rather than a corporate actor with outlandish decisional power. Given their influence is likely to endure, regulating them is more realistic than removing them.

The societal dimension is in parts already recognised in the law, and the DSA more specifically, though primarily through the lens of the potential (systemic) risks to consumers, society and societal values and freedoms[43] and the need to protect consumers from arbitrary and opaque decisions that influence the ability to determine their actions.[44] Having said so, a mere risk-based approach fails to account for the critical role of recommenders as a means to make a positive and meaningful contribution to the realisation of users' rights to self-determination and self-development. Instead, it is imperative to create the external conditions through which people can flourish not only map the risks but use technology to dismantle barriers.

We, therefore, argue that users should not only have a legitimate interest to be protected from risks that recommenders pose. There is also a need to acknowledge and respect the freedom to use recommender systems as a tool to understand and navigate the digital information economy, to advance their rights to self-development and self-determination using recommender systems as means of discovery and learning, to increase their visibility within society, to pursue the information goals they deem valuable, etc. A core deficit with optimization today is that it is difficult for any actor to hold specific optimization logics to account, to politicise them, to reject, refute or refuse them, or to steer them. Specific optimization logics are baked into the services consumers use and are to be accepted by consumers as a fact of life. Concretely, this means that the regulation of recommender systems cannot be left to the sole discretion of operators of recommender systems to decide the goals to optimise the recommendation algorithm.

Unfortunately, within the current climate, users cannot just stand up and leave to a different provider that has their political values. Users, then, have a legitimate interest in that a recommender system is optimised in a way that is inherently useful and meaningful to them. To do so requires a space of contestation to steer these values, dynamically and continuously. Constructive and accountable optimisation is a starting point for this. If optimisation systems can be made more societally responsive, not (just) at the level of the response of individuals within them but at the level of their aims, purposes and governance, then we may protect against harms while enabling positive navigation of digital society.

Constructive optimisation therefore not only refers to operators' ability to justify and defend the normative choices they have made. Constructive optimisation mandates the ex-ante

---

43 Art. 35 and 36 DSA.

44 Art. 27 DSA. See also: Jennifer Cobbe and Jatinder Singh, 'Regulating Recommending: Motivations, Considerations, and Principles' (2019) 10 European Journal of Law and Technology <https://ejlt.org/index.php/ejlt/article/view/686> accessed 28 July 2023.

possibility for end-users, civil society groups, regulators and others to participate in the processes through which those choices are made. Likewise, it should be possible to scrutinise and contest those choices ex-post.

To render optimisation systems more socially responsive, we need to reconfigure our understanding and representation of these technologies, considering the above-mentioned relational dynamics.

Operators and regulators would surely like nothing more than to tug out the 'algorithm', examine and assess it, and hold those responsible for its function to account. Recommendation and optimisation systems are not single pieces of software. There may well be underlying technologies but there are also layers of (latent) social norms and values, business rules, meetings, varied logics, oversight, manual intervention, alpha and beta tests, new interfacing products, features and initiatives, content moderation and compliance. There is not "one algorithm" to locate. Instead, recommenders must be understood as socio-technical, systems that have been designed, but whose functioning is socially embedded and constituted.[45]

To capture this complexity, we propose the metaphor of the optimisation stack as a more comprehensive imagination of the dynamic socio-economic technology structures that recommender systems are.

Thinking in terms of a stack does not get us all the way to grappling with the 'structure of economic relationships that data systems support', but it does unveil some of the components of these systems, and some of the functions of these data systems. Other areas of law and regulation — and politics in general — is necessary to consider reshaping economic systems.

The stack we propose has the following components.

- **Business to Consumer Interface (Hardware)** — *the material way individuals interact with a service, which constraints the possibilities for certain governance interventions*
- **Business to Consumer Interface (Software)** — *the software interface that is delivered through hardware interface(s), potentially more dynamic, adjustable, and individualised*
- **Functionality** — *more abstract capabilities of computing systems than interfaces, in this layer we find tasks that computing systems are designed to achieve for users, providers and others*
- **Engine** — *software systems designed to fulfil optimisation logics, drawing on data to provide functionality, interfaces and more*
- **Input data (content)** — *expressive forms of information that we associate with speech norms*
- **Input data (users and environments**) — *descriptive or predictive forms of information relating to users*
- **Business-to-Business Interface** — *the ways that businesses interact with a service and in turn with consumers, which facilitate certain interactions and business practices over others*
- **Connectivity Infrastructure** — *generic Internet technologies.*

45 Nick Seaver, *Computing Taste: Algorithms and the Makers of Music Recommendation* (University of Chicago Press 2022).

Sitting parallel to the stack we have several actors and agencies which inform many parts of the optimisation stack simultaneously — they are not part of it, but governing, steering and supporting them is key to understanding governance within the stack.

- **Operations and Management** — *Organisational functions within businesses intended to oversee all or part of the stack. Without capacity and links across the stack in this function, governance mechanisms would not be implementable*
- **Accountability Groups** — *Inclusive of research groups, journalists, civil society, standardisation bodies and regulators. Without capacity in this function, there would be a very limited audience for constructive accountability, transparency and contestation*
- **Individuals and (social) communities** – *Whether they find representation through the abovementioned accountability groups or not*
- **Advertisers**.

Optimisation Stack
Business to Consumer Interface (Hardware)
Business to Consumer Interface (Software)
Functionality
Engine
Input data (content)
Input data (users and environments)
Business-to-Business Interface
Connectivity Infrastructure

Across-stack Actors
Operations and Management
Accountability Groups
Individuals and communities
Advertisers

2.1 Contextualising the Stack

The stack metaphor recalls the layered architecture of the Internet. The Internet as we experience it is architecturally constructed from different abstract levels of technology, which both interact with each other to produce the end results we see, but are also conceptually isolated, insofar as the lowest levels of the Internet, which transfer packets end-to-end across the network, do so without regard to the applications being run on them, like the Web or e-mail. Scholars have emphasised that there are many perspectives to look at the Internet from, including this architectural approach, and a synthesis of perspectives is required for effective governance.[46]

46 William Lehr and others, 'Whither the Public Internet?' (2019) 9 Journal of Information Policy 1.

We argue that the same treatment needs to be given to recommender systems in order to ensure technology functions robustly. This follows from other work considering digital power and European governance of technologies through a stack model undertaken by the Ada Lovelace Institute.[47] One reason that a stack is a useful way to conceive an optimisation system is that individual and societal outcomes of interest from recommender systems stem from the interaction of many parts of the system. Not all parts of the system are controlled by the same actor, and over time, the actors who govern the stack and the functions within it might change.

We can also use the metaphor (and practice) of optimisation to describe what is going on in the digital consumer sector.[48] In other troubling sectors which have been accused of significant illegal behaviour, such as online display advertising, 'decentralisation' has made regulation more difficult. Different actors run different parts of these services. Where they are all controlled by a single actor, there may be hope to regulate through a particular 'choke-point' — such as an all-encompassing platform.[49] But e-commerce in Europe is subject to many players, who are increasingly part of complex algorithmic supply chains.[50] These set-ups are economically designed to separate liability from the actor extracting value from a platform, as the history of intermediary liability law tells us.[51] A website or a seller themselves is going to be enmeshed in a complex platform ecosystem, where their developers may feel powerless when faced with the changing services of a large platform they are integrated with.[52] Users too might even be attributed some responsibility for the governance of recommender and platform systems.[53]

PART 3: EU Regulation and The Stack

3.1 Toward Efficient Regulation: Toward efficient regulation along the optimisation stack

In Part I, we put forward self-determination and self-development as critical, social, egalitarian, and structural values that can be interpreted as informed by, and in response to, the relational dynamics that constitute the information society. In Part II, the optimisation stack was developed to account for the dynamicity of the digital environment. The conceptual foundation in the former, and technological ideation in the latter of this study, inform one another. Both

47 Valentina Pavel and others, 'Rethinking Data and Rebalancing Digital Power' (*Ada Lovelace Institute*, 2022) <https://www.adalovelaceinstitute.org/wp-content/uploads/2022/11/Ada-Lovelace-Institute-Rethinking-data-and-rebalancing-digital-power-FINAL.pdf>.

48 Bogdan Kulynych and others, 'POTs: Protective Optimization Technologies', *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (ACM 2020).

49 Jack L Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006).

50 Jennifer Cobbe, Michael Veale and Jatinder Singh, 'Understanding Accountability in Algorithmic Supply Chains', *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2023).

51 Lilian Edwards, '"With Great Power Comes Great Responsibility?": The Rise of Platform Liability' in Lilian Edwards (ed), *Law, Policy, and the Internet* (Hart Publishing 2019).

52 Tania Bucher, 'Objects of Intense Feeling: The Case of the Twitter API' (2013) 3 Computational Culture: A Journal of Software Studies.

53 Natali Helberger, Jo Pierson and Thomas Poell, 'Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34 The Information Society 1.

are integral to our endeavour to critically interrogate the regulation of recommender systems, which is the objective of Part 3.

Regulation cannot take aim at a single part of the system. For example, regulation that tries to moderate content misses the underlying recommender engine. Regulation aimed at the underlying logics of the recommender engine ignore the design dynamics which lead to certain patterns of input. Regulation which focuses on certain design dynamics of input might ignore the role or potential of communities to flag, steer, use or repurpose these systems. The stack offers a unique vantage point, and toolkit for others, which facilitates the identification of relevant legislation in a piecemeal manner, whereby each layer within the stack might be subject to different rules or even regulatory frameworks. Once we surmise which laws can apply to which layer, we can identify which provisions could positively contribute to self-development and self-determination. As the stack visualises interaction between layers, once laws have been mapped, the visualisation can help analyse how laws interact, including where they complement or conflict. Moreover, upon disentangling the stack, it becomes evident how the regulation of the online environment becomes a long-term project:

There is no one-size-fits-all regulatory solution for turning the digital environment into a living space conducive to human flourishing. Instead, technology governance is a step-by-step process dependent upon various institutions' and individuals' efforts and contributions, aided by multiple interacting laws.

Turning to the values of self-development and self-determination, we have shown how their realisation cannot be tied solely to metrics directed toward personal or individual relevance (as a typical commercial optimization goal). The right to constructive optimisation, as grounded in the right to self-determination and self-development, includes the need to take into account the legitimate interests of users, both as individuals and as members of social groups and non-social collectives. Self-determination and self-development can moreover not be realised by focusing on short-term goals and choices. Their enjoyment for all is dependent upon a well-functioning and healthy democratic society imbued by a strong respect for fundamental rights. Hence, due consideration must be given to the ways in which novel technologies can interfere with the social and institutional structures in which citizens navigate, as well as the physical, mental, social and economic capacities citizens require, to determine their actions, and the conditions of those actions on the one hand, and expand, develop, express and communicate their experiences and perspectives on the other hand.

3.2 Overarching Guidelines for Stack Governance

Drawing from our analysis thus far, and before we start our evaluation of applicable EU legal frameworks, we propose a set of overarching standards aimed to facilitate users to take active part in the governance of socio-technical eco-systems in ways that are seen and heard. More specifically, regulation should be positively aimed in assuring that those subjugated to recommender systems can:

- understand the rules of engagement, including how systems function, for which purposes they have been optimised, and the consequences such optimisation strategies entail on the content users see
- have an actual and actionable say in the optimisation goals pursued within digital ecosystems

- exercise meaningful choice and voice, which requires the presence of alternative options, both in relation to a particular recommender system's functioning and in relation to other operators, including service-providers and platforms
- be included, represented and having one's voice heard during the ideation, design, deployment and evaluation of recommender systems, meaning they should have access to participation and contestation mechanisms from cradle to the grave.

Moreover, to ensure equal enjoyment of self-development and self-determination, and equal participation in attempts to democratise recommender systems, particular attention must be paid to marginalised or otherwise vulnerablised communities. If not, the digital ecosystem will become an additional barrier to break down in the fight against the structural inequalities and injustice they already face. In this context, constructive optimisation also pertains to the interests of those who may not directly interact with a recommender or are (structurally) underrepresented and excluded because recommendation algorithms are not only a tool for users to discover information but also a means for non-users and other parties affected by the algorithmically mediated choices to be discovered.[54] Through their recommendation logics, recommender systems determine if and who gets seen and heard under which conditions, but also: who remains invisible and unheard. Likewise, the optimisation stack should be governed by strong labour protection and respect the rights of data workers involved in data production processes.[55]

After having thus defined the cornerstones of constructive optimisation as a balance between individual and societal interests whereby each person has access to the conditions needed to exercise self-determination and self-developments, we will in the next step undertake a critical analysis of the current legal approach to regulating recommender systems in the DSA and adjunct laws.

3.3 Regulatory Recommendations Across the Stack

In the following section, we outline the stack piece-by-piece. In each section, we characterise this aspect of the optimisation stack, including why it may be challenging to govern. In addition, we indicate any regulatory provisions from the current or proposed European digital *acquis* which relates to this section (or the absence thereof). We then make proposals within this section for rights that relate to this aspect of the stack.

This exercise is explicitly exploratory in nature. We aim to show how a stack approach affords one with a new, different perspective to approach questions on recommender system regulation. The overall aim is thus not to be exhaustive, but rather to show the reader how a stack approach to recommender systems allows one to draw on the entire (current or proposed) European digital acquis to address many different aspects related to optimisation strategies such as recommender systems but also where potential intervention points are to realise more

---

54 Philip Napoli and Sheea Sybblis, 'Access to Audiences as a First Amendment Right: Its Relevance and Implications for Electronic Media Policy' [2008] McGannon Center Working Paper Series <https://research.library.fordham.edu/mcgannon_working_papers/6>.

55 See also the work of: Milagros Miceli e.a., 'Documenting Data Production Processes: A Participatory Approach for Data Work' (arXiv, 9 augustus 2022), http://arxiv.org/abs/2207.04958; Milagros Miceli en Julian Posada, 'The Data-Production Dispositif' (arXiv, 24 mei 2022), http://arxiv.org/abs/2205.11963; Milagros Miceli, 'Whose Truth? Power, Labor, and the Production of Ground-Truth Data' (Technische Universität Berlin, 2022), https://depositonce.tu-berlin.de/handle/11303/19464.9 augustus 2022

accountable optimisation. As we already highlighted in the introduction, this exploratory stack approach can feel very mosaic, but that is more of a feature than a bug – the approach is meant to open up space for applying the European digital acquis to recommender systems. So, if anything, Part 3 should inspire the reader to get creative and use the stack as a model to embrace a wider, more dynamic perspective on recommender system regulation.

3.3.1 Business to Consumer Interface (Hardware)

Summary: the material way individuals interact with a service, which constraints the possibilities for certain governance interventions.

Hardware is not typically steered directly by legislation, and usually should not be. Yet, choices in hardware design can affect citizens in how they exercise and enjoy their rights. Where hardware decisions risk limiting people's ability to co-govern recommender systems, and these negative externalities cannot be effectively designed around, operators must correct this imbalance through other means.

Hardware is difficult to govern directly as it often supports many services and is released or designed prior to the development of services or platforms on it. To link them would be undesirable as it would restrict openness and competition. Legislators have proceeded warily with functional mandates relating to consumer hardware, with legislative action on harmonised chargers for mobile devices taking many years to come to fruition.[56]

Hardware decisions could positively contribute to people's navigation of the digital environment. For instance, visually-impaired consumers benefit from certain hardware modalities, such as audio or haptics, to experience their surroundings and to exercise rights. At the same time, hardware might also constrain the effectiveness of rights or obligations that can be placed on services that use it. For example, obligations on prior transparency before data collection,[57] the use of recommender systems,[58] or attached to pieces of content[59] can be more difficult to implement on interfaces like smart speakers that rely on auditory cues only. The compromises service-providers need to make as a consequence of hardware choices could thus leave a legislative gap. Ideally then, the obligations of actors in the optimisation stack should alter depending on the modalities through which they deliver their service.

---

56 Directive (EU) 2022/2380 of the European Parliament and of the Council of 23 November 2022 amending Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment OJ L 315/30.

57 e.g. GDPR, art 13.

58 e.g. DSA, art 29.

59 e.g. AIA Parliament Draft, art 52 [deepfake transparency]; DSA, art 31 [on traders].

Recommendation: Citizen-consumers' ability to exercise agency over recommender systems should not be negatively impacted due to their reliance on devices that have limited hardware support, but instead accommodated for. Among others, firms should be obliged to vary the form of transparency and ability to exercise agency according to the modalities their services are available on. Moreover, if there are true and hard limits to active and passive user rights that can be fulfilled, then other obligations or design strategies may need to be heightened and strengthened. An active reflection on such limitations should be promoted, for instance, through the performance of (periodic) risk assessments and ex-post monitoring obligations.

3.3.2 Business to Consumer Interface (Software)

Summary: The software interface that is delivered through hardware interface(s), which are potentially more dynamic, adjustable, and individualised in nature.

Interfaces are central to the optimisation stack, and are studied heavily in academic fields such as *interaction design*. Several existing provisions in the EU acquis relate directly and indirectly to business-to-consumer interfaces. In this section, we focus on the transparency of recommender system adjustments, the prohibition of manipulative design interfaces and the need to offer trader information.

3.3.2.1 Recommender System Adjustments and Transparency

At the core of the DSA's recommender provisions is the provision on recommender system transparency. This provision concentrates on the information presented to consumers. For one, providers of platforms that use recommender systems should "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."[60] This information is intended to give recipients insight into the why certain recommendations are made, and include the criteria most significant in determining the output suggested, and the reasons behind their relative importance.[61] Article 27(3) DSA (Recommender system transparency) concludes with an obligation for platforms that have multiple options for the configuration of recommender systems to make available a 'functionality that allows the recipient of the service to select and to modify at any time their preferred option'. Such functionality must be 'directly and easily accessible from the specific section of the online platform's online interface where the information is being prioritised'. These guarantees however hardly reach further down the stack into the operational and technical level of the service itself.

There is no general obligation for online platforms to offer multiple or alternative options to end-users concerning the configuration of recommender systems they are subject to. Indeed, only where the platform itself has chosen to make alternative options available, should end-users have the ability to easily and directly navigate between those alternatives. In other words,

60 Article 27, § 1 DSA.
61 Article 27, § 2 DSA.

meaningful, including alternative, choice is not viewed as an entitlement, but rather a privilege granted by platforms.

In this context, it is relevant to more profoundly consider what an 'option', and choice among options, would constitute. In practice, recommender systems are often deployed as 'hybrid' systems comprising many recommender systems. Mixed recommender systems stack the output of many recommenders — producing the content from a system perhaps trained on your behavioural data first, then following it by content that might be popular in your geographic region, and when data on that runs out, content that might be popular throughout the world.[62] Ensemble systems rank and weigh many recommenders and combine the results. These options are not necessarily surfaced to users (typically), even though they typically do exist in the backend. Individuals could be provided with just the most popular content in their geography, for example, even though knowledge concerning their likely preferences behaviour-wise could be given.

In ensuring granularity of choice over options, lessons could be drawn from data protection law. It could be argued that in order to comply with data protection law, systems *have to be* created to be decomposable: they must be able to run with limited profiling or personal data, otherwise their design is contrary to Article 25 GDPR (Data protection by design and by default).[63]

Recommendation*:* Regulators should take an expansive reading of Article 27 DSA and make it mandatory to offer consumers a meaningful choice through which they can realise their rights to self-determination and self-development, through among others, the choice among alternatives as a default.

In addition to the DSA, other interface-based information rights concerning the use of metrics or "main parameters" as part of recommender and ranking systems have been introduced. New additions in FB2BPR Article 5, UCPD Article 7(4a) and CRD Article 6a(a) requires users to be able to access the 'main parameters' of a ranking system when they search or conclude contracts with traders in various online settings. The purpose of these provisions when aimed at businesses is supposedly to 'improve predictability' and 'improve the presentation' of goods and services,[64] whereas for individuals the motivations are not explicit in the recitals.

While the term 'main parameters' includes 'any general criteria, processes, specific signals incorporated into algorithms or other adjustment or demotion mechanisms used in connection with the ranking', the instruments are clear that such parameters need not be customised per user.[65] A core problem however is that many recommender systems are tailored by user, including by having their weights and parameters significantly adjusted by a user's activity within a certain session.[66] In this case, the value of the generic notion 'main parameters' seems unclear, and in any case, highly technologically specific. This also means that aggregate analysis or reasoning based on these main parameters may be flawed, as there is potential for unwanted dynamics

62 Kim Falk, *Practical Recommender Systems* (Manning 2019), ch 12.
63 Case C-252/21 *Meta Platforms Ireland* ECLI:EU:C:2023:537.
64 FB2BPR, recital 24.
65 Omnibus Directive, recitals 22–23.
66 See eg Moumita Bhattacharya and Sudarshan Lamkhede, 'Augmenting Netflix Search with In-Session Adapted Recommendations' (arXiv, 5 June 2022) <http://arxiv.org/abs/2206.02254> accessed 28 September 2023.

such as discrimination or manipulation on an individual level based on variations across recommender manifestations, or the exclusion of voices in society.

A second challenge with 'main parameters' is that where the input data (see below) to recommender systems is abstract in nature, such as originating from telemetry data including gyroscopes, compasses, wireless connections, clicks and touches of devices, or in virtual reality applications, even eye gaze, it is very difficult to explain systems *in terms* of these data.[67] Explanation facilities for machine learning and similar systems struggle to communicate with humans when the building blocks of the data underlying a system are abstract. It is easy to imagine a system explaining that 'you received this advert because you are listed as enjoying holidays in Malta'. However, when a system is recommending this on the basis of telemetry data, there is no higher-level human concept that serves as an obvious mapping. As humans we appear to analyse the world in terms of these higher concepts — or at least we often *post hoc* reason that we do in our own heads. Machines don't need to. As such, 'main parameters can make little sense.

The above challenges broadly relate to the implementation of a right to 'know your digital alter ego', something that has been suggested in previous work.[68] Collectively, this would enable citizens to understand with whom they share their digital alter ego. Such a right requires us to reflect on what it would be to *know* such an alter ego given that it may be complex, extremely multi-faceted, dynamic and based on very abstract concepts with little human-interpretable meaning. European law in this area often attempts to square this circle by requiring complex information in plain and intelligible language, or similar. This is not an easy circle to square though, as a lot is lost by simplification — so much that it might undermine the faithfulness of an explanation as a whole. Presumably the purpose of transparency provisions is not to give comfort, but to allow individuals to benefit from and instrumentalise knowledge, which requires that knowledge can be mapped both onto their experiences and the functioning of the underlying systems. Transparency, action, and the building of understanding should all be interlinked.[69] This would seem to require a turn to more interactive and action-focussed forms of transparency. 'Main parameters' simply does not do this work — the requirement is for systems to be created in more playful, exploratory ways, that facilitate users understanding, customising and altering them.

---

67 Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18, 59.

68 https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf

69 See eg Cynthia Rudin, 'Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead' (2019) 1 Nature Machine Intelligence 206. See eg Motahhare Eslami and others, 'First I "Like" It, Then I Hide It: Folk Theories of Social Feeds', Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (ACM 2016); Nadia Karizat and others, 'Algorithmic Folk Theories and Identity: How TikTok Users Co-Produce Knowledge of Identity and Engage in Algorithmic Resistance' (2021) 5 Proceedings of the ACM on Human-Computer Interaction 305:1. Sarah Inman and David Ribes, '"Beautiful Seams": Strategic Revelations and Concealments', Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (Association for Computing Machinery 2019).Elias Storms, Oscar Alvarado and Luciana Monteiro-Krebs, '"Transparency Is Meant for Control" and Vice Versa: Learning from Co-Designing and Evaluating Algorithmic News Recommenders' (2022) 6 Proceedings of the ACM on Human-Computer Interaction 405:1.

Recommendation: The informative utility of giving insight into a system's 'main parameters' is flawed given the dynamic nature of recommendation and optimisation, and the abstract nature of underlying data. Information provided should enable users to understand the logic of the recommender system, the normative choices made therein, as well as the consequences of their own choices exercised in their interaction with recommender systems. This includes individual consequences (what users will see or not see) but also how companies took into account wider societal interests, such as the health of the public sphere, the interests of marginalised communities, the ecological footprint of technologies used and initiatives to protect workers' rights. Moreover, to assess the trustworthiness of the systems they partake in, they should also be told by whom those choices were made and to which end. The end-users should thus understand how the aforementioned areas affect what the end-users is and is not recommended and with whom they share their a so-called digital alter ego. Transparency obligations should (and can) be adapted to account for the dynamicity of the optimisation stack. To be able to act upon information, information should be clearly presented, rather than hidden away in opaque and complex terms and conditions.

Recommendation*:* The Commission should explore participatory design obligations, potentially in collaboration with research capacities or projects, where platforms have to make transparency interactive, meaningful, and linked to action as to accommodate the needs and interests of end-users. Such efforts should moreover pay sufficient attention and include marginalised, or otherwise vulnerable, communities and interest groups.

3.3.2.2 Prohibitions on Manipulative Interfaces

Article 25 DSA (Online interface design and organisation) prohibits online platform providers from designing interfaces in a way that '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', except where they relate to practices governed by the Unfair Commercial Practices Directive or the GDPR. The Commission can issue guidelines on how this article functions. This is the so-called 'dark patterns' provision. Paragraph 2 gives three examples, including presenting certain choices more prominently than others, using pop-ups to interfere with users' choices and making the procedure for terminating a service more complex than subscribing to it. The limited scope of the provision aside (excluding the GDPR and the UCPD), Article 25 DSA merely tackles the *presentation* of choices and not the actual choices themselves. Those choices can still derive from data-driven and dynamically adjustable operations that identify and commercially exploit people's preferences. Studies on dark patterns have indicated that it is both the presentation (e.g., how many layers down in a pop-up a decision-point is) and the content (e.g. is there a reject all button) that materially affects individuals' choices.[70]

Elsewhere in this report we discussed the lack of conceptual clarity in combination with the prerogative of platforms and private standardisation bodies to define the notion unilaterally as a fundamental problem of Article 25.[71] The stack perspective adds another critique: Arti-

70 Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence', *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2020)* (ACM 2020).

71 See Chapter II above - Helberger N, Sax M, Digital Vulnerability and Manipulation in the Emerging Digital Framework.

cle 25 DSA is no alternative for reaching further down the systems architecture and providing guidance for considering consumer interests (and vulnerabilities), such as regarding the way platform architectures are designed to collect data in the first place (**input data** level), how decisions about consumer data are made in the **operations and management capacity**, or which parameters the model is optimised for on the **engine** level.

Other EU law also contains constraints on manipulative interfaces which are slightly more general in nature and potentially reach beyond the interface level and deeper down into the technology stack. Article 5 UCPD prohibits a commercial practice, understood broadly, if 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.'

Article 5(1)(a) Draft AIA [EP] proposes that it is prohibited to place on the market, put into service or use 'an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm'. This reaches further down the stack somewhat as the AI system itself is considered as the underlying engine, however the recitals also limit the full connection across the stack. Recital 16 notes that the 'intention to distort the behaviour may not be presumed if the distortion results from factors external to the AI system which are outside of the control of the provider or the user, such as factors that may not be reasonably foreseen and mitigated by the provider or the deployer of the AI system.' One could argue that this recital excludes "intent" where the distortion can be linked to the input data for example. Furthermore, excluding factors that are "external to the AI system", appears to eliminate the need to duly consider the pervasive influence social conditions will have on the functioning of a system. To illustrate this tension, we can ask whether a system optimising for profit, where user or business input data makes it in practice act in a manipulative manner, would be considered as being "intended to manipulate."

Consumer law, the AIA and data protection law together represent a regime where firms are obliged to develop interfaces in *modular* ways, with manipulative components identified and prohibited. As it stands, manipulative systems which optimise to extract value from consumers are the norm, and the default. Personalised recommendations should be a staged, directed, opt-in system, where individuals are involved in choosing the reasoning behind presenting information, and to make their goals more explicit. This does not mean that we return to a world of search; simply that when individuals are presented with adaptive interfaces, much like they 'sort' products in a search, they can choose options that reflect their aims and preferences. Perhaps they would like to see products other people with similar purchasing histories, or some other data they bring, purchased? Perhaps they would like to see products that are more like other products when they browse? Perhaps they would like interfaces based on popularity with their geography, or other demographics. Ultimately, firms' ability to optimise for pure profit or clicks should be reduced — not removed, but placed as a subsidiary factor to an overarching logic that is chosen by a user.

Recommendation: Manipulative tactics undermine the opportunity for end-users to exert deliberate control over their digital environment (self-determination). Moreover, when end-users are manipulated to act in accordance with the operator's interests, they are also denied the opportunity to have their desires and interests heard and recognised (self-development). Whereas adaptive interferences often operate on a logic that is optimised for an aggregate concept such as profit or attention, and while there may be a role for including such goals in optimisation, they should be subsidiary to functional goals actively chosen by users. These considerations should inform the interpretation of Article 25 DSA, as well as the Commission when they issue guidelines on the application of Article 25 DSA on specific practices.

3.3.2.3 Product and Trader Information

Some further provisions interplay with the interface, effectively attempting to ensure that traders' information is effectively provided to consumers in the presence of intermediaries. Article 3(5) UCPD obliges online intermediation services to ensure that the identity of a business user providing goods is clearly available. Article 31 DSA (Compliance by design) obliges online platforms that allow consumers to contract with traders to ensure that interfaces are designed in such a manner which allows traders to comply with information provision obligations. Article 32(2) DSA (Right to information) requires providers to alter their online interfaces to inform consumers of illegal products if they cannot inform all concerned individuals directly. However, these are lopsided provisions. While platforms benefit from designing interactive, dynamic interfaces to deliver their business aims, regulatory goals cannot benefit from these tactics. If platforms can design compelling experiences for their own business ends, why can they not be obliged to design compelling experiences for regulatory ends? If platforms have information on what people might purchase, why should they not be obliged to 'advertise' to those same consumers, through optimization systems, that certain products they may have purchased on or off the service have been deemed to be illegal by a regulatory authority? This is not to say that all information should be targeted, but that more effort can be made in legislative drafting to bridge the disconnect between what 'looks like' a regulatory obligation, and what looks like a business feature.

Recommendation: Information provisions in consumer law should be subject to design obligations to communicate them effectively and dynamically, including within optimisation systems. This should lessen the divide between static regulatory requirements and the practical methods of information provision to users used by firms.

3.3.3 Functionality

Summary: The functionality layer refers to the more abstract capabilities of computing systems than interfaces, in this layer we find tasks that computing systems are designed to achieve for users, providers and others.

The functionality layer is deeper than the interface layer, although often is intertwined with it. Regulation aiming at the functionality layer obliges the creation of new or different underlying technologies, rather than just surfacing information about existing technologies, or providing options around such technologies that do not necessitate foundational redesign

or adjustment. In practice, interfaces could be considered functionality, while technologies such as recommender systems contribute to the functioning of interfaces, however we split the two by considering interfaces as the basic methods to view information and change settings provided by underlying functionality.

Functionality is often entwined with law. There are many functionalities related obligations we do not cover in this work, but which are relevant to platform regulation more broadly. Platform regulation has effectively obliged firms to create geolocation functionality to try and separate users by jurisdiction to treat them differently. Emerging regulation is demanding that firms create age verification or age 'assurance' tools to attempt to avoid certain features or content being accessible to minors. Here we zoom in on community stewardship functions however, which are the functions which interface with Accountability Groups and other users in order to attempt to 'open up' some of the operational functions and steering of optimisation systems — with mixed success and prospects.

3.3.3.1 Community Stewardship

Some legal provisions have obliged the creation of new functionality on online platforms that affects the optimisation stack.

According to Article 22 DSA, platforms should prioritise alerts to illegal content by trusted flaggers, acting within their designated area of expertise, provided the notice and action has been declared through the mechanisms set-out in Article 16. The status of trusted flagger is designated by the Digital Services Coordinator of the Member State in which the applicant is established. The powers offered might remain superficial, however. This is in large part due to the DSA's focus on content, rather than patterns or issues that concern the optimization stack in its entirety. For example, a news recommender can reproduce social stereotypes (e.g. only display negative information concerning certain demographic groups) even if those singular pieces of news information are not "illegal content" (e.g. hate speech) per se.

Article 40 DSA (data access and scrutiny) does offer a more elaborate and strengthened form of scrutiny to verify the overarching design obligations of operators (described below), as well as the social and democratic impact their choices, including those that comply with the law, might have. More specifically, Article 40 DSA creates new obligations on platforms to provide information to vetted researchers and involves a back-and-forth process to get to an agreed form of data to provide. In practice, it implies the creation of new functionality as platforms must develop automated systems and APIs for researchers to mitigate the cost of dealing with each request manually. Article 39 DSA (Additional online advertising transparency) obliges VLOPs or VLOSEs that provide online advertising services to provide an interface through which these can be searched and examined. These provisions interact with the **Accountability Groups,** including academia and civil society groups, that sit alongside the stack. More specifically, they provide entry points to those groups to hold the digital ecosystem accountable when optimization strategies generate externalities on individuals, societies and environments.[72] Effective scrutability is however contingent on there being sufficient well-intended

72 Bogdan Kulynych and others, 'POTs: Protective Optimization Technologies', Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (ACM 2020).

target groups who have the resources and expertise to scrutinise complex systems.[73] Still, unclarity remains. What happens when more structural issues are flagged? And more fundamentally, how easy is it for groups that discover unwarranted dynamics to flag them in the first place. Furthermore, given the many different laws that apply to interfaces, it might be difficult to identify which regulator to contact in case systemic risks are insufficiently addressed or which regulator should take the lead.

Recommendation: Trusted Flagging organisations should be able to raise complaints about the functioning of optimisation and recommendation systems to firms, rather than just about content.

Recommendation: Trusted Flagging organisations should also be able to submit a fast-track 'super complaint' to a body representing all relevant regulators in a jurisdiction, who should periodically discuss and assign responsibility for these issues amongst their (sometimes overlapping) competences. These should include consumer regulators, media regulators, data protection authorities, equality bodies, and the Digital Services Coordinator (if different).

Recommendation: Operators should explain and make available information that enables third-parties to test and scrutinise optimisation goals and their impact on/relationship to public values and societal interests (a right to observability and access). Such information, including auditable documentation standards, should not only pertain to the choices that impact the recommendation as such, but also provide insight into the data production processes and normative assumptions underlying recommender systems, which could include the labour conditions under which systems were developed, trained and deployed, and the instructions provided to team members regarding those data production processes.

3.4 Engine

Summary: Engines are software systems designed to fulfil optimisation logics, drawing on data to provide functionality, interfaces and more. Provisions targeting the optimisation engine require analysis and alteration of its functioning. Such systems directly require firms to tailor and alter the underlying technologies at the heart of optimisation — the engines that determine how optimisation functions should be calculated.

3.4.1 Alternative engines

As indicated above, interface provisions require platforms to allow users to switch between different engines where they exist. Article 38 DSA (Recommender systems) complements this provision, as it requires VLOPs and VLOSEs using recommender systems to provide at least one option not based on profiling. This might, for example, be a system that returns content chronologically, potentially further based on explicit choices of topics or individuals to follow.

73 Jakko Kemper and Daan Kolkman, 'Transparent to Whom? No Algorithmic Accountability without a Critical Audience' (2019) 22 Information, Communication & Society 2081.

Article 38 DSA is relevant for the realisation of the right to (individual) self-determination in the sense that it must give users a real choice between different recommendation logics – one profiled and a non-profiled one. This provision will potentially give users a choice to compare how the recommendations look with and without profiling, even if the freedom to do so is a very limited version of a potential right to self-determination. The limitation of Article 38 DSA is, yet again, obvious when applying the stack perspective. While the provision focuses on the technical, the engine level, it does not have a corresponding obligation on the level of input data (in the sense of an option not to have one's personal data collected or processed to profile the consumer). Concerning the latter, Article 28 DSA acts as the sole exception, limiting the profiling and personal data processing of minors.

Other regimes, such as the GDPR in general, and Article 5(2) DMA (prohibition to combine data across platforms) more specifically, may interact with this requirement, but as these provisions cover multiple regulators, it is difficult to imagine these being coherently enforced. The GDPR could be interpreted as that alternative recommenders *have* to exist (e.g., those which use fewer personal data), and this may interact with the interface provisions to ensure that such alternative engines are surfaced to all users. Again though, to piece together these provisions across regulators requires a level of cooperation and coordination we do not currently see in the EU.

There are also no corresponding obligations on the operations level (in the sense of considering a preference of consumers whether to be profiled in the first place). As a result, it is again entirely up to the discretion of the platform or search engine provider to continue profiling as long as consumers have the choice to receive recommendations that are not based on profiling. Seeing that the core business logic that informs the design of social media architectures is to sell access to individuals and groups, such as through targeted advertising shaped by profiling, it is unlikely that Article 38 DSA will do much to impact the design of these architectures more profoundly.[74]

Most importantly, an option that switches off profiling says nothing about the quality of the option that replaces it. If the alternative to a profiling-based recommender is one that sorts content in alphabetical order, this would undermine the point of the law. Recommenders that attempt to produce sensible and useful results without profiling users are possible, but the incentives to do so are not there. Firms are already litigating the DSA claiming that the opt-out alone would render irreversible economic damage to them (although the General Court has refused such arguments), and we will likely see this continue to be a contentious area.[75] Firms should be obliged to make alternatives for existing profiling methods and to evaluate them and continually improve them.

Recommendation: End-users should have a right to demand alternative recommendation options, and where technically feasible, a right to have third-party (stand-alone) recommenders to offer alternative recommendations. These too however, should align with the set of standards promoted as part of this study.

---

74 Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

75 Case T-367/23 R *Amazon Services Europe Sàrl* ECLI:EU:T:2023:589 (Order).

Recommendation: Where engines that do not use profiling are selected, this should also trigger related obligations, such as a right to object under data protection law, ensuring that the underlying profiling never occurs, rather than is simply not shown.

Recommendation: As it stands, recommender rules allow users of large platforms to opt-out of seeing profiling-based recommendations, but provide no assurance that firms will invest capacity into running and maintaining useful and desirable alternatives. Structures which incentivise the production of these alternatives and align them with societal interests rather than private profit are required in all areas of EU law touching on optimisation.

Other regimes have a direct implication on the engines themselves. Article 17 GDPR (Right to erasure ('right to be forgotten')), read in conjunction with the chain of case law beginning with *Google Spain*,[76] has a direct effect on the requirements of certain optimisation systems produced by search engines. It requires them to have the functionality to remove certain records from appearing in these results, if they have succeeded in an erasure request. Further case law places new obligations on these systems. In particular, the *GC and Others* case requires operators to be able to alter their recommender system such that, whenever they receive a request for a delisting relating to a criminal proceeding, and regardless of the request's success, 'the overall picture [the list of results] [given to'] the internet user reflects the current legal position, which means in particular that links to web pages containing information on that point must appear in first place on the list.'[77] The European Parliament version of the draft AI Act includes recommender systems of Very Large Online Platforms as 'high-risk' AI systems, which means there are obligations placed directly upon the design of the recommender. Such obligations include considerations of accuracy, bias, data representativeness, cybersecurity, and the potential for human oversight by the users of these systems. Under the current approach, these provisions are proposed to be elaborated by private standard-setting bodies CEN and CENELEC.

Further requirements for engine design may be derived from obligations relating to the processing of 'special category data'. Optimisation systems often place individuals and content inside a common geometric space, where content can be structured and grouped, alongside individuals, across thousands or even millions of 'dimensions. Both content and individuals move as their optimal positions become apparent. Though these spaces can be constructed in abstract terms in the sense that they have no human interpretable meaning, the information they convey can nonetheless reveal interests or personal information that is deemed sensitive, such as a person's sexual orientation or political beliefs. Moreover, this structuring of content might occur automatically, without direct human interference or direction of the platform. In this context, the Court of Justice has confirmed that special categories of data also include data that would indirectly disclose 'following an intellectual operation involving deduction or cross-referencing'.[78] This conclusion places an indirect pressure onto operators to develop engines which can avoid this dynamic occurring, although whether that is possible at all remains an open question. At the same time however, Article 9 GDPR enables the processing of special categories of data when based upon explicit consent, which could result

76 Case C-131/12 *Google Spain* ECLI:EU:C:2014:317.
77 Case C-136/17 *GC and Others* ECLI:EU:C:2019:773, para 78.
78 Case C-184/20, *Vyriausioji tarnybinės etikos komisija* ECLI:EU:C:2022:601.

in an overreliance of operators to use consent as their legal basis. Whereas Article 26(3) DSA prohibits profiling based on special categories of data, this prohibition only covers the presentation of advertisements. Finally, the logic established by the CJEU in *Meta Platforms* might entail that consent cannot be relied on when no viable recommender alternatives are provided to the end-users, whereby the notion "viable alternative" moreover cannot be interpreted to include the abandonment of the platform altogether.[79]

Recommendation: Engines should be developed to promote self-determination and self-development for all, and the efforts thereto made available. To that end: a) the design team should be diverse, and, b) meaningfully engage with citizens and affected communities during the design process, including subsequent evaluation and iterations of the design, c) auditable documentation should be available as to how these interactions informed the design in a demonstrable or scrutable manner, d) metrics should be tested for their impact on people's self-development and societal implications, for example for media pluralism. Design processes should include periodic considerations for public values and value-sensitive design strategies.

3.5 Input Data

Summary: We separate layers of the stack which deal with primarily expressive content from content which is primarily descriptive due to the different interests they entail. This divide is naturally imperfect and the data itself overlaps. The boundaries are also becoming less clear as traditionally expressive content such as images and text are now becoming automatically processable in.

In this Section, we make a distinction between considerations that concern the content of input data, and those that concern the users and environments affected by content data. There are some overarching recommendations that we believe could generally apply to the governance of input data:

Recommendation: An optimisation system producing diverse and varied outputs cannot do so without sufficiently diverse and varied inputs. Encouraging this should be the subject of multiple areas of regulation which happen in concert with changes to engines and interfaces to support a full-stack approach to governance.

Recommendation: Operators should provide end-users, research institutions and civil society, the ability to contest data and moderation decisions that could have a negative effect on the lawful representation of particular cultural or political groups, languages and forms of expression.

Recommendation: Operators should provide transparency on the content curation pool and the metadata they use.

79 C-319/20 *Meta Platforms Ireland* ECLI:EU:C:2022:322.

Recommendations: In case operators make use of curation, they should consider the diversity of the content pool, and the impact current content pools have on marginalised and vulnerable individuals and social groups.

Recommendation: End-users should be given a functionality to curate profiles, including what personal information of theirs can be used, and give end-users the functionality to indicate, and make changes to, their own preferences and interests. When this is the case, end-users should be periodically reminded of the preferences and interests they chose and have the possibility to be redirected to an area where they can make changes to those preferences and interests.

3.5.1 Input Data (Content)

3.5.1.1 Limits of illegal content focus

Provisions concerning content have typically focussed on the removal of illegal content. Until the DSA, across Europe there were few obligations to remove content. Article 9 DSA constitutes a remarkable change in this regard, imposing orders to act against illegal content across Europe. Furthermore, Article 14(4) DSA obliges providers to act proportionately and in a way that respects fundamental rights when they enforce their own terms and conditions. This type of provision is emerging across the world, where laws operate via a two-step approach of a) mandating firms to place certain provisions in their terms and conditions, and b) obliging them to apply such terms consistently and proportionately.[80] This allows an expansion of the obligations in the DSA through the mechanism of obliging an alteration of terms of service, without the creation of new enforcement or monitoring structures. This regulatory tool however also re-enforces the privatisation of consumer regulation.

Some types of illegal trading are more difficult for platforms to detect or be reactive to than others. In addition, certain providers might have poor records of adhering to consumer rights, or uphold illegal practices around data collection, service and warranties, consumer information and similar. Such information may be held by consumer protection authorities, if they take action against these firms, or other bodies which retain records of compliance. Consumer bodies regularly provide tools and data ranking services, and third parties also aim to provide such data on trustworthy providers of goods and services. It may be worth allowing these factors to influence optimisation systems on large marketplaces.

Recommendation: Large commercial platforms selling goods and services through optimisation systems should be obliged to consider datasets produced by consumer organisations in rankings, as long as they are made to high standards. This should be initially explored through a code of practice.

80 See e.g. Online Safety Bill (HL Bill 164 (as amended on Report), 2023, United Kingdom).

3.5.1.2 Data collection or labelling mandates?

Optimisation systems cannot produce diverse results without a diverse set of content, reflecting different perspectives, topics and genres. If a recommendation system were to contribute to the self-development and self-determination of a diverse set of users, it would need to be able to draw on a pool of information that is reflective of the diversity of its users. The approach that the DSA takes is a different one. As mentioned above, there are no quality requirements at the input level as long as the content is lawful. For example, there are no requirements that the pool of information must not be biased towards certain political views, cater to minorities or reflect different languages. Such requirements may be present in the AIA if the Parliament version passes, at least to some extent, as that regulation would place obligations around bias and the provenance of training data — although there is significant leeway for providers to interpret them as they see fit.

If more or less of certain content is desired — content of a certain 'quality'; linguistic or cultural relevance; a political nature, or similar — then that content has to be labelled as such at some point in the stack. Doing so might be cheap or costly depending on the characteristics. Firms may not always wish to label content if doing so may bring obligations to change its distribution in ways that may not be profitable. For example, firms may not want to deter popular influencers from their platform by attempting to identify and label sponsored content that has not been declared. Similarly, when such labelling occurs, it is important that it is public and contestable. Labelling systems create ontologies of the world which can reify and reinforce biases.[81]

As it stands, there is no obligation in the DSA or similar regulations to actively label data such that other functions can be fulfilled. Labelling of data for downranking, shadow banning, reporting or on the basis of reports happens constantly. Running optimisation systems with certain preferences require and rely on such labelled data. Accountability groups can use such labels to study and scrutinise the functioning of systems.

Labelling mandates are complex to apply because they can be labour intensive, although systems like language models and computer vision claim to be able to reduce the cost of these. Such systems may be useful, but will need constant scrutiny of their performance and taxonomy due to the inherent challenges of algorithmic content moderation.[82] A first step would be to publish these taxonomies and the labels on visible content.[83] Plenty of technologies already exist for this, many created by the industry itself, such as schema.org, which underpins the metadata consumers use for seeing e.g. opening times in services like Google or Apple Maps.

---

81 Geoffrey C Bowker and Susan Leigh Star, *Sorting Things Out: Classification and Its Consequences* (MIT Press 1999); Kate Crawford and Trevor Paglen, 'Excavating AI' <https://excavating.ai>; Abeba Birhane, Vinay Uday Prabhu and Emmanuel Kahembwe, 'Multimodal Datasets: Misogyny, Pornography, and Malignant Stereotypes' (arXiv, 5 October 2021) <http://arxiv.org/abs/2110.01963>.

82 Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 Big Data & Society 2053951719897945.

83 Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé III, and Kate Crawford. 2021. Datasheets for datasets. Commun. ACM 64, 12 (December 2021), 86–92. https://doi-org.kuleuven.e-bronnen.be/10.1145/3458723; Milagros Miceli, Tianling Yang, Adriana Alvarado Garcia, Julian Posada, Sonja Mei Wang, Marc Pohl, and Alex Hanna. 2022. Documenting Data Production Processes: A Participatory Approach for Data Work. Proc. ACM Hum.-Comput. Interact. 6, CSCW2, Article 510 (November 2022), 34 pages. https://doi-org.kuleuven.e-bronnen.be/10.1145/3555623

Finally, where content is user generated, imposing direct requirements on platforms is hardly feasible, and platforms cannot or should not be expected to curate input content actively. However, this highlights the importance of the contestability of moderation decisions and the Terms of Use and Usage Policies those decisions are based on. The ability of, e.g. minority groups to effectively contest moderation or curation actions that unjustifiably limit the visibility of their content also matters for a right to meaningful optimisation.

Recommendation: Optimisation systems rely on explicitly or implicitly labelled data in order to function in line with user demands, and to meet legal requirements. Such labels should be publicly associated with records so they can be scrutinised. Taxonomies should also be publicly available to researchers and updated when they change in order so that the consequences of labelling the world in certain ways can be examined.

Recommendation: Whether the labelling of data is done internally or outsourced to third parties, it should be ensured that data work is performed under appropriate data labour standards as to avoid people's undue and unprotected exposure to mental and physical harm.

Recommendation: Content moderation decisions as well as the underlying Terms of Use themselves must be contestable and subject to scrutiny, including their proportionality and consequences for the ability of users to benefit from and exercise their fundamental rights.

3.5.2 Input data (users and environments)

User and environment data is a broad term that we use here to refer to data which does not relate to content. The term 'personal data' is inadequate for this because content may also be personal data of the individuals that it identifies and relates to. User data, in contrast, refers to the activities of users that are captured by actors within the optimisation stack. This may be data on clicks, views, follows, 'likes', telemetry data from sensors of devices like gyroscopes or Bluetooth, or data from the usage of other services that are captured by embedded trackers, such as 'pixel' trackers or software development kits (SDKs).

3.5.2.1 Sensitive data

As indicated above, individuals inside optimisation systems may be implicitly (and easily) grouped in ways which correlate to sensitive data categories. Article 9 GDPR (Processing of special categories of personal data) in effect requires private commercial entities to get explicit consent before the processing of certain categories of data that have been noted as relevant for recommender systems, such as sexuality, ethnicity or political opinion. While there are alternatives to consent, few will apply, and none routinely (see in this context, also our discussion above, including the pitfalls of relying on consent as a protective mechanism for individuals). Assessing the extent to which optimization systems create sensitive data from input data which has latent potential to be sensitive is a difficult task when labels for these

groups are not immediately available.[84] Some proposals for approaches which are privacy preserving exist, such as those using encrypted computation,[85] or those focussing on demographic data.[86] However, these methods need further exploration in context. The first step is to create knowledge of sensitivity in the context of optimisation systems, focussing on input data that may be permissible or impermissible to hold or collect.

The special categories of data show a strong connection with the "protected grounds" found in European non-discrimination law (the EU Equality Directives prohibit discrimination based on so-called race and ethnicity, sex, religion or belief, disability, age and sexual orientation). Yet, the efficacy of both applying and enforcing non-discrimination law in the digital environment has been questioned by scholars.[87] Among others, in discrimination law, a distinction is commonly drawn between direct and indirect discrimination on the basis of whether factors are explicitly used, or whether discriminatory effects can be observed. Unless expressly mandated, direct forms of discrimination are prohibited. Indirectly discriminatory rules or provisions can be objectively justified when they pursue a legitimate aim and the means of achieving that aim are appropriate and necessary. Due to the emergence of machine learning technologies, the conceptual distinction between direct and indirect discrimination has become increasingly blurred however: for instance, should the reliance on data that strongly correlates with a protected ground (i.e., proxy discrimination) be categorised as direct or indirect discrimination, and consequently, as justifiable or not? Moreover, in an era where people's self-determination and self-development can be undermined based on a variety of characteristics, one can question whether a narrow focus on a select number of exhaustively enumerated grounds can be maintained. Furthermore, each equality directive has a narrowly constructed scope, both on a personal (the protected grounds they cover) and material (the (market) domains in which they apply) scope, further limiting the amount of contexts and settings in which recommender systems could be captured by them.

Recommendation: Digital Services Coordinators should proactively work with data protection supervisory, equality bodies and vetted researchers to identify data that is likely to be sensitive or discriminatory in the context of an optimisation system, and to either mitigate its sensitivity and abusive or discriminatory use at the point of collection or to restrict its use. Such an evidence base will support the enforcement of both regimes.

---

84 Michael Veale and Reuben Binns, 'Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data' (2017) 4 Big Data & Society 205395171774353.

85 Niki Kilbertus and others, 'Blind Justice: Fairness with Encrypted Sensitive Attributes' in Jennifer Dy and Andreas Krause (eds), Proceedings of the 35th International Conference on Machine Learning, vol 80 (PMLR 2018) <http://proceedings.mlr.press/v80/kilbertus18a.html>.

86 McKane Andrus and others, 'What We Can't Measure, We Can't Understand: Challenges to Demographic Data Procurement in the Pursuit of Fairness', Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (ACM 2021) <https://dl.acm.org/doi/10.1145/3442188.3445888>.

87 Frederik J Zuiderveen Borgesius, Discrimination, Artificial Intelligence, and Algorithmic Decision-Making (Directorate General of Democracy, Council of Europe 2018). Jeremias Adams-Prassl, Reuben Binns and Aislinn Kelly-Lyth, 'Directly Discriminatory Algorithms' (2023) 86 The Modern Law Review 144. Janneke Gerards and Raphaele Xenidis, Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non Discrimination Law (Publications Office of the European Union 2021) <https://data.europa.eu/doi/10.2838/544956> accessed 12 August 2021. Naudts (2023), Fair or Unfair Differentiation? Reconsidering the Concept of Equality for the Regulation of Algorithmically Guided Decision-Making (Doctoral Dissertation)

3.5.2.2 Device data

Some optimisation stacks have been known to seek access to data obtained by or stored on users' *terminal devices*, such as their smartphones. Such data might include information about how users act, or information about users' environments, such as from sensors on the device, fitness trackers, or similar. Article 5(3) ePrivacy Directive (hereafter ePD) on the confidentiality of communications renders access to such data prohibited if not necessary for a service requested by the user, or not accompanied by the explicit consent of the user. Consent under Articles 4 and 7 GDPR, to which the definition in the ePD is linked, requires it to be specific and separate from other matters. However, as it stands, data from users' devices seems frequently used within optimisation systems without attempts to gather such consent. The issue is compounded by the limited fines possible under the ePD, although some Member States, such as France, have heightened them in national law to match those possible under the GDPR. It is further compounded by dispersed competences — while some countries have data protection and e-Privacy law handled by the same regulator, others place it in the hands of another regulator, typically a telecommunications regulator.

As it stands, little progress is being made on an ePrivacy Regulation, which would ideally place the responsibilities for enforcement in the same location as the data protection authority. Therefore it is important that regulatory co-operation includes the ePrivacy regulators in each member state.

As with other forms of data, the legal obligation to obtain free and informed consent in terms of device data echoes forward and seemingly obliges firms to be able to run recommendation *without* such data. Digital Services Coordinators and the Commission should both ensure that recommenders without device data are available as the selectable 'options' in terms of the regulation at the interface layer.

Recommendation: Regulatory co-operation should include national e-Privacy regulators.

Recommendation: As it should be optional to provide device data to a service for the unnecessary purpose of recommendation, such cooperation should ensure that a recommender without device data is selectable by all users explicitly.

3.5.2.3 Data access

Access to data is a fundamental right in the European Union under Article 8 Charter, and is enshrined, inter alia, in the GDPR, the Digital Markets Act (as portability), and potentially in the forthcoming Data Act (in relation to specific devices).[88] Data access in some of these instruments is not limited to data that is observed about an individual, but also that which is inferred

88 GDPR, art 15; Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89 (Law Enforcement Directive), art 14; 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) OJ L 265/1, art 6(9); European Commission, 'Proposal for a Regulation of the European

about them, such as opinions, whether from a computer or a human.[89] In theory, this would seem to allow an individual (or collectives of individuals) to inquire about what a recommender system 'thought' about them.

However, the data people get access to is often highly abstract in nature, as it has been turned into an 'embedding' — effectively a way of turning diverse sources of data into a way that can be used to compare people geometrically to how close they are to certain pieces of content, and each other. These embeddings have no direct human interpretation — they may be a vector of thousands of numbers between -1 and 1 that effectively represent coordinates in a high-dimensional space. On some of these dimensions, content may be close together (for example representing the fact they are in the same language, or in the same genre) while on other dimensions they may be further apart, in the various ways they are distinct. But this data is effectively *relative*. Having a copy of the embedding that describes a user or a piece of content is highly meaningful in the context of the wider infrastructure, but totally meaningless on its own, *because users have nothing to compare it to*. As a consequence, the right to access fails at its one of its main functions of allowing scrutiny and promoting accountability. This means that individuals looking for their digital 'alter ego' are unlikely to find it sufficiently using this approach.

Other approaches can be envisaged. Interactive services and explanations may be better at explaining the position of users within the data that is collected about them, but they would need proactive engineering to create. Regulators from multiple domains should collaborate to ensure these rights make sense within optimisation environments where data does not have human interpretable meaning.

Recommendation: Where services cannot provide effective scrutiny in response to rights of access due to the nature of the datasets and data systems, they should be obliged to invest in the creation of practical, interactive systems that serve an equivalent function, with suitable fidelity and detail.

3.6 Business-to-Business Interface

Summary: the ways that businesses interact with a service and in turn with consumers, which facilitate certain interactions and business practices over others. B2B interfaces are important as they mediate what information, settings and similar traders can provide in their interactions with platforms and online marketplaces. They have implications for liability across the supply chain as well as the location of the responsibility for compliance. They are important parts of the broader picture, and are regulated by the Fairness in B2B Platforms Regulation, and parts of the DSA, among others. We draw attention to it here but do not analyse it in detail, as it sits outside of the main focus of consumer groups.

Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM(2022) 68 final' (23 February 2022), art 5.

89 Jef Ausloos and Michael Veale, 'Researching with Data Rights' [2020] Technology and Regulation 136.

3.7 Connectivity Infrastructure

In certain systems, the underlying connectivity infrastructure can be important. For example, the governance of the optimisation systems of Facebook has been significantly changed by their Internet.org/Facebook Free Basics programmes, which increase reliance on those services and optimisation ecosystems compared to others, such as search engines on the open Web. These programmes are tie-ups with national telcos for zero-rating agreements for certain services, such as Facebook, while others outside the ecosystem, such as other apps and services, and access to search engines and their results more generally, cost more or require connection to WiFi.[90] In some jurisdictions, people reportedly use the Facebook search bar as a general search engine, which effectively heightens the reliance on certain types of optimisation as well as widens the number of use cases and societal role for these systems, heightening the governance stakes and scope.[91] In the EU, zero-rating is prohibited by the Open Internet Regulation, the EU's net neutrality instrument.[92] However, looking ahead, there is significant lobbying to undo and alter net neutrality in the EU, and the issue of connectivity infrastructure within the optimisation stack may become more relevant. This may particularly be the case in high mobile bandwidth areas such as virtual reality.

3.8 Whole-Stack Governance

Some regulatory provisions as well as some actors span the stack to a greater or lesser degree. These include

- **Operations and Management**
- **Accountability Groups, including civil society, (academic) research institutions, regulators and standardisation bodies**
- **Advertisers**
- **Individuals and communities**.

3.8.1 Operations and Management

Operations and Management encompasses the organisational aspects of platforms. They span the stack insofar as an actor is influential across it. A more centralised, vertically integrated platform might build the hardware, most of the apps, interfaces, collect the data, control the cloud services, and even run connectivity. Amazon, for example, builds a smart speaker (Echo), determines a lot of its interface (and steers the apps, or 'Skills', it does not), collects significant audio and transcription data, builds functionality with other 'smart home' tools in e.g. the Amazon Ring range, runs a huge proportion of the world's cloud services and machine learning tools, provides a business-to-consumer marketplace in the form of various online stores, and even runs its own telecoms network to link these devices together (Amazon Sidewalk). Other services, like Twitter/X, sit as an app with very little influence in domains of hardware or connectivity.

---

90 Toussaint Nothias, 'Access Granted: Facebook's Free Basics in Africa' (2020) 42 Media, Culture & Society 329.

91 Peter Cihon and Helani Galpaya, 'Navigating the Walled Garden: Free and Subsidized Data Use in Myanmar' (*LIRNEasia*, 2017) <https://perma.cc/22ED-CKKZ>.

92 See e.g. Case C-5/20 *Vodafone (Tethering)* ECLI:EU:C:2021:676.

In practice, the operations layer is a layer of human problem-solving capacity to deal with often unexpected, undesirable and unintended effects of running optimisation systems. Recommender systems require constant maintenance and can't just be left running. To consider aspects such as fairness takes continuous analytic capacity and significant organisational effort.[93]

Article 41 DSA (Compliance function) directly regulates compliance aspects of this layer, requiring compliance units of VLOPs and VLOSEs to be 'independent from their operational functions' and have 'sufficient authority, stature and resources [..] to monitor the compliance of that provider' with the DSA. The head of this function can only be removed by the management board of the VLOP or VLOSE. The GDPR or the draft AIA have no comparable direct requirements on firms, and it is notable these provisions apply only to VLOPs and VLOSEs — smaller entities do not have capacity obligations for their compliance functions.

This layer is ultimately responsible for compliance with individual aspects of governance in the stack, but it also has several overarching obligations which span these layers. Article 34 DSA (Risk assessment) requires VLOPs and VLOSEs to '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'. Article 37 DSA (Independent audit) requires the organisation of audits of certain DSA requirements, at those organisations' expense. Similarly, large-scale profiling of the sort carried out by entities in the optimisation stack is likely to trigger Article 35 GDPR (Data protection impact assessments), which require consideration of an extensive array of rights and freedoms. Other assessments may be required of users of recommenders as high-risk AI systems, if those provisions from the Parliament version of the draft AIA become law.

While, as we have seen, most consumer rights that the DSA offers concerning the regulation of recommenders do not go much deeper than the B2C interface level, the systemic risk provisions in Article 34 DSA are an example of a provision that potentially addresses the deeper layers of the recommender systems stack. The risk assessment must take place along the levels of the stack, including the B2C interface level (amplification and wide dissemination of illegal content), the operations level itself (decisions regarding the applicable terms and conditions), the input level (data-related practices of the provider), and the engine level (systems for selecting and presenting advertisements and design of the recommender system pursuant to Article 34(2)). Correspondingly, the mandatory mitigation measures can comprise different levels of the stack, including interaction with accountability groups such as trusted flaggers.

Articles 34 and 35 DSA acknowledge that recommendations can result from a complex interplay between different players and functionalities at different levels in the provision of recommendation services. Potential conflicts with, or failures to realise a right to self-determination and self-development can become relevant in the sense of systemic risks to the fundamental rights to human dignity, data protection, freedom of expression and non-discrimination to which Article 34 (1) explicitly refers. Having said so, identifying such a risk is left mainly to the platform's discretion. It does not include a corresponding obligation to design a recommender system in a way that promotes self-development and self-determination. This is likely a result of a difficulty in identifying a particular value to align with, but this can also be remediated by bringing representation, politics and accountability constructively *into* the process itself. The

93 Henriette Cramer and others, 'Assessing and Addressing Algorithmic Bias in Practice' (2018) 25 Interactions 58.

operationalisation of complex and nuanced values cannot be done in one go, but requires a process — the politicisation of the algorithmic, and the opening up of future possibilities.[94]

Recommendation: The DSA has a sufficient focus on risks but fewer focuses on positive, societally steered aims that optimisation systems might aim at. Participatory functions should be envisaged which create positive design obligations for actors behind optimisation stacks, rather than just a focus on avoiding downsides and pitfalls.

Recommendation: There should be organisational safeguards at the Operations/Management level to consider individual and societal interests, such as the right to self-determination and self-development, for example a dedicated role or team and processes to engage with external stakeholders and members of accountability groups as part of the process of defining optimisation goals. There should also be institutional support for individual and collective efforts to responsible recommender design, room for experimentation and learning and acknowledgement, for example as part of performance reviews.

In practice, the DSA seeks to provide additional capacity through Article 40 DSA (Data access and scrutiny) providing resources to external vetted researchers. However, the impact of this research — the closing of the loop from discovery to response or mitigation — is unclear. While Recital 90 DSA counsels that when carrying out risk assessments, providers should consider the state of the art, there is no obligation on providers to respond to the findings of researchers who have used their data in an open forum. Such a mechanism of dialogue is common in the security community, which has developed norms around responsible disclosure that rely on a dialogue with firms. A parallel obligation to foster such norms could be placed in this case.

Recommendation: Compliance and Risk Assessment Functions of organisations should have an obligation to consider and respond to research on their functionality. This obligation should require firms to publicly acknowledge issues discovered in optimisation systems, and publicly describe the actions they have and will take in response.

3.8.2 Accountability Groups

Where accountability groups are concerned, the EU's digital acquis concerning platforms relies heavily on external bodies for analysis and policing. Of particular relevance are the *vetted researchers* and *trusted flaggers* in Articles 22 and 40 DSA; the *representative bodies* in Article 80(2) GDPR; representatives of civil society and consumer protection organisations, and *worker groups* in Article 9 draft Platform Work Directive. Regulators too are accountability groups, and feature in most European legislation in this area in various forms and guises.

Such groups require capacity to operate. Funding is often scarce, and as such provisions that imagine a high-capacity sector just ready to go are often to face resourcing challenges

94 Louise Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others* (Duke University Press 2020).

undermining their effectiveness. This will be unevenly spread across the Union — certain jurisdictions simply have greater capacity in civil society than others.

Recommendation: Funding instruments for civil society and research organisations to hold optimisation systems to account should be considered. The independence of researchers that contribute to monitoring and enforcement actions must be respected and protected. The way research performances are evaluated and rewarded must be adjusted to acknowledge the activities that researchers engage in as part of their societal role under the new digital framework.

Other parts of the proposed digital *acquis* may provide inspiration for further provisions. The proposed Platform Work Directive creates roles for representatives to act on behalf of platform workers to scrutinise systems, with the support of technical experts if required.[95] Consumer bodies exist in every European jurisdiction and may play a similar role. In the draft Platform Work Directive, the ability to trigger an expert examination occurs when a significant change is made — this could be a trigger which requires e-commerce or similar platforms meeting a functionality and size threshold to consult with consumer bodies, and if the concern is significant, a cost transfer or cost sharing arrangement similar to the draft Platform Work Directive to fund an external expert with privileged access to systems could be envisaged.

Recommendation: The Commission should take inspiration from the draft Platform Work Directive and its provisions on supporting external expert analysis of platforms at a moment of significant change to consider a similar provision in relation to consumer bodies.

3.8.3 Individuals and Communities

Individuals and groups play a prominent role where rights are concerned. These may be existing rights, such as the right to access, the right to have certain recommender options, the rights to make complaints to platforms, or rights to judicial remedies against digital actors or their regulators.

To ensure whole-stack governance, regulators should establish an environment in which the actions and decisions of all actors that control the optimization stack, can be scrutinised. In order to establish a healthy digital ecosystem, processes should be envisaged that promote the democratic inclusion of those affected, or their representations.

Recommendation: During the ideation, design and development stage, operators should include meaningful consultation and representation of affected communities and consumers. Public consultations should be documented, including for what reasons citizens and communities were heard and how their feedback contributed to the design of the recommender systems in a demonstrable way.

95 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on Improving Working Conditions in Platform Work COM/2021/762 final' (9 December 2021), art 9(3).

Recommendation: Operators should enable third-parties (end-users, affected communities, civil society, etc.) to complain and make constructive suggestions.

Recommendation: Operators should explain and make available that enables third-parties to test and scrutinise optimisation goals and their impact on/relationship to public values and societal interests (a right to observability and access).

Recommendation: Operators should perform diversity, human rights, and systemic risk, impact assessment, taking into account individual, collective, social and democratic risks .

Recommendation: Operators should provide, either publicly, or through auditable documentation standards, insight into the data production processes and normative assumptions underlying recommender systems. This information could include the labour conditions under which systems were developed, trained and deployed he instructions provided to team members regarding the data production processes.

3.8.3.1 Right to be treated anonymously in commercial contexts?

Previous work from BEUC has indicated that it would be desirable to have a right to be treated anonymously in commercial contexts — or to 'shop anonymously'. This would not mean that no information is collected about individuals (after all, they need goods paid for and shipped to them), but instead their commercial environment is not optimised. This is related to, but not identical to, 'do-not-track' proposals in data protection and e-Privacy law.

A few considerations need to be made in this respect. Firstly, being online, on a website or an app, is structurally not anonymous. Tracking mechanisms abound, many of them illegal in nature.[96] Insofar as these are integrated with recommendation and optimisation, the problem of shopping anonymously is entwined with the problem of *browsing anonymously*. As a consequence, it is key to pay attention to the recent judgment in *Meta Platforms*,[97] which tries to place some data protection firewalls between online tracking and experiences in platform optimisation systems. Enforcement of existing data protection law is necessary to make such a right to shop anonymously even possible in the first place.

A second relevant dynamic here is the supply chain of plugins, software development kits, APIs and similar that underpin much e-commerce. A constant challenge is that commercial sites may simply not be aware of the ways in which their ranking, recommendation and tracking systems function. This breaks some of the logics behind, for example, data protection law, which requires data protection by design in Article 25 GDPR, but does not extend this requirement to suppliers of data services and tools which European businesses integrate. As a result, it cannot be said that many good parts, or building blocks, can be combined to make a good — or even basically compliant — whole. Only by grappling with this supply chain, which requires thinking across the stack, can this right be realistically accommodated.

---

96 Michael Veale and Frederik Zuiderveen Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law" (2022) 23 German Law Journal 226.

97 Case C-252/21 *Meta Platforms Ireland* ECLI:EU:C:2023:537.

Recommendation: A right to be treated anonymously in commercial context would require some foundational changes to the stack to be effective, including placing obligations on actors who are not data processor or controllers to only provide compliant or tracking-free tools.

While such a right to be treated anonymously could be accommodated quite easily for individuals who have logged in accounts, the logistics of this would need to be carefully considered for individuals who are browsing without logging in — presumably typical behaviour of individuals with these concerns, as consumers are already often advised to make use of 'private windows' and similar within Web browsers to avoid being judged and dynamically priced based on previous visits that have been associated with them through technologies such as cookies. One option is to present individuals with an option, like a pop-up or banner, upon entering every shop. This is likely to provoke significant backlash in an era of 'consent fatigue' (predominantly caused by firms attempting to continue to track illegally and gather invalid consent in the face of a *de facto* ban in European law). A better option, although an arguably more extreme one, is to forbid personalisation by default in situations where an individual is not 'logged in'. This effectively would forbid the commercial use of third-party tracking where an organisation did not have a pre-existing relationship with a user. Businesses may state that this is a disadvantage to smaller organisations, as large online marketplaces would have a greater likelihood an individual would be logged in, and potentially consent to such optimisation. However, this issue can be remedied with a series of federated and interoperable logins, such as OAuth 2.0. These do not share data (e.g., tracking data), but instead allow authentication without constant registration. Individuals using these (or affiliating existing accounts to them) can durably set preferences for or against optimisation (or on preferences as to which types, they prefer) that follow them across contexts. Preferences such as this cannot be set in a browser without creating a 'fingerprinting' risk (i.e. allowing users to be more easily tracked against their will).

Recommendation: The best way to implement a right to shop anonymously is to prohibit tracking and optimisation of marketplaces where a user is not logged in — where that shop does not have a relationship with that user, and thus cannot ascertain durable preferences. To tackle the dominance related issues this might cause, the Commission should promote and invest in federated, interoperable logins, and require them to be supported in certain contexts.

Conclusion

Recommender systems are not simply a service or tool to push certain contents on users – recommender systems are the engines that enable and shape the digital experience and interactions of users and form an important part of the overall digital communications infrastructure. They have become an invaluable tool in our understanding and navigation of digital information society; a means to discover, learn and pursue the information goals people deem valuable economy. Seeing the central role of recommenders in the digital marketplace, we argue that users should not only have a legitimate interest to be protected from risks that recommenders pose to fundamental rights or other legitimate interests. Instead, recommender systems should be regulated with the goal of promoting self-development and self-determination *for all*; positively harnessed to dismantle, rather than reinforce (structural) inequalities,

or realise the self-serving interests of a select few private actors. End-users and non-end-users, as individuals or as members of social groups or collectives, too have a legitimate interest in optimisation strategies that are inherently useful and meaningful to them. The citizen-consumer should be accounted for, and be given (constructive) account within, and as part of, optimisation. Concretely this means a need to rethink the governance of the recommender system from the perspective of users and society. Citizen-consumers should:

- Be enabled to understand the rules of engagement, including how systems function, for which purposes they have been optimised, and the consequences such optimisation strategies entail on the content users see
- Have an actual and actionable say in the optimisation goals pursued within digital ecosystems
- Exercise meaningful choice and voice, which requires the presence of alternative options, both in relation to a particular recommender system's functioning and in relation to other operators, including service-providers and platforms
- Be included, represented and having one's voice heard and recognised during the ideation, design, deployment and evaluation of recommender systems, meaning they should have access to participation and contestation mechanisms.

To realise such a right to constructive optimization we also need to change the metaphors we use when talking about recommender systems. Instead of the popular 'black box' metaphor that has informed the way recommender systems are regulated in the DSA and the AI Act, we propose using the stack metaphor. Recommenders are not a box. They are the result of a complex dynamic interplay between different processes, technology layers and actors. Using the stack metaphor, we were able to demonstrate the futility of an easy regulatory quick fix to achieve constructive optimization but we also demonstrated that there are various intervention points, regulatory options and frameworks that can and should be used. The stack metaphor also highlighted the current fragmented nature of recommender governance, and the need for more consistency across the interpretation, application and enforcement of the different relevant frameworks, like the DSA, DMA, AI Act and the Platform Workers Directive.

IV. Dissolution of EU Consumer Law Through Fragmentation and Privatisation

Hans-W. Micklitz[1]

1 I would like to thank Natali Helberger, Monika Namyslowska, Laurens Naudts, Marijn Sax, Peter Rott, Michael Veale – the co-authors of the anthology as well as Kasper Drazewski, Ursula Pachl from BEUC and Mateusz Grochowski for their comments, which helped me to sharpen my ideas. The responsibility remains mine alone.

1. Argument and methodology

The purpose of the report is to demonstrate how the existing consumer law acquis is superimposed by the EU Digital Policy Legislation, thereby accelerating a trend, which started much earlier together with the rise of services in the EU Internal Market. Two phenomena are of particular relevance, the *first* is the ever more sophisticated scope *sedes personae* on both sides of the consumer law acquis, on the side of the consumer, who became a customer in the service economy[2] and who is now turning into a citizen consumer[3] – to free ride on a language the European Commission tried to establish already in the service economy; on the side of the trader, through the differentiation in ever more fine-grained economic actors in the supply chain, which began in the EU product safety and product liability regulation in 1985 and which the EC and the EP are promoting in the EU digital policy legislation. The *second* phenomenon is what Natali Helberger calls the privatization of consumer law through the ever-stronger rise of due diligence obligations and the privatization of enforcement via compliance and conformity assessment with or without third parties.

The paper pursues a bottom-up approach in focusing on two pieces of the EU Digital Policy Legislation, – the AIA and the DSA – which are the ones that come closest to the EU consumer law acquis, even if they are not the only ones.[4] The intention is to lay bare the policy objectives of the EU as such, but also of the European Commission and the European Parliament. Therefore it does not suffice to look into the Articles of the AIA and the DSA but to analyse carefully the recitals in which many of the major conflicts are hidden as well as the different layers of regulation which result from the reliance on the New Approach/New Legislative Framework in the AIA and to some extent also in the DSA.[5] The bottom-up approach allows for highlighting differences between broadly worded policy objectives in the recitals and the rather opaque and underdeveloped concretisation in the articles of the AIA and the DSA, which open up space for private regulation, be it through (harmonised) technical standards, due diligence or codes of practices.

The argument is developed in the following way: the *second* part deals with scope *sedes personae* and indirectly with the scope *sedes materiae*. Analysing the two together is a necessary consequence of how consumer law has been built. The abstract categories of civil codes have been complemented by the consumer and the supplier/trader who are both defined through the activities they pursue. The analysis will demonstrate that ever more fine-grained categories on the side of the consumer and the trader can only be understood in connection to the rights and duties they are granted. The *third* and *fourth* parts dive deep into these obligations, now officially termed due diligence obligations, imposed on the supplier/trader/operator in the AIA and the DSA, to bring clarity into what exactly is expected from whom and what kind of guidance is provided by the law on the implementation of the due diligence obligations

2 A. Johnston, 'Seeking the EU 'Consumer' in Services of General Economic Interest', in D. Leczykiewicz and St. Weatherill (eds.), The Images of the Consumer in EU Law. Legislation, Free Movement and Competition Law (Oxford: Hart Publishing, 2016), pp. 93–138.

3 J. Davies, The European Consumer Citizen in Law and Policy (Basingstoke: Palgrave Macmillan, 2011).

4 Under Art. 3(25), personal data should be understood in line with GDPR, i.e. as data of natural persons (basically: of consumers). Art. 5(2) DMA speaks of end users which can be both natural and legal persons. In the outcome, we get the concept of personal data of a legal person introduced through the back door. For an extremely useful overview on the EU Digital Policy Legislation, G. Spindler, EU Internet Policy in the 2020s in A Savin and J. Trzaskowski (eds.), Research Handbook in Internet Law, Second Edition, 2023, pp. 2–39.

5 H.-W. Micklitz, The Role of Technical Standards in the EU Digital Policy Legislation, 2023.

through compliance and conformity assessment. This kind of stock-taking is a necessary step in identifying the regulatory gaps which result from the privatization of consumer law within a broadly defined regulatory frame. The *fifth* part brings together the intermediary findings of parts two, three and four, translated into long-term and short-term recommendations for policy action.

2. Consumers/Traders, the Vulnerable, Operators and Intermediaries

The AIA and the DSA, this is the overall hypothesis, are gradually deconstructing the rather well-established distinction between 'the consumer' and the 'supplier/trader' in EU (private) consumer law, in consumer contracts and commercial practices. Both are defined by way of their activities, the consumer through their non-commercial activities and the supplier/trader through their commercial activities. In EU (public) consumer law, most prominently in product safety regulation, which serves as a blueprint for the EU digital policy legislation, the starting point is different. Product safety regulation is meant to protect consumers against risks to their health and safety resulting from products intended to be used by consumers or are likely to be used by the consumers under reasonably foreseeable conditions. In the product liability directive, the consumer is also protected against economic harm.[6] In both product safety and product liability regulation, the addressees are defined through the products and their potential use and not via the type of activities – commercial/non-commercial.[7] The definition of the addressees via the type of products and the type of activities are standing side by side. The GPSR repeats the classical definitions of consumer versus supplier/trader of EU private consumer law.[8] The consequences of a product-related approach become even more visible on the side of the trader/supplier. The generic term is the economic operator, which comprises the manufacturer, the distributor, the importer, the service provider, the authorized representative and so on. The GPSR allocates the type of scope of responsibilities to the addressees in line with their suggested capacities to manage potential risks in the supply chain. The differentiation in product safety regulation is much more sophisticated than in the product liability directive, which begs the question of whether and to what extent the two pieces of EU law, can and should be aligned.[9]

The EU digital policy legislation follows the regulatory approach of the EU product safety regulation, with a decisive though crucial difference. The range of addressees is again defined through the subject matter – in the AIA health and safety and to some extent economic harm of the EP proposal and in the DSA through a *'safe, predictable and trusted online environment'*[10] – *but* contrary to product safety regulation the consumer and private consumption is only indirectly affected, at least in the EC proposal on the AIA, contrary to the EP proposal. The DSA contains one subsection dealing with the triangular relationship of platforms, consumers, and traders, but in all other parts, the consumer is not directly addressed. The EU digital policy legislation

6 M. Namyslowska, Future-Proofing the Unfairness Test in this report.
7 Art. 3 (1) Reg. 988/2023 GPSR
8 Art. 3 (17) and (18) Reg. 988/2023 GPSR
9 A. Beckers, Global Value Chains in EU law, Yearbook of European Law, forthcoming, Ch. Busch, 'When Product Liability Meets the Platform Economy: A European Perspective on Oberdorf v Amazon', (2019) Journal of European Consumer and Market Law, 173, 174.
10 Art. 1 (1) Reg. 2022/2065 DSA.

regulates the digital economy and the digital society. The scope is therefore much broader, in terms of the subject matter and terms of the addressees. The addressee is *the* digital economy – *digital business* per se and *the* digital society – no longer the consumer but the *citizen*, all citizens of the EU.[11] Somewhat emphatically one might argue that the EU is about to establish a genuine new economic order one that no longer distinguishes between various addressees but concerns the *'the economic operator'* and *'the affected'* to use the language of the DSA and the AIA in the EP proposal. The categories of the 'economic operator' and the 'affected' are not entirely homogenous though. Under the surface of an all-encompassing terminology reappears the broad array of economic operators known from product safety regulation and the ever-stronger distinction between 'the affected' and the 'vulnerable' as an umbrella term for the *'discriminated'*, the *'handicapped'*, the *'minors'* and the *'customers of universal services'*. In the following, we 'deconstruct' the manifold concepts used in the AIA, the DSA, ISO/IEC and IEEE – the three international standardisation organisations – on both sides of economic transactions and then re-construct the key categories in light of their impact on the EU consumer law acquis. The AI standards on which we rely are taken from previous research.[12]

a) Scope of AIA and DSA

According to Art. 2 AIA-EC the 'Regulation applies to: (a) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country; (b) users of AI systems located within the Union; (c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union. Art. 2 AIA-EP enlarges the scope in two ways, it includes the 'deployers of AI systems,' mentions importers and distributors more prominently, but addresses:

> *(cc) affected persons as defined in Article 3(8a) that are located in the Union and whose health, safety or fundamental rights are adversely impacted by the use of an AI system that is placed on the market or put into service within the Union.*

In theory, everyone can be affected by an AI system. The potential addressees are therefore all citizens. However, there remains a difference between the citizens and the 'affected'. The definition requires that the affectedness is triggered through the realisation of risks which are subject to specification in the AIA and controversy between the EC (health and safety) and the EP (also economic harm).

Art. 2 (5b) AIA-EP clarifies that this *'regulation is without prejudice to the rules laid down by other Union legal acts related to consumer protection and product safety'*, which sounds as if the AIA shall go beyond health and safety and the fundamental rights rhetoric and include the hard core of EU consumer law – the protection of their economic interest. However, a closer look reveals that the EP proposal lacks consistency. Recital 16 AIA EP looks promising, at least when regarded through the consumer lens: AI systems, that have the *'effect of materially distorting*

---

11 N. Helberger/ O. Lynskey/ H.-W. Micklitz/ P. Rott/ M. Sax/ J. Strycharz, EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets, A joint report from research conducted under the EUCP2.0 project, BEUC, March 2021, 207 pages; https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf.

12 H.-W. Micklitz, Role of Technical Standards in EU Digital Policy Legislation, 2023.

the behaviour of a person and in a manner that causes or is likely to cause significant harm to that or another person or groups of persons, including harms that may be accumulated over time' ....'as long as such harm results from the manipulative or exploitative AI-enabled practices'. The inclusion of economic harm is then concretised in Art. 5 AIA-EP:

> *The following artificial intelligence practices shall be prohibited (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm;*

Attention is to be drawn to 'significant harm'. The EP does not provide for a definition, neither for harm nor for signification harm, but concretises the meaning through the newly introduced distinction between 'risks' and 'significant risks':

> *Art. 3 Definitions*
>
> *(1a) 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm;*
>
> *(1b) 'significant risk' means a risk that is significant as a result of the combination of its severity, intensity, probability of occurrence, and duration of its effects, and its ability to affect an individual, a plurality of persons or to affect a particular group of persons;*

The AIA-EP is somewhat contradictory and full of highly conflictual terminology. The scope, Art. 1, does not mention economic harm. This only happens to be in Recital 61 and then more specifically in Art. 5 AIA-EP. The overall rationale seems to be that the economic harm might result from intentional manipulation or – much broader from *'deceptive techniques'*. However, not every harm is covered, only those which can be ranked as 'significant'. The regulatory technique is irritating as 'risks' resulting from the AI system and 'harm' the AI system might produce are put on an equal footing. The definition in Article 3 is not particularly illuminating. The language seems to relate to the control of unfair commercial practices in the UCPD which requires that the commercial practice is or is likely to *'materially'* distort the behaviour of the consumer, a criterion which is subject to extensive debate in legal scholarship, and which has not yet been clarified by the CJEU.[13] One may therefore doubt when and under what condition consumer harm is included. Manipulation requires intention, which the consumer may hardly be able to prove. The only variant which matters is *'deceptive techniques',* which includes the design and the architecture of the AI system.

Seen through the lens of the distinction between safety-related and non-safety-related economic consumer policy issues, the DSA is to be situated on the economic side. Art. 1 (1) requires that the *'safe, predictable and trusted online environment'* can only be achieved if the fundamental rights in the Charter and the *'principle of consumer protection'* are respected. Health, if it shows up at all, is mainly related to public health but without providing a definition, and consumer safety is taken care of only randomly. Thus far one might understand the DSA as the

13 Art. 1 e) Dir. 2005/29, H.-W. Micklitz/M. Namyslowska, Kommentierung der Richtlinie über unlautere Geschäftspraktiken, in: Münchener Kommentar zum UWG, 3. Auflage, 2020, Art. 5 Rdnr. 42

economic complement to the health-and-safety-related AIA (also in the revised EP proposal). The DSA leaves more space for freedom to do business and therefore limits itself, either to impose duties on the various addressees of the obligations or to encourage them to take voluntary measures and to establish and ensure self-compliance.

The 'principle of consumer protection', however, is the one enshrined in the existing consumer acquis. The DSA is going beyond the consumer acquis in at least a threefold way. The concept of advertising and contract terms is broader than the ones of the consumer acquis:

> *Art. 3 (r) 'advertisement' means information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and presented by an online platform on its online interface against remuneration specifically for promoting that information;*
>
> *(u) 'terms and conditions' means all clauses, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services and the recipients of the service;*

Advertising covers also '*non-commercial purposes*' and '*terms and conditions*' are not bound to standard terms.[14] Whilst the broadening of advertising results from the focus on content moderation in the DSA, the inclusion of even individually negotiated terms in B2B relations comes as a surprise as it seems to advocate what consumer activities have been longing for more than 30 years.[15] Article 25 DSA (dark patterns) has the potential to increase the protection of consumers, as *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*.[16] However, Article 25 (2) DSA immediately takes away this opportunity by stating: *The prohibition in paragraph 1 shall not apply to practices covered by Directive 2005/29/EC or Regulation (EU) 2016/679*. This exemption or reduction met strong resistance from BEUC but was nevertheless integrated into the final version of the DSA.[17]

b) Consumers

The benchmark, against which the AIA and the DSA are measured is the classical understanding of the consumer, who is buying products or services for non-commercial purposes.

---

14 On tendencies to use consumer law to deal with free speech, see M. Grochowski, Freedom of Speech, Consumer Protection and the Duty to Contract in. C. Mak and B. Kas (eds.) Civil Courts and European Polity, The Constitutional Role of Private Law Adjudication in Europe, 2023, 123.

15 On the conflict H. E. Brandner, P. Ulmer, The Community Directive on Unfair Terms in Consumer Contracts: Some Critical Remarks on the Proposal Submitted by the EC Commission, Common Market Law Review, Volume 28, Issue 3 (1991) pp. 647 – 662, https://doi.org/10.54648/cola1991036

16 P. Rott, Dark patterns im Verbraucherrecht, in: Maria Reiffenstein (ed.), Konsumentenpolitisches Jahrbuch 2023 (Verlag Österreich 2023), forthcoming.

17 Interview with BEUC and informal position paper on file with the author.

aa) AIA

The AIA-EC does not address consumers directly, nor can it be seen as a piece of consumer law. Nonetheless, the rules it establishes do affect consumers considerably, if indirectly through the establishment of a particular market order. The primary addressee is the professional 'user', Art. 3 (4) There is one notable and extremely relevant exception. Art. 52 (1) and (2) reach out to 'natural persons', this also means consumers. 'Certain risks' are all those which are neither prohibited nor high risks, in essence, all risks which result from online commercial transactions. The consumers should be *'informed that they are interacting with an AI system unless this is obvious from the circumstances and the context of use'*. The deficits of the endless stringing together of information obligations are well known. Here they are even more serious as the regulation does not provide for the obligation to explain neither the AI system as such nor what the possible result of the interaction might be. This gap is partly filled through ISO and IEEE standards in a way that forestalls future European harmonised standards, but that raises questions far beyond content about the legitimacy of putting the concretisation into the hands of standardisation organisations.[18]

The AIA-EP does not address consumers but introduces a new category of 'affected persons': Art. 3 (8a) *'affected person' means any natural person or group of persons who are subject to or otherwise affected by an AI system*'. The approach follows the rationale of product safety regulation. 'Consumer products' are replaced by 'AI systems' which are defined in Art. 3 (1) AIA-EC and AIA-EP. However, not least through the broad design of AI systems, the EP had to face the problem of how to recalibrate the scope of *sedes personae*. The AIA-EC very much builds on the purpose for which the AI system has been designed and which should be defined by the providers themselves. Throughout the AIA-EC the respective rules built on the 'intended purpose' – suggesting that it is for the provider of the AI system to delimit the potential purpose thereby excluding the perspective of potential users of the AI system. The AIA-EP broadens the scope in line with the inclusion of economic harm towards *'foreseeable mis/use'*[19] in the set of obligations imposed on high-risk system providers in Chapter 2, thereby opening the way to address all those who might *potentially* come into contact with the said AI system. These are the natural persons or – which is another novelty 'group of persons'. While the meaning of natural persons is plain, it is by no means clear from when it is possible to speak of 'a group'. The distinction might matter about deciding when economic harm is to be regarded as a 'significant risk', Art. 1) b) AIA-EP, where the same language applies. In sociology and psychology, three persons are already regarded as a group, in law there is no such commonly agreed understanding. Art. 72 AIA-EP makes the 'number of affected persons' one of the parameters to be considered when defining the sanction of a potential infringement. Recital 84b) AIA-EP seems to insinuate that the AI provider can identify the *'affected'* in advance and provide them with *'appropriate information'*, an idea which hardly makes sense in case of foreseeable misuse. The AI provider might eventually be able to foresee the misuse, but certainly not the potentially

18 See Micklitz, Role of Standards, loc. cit. pp. 63.

19 There is a huge debate in product safety regulation on the degree to which foreseeable use/misuse has to balanced out the intended use, Ch. Joerges/ J. Falke/ H.-W. Micklitz/ G. Brüggemeier, Sicherheit von Konsumgütern und die Entwicklung der Europäischen Gemeinschaft, (Englische Fassung: European Product Safety, Internal Market Policy and the New Approach to Technical Harmonisation and Standards – Reissued), Hanse Law Review 2010 Special Issue, http://hanselawreview.eu/wp-content/uploads/2016/08/HanseLRVol6No02.pdf.

'affected' in light of the overall difficulty of predicting the potential use of AI systems.[20] Particular problems result from the benchmark, the EP has in mind, which is the 'average consumer':

> *AIA-EP Recital (84b) Affected persons should always be informed that they are subject to the use of a high-risk AI system, when deployers use a high-risk AI system to assist in decision-making or make decisions related to natural persons. This information can provide a basis for affected persons to exercise their right to an explanation under this Regulation. When deployers provide an explanation to affected persons under this Regulation, they should take into account the level of expertise and knowledge of the average consumer or individual.*

Since the 1990s there has been a hot and never-ending debate on who the average consumer is and whether the average consumer should be counterbalanced through references to the vulnerable consumer.[21]

bb) DSA

The DSA reiterates the well-known concept of the consumer as a natural person not acting for purposes outside their trade, business, craft or profession, but then adds two new categories, the '*recipient*' and the '*active recipient*'. According to Art. 3 b) (b) DSA '*recipient of the service' means any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible*'. The definition includes the consumer in the broad variety of interactions they initiate with online platforms or online search engines. It is tied to a very particular activity – information seeking or information supply. Provided the activities reach beyond information seeking and providing, they are becoming 'active recipients' in the meaning of Art—3 (p) and (q), which again encompasses the consumer.

The side-by-side of consumer and recipient entails that the DSA ties particular rights and/or duties to the different addressees. The inclusion of 'additional provisions to providers of online platforms allowing consumers to conclude contracts with traders in section 4, dealing with traceability, compliance by design and information makes the distinction between consumers and recipients necessary. All other sections – the different layers of regulation imposing due diligence obligations dealing with the recipients as potential addresses – address consumers and businesses. Art. 6 (3) DSA enables the consumer to hold the online platform responsible if the information provided makes them believe that the platform is the trader.[22]

cc) ISO/IEC and IEEE

International standardisation organisations are involved in the elaboration of technical standards which are providing for definitions. Both ISO/IEC and IEEE are particularly active. These standards are to some extent publicly available, usually via the website of the organisations. However, they are copyright-protected, which is why they cannot be reproduced. The analysis

---

20 Computer scientists, mathematicians and physicists seem to agree that the potential use of an AI system cannot be foresee, see on use cases H.-W. Micklitz, Role of Standards, Role of Technical Standards, pp. 158.

21 More recently there is a growing interest in conceptualizing the vulnerable consumer, see below 2. c).

22 H.-W. Micklitz/ L. Adam, Information, Beratung und Vermittlung in der digitalen Welt, Workingpaper 6/2016 des Sachverständigenrates für Verbraucherfragen, Dezember 2016, http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP06_Information_Beratung_Vermittlung.pdf

is therefore limited in a twofold sense, by what is publicly available and by the limits set by copyright law. These standards have a manifold purpose. The aim is to make legal concepts accessible to the non-lawyers the engineers, the computer scientists, the software developer, the mathematician, and the physicists. So far, the standardisation organisations are quite successfully trying to translate legal language into accessible/colloquial language often complemented by examples for illustrative purposes. Their self-understanding is that standards are merely technical. Usually, they do not contain references to legal systems and if they refer to the law at all, international standardisation organisations state that this and that definition must be adapted to the particular legal environment in which the standard will be used. However, the borderline between translation into accessible language and delivering an interpretation of legal concepts is far less clear. In the European context, technical standards are opening markets, if they fulfil the requirements of harmonised technical standards, published in the Official Journal of the EU. Compliance with harmonised standards suggests a presumption of conformity with EU law, guaranteeing access to the EU Internal Market. Often EU harmonised technical standards as well as non-EU harmonised standards are elaborated on the basis and timewise after international standards.[23]

The ISO 22458:2022 *Consumer vulnerability — Requirements and guidelines for the design and delivery of inclusive service*[24] is a typical example of how ISO/IEC technical standards are operating. The preview allows one to read half of the overall standard and provides a table of contents, which suffices to understand the function and the purpose. ISO 22458:2022 deals with consumer vulnerability. To do so it contains under 3.3. a definition who is regarded as an individual member of the public, the end user of services or service-related products. The standard is accompanied by two notes, which explain by way of examples the range of potential and existing services. IEEE 7000-2021[25] follows a similar pattern, with a particular focus on AI though. Membership to the public is connected to the purchase of products for private purposes. IEEE 82079:1:2019[26] complements the notion of the consumer with a definition of the customer referring to a joint standard of ISO/IEC and IEEE. The customer can also be a legal person – an organisation, it can be a consumer, a client a user, an acquirer a buyer or a purchaser (ISO/IEC/IEEE12207).[27] The international standardisation organisations remain within the ambit of the classical understanding of the consumer in the meaning given to it by EU law.

c) Vulnerabilities

The rise of consumer law nationally, EU- and worldwide is inherently connected to the understanding that consumers need protection that they are weaker than businesses and that regulatory means are necessary. There was no distinction between the consumer and the weak consumer. In the 1970s or 1980s, it would have been a pleonasm to speak of a 'weak consumer'. The wind turned with the EU taking over consumer protection in the aftermath of the Single European Act. Now hand in hand with the CJEU's case-law the national advertising laws restricting market freedoms, the notion of the average consumer both born, which had to be delineated from the weak consumer for instance in the protection against unfair

23 P Delimatsis (ed), The Law, Economics and Politics of International Standardisation, CUP 2015.
24 https://www.iso.org/standard/73261.html
25 https://engagestandards.ieee.org/ieee-7000-2021-for-systems-design-ethical-concerns.html
26 https://www.beuth.de/de/norm/iec-ieee-82079-1/309141461
27 https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:12207:ed-1:v1:en

terms.[28] The recent two decades saw a revival of the weak consumer, now in the disguise of the vulnerable consumer.[29]

Three different strands are coming together: *first* the liberalization and partly privatization of formerly state-owned companies in the fields of finance, telecom (today electronic communication), energy and transport made it necessary to distinguish between 'customers' who could pay the market price and those who could not. The latter needs access at an economically affordable price. For decades there has been a debate on what exactly belongs to universal services, let alone the definition of economically affordable.[30] Here vulnerability is connected to the lack of economic resources. The *second* strand results from the harmonization of unfair commercial practices law, where an agreement on a full harmonization approach could only be reached once the notion of the average consumer was complemented through the newly introduced vulnerable consumer in Art. 5 (3) 2005/29/EC on Unfair Commercial Practices. Protection is limited to a 'clearly defined group' (sic!) being vulnerable due to their '*mental or physical infirmity, age or credulity*'. Legal scholarship spent a lot of ink[31] on concretising the four categories. In practice, however, Art. 5 (3) did not gain much importance, maybe because of the barriers to identifying the group, maybe because courts, in the Member States and the CJEU sought the solution in lowering the average consumer standard.[32] Timid efforts to re-introduce the vulnerable consumer in the EU consumer contract acquis led to a recital in the Consumer Rights Directive 2011/83 obliging traders to take the different capacities of consumers in the processing of information into account. The recitals still wait to be awakened to life.[33]

The *third* strand is deeply connected to the EU digital policy legislation. The horizontal character of the regulation, which concerns *the* digital economy and *the* digital society, might explain why already well-known vulnerabilities from the two previous strands are now mixed up with new ones such as discriminatory practices in AI systems running contrary to EU non-discrimination law and the increased vulnerabilities of handicapped people and of minors, which are more obvious and better visible in the digital economy and the digital society. It will have to be shown that the AIA and the DSA are bringing together all these different forms of vulnerabilities in a relatively unsystematic and incoherent way. That is not all yet. The EU digital policy legislation refers to vulnerabilities of AI systems, conquering the concept and giving it a twist, which points in a very different direction, away from personal vulnerability for whatever reason to system vulnerability, to the risk of cyber-attacks and the like (recital 53 AIA). The parallel to the European Convention of Human Rights springs to mind when plaintiffs – businesses and

28 H. Unberath, and A. Johnston, 'The double-headed approach of the ECJ concerning consumer protection' (2007) 44 Common Market Law Review 1237–1284.

29 M. Grochowski, Does European contract law need a new concept of vulnerability? EuCML 4/2021, 133 – 135.

30 M. Bartl, 'The Affordability of Energy: How much protection for the vulnerable consumer?' (2010) 33 Journal of Consumer Policy 225–245; A. Johnston, 'Seeking the EU 'Consumer' in Services of General Economic Interest', in D. Leczykiewicz and St. Weatherill (eds.), The Images of the Consumer in EU Law. Legislation, Free Movement and Competition Law (Oxford: Hart Publishing, 2016), pp. 93–138.

31 D. Leczykiewicz and St. Weatherill (eds.), The Images of the Consumer in EU Law. Legislation, Free Movement and Competition Law (Oxford: Hart Publishing, 2016)

32 H. Schebesta and K.P. Purnhagen, The Behaviour of the Average Consumer: A Little Less Normativity and a Little More Reality in the Court's Case Law? Reflections on Teekanne (June 6, 2016). 41 European Law Review, 2016, p.590–598, Available at SSRN: https://ssrn.com/abstract=2790994

33 Sachverständigenrat für Verbraucherfragen, Personalisierte Verbraucherinformation: Ein Werkstattbericht, Dokumentation einer Veranstaltung des SVRV, Veröffentlichungen des Sachverständigenrats für Verbraucherfragen, 2022, https://www.conpolicy.de/aktuell/personalisierte-verbraucherinformation-ein-werkstattbericht

citizens/consumers – discovered the potential to turn economic rights into human rights.[34] There is an urgent need to conceptualise vulnerability, a task, which reaches beyond the purpose of this report.[35] In the following we will proceed as follows: first, we will demonstrate how the AIA, the DSA, ISO/IEC and IEEE are referring to all sorts of vulnerabilities before we look deeper into two forms, which are about to gain a certain prominence: disabilities and minors. The few references in the investigated material do not justify a separate analysis of the relationship between vulnerability and universal service obligations.

aa) AIA-EC and AIA-EP

Overall, the AIA-EP is more developed and more specific on what vulnerabilities might mean. The *bold* parts in the reprints are taken from the original document of the EP. The non-bold parts are the ones in the original EC proposal.

The first set of references in Amendment 38 deals with brain-computer interfaces and the reasons why they should be prohibited. Recital 16 combines the second strand (Art. 5 (3) UCPD with vulnerabilities resulting from the social and economic situation.

> (16) The placing on the market, putting into service or use of certain AI systems ***with the objective to or the effect of materially distorting*** human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. ***This limitation should be understood to include neuro-technologies assisted by AI systems that are used to monitor, use, or influence neural data gathered through brain-computer interfaces insofar as they are materially distorting the behaviour of a natural person in a manner that causes or is likely to cause that person or another person significant harm.*** Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of ***individuals*** and ***specific groups of persons*** due to their ***known or predicted personality traits,*** age, physical or mental incapacities***, social or economic situation***.

EP Amendment 39 inserts a new recital on the prohibition of profiling, highlighting the risk of discrimination under reference to the Charter. The AIA-EC does not contain such a prohibition.

> ***(16a) AI systems that categorise natural persons by assigning them to specific categories, according to known or inferred sensitive or protected characteristics are particularly intrusive, violate human dignity and hold great risk of discrimination. Such characteristics include gender, gender identity, race, ethnic origin, migration or citizenship status, political orientation, sexual orientation, religion, disability or any other grounds on which discrimination is prohibited under Article 21 of the Charter of Fundamental Rights of the European Union, as well as under Article 9 of Regulation (EU)2016/769. Such systems should therefore be prohibited***.

EP Amendment 40 addresses social scoring, pointing to dignity, non-discrimination, equality, and justice without reference to the Charter though-

---

34 J. Abrisketa, C. Churruca, C. de la Cruz, L. García, C. Márquez, D. Morondo, M. Nagore, L. Sosa, A. Timmer, Human rights priorities in the European Union's external and internal policies: an assessment of consistency with a special focus on vulnerable groups, European Commission 2015.

35 G. Malgieri, Vulnerability and Data Protection Law, OUP 2023.

> *(17) AI systems providing social scoring of natural persons for general purpose may lead to discriminatory outcomes and the exclusion of certain groups. They violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify natural persons* ***or groups*** *based on* ***multiple data points and time occurrences related to*** *their social behaviour in multiple contexts or known****, inferred*** *or predicted personal or personality characteristics. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. Such AI systems should be therefore prohibited.*

Amendment 40 deals with remote biometric identification and stresses the risks to age, ethnicity, sex or disabilities.

> *(18) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces* ***is*** *particularly intrusive* ***to*** *the rights and freedoms of the concerned persons,* ***and can ultimately*** *affect the private life of a large part of the population, evoke a feeling of constant surveillance****, give parties deploying biometric identification in publicly accessible spaces a position of uncontrollable power*** *and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights* ***at the core to the Rule of Law. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities****....*

Amendment 50 prohibits the use of AI by law enforcement authorities to make predictions, due to the risk of discrimination, of infringing human dignity and the principle of the presumption of innocence.

> ***(26a) AI systems used by law enforcement authorities or on their behalf to make predictions, profiles or risk assessments based on profiling of natural persons or data analysis based on personality traits and characteristics, including the person's location, or past criminal behaviour of natural persons or groups of persons for the purpose of predicting the occurrence or reoccurrence of an actual or potential criminal offence(s) or other criminalised social behaviour or administrative offences, including fraud predicition systems, hold a particular*** *risk of discrimination against certain persons or groups of persons, as they violate human dignity as well as the key legal principle of presumption of innocence****. Such AI systems should therefore be prohibited****.*

Amendment 52 concerns the justification for the prohibition of tracing the emotional state of individuals legitimated through insufficient and unreliable technology, particularly regarding border control, workplace and education.

> ***(26c) There are serious concerns about the scientific basis of AI systems aiming to detect emotions, physical or physiological features such as facial expressions, movements, pulse frequency or voice. Emotions or expressions of emotions and perceptions thereof vary considerably across cultures and situations, and even within a single individual. Among the key shortcomings of such technologies, are the limited reliability (emotion categories are neither reliably expressed through, nor unequivocally associated with, a common set of physical or physiological movements), the lack of specificity (physical or physiological expressions do not perfectly match emotion categories) and the limited generalisability (the effects of context and culture are not sufficiently considered). Reliability issues and consequently, major risks for abuse, may*** *especially* ***arise when deploying the system in real-life situations related*** *to law enforcement, border management, workplace and educational institutions****. Therefore, the placing on the market, putting into service, or***

use of AI systems intended to be used in these contexts to detect the emotional state of individuals should be prohibited.

Amendment 54 deals with the reasons which could be brought forward to amend the list of prohibited practices: fundamental rights, democracy, rule of law, environment but not vulnerabilities.

(27) High-risk AI systems should only be placed on the Union market, put into service ***or used*** *if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law,* ***including fundamental rights, democracy, the rule of law or the environment. In order to ensure alignment with sectoral legislation and avoid duplications, requirements for high-risk AI systems should take into account sectoral legislation laying down requirements for high-risk AI systems included in the scope of this Regulation, such as Regulation (EU) 2017/745 on Medical Devices and Regulation (EU) 2017/746 on In Vitro Diagnostic Devices or Directive 2006/42/EC on Machinery.***

Amendment 56 lays down and specifies the fundamental rights to be considered when assessing the adverse impact of AI systems. Consumer protection is mentioned but not in the context of harm contrary to environmental protection.

(28a) The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and nondiscrimination, right to education, *consumer protection,* ***workers' rights, rights of persons with disabilities, gender to an effective remedy and to a fair trial, right of defence and the presumption of innocence, right to good administration. In addition to those rights, it is important to highlight that*** *children* ***have specific rights as enshrined in Article 24 of the EU Charter and in the United Nations Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the*** *children's vulnerabilities* ***and provision of such protection and care as necessary for their well-being. The fundamental right to a*** *high level of environmental protection* ***enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons or to the environment.***

Amendment 65 deals with the use of AI systems in education being classified as high-risk carrying risks to perpetuate historical patterns of discrimination***, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation.***

(35) Deployment of AI systems in education is important in order to help modernise entire education systems, to increase educational quality, both offline and online and to accelerate digital education, thus also making it available to a broader audience... such systems ***can be particularly intrusive and*** may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination***, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation***

Amendment 65 handles risks to the users of universal services (broadly understood) and participation in society, resulting in particular from credit scoring and the justification for being classified as high risk.

> *(37) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services, including healthcare services, and essential services, including but not limited to housing, electricity, heating/cooling and internet, and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, gender, disabilities, age, sexual orientation, or create new forms of discriminatory impacts.* ***However, AI systems provided systems provided for by Union law for the purpose of detecting fraud in the offering of financial services should not be considered as high-risk under this Regulation.*** *Natural persons applying for or receiving public assistance benefits and services from public authorities, including healthcare services and essential services, including but not limited to housing, electricity, heating/cooling and internet, are typically dependent on those benefits and services and in a* ***vulnerable*** *position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be denied, reduced, revoked or reclaimed by authorities, they may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy. Similarly, AI systems intended to be used* ***to make decisions or materially influence decisions on the eligibility of natural persons for health and life insurance may also have a significant impact on persons' livelihood and may infringe their fundamental rights such as by limiting access to healthcare or by perpetuating discrimination based on personal characteristics****. Those systems should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. Finally, AI systems used to evaluate and classify* ***emergency calls by natural persons*** *or to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.*

The rather extensive references to the different variations of vulnerabilities are not or only to a very limited extent reflected in the Articles of the AIA themselves. They show up three times, in Art. 5 regulating the placing on the market of AI systems, in Art. 15 (4) sub (3) dealing with vulnerabilities of the system and in Art. 65 dealing with market surveillance. They do not reappear in the various Annexes, listing the prohibited risks, the high risks and/or the conditions under which the list could be amended.

> *Art. 5 (1) The following artificial intelligence practices shall be prohibited:*
>
> *(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a* ***person or a*** *specific group of persons* ***including characteristics of such person's or a such group's known or predicted personality traits or social or economic situation*** *age, physical or mental* ***ability with the objective or to the effect of*** *materially* ***distorting*** *the behaviour of* ***that person or*** *a person about that group in a manner that causes or is likely to cause that person or another person* ***significant*** *harm;*

> *Art. 65 (2) Where the national supervisory authority of a Member State has sufficient reasons to consider that an AI system presents a risk as referred to in paragraph 1, it shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation. When risks to fundamental rights are present, the* ***national supervisory authority*** *shall also* ***immediately*** *inform* ***and fully cooperate with*** *the relevant national public authorities or bodies referred to in Article 64(3);* ***Where there is sufficient reason to consider that that an AI system exploits the vulnerabilities of vulnerable groups or violates their rights intentionally or unintentionally, the national supervisory authority shall have the duty to investigate the design goals, data inputs, model selection, implementation and outcomes of the AI system. The relevant operators shall cooperate as necessary with the selection, implementation and outcomes of the AI system. The relevant operators shall cooperate as necessary with the national supervisory authority and the other national public authorities or bodies referred to in Article 64(3);***

The mismatch between the extensive recitals and the rather underdeveloped reflection of the arguments about vulnerabilities in the Articles themselves is highly problematic. The EU legislature neither the European Commission nor the European Parliament has made any effort to think more systematically about vulnerabilities and how they could be integrated into EU digital policy legislation. Sometimes one gets the impression that the references are sprinkled into the text to inflate it and to create links to other EU rules, such as the UCPD, non-discrimination law, universal services, consumer credit, and life and health insurance.

bb) Summary of Arguments in the AIA

The following table sums up the arguments brought forward mainly in the recitals justifying the prohibition of AI systems as well as the conditions under which high-risk AI systems may operate. The regulatory technique invites all those who are defending the interests of the vulnerable, such as non-governmental organisations to extend the list of references to rights or particular forms of discrimination to make sure that the interests of their clients are fully taken care of. From a consumer law perspective, one might easily raise questions about why a particular right, a particular form of discrimination or a particular group of vulnerable persons is mentioned and others are not. The more targeted the prohibition the easier to identify vulnerabilities and vice versa.

The *first* horizontal column is characterizing the type of risk – prohibited, high-risks, the *second* is the type of AI system at stake and the *third* is the reasons brought forward. The last line provides for a preliminary assessment. It tries to identify the overall regulatory rationale through the lenses of consumer protection and more particularly considering the EP proposal to include economic harm to consumers, to a limited extent though. It is hard to identify patterns in the references, for instance, to relate risks to various forms of vulnerabilities.

Type of risk prohibited	prohibited	prohibited	prohibited	prohibited	prohibited	amending list of high-risks	adverse impact of AI systems on FR	high risk	high risk
Type of AI system brain-computer interface	profiling	social scoring	biometric identification	prediction in law enforcement	emotional stage of the individual	new risks to be identified	generally applicable	education	credit scoring, universal services, social participation, life and health insurance
Reasons social and economic situation	non-discrimination under the Charter	dignity, non-discrimination, equality and justice	age, ethnicity, sex, disabilities	discrimination, human dignity, presumption of innocence	insufficient technology, law enforcement, border control, workplace, education	fundamental rights, democracy, rule of law, environment	fundamental rights are specified, as consumer protection	historical patterns of discrimination against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation	credit = discrimination, Universal services = right to social protection, non-discrimination, human dignity or an effective remedy insurance = non-discrimination
comments social and economic situation – vulnerable consumers				future key role of ODR as a de facto substitute for judicial litigation	vulnerabilities of consumers in video run online dispute resolution	vulnerabilities are not mentioned as an overall category	consumer protection is mentioned but not in the context of economic harm different from the environment		social participation – and the role of consumers in the consumption process

cc) DSA

The DSA whilst dealing with consumers and whilst containing a whole chapter on distance contracts consumers may conclude with traders through online platforms, there are safeguards to protect vulnerable consumers particularly or vulnerable groups more broadly within the various rules addressed to large and very large online platforms. The search for references to vulnerabilities leads to some meagre references in connection with trusted flaggers, advertising, recommender systems and codes of conduct.

The first reference in Recital 62 is related to trusted flaggers, which after registration and after approval of the national competent authorities are entitled to submit notices to online platforms to push them into action. In a richly convoluted language, the recital seems to refer to trusted flaggers which are focusing their capacities on the protection of 'vulnerable recipients', which could also be consumers. The only category mentioned is minors. The DSA does not, however, provide for safeguards or priorities for trusted flaggers focusing on the protection of the vulnerable recipients – in the large meaning given to it in the EU digital policy legislation.

> *(62) The rules of this Regulation should not prevent the providers of online platforms from making use of such trusted flagger or similar mechanisms to take quick and reliable action against content that is incompatible with their terms and conditions, in particular against content that is harmful to* ***vulnerable recipients of the service, such as minors*** *(emphasis added HWM).*

In the context of the advertisement, Recital 69 refers to what is broadly understood as personalised advertising[36] and the risk resulting from the exploitation of vulnerabilities (again not defined). The recital refers to Art. 22 GDPR on profiling and must also be read in connection with the prohibitions and limitations provided for in the AIA, once adopted. As a self-standing policy, Recital 69 is not very helpful. The mentioned rules on setting an end to dark patterns do not address B2C relations but are limited to B2B. About b2c relations, the European Commission relies on the available tools under the UCPD.[37]

> *(69)* ***When recipients of the service are presented with advertisements based on targeting techniques optimised to match their interests and potentially appeal to their vulnerabilities,*** *this can have particularly serious negative effects. In certain cases, manipulative techniques can negatively impact entire groups and amplify societal harms, for example by contributing to disinformation campaigns or by discriminating against certain groups. Online platforms are particularly sensitive environments for such practices and they present a higher societal risk. Consequently, providers of online platforms should not present advertisements based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679, using special categories of personal data referred to in Article 9(1) of that Regulation, including by using profiling categories based on those special categories. This prohibition is without prejudice to the obligations applicable to providers of online platforms or any other service provider or advertiser involved in the dissemination of the advertisements under Union law on protection of personal data (emphasis added HWM).*

Recommender systems are playing in key role in the daily business of platforms and search engines. They are dealt with in a separate part of the report.[38] Recital 94 addresses recommender systems of VLOPs and the VLOSs which are obliged to offer two different sets of services – one based on profiling within the limits of the GDPR and AIA, one not based on profiling – about the main parameters. The same recital aims at the protection of personalised information that might lead to discrimination of persons in vulnerable situations – without specifying and explaining what kind of vulnerable situations the DSA has in mind. All that we learn is vulnerability must be examined and assessed on a case-by-case basis. Such a mandate is vague. Mitigating risks requires a definition of what should be the subject matter. Here we are back to non-discrimination which seems to be somehow equated with vulnerabilities.

> *(94) The obligations on assessment and mitigation of risks should trigger,* ***on a case-by-case basis****, the need for providers of very large online platforms and of very large online search engines to assess and, where necessary, adjust the design of their recommender systems,* ***for example by taking measures to prevent or minimise biases that lead to the discrimination of persons in vulnerable situations****, in particular where such adjustment is by data protection law and when the information is* ***personalised*** *on the basis of special categories of personal data referred to in Article 9 of the Regulation (EU) 2016/679. In addition, and complementing the transparency obligations applicable to online platforms as regards their recommender systems, providers of very large online platforms and of very large online search engines* ***should consistently*** *ensure that recipients of their service enjoy alternative options which are not based on profiling, within the meaning of Regulation (EU) 2016/679, for the main parameters of their recommender systems. Such choices should be directly accessible from the online interface where the recommendations are presented. (emphasis added HWM)*

---

36 Helberger et al. loc. cit. EU Consumer Protection 2.0.

37 COMMISSION NOTICE, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, OJ 29.12.2021, C 526/1

38 N. Helberger and M. Sax Digital Vulnerability and Manipulation in the Emerging Digital Framework, in this report.

> *(95) Advertising systems used by very large online platforms and very large online search engines pose particular risks and require further public and regulatory supervision on account of their scale and* ***ability to target and reach recipients of the service based*** *on their behaviour within and outside that platform's or search engine's online interface. Very large online platforms or very large online search engines should ensure* ***public access to repositories of advertisements*** *presented on their online interfaces to facilitate supervision and research into emerging risks brought about by the distribution of advertising online, for example in relation to illegal advertisements or manipulative techniques and disinformation with a real and foreseeable negative impact on public health, public security, civil discourse, political participation and equality.* ***Repositories should*** *include the content of advertisements, including the name of the product, service or brand and the subject matter of the advertisement, and related data on the advertiser, and, if different, the natural or legal person who paid for the advertisement, and the delivery of the advertisement, in particular where targeted advertising is concerned.* ***This information should include both information about targeting criteria and delivery criteria, in particular when advertisements are delivered to persons in vulnerable situations, such as minors*** *(emphasis added HWM).*

Codes of conduct are at the very end of the six different layers of EU Digital Policy legislation, ranging from binding to semi-binding law to voluntary codes.[39] The DSA provides for a whole bunch of codes of conduct about various practices and differing purposes, Articles 44–47. There is only one form of vulnerability which is addressed in recital 102 as well as in the DSA – this is the protection of minors.[40]

(104) It is appropriate that this Regulation identify certain areas of consideration for such codes of conduct. In particular, risk mitigation measures concerning specific types of illegal content should be explored via self- and co-regulatory agreements. Another area for consideration is the possible negative impacts of systemic risks on society and democracy, such as disinformation or manipulative and abusive activities or any ***adverse effects on minors****. This includes coordinated operations aimed at amplifying information, including disinformation, such as the use of bots or fake accounts for the creation of intentionally inaccurate or misleading information, sometimes with a purpose of obtaining economic gain,* ***which are particularly harmful for vulnerable recipients of the service, such as minors****. In relation to such areas, adherence to and compliance with a given code of conduct by a very large online platform or a very large online search engine may be considered as an appropriate risk mitigating measure. The refusal without proper explanations by a provider of an online platform or of an online search engine of the Commission's invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform or the online search engine has infringed the obligations laid down by this Regulation. The mere fact of participating in and implementing a given code of conduct should not in itself presume compliance with this Regulation (emphasis added HWM).*

The four different types of voluntary action concern standards, codes of conduct in general and codes of conduct for online advertising and accessibility. The regulatory approach is interesting in that the European Commission is supposed to take the role of driver. But none of them deals with vulnerabilities more generally. The 'standards' refer to the protection of minors and the codes of conduct for accessibility for disabilities.[41]

---

39 H.-W. Micklitz/G. Sartor Compliance and Enforcement in the AIA in G. De Gregorio, O. Pollicino, P. Valcke (eds.) Oxford Handbook on Digital Constitutionalism, OUP upcoming 2024.

40 See for more details under 2 e).

41 For details see under 2 d) and e).

dd) ISO

ISO is at the forefront of the development in using technical standards to design vulnerabilities first in product safety and today in AI. Product Safety Standard ISO 10377 has a clearly worded section on understanding consumers and how they use products in generic terms. ISO 22458 on Consumer Vulnerability provides a well-drafted generic practice for obtaining information about consumers for the design of online services. Both standards are promising at a generic level of what good practice looks like. However, when it comes to specific physical access capabilities the conflicts between those who draft the standards and those who are affected immediately burst. The shifting focus to mental capacities in the digital economy and society has not yet reached the standardisation bodies.

ISO 10377:2013[42] provides practical guidance to suppliers on assessing and managing the safety of consumer products, including effective documentation of risk assessment and risk management to meet applicable requirements. ISO 10377:2013 describes how to identify, assess, reduce or eliminate hazards; manage risks by reducing them to tolerable levels; and provide consumers with hazard warnings or instructions essential to the safe use or disposal of consumer products. ISO 10377:2013 is intended to apply to consumer products but might also apply to decisions concerning safety in other sectors. Under 2.30 it lays down a definition of the vulnerable consumer, resulting from age, reduced literacy, physical disabilities or access to information. [43]

ISO 22458:2022 Consumer Vulnerability — Requirements and Guidelines for the Design and Delivery of Inclusive Services[44] specify requirements and guidelines for organisations on how to design and deliver fair, flexible and inclusive services that will increase positive outcomes for consumers in vulnerable situations and minimise the risk of consumer harm, even through the exclusion of children from particular services. The standard deals with organizational culture strategy, and inclusive design and guides how to identify and respond to consumer vulnerability. The publicly available preview delivers first a circumscription of what consumer vulnerability might be – under 01 and then defines under 02 the possible impact factors of vulnerability on individuals.

The approach in ISO 22458:2022 is to be taken as a serious effort to conceptualize 'vulnerability' very differently and far more forward-looking than the EU legislation, be it the consumer acquis or the digital policy legislation. Two constitutive elements of the ISO concept on vulnerability are worth mentioning: vulnerability is regarded as an individual personal characteristic – everybody can be vulnerable, the second is the broad set of impact factors which may trigger vulnerability – they can be personal – result from limitations in individual capacities, – situational resulting from managing information; getting access or choose suitable services; having difficulties to make decisions in the best interests, understanding their particular rights or pursue their rights – coming from the market environment – a criterion which is mentioned but seems rather underdeveloped at least in the preview. These explanations and interpretations are then translated into a definition of consumer vulnerability under 3.5. and of vulnerable situations, which can be temporary, sporadic, or permanent.[45] What is missing though or what at best hints here and there is the structural dimension of vulnerability. It is enshrined in the market environment dimension and the permanent character of vulnerable situations but is not

42 https://www.iso.org/obp/ui/en/#iso:std:iso:10377:ed-1:v1:en
43 https://www.iso.org/obp/ui/en/#iso:std:iso:10377:ed-1:v1:en
44 https://www.iso.org/standard/73261.html
45 https://www.iso.org/obp/ui/en/#iso:std:iso:22458:ed-1:v1:en

concretised. However, business is encouraged to actively address vulnerabilities to improve their image and their business opportunities.

ee) EC standardisation request and ESOs

The standardisation request mandated by the European Commission forms the core of the New Approach/New Legislative Framework which governs the elaboration of harmonised standards through the European Standardisation Organisations – the ESOs. The standardisation request can be accepted or rejected by the ESOs. If they accept, they receive co-financing from the European Commission and the final result, once approved the harmonised standard is published in the Official Journal. [46] Compliance with harmonised standards guarantees the presumption of conformity with binding legal requirements in EU product safety regulation, now with the EU digital policy legislation and paves the way for EU-wide marketing of the product/AI system.

In parallel with the ongoing finetuning of the AIA and before the adoption of the AIA, the European Commission developed a working programme on AI standards and published a Standardisation Request which mirrors the different due diligence obligations imposed on the AI service provider or deployer (in the EP proposal) under 'Title III High-Risk AI Systems Chapter 3 Obligations of providers and deployers of High-Risk AI Systems'.[47] They are translated into 10 mandates: Risk management system for AI systems, Data and data governance, Record keeping through logging capabilities, Transparency and information to the users, Human oversight, Accuracy specifications for AI systems, Robustness specifications for AI systems, Cybersecurity specifications for AI systems, Quality management system for providers of AI systems, including post-market monitoring process, Conformity assessment for AI systems.

The main text of the Standardisation Request does not have a single reference to 'vulnerability'. 'Disabilities' are mentioned once. In the Annex where the ten mandates are specified, vulnerability is only referred to in connection with the vulnerability of the AI system. One has to let this finding melt on the tip of one's tongue. Vulnerabilities are referred to in the recital, watered down in the Articles of the AIA and the DSA and vanishing in the mandated technical standards. It seems as if the EC wanted to avoid the term. The respective standard, this is how the European Commission formulates, has to establish '*procedures for detecting and addressing biases and potential for proxy discrimination or any other relevant shortcomings in data*' and the envisaged standard on 'Transparency and information to the users' has to provide for specifications on *'the need to identify and appropriately distinguish information, that is relevant and comprehensible for different professional user-profiles and non-professional users'*. There is no mandate to develop harmonised standards on the technical documentation. It is highly likely though that the addressees of the documentation duties will develop a standardised format, together with Article 12 'Recording keeping' which requires a machine-readable format.

The only document I could find is the CEN-CENELEC Workshop on 'Age Appropriate Digital Services Framework'[48] OVE and IEEE SA identified a need for developing a framework on

46 Details in H.-W. Micklitz, Role of Technical Standards, loc.cit. pp. 129.

47 Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, Brussels, 22.5.2023, C(2023) 3215 final with Annexes and their analysis, Micklitz, Role of Technical Standards, loc. cit.

48 https://www.cencenelec.eu/news-and-events/news/2022/workshop/2022-03-28-digitalservices/

age-appropriate digital services for situations where users are children, and by doing so, tailors the services that are provided so that they are age appropriate: *The framework will consider the following areas: 1. Their rights, 2. Their vulnerabilities, 3. Their autonomy, 4. Their health and well-being, 5. Their age and capacity, 6. Their need to fully understand, and well-being 5, Their age and capacity, 6. Their need to fully understand, 7. Duties of digital service providers.* This document has to be read against the much more advanced and much more developed ISO/IEC and IEEE standards on age verification to be dealt with later.[49]

d) Disabilities

The integration of disabilities into 'vulnerabilities' has already been analysed. Disabilities are seen as one form of vulnerability very much aligned with non-discrimination law. A deeper look is needed as disabilities are one of the two forms that are constantly reiterated in the AIA and DSA, with an overwhelming prominence in the recitals and not much concretisation of what kind of action the EU Digital Policy Legislation requires.

aa) AIA and DSA

Article 5 b) AIA-EC lists physical and mental disabilities as one possible justification for prohibiting AI systems. However, the proposal does not contain any guidance on how this should be operationalised. The AIA-EP goes beyond the AIA-EC through the introduction of recital 53 a) which is meant to strengthen the position of persons with disabilities. The last sentence is of particular relevance.

> *(53a) As signatories to the United Nations Convention on the Rights of Persons with* ***Disabilities*** *(UNCRPD), the Union and the Member States are legally obliged to protect persons with* ***disabilities*** *from discrimination and promote their equality, to ensure that persons with* ***disabilities*** *have access, on an equal basis with others, to information and communications technologies and systems, and to ensure respect for privacy for persons with* ***disabilities****. Given the growing importance and use of AI systems, the application of universal design principles to all new technologies and services should ensure full, equal, and unrestricted access for everyone potentially affected by or using AI technologies, including persons with* ***disabilities****, in a way that takes full account of their inherent dignity and diversity. It is therefore essential that Providers ensure full compliance with accessibility requirements, including Directive (EU) 2016/2102 and Directive EU) 2019/882. Providers should ensure compliance with these requirements by design.* ***Therefore, the necessary measures should be integrated as much as possible into the design of the high-risk AI system****.*

The AIA-EP does not introduce a binding obligation of providers and deployers to design the AI system in line with the rights of persons with disabilities, as concretised in the UNCRPD and later on in Directives 2016/2102 and 2019/882. In theory and in line with the key role of harmonised European standards, such an obligation would have put pressure on the ESOs to design appropriate standards. Instead, the AIA-EP postpones protection by design to the future, in that the newly proposed Art. 54 a) AIA-EP requires the Member States to promote research *'including but not limited to development of AI-based solutions to increase accessibility for persons with disabilities, tackle socioeconomic inequalities.'* The issue is taken up in Art. 84 dealing with the 'evaluation and review' of the AIA. When considering a possible amendment,

49 For a deeper debate H.-W. Micklitz, The Role of Technical Standards, loc. cit. pp. 117.

the European Commission shall consider *'the effect of AI systems on health and safety, fundamental rights, the environment, equality, and* ***accessibility for persons with disabilities*** *(emphasis added HWM), democracy and the rule of law and in the light of the state of progress in the information society'*. The only concrete measure to increase the protection of persons with disabilities does not concern high-risk AI systems, but those coming under the category of 'certain risks', where the obligations of the provider and deployer are limited to transparency. Amendment 488 is meant to ensure that the information to be provided *'shall be accessible to vulnerable persons, such as persons with disabilities or children, complete, where relevant and appropriate, with intervention or flagging procedures for the exposed natural person taking into account the generally acknowledged state of the art and relevant harmonised standards and common specifications'*.

The short-hand solution is seen in protecting persons with disabilities through the promotion of codes of conduct, very much in line with the rules foreseen in the already adopted DSA. Article 69 AIA-EC is explicitly referring to the need to increase accessibility for persons with disabilities through the design of the AI system. The revised version of the EP is even more outspoken and proposes a long list of criteria, inter alia *'b) to assess to what extent their AI systems may affect vulnerable persons or groups of persons, including children, the elderly, migrants and persons with disabilities or whether measures could be put in place to increase accessibility, or otherwise support such persons or groups of persons.*

The ruling in the DSA and the proposed solution look like a blueprint for the pending AIA. Recital 105 sets the tone for the level of regulatory intervention, not binding action, but voluntary measures, not every platform but only very large platforms and search engines; Article 3 DSA, contrary to the AIA, provides for an explicit definition, taken from the EU Directive and Article 47 DSA lays down details on how a code of conduct to increase accessibility inter alia of persons with disabilities should look like.

> *(105) The codes of conduct should facilitate the accessibility of very large online platforms and very large online search engines, in compliance with Union and national law, in order to facilitate their foreseeable use by persons with disabilities. In particular, the codes of conduct could ensure that the information is presented in a perceivable, operable, understandable and robust way and that* ***forms and measures provided pursuant to this Regulation are made available in a manner that is easy to find and accessible to persons with disabilities*** *(emphasis added HWM)*

Article 3 DSA Definitions

> *(v) 'persons with* ***disabilities'*** *means 'persons with disabilities' as referred to in Article 3, point (1), of Directive (EU) 2019/882 of the European Parliament and of the Council;*[50] *(which says the following) 'persons with* ***disabilities'*** *means persons who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others;*

Article 47 Codes of conduct for accessibility

> *1. The Commission shall encourage and facilitate the drawing up of codes of conduct at Union level with the involvement of providers of online platforms and other relevant service providers,*

50 Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services, OJ L 151, 7.6.2019, p. 70–115, which is called European Accessibility Act.

> *organisations representing recipients of the service and civil society organisations or relevant authorities to promote full and effective, equal participation,* ***by improving access to online services that, through their initial design or subsequent adaptation, address the particular needs of persons with disabilities.***
>
> *2. The Commission shall aim to ensure that the codes of conduct pursue the objective of ensuring that those services are accessible in compliance with Union and national law, in order to maximise their foreseeable use by persons with disabilities. The Commission shall aim to ensure that the codes of conduct address at least the following objectives: (a)* ***designing and adapting services to make them accessible to persons with disabilities by making them perceivable, operable, understandable and robust****; (b) explaining how the services meet the applicable accessibility requirements and making this information available to the public in an accessible manner for persons with disabilities; (c) making information, forms and measures provided pursuant to this Regulation available in such a manner that they are easy to find, easy to understand, and accessible to persons with disabilities (emphasis added HWM).*

Just like in the AIA the European Commission shall promote and encourage, but not survey and monitor their application in practice. As neither the AIA nor the DSA are providing incentives it remains open whether and to what extent the VLOPs, VLOSs, the AI system providers and deployers are willing to invest in the elaboration of such codes. The only risk they take in case of non-action is that the European Commission will shift from voluntary measures to binding measures.

bb) ISO/IEC, IEEE and ESOs

International standardisation organisations have been involved in the elaboration of technical standards to improve accessibility for a couple of years. One such example is the ICT standard EN 301 549 'Accessibility requirements for ICT products and services', where Europe is ahead of the international standardisation organisations.[51] ETSI supported its transformation into an ISO/IEC JTC 42 standard, while CEN-CENELEC did not. EN 301 549 carries the logos of all 3 ESOs. The standard was criticized by stakeholder organisations, inter alia ANEC and EDF, due to the insufficient safeguards to protect the interests of people with disabilities and the insufficient respect for the European Accessibility Act – Directive 2019/822. After its adoption, interested business circles pushed for the transformation of the European standard into an international standard. Some countries even started using EN 301 549 for their national accessibility policies (Mexico, Kenya, Japan, India, and Canada). The conflict is still pending.[52]

One therefore wonders how a code of conduct fits into the picture. There is a strong overlap between the ongoing work in standardisation, internationally and at the European level and the intended elaboration of codes of conduct. The European Commission could have solved possible conflicts by using harmonised European standards as the appropriate design. However, this would have required binding legal requirements in the AIA and the DSA, which neither the European Commission nor the European Parliament are ready to do.

If any, there is room for the elaboration of voluntary industry standards. The EU digital policy legislation limits the future codes of conduct in three ways – in the AIA in that they shall only

---

51 https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf

52 Information made available from a representative of European stakeholder organisations.

cover non-high-risk AI systems, in the DSA in that the addressees are only VSOPs and VSOSs and in the AIA and the DSA through the promoted minimum requirements. The legal boundaries imply that the standardisation body would be ready to respect EU law, which runs counter to the philosophy of ISO/IEC and IEEE which do not take a stand on the applicable law. The ESOs are in a pole position as they have to comply with EU law when mandated by the European Commission. The New Approach/New Legislative Framework allows to request not only harmonised standards but also voluntary standards and to contribute through co-financing the work of the ESOs. The other option leaving the elaboration of the codes to AI companies and/or AI business organisations at the European level is not at all thought through either in the AIA or the DSA. Both rules are so underdeveloped that it is hard to grasp how they could be put into action.

e) Minors – Children

Just like about disabilities, the position of minors/children has already been outlined in the search for meaning to 'vulnerabilities'. In the following, the focus is put on those provisions dealing with the position of minors interchangeably used with children. EU law does not know a definition either of minors or of children, not even Article 23 EUCFR. The UN Convention defines as a child every human being below the age of eighteen years, Art. 1.[53] It does not use 'minors'. However, neither the AIA nor the DSA closes the definitional gap through reference to the UN Convention. If the Convention is mentioned, both pieces are speaking of the rights mentioned deliberately avoiding a clarification.[54]

aa) AIA

Setting aside the different positions of the Council, the Commission and the European Parliament on the lawfulness of biometric recognition systems,[55] the conflict around Article 5 and the list of prohibited AI systems, the AIA contains one single reference to children as one of the indicators in the risk management in that *'specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children', subject to amendment by the EP: 'is likely to* ***adversely*** *impact* ***vulnerable groups of people or*** *children'*.

The EP goes beyond the EC in that AI providers and deployers who are subject to Article 52 b) (3) AIA-EP shall take the information capabilities of children into account when drafting the transparency requirements. Similar amendments can be overserved about the minimum criteria codes of conduct have to meet. Article 69 (2) AIA-EP requires on top to ***(b) assess to what extent their AI systems may affect vulnerable persons or groups of persons, including children, the elderly, migrants and persons with disabilities or whether measures could be put in place in order to increase accessibility, or otherwise support such persons or groups of persons.***

---

53 Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49 https://www.ohchr.org/sites/default/files/crc.pdf

54 Recital 28 AIA-EC/EP.

55 Insightful comparison of the different positions https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence

bb) DSA

The DSA mentions the need to protect minors in the platform economy throughout the text. The website where the EU presents the DSA devotes one paragraph to the 'strong protection of minors'. The language sounds like marketing: *'platforms will have to redesign their systems to ensure a high level of privacy, security, and safety of minors; targeted advertising based on profiling towards children is no longer permitted; special risk assessments including for negative effects on mental health will have to be provided to the Commission 4 months after designation and made public at the latest a year later; platforms will have to redesign their services, including their interfaces, recommender systems, terms and conditions, to mitigate these risks'*.[56] The prohibition of profiling children for market purposes is by far the most important ruling.

The many references to 'minors' not to children in particular in the recitals unfold an impressive language on the comprehensibility of terms and conditions (recital 46), on an appropriate design of the interface, (71 + 81), on the accessibility of notice and action, on complaint mechanisms (89), and content impairing their physical, mental or moral development (89).

> *(46) Providers of intermediary services that are primarily directed at **minors**, for example through the design or marketing of the service, or which are used **predominantly by minors**, should make particular efforts to render the explanation of their terms and conditions easily **understandable to minors** (emphases added HWM)*
>
> *(71) The protection of **minors** is an important policy objective of the Union. An online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes. Providers of online platforms used by minors should take appropriate and proportionate measures to protect minors, **for example by designing their online interfaces** or parts thereof with the highest level of privacy, safety and security for minors by default where appropriate or adopting standards for protection of minors, or participating in codes of conduct for protecting minors. They should consider best practices ... and the principle of data minimization.... Thus, this obligation should not incentivise providers of online platforms to collect the age of the recipient of the service prior to their use. It should be without prejudice to Union law on protection of personal data (emphases added HWM).*
>
> *(81) A second category concerns the actual or foreseeable impact of the service on the exercise of fundamental rights, as protected by the Charter, including..., the **rights of the child and consumer protection**. Such risks may arise, for example, in relation to the design of the algorithmic systems.... When assessing risks to the rights of the child, providers of very large online platforms and of very large online search engines should consider for example how easy it is **for minors to understand the design and functioning of the service**, as well as how minors can be exposed through their service to content that may impair minors' health, physical, mental and moral development. Such risks may arise, for example, in relation to the design of online interfaces which intentionally or unintentionally exploit the weaknesses and inexperience of minors or which may cause addictive behaviour (emphases added HWM).*
>
> *(89) Providers of very large online platforms and very large online search engines should take into account the best interests of minors in taking measures such as adapting the design of their*

56 Website of the European Union https://www.eu-digital-services-act.com

> *service and their online interface, especially when their services are aimed at minors or predominantly used by them. They should ensure that their services are organised in a way that allows minors to* ***access easily mechanisms provided for in this Regulation, where applicable, including notice and action and complaint mechanisms****. They should also take measures to protect minors* ***from content that may impair their physical, mental or moral development*** *and provide tools that enable conditional access to such information. In selecting the appropriate mitigation measures, providers can consider, where appropriate, industry best practices, including as established through self-regulatory cooperation, such as codes of conduct, and should take into account the guidelines from the Commission (emphases added HWM).*

These overall purposes are reflected in two provisions. Article 14 Terms and Conditions introduced a ruling which opens a new page in the control of standard terms, which raises the question of the interaction between the DSA and Directive 93/13. One may understand Article 14 DSA as an integral part of the transparency requirement in Article 4 Directive 93/13, which would imply that consumer agencies and consumer organisations enjoy standing, a reading which is indirectly supported through the integration of the DSA into the Annex of Directive 2020/1828 on representative action, Article 90 DSA. Art 14 DSA runs like this:

> *1. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. It shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format.*

> *3. Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that* ***minors can understand*** *(emphasis added HWM).*

On top, the DSA devotes one single article to the 'online protection of minors', Article 28. The high level of privacy, safety and security in connection with the recitals calls for an appropriate algorithmic design. Again, the question arises of how to qualify this obligation, is it an obligation unfolding effects between the parties – the platform and the consumers/minors or only between the platforms and the enforcement authorities? In the first variant, Art. 28 (1) may be integrated into the broad concepts of transparency and fairness in the UCTD.

> *(1) Providers of online platforms shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security on their service, (2) Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the* ***recipient of the service is a minor****, (3) Compliance with the obligations set out in this Article shall not oblige providers of online platforms to process additional personal data in order to assess whether the recipient of the service is a minor, (4) The Commission, after consulting the Board, may issue guidelines to assist providers of online platforms in the application of paragraph 1 (emphasis added HWM).*

These somewhat promising tendencies in Articles 14 and 28 DSA are thwarted when confronted with how the DSA seeks a solution on the promotion of the rather ambitiously worded protection of the minors. Recital 102 and Art. 44 DSA deal with 'standards' which are all voluntary, not

semi-binding harmonised European standards. The protection of minors shall be promoted to the least stringent regulatory measure, through voluntary standards.

(102) To facilitate the effective and consistent application of the obligations in this Regulation that may require implementation through technological means, it is important to promote ***voluntary standards*** *covering certain technical procedures, where the industry can help develop standardised means to support providers of intermediary services in complying with this Regulation, such as allowing the submission of notices, including through application programming interfaces, or standards related to terms and conditions or standards relating to audits, or standards related to the interoperability of advertisement repositories. In addition, such standards could include standards related to online advertising, recommender systems, accessibility and the protection of minors online. Providers of intermediary services are free to adopt the standards, but their adoption does not presume compliance with this Regulation. At the same time, by providing best practices, such standards could in particular be useful for relatively small providers of intermediary services. The standards could distinguish between different types of illegal content or different types of intermediary services, as appropriate (emphasis added HWM).*

Art. 44 DSA

> *1. The Commission shall consult the Board, and shall support and promote the development and implementation* ***of voluntary standards set by relevant European and international standardisation organisations,*** *at least in respect of the following:(a) electronic submission of notices under Article 16; (b) templates, design and process standards for communicating with the recipients of the service in a user-friendly manner on restrictions resulting from terms and conditions and changes thereto; (c) electronic submission of notices by trusted flaggers under Article 22, including through application programming interfaces; (d) specific interfaces, including application programming interfaces, to facilitate compliance with the obligations set out in Articles 39 and 40; (e) auditing of very large online platforms and of very large online search engines pursuant to Article 37; (f) interoperability of the advertisement repositories referred to in Article 39(2); (g) transmission of data between advertising intermediaries in support of transparency obligations pursuant to Article 26(1), points (b), (c) and (d); (h) technical measures to enable compliance with obligations relating to advertising contained in this Regulation, including the obligations regarding prominent markings for advertisements and commercial communications referred to in Article 26; (i) choice interfaces and presentation of information on the main parameters of different types of recommender systems, in accordance with Articles 27 and 38; (j)* ***standards for targeted measures to protect minors online*** *(emphasis added HWM).*

Art. 34 (1) b) DSA requires respect for the rights of the child enshrined in Article 24 of the Charter, and a high level of consumer protection enshrined in Article 38 of the Charter. One could have expected that the EU legislature would have imposed clear obligations on what the platforms would have to do, not least in light of the experience made in the monitoring

and surveillance of TikTok.[57] In its assessment, the European Commission regards the different safeguards enshrined in the DSA nevertheless as a major success.[58]

cc) IEEE and ISO/IEC

It is not surprising that the standardisation organisations are about to fill that gap. IEEE is ahead of the curve. IEEE 2089™-2021 establishes a framework that can help organisations recognize and respond to the needs of children and young people encompasses, through (1) Recognition that the user is a child, (2) acknowledgement of the diversity of children and young people, (3) Presentation of information in an age-appropriate way, (4) Utilization of fair terms appropriate for children, and (5) Prioritization of children's best interests over commercial interests. IEEE P7004™ – Standard on Child and Student Data Governance[59] provides stakeholders with certifiable and responsible child and student data governance methodologies. Details are not publicly available. A second major issue, hotly debated in the affected business circles as well as in AI research is technological means of age verification. The EU is also involved. I have analysed the state of affairs elsewhere demonstrating the conflicts between international and European standards, as well as what it means in practice that the DSA relies on voluntary standards instead of harmonised European standards.[60]

f) Traders/Supplier and Economic operators

In the consumer private law acquis, the trader and/or the supplier are the counterpart to the consumer. The concept introduced in 1985 in Directive 85/577/EEC on doorstep selling has survived all the various amendments, all the modernising and all the adaptations to the various challenges, be it digitisation or sustainability. However, maybe somewhat less in the limelight is a second strand, conceptualising the counterpart to the consumer. It also started in 1985 with the product liability directive 85/374/EEC, which distinguishes – equally until today between the producer, the manufacturer, the quasi-producer, the dealer and the importer. Product liability law is a special branch of tort law, just like consumer law is a subsection of civil law. Tort law knows the 'wrongdoer' and the 'victim' and circulates the scope and breadth of the duties of care and the targeting of the 'victim'. Product liability law differentiates these categories on both sides, more sophistically on the side of the wrongdoer though. The father of the directive, Hans-Claudius Taschner, always argued that the Directive is not a piece of consumer legislation. The consumer only comes in through the product categories which are covered by the Directive and these are consumer goods only. The potential victim is defined through the product category and behind the products there is the whole chain of supply – the producer, the manufacturer, the dealer and the importer. Product liability law must be read together with product safety law, the adoption of the product safety Directive 92/59, amended through

---

57 M. Cantero Gamito/H.-W. Micklitz, Too much or too little? Assessing the Consumer Protec-tion Cooperation (CPC) Network in the protection of consumers and children on TikTok (BEUC, 17-02-23) 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

58 See the stocktaking in Brussels, 11.5.2022 COM(2022) 212 final A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212&from=EN

59 https://site.ieee.org/sagroups-7004/

60 Under Micklitz, Role of Standards loc. cit. pp. 130..

Directive 2001/95, now transformed into Reg. 2023/988. Each revision led to a further differentiation on the side of the 'responsible' – now reconceptualised through the umbrella term of the 'operator'. The EU digital policy legislation, whether dealing with AI or with platforms, is based on the search for the responsible actor, for designing the scope of responsibilities and assigning them according to their capabilities. This is the common basis of a product safety-related, perhaps better public law 'risk-based' approach, which is superimposed on private law relations, on the consumer law acquis and successively permeates and shapes it.

aa) AIA

Below is the impressive list of potential addressees, which remains 'empty' if not connected to the type of due diligence obligations imposed on them. All definitions concern the business side. This is also true for the user, a category which could be associated with a 'consumer' using a 'dangerous' product. Therefore, the EC proposal clarified that consumers are not users of an AI system. The EP wants to see the user replaced by a deployer, which helps to avoid confusion. Special attention will be devoted to SMEs and start-ups below.

> *Art. 3*
>
> *(2) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;*
>
> *(3) 'small-scale provider' means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC61;*
>
> *(4) 'user' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity; (EP deployer HWM)*
>
> *(5) 'authorised representative' means any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;*
>
> *(6) 'importer' means any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union;*
>
> *(7) 'distributor' means any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties;*
>
> *(8) 'operator' means the provider, the user, the authorised representative, the importer and the distributor;*

EU Digital Policy Legislation breaks down the potential addressees into ever more fine-grained categories, reaching even beyond the GSR 2023/988. The key addressees are the provider of an AI system and the deployer of an AI system. All others are 'operators' within the AI supply chain, as it is termed in the AIA, the importers, the dealers and now the 'authorised representative' of an AI system provider who is providing AI systems to the EU from outside the EU. The purpose is obvious. EU law insists on the need to have a person located on EU territory as an

addressee who can be approached more easily than the main office which could be located somewhere in the world.

The list, as long as it might be, is not (never?) complete. The manufacturer is not listed although the AIA is meant to cover AI components built into products. The AIA relies directly on EU product safety regulations. Both the EC and the EP distinguish between providers of AI systems and providers of sandboxes, Art. 53. The EP adds another layer. the provider of foundational models which is meant to address general-purpose AI. This is not all yet. Throughout the AIA, the EC and the EP make references to third parties in different contexts, the notified body – certification bodies are treated as third parties, but also those abusing an AI system or more broadly 'third parties' in the AI value chain. One might wonder to what extent the AIA prepares the ground for further differentiation and /or whether 'third parties' are coming under the umbrella term of 'operator' and if this is so, what the potential implications are. Seen through the consumer lens, the key question is whether and to what extent all these operators can be held liable for a possible infringement of the obligations imposed on them through the AIA. The mismatch between the AIA and the PLD opens the door to national tort and eventually national contract law.

bb) DSA

The DSA combines *three* different approaches to define the *sedes personae*. The subsection on the providers of online platforms enables businesses between the 'consumer' and the 'trader'. The newly introduced 'active recipient' uses the platform for commercial purposes, not for private ones. This is the first extension.

> Art. 3
>
> (f) 'trader' means any natural person, or any legal person irrespective of whether it is privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession;
>
> (p) 'active recipient of an online platform' means a recipient of the service that has engaged with an online platform by either requesting the online platform to host information or being exposed to information hosted by the online platform and disseminated through its online interface;
>
> (q) 'active recipient of an online search engine' means a recipient of the service that has submitted a query to an online search engine and been exposed to information indexed and presented on its online interface;

The *second* focuses on the regulation of platforms, without defining what a platform is. The EC did not want to open Pandora's box, as there is no agreement on the definition.[61] Instead and in line with the thinking behind product safety regulation, the DSA defines the type of 'service' offered. The technique allows the European Commission to enlarge the type of services if needed. At the same time, there is the risk that the defined activities are too narrow and not future-proof.

---

61 Specht-Riemenschneider, Louisa & Micklitz, Hans & Dehmel, Susanne & Kenning, Peter. (2020). Grundlegung einer verbrauchergerechten Regulierung interaktionsmittelnder Plattformfunktionalitäten, Sachverständigenrat für Verbraucherfragen.

> (g) 'intermediary service' means one of the following information society services: (i) a 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network; (ii) a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request; (iii) a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service;
>
> (i) 'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation;
>
> (j) 'online search engine' means an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found;
>
> (s) 'recommender system' means a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed;

The classification of the providers of generative AI revealed the intricacies of such a targeted approach. Such providers seem to be outside the scope of the DSA as the providers can neither be regarded as 'hosts' nor as 'an online search engine'. That is why the DSA is about to fail the first serious acid test.[62]

The *third* approach follows the recently adopted DMA. The DSA distinguishes between the size of the providers of the online services and allocates obligations accordingly. The legislative technique, however, is strange, to say the least. The distinctions have to be searched for in the respective subsections.

- the *first* deals with *all* providers of the *intermediary services* as defined in Article 3 (i) independent of the size of the platform, Articles 12–15
- the *second* defines *additional* provisions to providers for *hosting services*, including platforms, as defined in Art. 3 (i) and (j), Articles 16–19
- the *third* introduces *additional* provisions to *online platforms*, Articles 20–28 – except SMEs
- the *fourth* contains particular rules for providers of online platforms, allowing *for b2c contracts*, Articles 329-32 – except SMEs.

62 Ph. Hacker/A. Engel/M. Maurer, Regulating ChatGPT and other Large Generative AI, In 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23), June 12–15, 2023, Chicago, IL, USA. ACM, New York, NY, USA https://dl.acm.org/doi/pdf/10.1145/3593013.3594067

- the *fifth* imposes additional duties for *very large online platforms and very large online search engines only*, Articles 33–43
- the *sixth* is a kind of omnibus section addressing various tools and differentiating between the potential addressees, including actors which are not mentioned and not defined in Article 3, Articles 44–48.

Contrary to the AIA, the SMEs are not added to the catalogue of definitions, although the reference remains the same, Recommendation 2003/361/EC. Article 33 relates the size of the company to the average number of monthly active recipients. The provision delegates powers to the Commission to adjust the numbers as all as to develop an appropriate methodology.

> Art. 33 (1) This Section shall apply to online platforms and online search engines which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines pursuant to paragraph 4.

The paraphrasing of the various activities and the various types of providers – start-ups below the threshold of SMEs, SMEs, platforms and search engines, very large online platforms and very large search engines – remains anaemic if they are not linked to the consequences that the DSA attaches to the exercise of the activities, the obligations which the DSA imposes on the 'providers' of such activities and the possible consequences in case of infringements. Here similar questions arise as in the AIA about the nature of the obligations, and whether they unfold effects in private relations.

Contrary to the AIA, the DSA establishes a liability regime, which is taken from the E-commerce Directive and is still based on the overall idea that platform providers are not responsible for the content of the services they perform. Article 6 (3) DSA enables the consumer to hold the provider of the platform liable if they have legitimate reason to believe that the provider is the 'trader'.[63] This ruling applies independently of the size of the platform.

g) SMEs, Startups and Sandboxes

The particular role of SMEs, start-ups and sandboxes deserves to be treated separately, in line with the attention the EC and the EP devote to their rights and responsibilities in the design of the EU digital policy legislation. Start-ups have the reputation to be the drivers of innovation. If the regulatory burden on them is too high, so the argument goes, their innovative potential might be suffocated. There is evidence that start-ups and SMEs are already suffering from the administrative burden imposed on them by the GDPR.[64] The Fintechs at least seem to have found ways and means to find the space they need, – in a grey legal area.[65]

---

63 This is not the place to go more deeply into the liability regime, which was one of the cornerstones in the legislative procedure, G. Spindler, G Spindler, Digital services act: Adapting commercial and civil law rules for commercial entities operating online: Legal assessment in N Lomba/T Evas European Parliament, Digital Services Act, European Added Value Assessment, Annex II, European Parliamentary Research Service, September 2020

64 Przemysław Pałka, Data Management Law for the 2020s: The Lost Origins and the New Needs, 68 Buff. L. Rev. 559 (2020)

65 A. M. Nowak, Regulating investment capitalism, An ethnograph of Fintech EUI phd 2022.

aa) AIA

One of the major objectives of the amendments proposed by the EP is to take due care of SMEs, start-ups and sandboxes. One of the most striking examples is the prohibition of contract terms which result from the stronger bargaining position of 'one party'. Here are the amendments to the EP, in bold letters:

> ***(60a) Where one party is in a stronger bargaining position, there is a risk that that party could leverage such position to the detriment of the other contracting party when negotiating the supply of tools, services, components or processes that are used or integrated in a high risk AI system or the remedies for the breach or the termination of related obligations. Such contractual imbalances particularly harm micro, small and medium-sized enterprises as well as start-ups, unless they are owned or sub-contracted by an enterprise which is able to compensate the sub-contractor appropriately, as they are without a meaningful ability to negotiate the conditions of the contractual agreement, and may have no other choice than to accept 'take-it-or-leave-it' contractual terms...***
>
> ***(60b) Rules on contractual terms should take into account the principle of contractual freedom as an essential concept in business-to-business relationships. Therefore, not all contractual terms should be subject to an unfairness test, but only to those terms that are unilaterally imposed on micro, small and medium-sized enterprises and start-ups. This concerns 'take-it-or-leave-it' situations where one party supplies a certain contractual term and the micro, small or medium-sized enterprise and start-up cannot influence the content of that term despite an attempt to negotiate it...***

Art. 28 (a) AIA-EP regulates standard terms which 'an enterprise' unilaterally imposes on SMEs or start-ups, by stating that certain categories of terms are to be considered unfair, and therefore non-binding. This is the third time that the E has dealt with the fairness of standard terms in B2B relations, value chains in the food sector,[66] platform regulation[67] and now AI systems. If the proposal is approved in the trialogue, freedom of contract would be considerably limited.[68]

Much vaguer is the overall intention of the EP to improve the communication between the SMEs, startups and 'other innovators' and the national supervisory authorities.

> *(73)... In order to promote and protect innovation, it is important that the interests of small-scale providers and users of AI systems are taken into particular account. To this objective, Member States should develop initiatives, which are targeted at those operators, including on* ***AI literacy****, awareness raising and information communication.* ***Member States shall utilise existing channels and where appropriate, establish new dedicated channels for communication with SMEs, start-ups, user and other innovators to provide guidance and respond to queries about the implementation of this Regulation..... Where appropriate, these channels shall work together to create synergies and ensure homogeneity in their guidance to startups, SMEs and users.***

To give more weight to the argument the EP proposes to introduce a particular ruling in Article 1, which defines the overall purpose of the AIA. Article 1 – paragraph 1 – shall be complemented

---

66 Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain *OJ L 111, 25.4.2019, p. 59–72*

67 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services *OJ L 186, 11.7.2019, p. 57–79*

68 This is the language of the Directive 93/13/EEC on unfair terms in consumer contracts, Art. 6 (1).

by laying down ***'(ea) measures to support innovation, with a particular focus on SMEs and start-ups, including on setting up regulatory sandboxes and targeted measures to reduce the regulatory burden on SMEs and start-ups'.***

In the same recital (73) the EP insists on reducing the costs for compliance charged by notifying bodies (certification bodies). There is no cap or the like, but the Commission is encouraged to report and assess the compliance and certification costs

> *(73) Moreover, the specific interests and needs of small-scale providers shall be taken into account when Notified Bodies set conformity assessment fees.* ***The Commission shall regularly assess the certification and compliance costs for SMEs and start-ups, including through transparent consultations with SMEs, start-ups and users and shall work with Member States to lower such costs. For example,*** *translation costs related to mandatory documentation and communication with authorities may constitute a significant cost for providers and other operators, notably those of a smaller scale. Member States should possibly ensure that one of the languages determined and accepted by them for relevant providers' documentation and for communication with operators is one which is broadly understood by the largest possible number of cross-border users...*

Art. 30 (8) Notifying Authorities last sentence...***Particular attention shall be paid to minimising administrative burdens and compliance costs for micro and small enterprises as defined in the Annex to Commission Recommendation 2003/361/EC*** and Art. 43 (4a) Conformity Assessment: ***The specific interests and needs of SMEs shall be taken into account when setting the fees for third-party conformity assessment under this Article, reducing those fees proportionately to their size and market share***.

The next privileges proposed by the EP might be of particular relevance far beyond the overall aim to reduce the administrative burden. Article 11 – paragraph 1 – subparagraph 1 frees the SMEs from the obligation to produce technical documentation in connection with Annex IV which serves as a starting point for public enforcement and which might turn into a battlefield in private litigation as access to the document might be premature.[69] What is an equivalent documentation? And what does it mean that there are no EU-wide guidelines against which the sub-standard documentation can be measured?

> *The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national supervisory authorities and notified bodies with the necessary information to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV* ***or, in the case of SMEs and start-ups, any equivalent documentation meeting the same objectives, subject to approval of the competent national authority.***

Similar concerns exist about Article 29 a) AIA EP which provides for '***fundamental rights impact assessment for high-risk AI systems***' which exempts SMEs. While such an impact assessment is certainly burdensome, the SMEs just as the local provider of AI systems could benefit considerably from common standards on testing. These methods should not be developed at the company level, but minimum testing standards should be freely available.[70]

---

69 H.-W. Micklitz/G. Sartor Compliance and Enforcement in the AIA in G. De Gregorio, O. Pollicino, P. Valcke (eds.) Oxford Handbook on Digital Constitutionalism, OUP upcoming 2024.

70 See J Laux, S Wachter and B Mittelstadt, 'Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act' (February 20, 2023). Available at SSRN: https://ssrn.com/abstract=4365079 or http://dx.doi.org/10.2139/ssrn.4365079.

bb) DSA

The various recitals reveal a rather incremental approach. There are exemptions from reporting obligations and perhaps more importantly from the consumer perspective from the whole subsection dealing with the role of online platforms in B2C transactions. SMEs are exempted from the obligation to ensure traceability, compliance by design regarding information requirements, and the obligation to inform the consumer, Articles 30–32.

> *(49) However, in order to avoid disproportionate burdens,* ***those transparency reporting*** *obligations (producing an annual report HWM) should* ***not apply*** *to providers that are* ***micro or small enterprises*** *as defined in Commission Recommendation 2003/361/EC(25)and which are not very large online platforms within the meaning of this Regulation.*

> *(57) To avoid disproportionate burdens, the additional obligations imposed under this Regulation on providers of online platforms, including platforms allowing consumers to* ***conclude distance contracts with traders,*** *should* ***not apply*** *to providers that qualify as* ***micro or small enterprises*** *as defined in Recommendation 2003/361/EC..... Nothing in this Regulation precludes providers of online platforms that are covered by that exclusion from setting up, on a voluntary basis, a system that complies with one or more of those obligations (emphasis added HWM).*

Voluntary standards play a key role in the implementation of the various policy objectives enshrined in the DSA. As their elaboration is voluntary anyway, there is no room for exemption rules. It is even more interesting that the DSA regards voluntary standards developed by companies which have the necessary technological means as a kind of help and support for SMEs. This is a problematic assumption in light of the specific needs of SMEs, which led the EU to grant them legal standing in the elaboration of technical standards within Reg. 1025/2012.

> *(102) To facilitate the effective and consistent application of the obligations in this Regulation that may require implementation through technological means, it is important* ***to promote voluntary standards*** *covering certain technical procedures, where the industry can help develop standardised means to support providers of intermediary services in complying with this Regulation,.... Providers of intermediary services are free to adopt the standards, but their adoption does not presume compliance with this Regulation.* ***At the same time, by providing best practices, such standards could in particular be useful for relatively small providers of intermediary services****.....(emphasis added HWM).*

h) Regulatory Sandboxes

The AIA deals under Title V with 'Measures in Support of Innovation' introducing rules on so-called regulatory sandboxes. The exact scope and content are subject to controversy between the EC and the EP. The EP proposes 37 amendments on the three articles all aiming at clarifying the conditions under which they are operating as well as making sure that the criteria are to some extent comparable between the Member States and that SMEs can benefit from the regulatory framework. Contrary to the EC the EP provides a definition:

> ***(44g) 'regulatory sandbox' means a controlled environment established by a public authority that facilitates the safe development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan under regulatory supervision;***

The AIA does not limit the potential addresses. These can be '*SMEs, start-ups, enterprises, innovators, testing and experimentation facilities, research and experimentation labs and digital innovation hubs, centers of excellence, individual researchers'* Art. 53 a) AIA-EP. The rules in the EC proposal and even more so in the EP amendments are guided by the concern that in particular SMEs (but also universities) may be barred from participating due to high access barriers. Art. 53 a) AIA-EP puts pressure on Member States to take all kinds of measures to avoid exclusion.

i) Intermediaries

The classical intermediaries are online platforms, which are dealt with under the category of a 'provider'. The key question for all intermediaries is whether they act on their behalf or whether their action is attributable to a third party, typically the trader from the consumer's point of view. An almost classic is influencer marketing. When does the influencer act in his name and when does he act in the name or on behalf of the trader, Article 2 b) UCPD? The European Commission deals with the liability of influencers in its Guidance adopted in 2021, without, however, providing clarity on the demarcation.[71] In *Peek & Cloppenburg*[72] the CJEU had to decide on what exactly counts as payment holding that some consideration suffices if there is an added value which must not be money. More importantly, the Court highlighted the relevance of '"covert" *advertising on the internet through the dissemination of comments on social networks, forums or blogs, which appear to come from consumers themselves, whereas they are advertising or commercial messages, directly or indirectly created or paid for by economic operators, and insists on the harmful effects of such practices on the consumer.*'[73] There is also case law at the national level dealing with influencer marketing[74] and there is an upcoming discussion on the interrelationship between the DSA and the UCPD more generally.[75]

The relationship between the DSA and the UCTD deserves a separate investigation. The DSA regulates 'terms and conditions' mainly for content moderation. In line with the rationale of the DSA, the obligations correlate with the size of the platforms. However, the 'terms and conditions for content moderation' might equally affect the consumer and might therefore interact with the UCTD. Provided the standards are higher than the provisions of the UCTD, they would have to be reinterpreted considering the DSA, as Article 25 (2) refers to the UCPD only. What matters in our context though is the distinction in Article 7 DSA between the user and recommender of standard terms. The recommender might be a business organisation and the user is the company which is referring to the terms. The business organisation could be regarded as a particular kind of intermediary which could become the direct addressee of actions for

71 COMMISSION NOTICE, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, OJ 29.12.2021, C 526/1 under 4.2.6. pp. 97.

72 CJEU C-Case 371/20Judgment of the Court (Sixth Chamber) of 2 September 2021, Peek & Cloppenburg KG, v Peek & Cloppenburg KG. ECLI:EU:C:2021:674; J. and C. Goanta, '#paidpartnership Means More than Money: Influencer Disclosure Obligations in the Aftermath of Peek & Cloppenburg' (2022) 11(5) Journal of European Consumer and Market Law 188–191., Available at SSRN: https://ssrn.com/abstract=4282364 or http://dx.doi.org/10.2139/ssrn.4282364

73 At 43.

74 The distinction seems to result from the German Gesetz zur Regelung der Allgemeinen Geschäftsbedingungen (Unfair Terms Legislation 1976), which, however, lost importance in Germany after the Act had been amended and recommendations were no longer to be notified to the German Cartel Office

75 B. Duivenvoorde & C. Goanta The Regulation of Digital Advertising under the DSA: A Critical Assessment, unpublished manuscript on file with the author.

injunction.[76] Neither the DSA nor the AIA are dealing with 'recommenders' in the meaning given to it by the UCTD. However, both the AIA and the DSA refer extensively to 'private regulation' (voluntary standards and codes of practice). Provided the private regulation qualifies as a 'contract term' in the meaning of the UCTD, the question arises whether the European Commission and/or the Member States are to be regarded as recommenders. Such a reading might be exacerbated by the regulatory technique. Both define minimum standards which have to be respected by the addressees of the AIA and the DSA in the elaboration of the codes.

Under Article 69 (1) AIA the European Commission and the Member States shall 'encourage' and 'facilitate' the drawing up of codes of conduct, '***including where they are drawn up in order to demonstrate how AI systems respect the principles set out in Article 4a and can thereby be considered trustworthy (EP),*** to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 based on technical specifications and solutions that are appropriate means of ensuring compliance' and under Article 69 (2) 'to foster the voluntary application to AI systems of requirements related for example to environmental sustainability, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams based on clear objectives and key performance indicators to measure the achievement of those objectives'. The EP goes far beyond and proposes to replace Art. 69 (2) through a whole set of mandatory minimum requirements.

Subsection 6 of the DSA is full of similar rules about 'standards' Article 44, 'codes of conduct' Article 45, 'codes of conduct for online advertising', Article 46 and 'codes of conduct for accessibility'. All articles contain lengthy and detailed minimum requirements which have to be met by the providers of the platforms, depending on their seize. All relevant Articles start with similar language, the European Commission shall 'support and promote', shall 'encourage and facilitate'. Is the Commission turning into a recommender who could be held liable under Directive 93/13 provided the rules are to be regarded as unfair, addressed to consumers and infringe the indicative list or do not meet the fairness test under Article 3? If they do not qualify as recommenders because Directive 93/13/EEC restricts the scope of application to private parties and leaves little room for the integration of the control of contract terms provided by public entities, the question remains of who is in charge to survey and monitor the compliance of the codes of practices and the standards? Neither the DSA nor the AIA deals explicitly with the enforcement of voluntary standards and codes of practice. Therefore, the enforcement would have to be integrated into the complex net of competent national and European supervisory authorities and the European Commission. Consumer agencies, however, are not integrated.[77] That is why there might be an overlap between contract terms under the control of consumer agencies/consumer organisations and those under the AIA/DSA authorities.

j) Observations and Recommendations

The pair of consumer/trader or consumer/supplier in the consumer law acquis is about to be replaced through the 'affected' and the 'operator. Both terms considerably enlarge the potential

76 Federal Supreme Court of Germany (Bundesgerichtshof) 09.09.2021, I ZR 90/20, I ZR 125/20, I ZR 126/20 and 13.01.2022, I ZR 9/21, I ZR 35/21.

77 H.-W. Micklitz/G. Sartor Compliance and Enforcement in the AIA in G. De Gregorio, O. Pollicino, P. Valcke (eds.) Oxford Handbook on Digital Constitutionalism, OUP upcoming 2024.

addressees of the 'new' consumer law and therefore go to the core of consumer law, which is based on the diachronic relationship between the consumer and the supplier/trader. I will first point to the long-term dimension, lay out the problems behind such a watering down of the categories and then move on to the short term perspectives, which require action within the existing consumer acquis.

aa) Long Term Recommendations

Below the two generic terms are a bunch of subcategories – on the consumer side these are all those who are sailing under the flag of 'vulnerabilities'. These are the societally discriminated – those who come under the EU non-discrimination law, the economically discriminated – those who are potential customers of universal services (without any specification though), the disabled persons – those defined by the UN Convention and the children/minors, who remain undefined under EU law contrary to the respective UN Convention. There does not seem to be a clear perspective, underpinning the AIA and the DSA. The term is used at random, perhaps with a certain tendency to equate vulnerabilities with societal discrimination. Economic vulnerability remains underdefined. ISO 22458:2022 is the only document that points towards some sort of a concept. The standard distinguishes between three indicators of vulnerability: personal, situational and market environment. This seems to be a promising start.

A similar development can be discovered on the side of the trader/supplier. Two different strands can be identified. On the one hand, there are all the different actors in the supply chain, – the manufacturer, the dealer, the importer of products, etc. the provider of generative AI, the provider of AI systems, the deployer (user) of A systems, the dealer, the importer, the authorised representative of AI systems etc. On the other hand, there is a move to break down businesses according to their size – start-ups, SMEs, large companies and very large companies.

The rights and duties of the parties are associated and differentiated according to the addressees: the consumer or the affected, the vulnerable consumer in all its variations as well as the trader/supplier in supply chains and the economic operators broken down according to their seize. The result is a fragmentation of the material substance.

Whilst there is certainly a need to conceptualise vulnerabilities, supply chains and seize, there is an even more important need to search for the reasons behind the new unclarity – the German words *Neue Unübersichtlichkeit*[78] seem much better suited to understand the political economy behind the development and to identify counter strategies. A radical explanation would be that the consumer society which developed after the Second World War is now gradually replaced by the digital society in search of its generic terms and its legal order. The Procrustes bed of the narrow definition of the consumer is inappropriate to handle the transformation of the key actors. In such a perspective the European Commission again is the driver of the transformation of consumer law beyond the acquis. The adaption of consumer law does not occur from within – through a revision of the consumer acquis, but from without – through the EU Digital Policy Legislation and maybe through the EU Green Deal (although this is not part of the study). The obvious counterargument that the EU tries to modernise the consumer law acquis through the Digital Content Directive and the pending proposals on the greening

78 J. Habermas, Die Neue Unübersichtlichkeit, Suhrkamp 1985.

of the EU law on unfair commercial practices does not hold. The proposed amendments are simply too symbolic and do not take the economic and societal ruptures into account.[79]

The more substantial transformations seem to occur outside consumer law. The EU is about to develop a digital market order in which the supplier/trader is the economic 'operator' and the consumers are the 'affected'. The pair of consumers/traders is tied together through the scope of their activities. Being a consumer or a trader grants a status. I am a consumer and I have these rights granted under EU law. I am a supplier, I have rights but also obligations towards the consumer. The new pair operator and affected uncouples the actors from their activities. EU law speaks of 'operator' and 'affected', not of the *economic* operator and the *economically* affected. The tendency becomes obvious when content moderation reaches deep into society and when the concept of advertising is no longer tied to money-making. The widening, however, comes at a price. Both generic terms have loose contours. The operator is a circumscription of a potential activity which can point in all directions. The affected is no longer a status but defines the potentiality of being the victim of a risk which materialises in his or her integrity.

If the suggested interpretation of the trends in EU law can be taken for granted, the question arises if and how the existing body of consumer law can be transferred from the consumption economy to the digital economy because the new consumer law covers commercial and non-commercial activities *and* is no longer focused on products, but on services – the so-called servicification. The third part of the paper will provide some insight into recent developments summed up under the heading of privatisation, which begs the question of whether the EU is gradually dismantling or perhaps better circumventing the consumer law acquis.

bb) Short-Term Recommendation

There are two major problems which call for a short-term solution – the first is the integration of providers of generative AI not only in the AIA – what might happen provided the trialogue follows the proposal of the EP – but also in particular in the DSA. Otherwise, the providers of generative AI will develop a governance structure which escapes by and large the control of EU law, except Directive 93/13 and perhaps the transparency requirements laid down in Art. 52 AIA.[80]

The second is the role, the function, the responsibilities and the liabilities of 'intermediaries'. The term needs to be freed of the meaning given to it in the Directive on Unfair Commercial Practices and be understood as the ensemble of the actors involved in the digital value chain. The consumer law acquis and to some extent the EU Digital Policy Legislation is very much based on the search for the 'ultimate responsible' – at least when it comes to the providers of online platforms or search engines in the DSA. The complicated collaboration of the many different actors in the development of recommender systems is not even mentioned.[81] The platforms appear as a single block. The AIA goes beyond as the draft tries to allocate responsibilities to

---

79 Ch. Twigg-Flesner, Disruptive Technology – Disrupted Law? How the Digital Revolution Affects (Contract) Law, Alberto de Franceschi (ed.), European Contract Law and the Digital Single Market. Implications of the Digital Revolution, Intersentia, 2016

80 L. Edwards, Governance of Generative AI, paper presented at the EUI on the 19th October 2023, on file with the author.

81 See L. Naudts, N. Helberger, M. Sax, M. Veale, Toward Accountable Optimisation: Aligning the Recommender Stack under EU Law, in this report.

the different economic actors in the digital supply chain. Such an approach seems to be more promising than the search for the 'ultimate responsible'. The upcoming revision of the Product Liability Directive and the proposal of AI Liability points to a similar reaction.

However, deeper problems are lurking behind the responsibilities/liabilities of intermediaries. There is first and foremost the question, of whether the differentiation in the AIA-P, which follows EU Product Safety Regulation, can be transferred from the public sphere to the private sphere. The European Commission is not bringing up a possible match either in the proposal for a revision of the PLD or in the proposed AI Liability Act. Both proposals extend the potential addressees of the liability, thereby enlarging the range of economic actors, consumers are entitled to sue for compensation. However, there is no comparison of the two worlds – the differentiation in Product Safety/AI Regulation about public enforcement and – the established differentiation in EU product/AI liability, which is much narrower and in no way coordinated with the public sphere. The elephant in the room is a joint liability, which allows the victim to select the potential wrongdoer – well-known under the formula of a deep pocket in tort law. There are proposals on how to find a fairer solution, by limiting the liability of each economic operator to the respective market share.[82] Deeping such a possible alternative way of organising product liability would require including tendencies to extend contractual liability beyond the direct contracting partner.[83] A full analysis reaches far beyond the scope of the paper.

What remains is a possible amendment of the Directive on Unfair Commercial Practices, to include intermediaries against which consumer agencies, consumer organisations or even individual consumers may launch an action for an injunction to set an end to unfair, misleading or aggressive advertising. Directive 2005/29 is based on the idea that the responsible is the one who posted the advertising. However, it is plain that the vast majority of companies which post advertisements on the internet are buying the data from the GAFAs. Potential detrimental effects of the posted advertising may result from the data sets bought from the GAFAs, such as implicit biases or hidden discrimination.[84] An enlargement of the 'intermediaries' in the UCPD has to take the complex interaction between the supplier of the data and the user of the data into account. A possible solution could be thought along the lines of Directive 2019/771, where the seller may seek redress from the supplier, Art. 18. The trader who is held liable for a misleading or unfair commercial practice which results from data provided by a third party, should therefore be given a right to redress against the party who provided the data. Additionally, one might think of extending the liability under the UCPD to that party.[85] However, it should not be on the consumer, consumer agencies or consumer organisations to find out where the data are coming from and whether the user of the data was in a position to control the quality and the compliance of the data. Therefore, one might consider reserving the burden of proof and leaving it for the user to eventually seek redress from the supplier for the data.

82 E.g. G. L. Priest, Market Share Liability in Personal Injury and Public Nuisance Litigation: An Economic Analysis, Supreme Court Economic Review, Volume 18 , 2010, 1–280, https://www.journals.uchicago.edu/doi/epdf/10.1086/659983

83 See the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on common rules promoting the repair of goods and amending Regulation (EU) 2017/2394, Directives (EU) 2019/771 and (EU) 2020/1828, COM/2023/155 final

84 M. Namyslowska, Future Proofing the Unfair Test, in the report.

85 P. Rott, Burden of Proof, under F., in the report.

3. Privatisation of Consumer Law Through Due Diligence

In human rights, and sustainability due diligence principle 17 of the UN principles is the gold standard: *„In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed."*[86] Perhaps better suited for our purposes are the OECD guidelines on responsible business conduct von 2023: *„due diligence is understood as the process through which enterprises can identify, prevent, mitigate and account for how they address their actual and potential adverse impacts as an integral part of business decision-making and risk management systems."*[87] The EU digital policy legislation sets a binding regulatory frame, often stretched over several layers of regulation, which then has to be implemented by the respective companies. Part of the implementation exercise is comprehensive internal mechanisms of compliance, complemented through auditing and eventually third-party certification. This body of rules establishes a world in itself that enshrines sometimes explicitly most of the time implicitly consumers and the consumer law acquis.

Due diligence is omnipresent in the DSA, thereby setting a benchmark for its role and function in digital policy legislation and how consumer matters are included or not included. That is why the analysis starts with the DSA. This allows us to develop an understanding against which the AIA can be analysed. Contrary to the DSA, the AIA does not use the language of 'due diligence' but the one of the New Approach/New Legislative Framework. This does not mean though that the AIA does not provide for due diligence obligations which meet the requirements of the OECD definition.

a) Due diligence under the DSA

Recital (3) of the DSA expresses the spirit of the regulation and the aim to be achieved:

> *(3) Responsible and diligent behaviour by providers of intermediary services is essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union (the 'Charter'), in particular the freedom of expression and information, the freedom to conduct a business, the right to non-discrimination and the attainment of a high level of consumer protection.*

Seen through the lens of the distinction between safety-related and non-safety-related economic consumer policy issues, the DSA is to be situated on the economic side. Health, if it shows up at all, is mainly related to public health without providing a definition, and consumer safety is taken care of only randomly. So far one might understand the DSA as the economic complement to the health and safety related AIA-EC. In the field of economics – this is the message the DSA tells – there is no room for health and safety-related harmonised standards; for a strong involvement of the European Commission; for public finance or public oversight.

---

86 Principle 17 of the UN-Guidelines.

87 OECD guidelines on responsible business conduct von 2023 (Commentary on General Policies, para 15, p. 17

The DSA leaves more space to the 'freedom to do business' and therefore limits itself, either to impose duties on the various addressees of the obligations or to encourage them to take voluntary measures and to establish and ensure self-compliance – towards 'recipients' and/or 'consumers', Art. 3 (b) and c) DSA. These are the due diligence obligations. Recipients are natural and legal persons who use an intermediary service.

Chapter III deals with '*due diligence obligations for a transparent and safe online environment*'. Setting aside Chapter IV on enforcement, Chapter III is by far the most relevant not only for consumers but also for business. It is broken down into six subsections, many (if not most of them) concern consumers. The perspective is always the same. The EU legislature imposes obligations or encourages the elaboration of non-binding self-regulation and the addressees have to implement them through appropriate measures. The DSA does not define due diligence but takes its meaning for granted. The DSA subsumes all sorts of obligations under that category: the obligation to deliver fair contract terms; not to mislead and deceive; to provide for inhouse complaint handling and ODR mechanisms, and to develop voluntary standards. Understanding voluntary industry standards as being an integral part of due diligence obligations looks like a novum in EU legislation. Getting to grips with the true meaning of all the due diligence obligations is rendered more difficult through the differentiation between the various addressees, the SMEs – which are largely excluded –, the LOPs and the VLOPs. The DSA is not conceived as a piece of regulation which regulates the rights and duties in private relations, whether b2b or b2c.[88]

The analysis will first explain the structure and the layers of regulation which define the scope and reach of the due diligence obligations. The details are then presented along the line of the distinction drawn in the DSA, which relates the due diligence obligations to the type of potential addressees.

aa) Overview, Structure and Layers of Regulation

Chapter III Due Diligence Obligations for a Transparent and Safe Online Environment is the core of the DSA. The following table relates the different addressees defined in the six subsections to the layers of regulation. It is not easy to understand why and where the EU may adopt delegating or implementing acts and where this is not possible. The same is true about the role and function of guidelines.

88 G Spindler, Digital services act: Adapting commercial and civil law rules for commercial entities operating online: Legal assessment in N Lomba/T Evas European Parliament, Digital Services Act, European Added Value Assessment, Annex II, European Parliamentary Research Service, September 2020, 185.

	Subs. 1 Providers of intermediary services, Art. 3 g)	Subs. 2 Additional provisions applicable to hosting services + platforms	Subs. 3 Providers of online platforms	Subs. 4 Providers of online platforms allowing B2C contracts	Subs. 5 Providers of VLOPs and VLSEs	Subsec. 6 other provisions on due diligence
Addressee (supply side)	Intermediary services, Art. 3 g)	Hosting services, Art. 3 g) (iii) and online platforms, Art. 3 (i)	Art. 19 Online platforms Art. 3 (i) NOT when SMEs, Art. 19 (1) VLOPs Art 33 always	Art 29, as Art. 19	Art 33 definition of both 45 million recipients	Artt. 44 Commission leads, under varying participation according to the subject matter
Binding legal requirements	Artt. 11–15	Artt. 16–18	Art. 19–28	Art. 29–32	Art. 33–43	Artt. 44–48
Delegated and implementing acts	Art. 15 (3) Reporting implementing act		Art 24 (2) Reporting, delegated act Art. 24 (6) Reporting, template, implementing act		Art. 37 (7) independent audit, delegated act Art. 40 (13) data access, delegated act	
Guidelines			Art. 22 (8) trusted flaggers Art. 25 (3) online interface design Art. 28 (4) on minors		Art. 35 (3) mitigation of risk Art.-39 (3) advertising transparency	
Voluntary Standards and Codes of Conduct Applicable to all subsections						

The analysis proceeds in the following way: the different subsections are presented one by one following the same structure: the identification of the parties on the supply side and the demand side with particular emphasis on potential overlaps to the notion of the consumer, the analysis of the content of the provision guided by the potential impact on the consumer acquis – rules in the pre-contractual stage – advertising and information, rules which affect the contract with the consumer itself or impacts the liability of the provider/supplier and last but not least rules on the enforcement of individual rights such as complaint handling, ODR and particular rights to redress, last not least organization matters imposed on the providers which interfere into the internal governance of the company.

bb) Providers of intermediary services

The scope of providers is broad, all intermediary services are addressed. This is a kind of general clause, laying down the very basics of what (nearly) all providers have to do. The system of enlarging the scope and/or restricting it about the different types of providers addressed does not facilitate access.

The most remarkable rules are probably those dealing with terms and conditions, Art. 14 DSA. As the addressee is the 'recipient' in Art. 3 b) DSA, the obligation affects b2b and b2c relations. The DSA establishes a new layer, a kind of safety net addressing all providers, independent of whether the recipient is a consumer or a supplier and independent of whether the terms have been individually negotiated or whether they are standardized terms. Only VLOPs and

VLSEs are obliged to provide the standard terms in the language in which they offer the service, Art. 14 (6) DSA.

Reporting duties are crucial for understanding what kind of measures the providers have taken on content moderation, on notification of a recipient, their in-house complaint handling or in reaction to an order received from the Member States. The DSA introduces a momentous differentiation between additional obligations on reporting for VLOPs and VLSEs and at the same time releasing the SMEs from that burden. The exact design of the annual report will have to be concretised by the European Commission through an implementing act, Art. 15 (3) DSA.

Subsection 1/type of obligations				
Providers of intermediary services, Art. 3 g)	Art. 12 points of contact for recipients to facilitate communication	Art. 13 Legal representatives	Art. 14 terms and conditions on content moderation	Art. 15 reporting obligations every year
Specifying the scope *sedes personae*			VLOPs and VLSEs, Art. 14 (5) + (6) machine-readable + official language	hosting services, Art. 15 (1) b) Additional obligations for VLOPs and VLSEs on in-house complaint handling Art. 20 SMEs, exempted Art. 15 (2)
Addressee	Recipient Art. 3 b) natural and legal persons		Recipient, Art. 3 b) natural and legal persons Art. 4 (3) special protection of minors	Public at large in machine-readable format, Art. 15 (1)
An additional layer of regulation	Voluntary standards on template design and process of communication with the recipient, Art. 44 (1) b)			Template via implementing act of the EC
Comments	User-friendly, not solely via automated tools		Information on the use of algorithmic decision-making	

The provisions can be classified in the following way, Artt. 12, 13 and 15 DSA fall under the category of organizational matters. Here the supervision and control lie in the hands of public authorities. The consumer has no right for instance to sue the provider for a non-delivery of the yearly due report. The only provision which directly affects the consumer is the rules on content moderation in the 'terms and conditions'. As the recipient can also be a consumer, the terms and conditions are subject to control via Directive 93/13 on fair terms. To open the scope of the application the terms and conditions must qualify as non-negotiated, which will be the standard in reality.

cc) Providers of hosting services/online platforms

Subsection 2 deals with the moderation of illegal content, the identification, the notification, the potential decision, the reasons behind the decision which may lead to restrictions and the availability of the necessary information to initiate litigation against the trader, Art. 17 (4) in combination with Art. 3 f) DSA.

The definition of illegal content is extremely broad. Any information must comply with EU and national law *'irrespective of the precise matter of the nature of the law'*, Art. 3 (h) DSA. A first reading suggests a broad responsibility of the provider, imposing on them a premature compliance check with consumer law. However, reality looks different. There is no *'ex officio'*

obligation of the provider to monitor the incoming information, Art 8 DSA. Quite to the contrary. The rules are not meant to shape the monitoring and surveillance duties of providers but to limit and restrict the liability of the providers for the illegal content as mere intermediaries.[89] The consumer advocates set their hopes on a revision of the exclusion of liability in the e-commerce Directive when the European Commission announced the elaboration of a revision, which turned into the DSA. The European Law Institute (ELI) developed a sophisticated proposal providing for a kind of subsidiary liability of the platforms.[90] All these attempts and critiques did not reach the political fora. The benchmark for a potential liability of the provider of intermediary services (in colloquial language the platforms) is high. The provider of intermediary services has to take action only in case he *knows* the illegal activity or illegal content or is *aware* of facts which render the illegality *apparent*. *Knowledge*, *awareness* and *appearance* are high benchmarks to meet. As it would be for the potential plaintiff to provide the necessary evidence, rules in the DSA are coming close to an exclusion of liability. The only exception is foreseen in Art. 6 (3) DSA which translates the case law of national courts. It requires an average consumer to be misled and to be entitled to believe that the platform is their contractual partner. Art. 6 (3) DSA does not identify the possible remedies. This is left to the national legal orders.

The rest of the subsection deals with complaint handling, the notice and action mechanism and how it shall be handled by the provider. Art. 16 and 17 DSA regulate in all detail, what exactly the provider has to do to facilitate the submission of the notice and the reasons the provider has to give in case he takes action. However, high-volume mass communication does not come under the scope of Art. 17 DSA. That is why the provider might all too often be released to properly inform the consumers who are affected.

Subs. 2/type of obligations		
Additional provisions applicable to providers of hosting services + platforms **Applicable to all, independent of size**	Art. 16 notice and action mechanism of illegal content	Art. 17 Statement of the reason for service restrictions
Restrictions of the scope		Art. 17 (2) does not apply to high-volume commercial content
Addressee/major content	Art. 16 (1) any individual or entity Art. 16 (2) minimum requirements of the submission and the decision	Art. 17 (1) any affected recipient, Art. 3 b) minimum requirements on content, (3)
An additional layer of regulation	Voluntary standards Art. 44 (1) a) Codes of Conduct Art. 45 (1) inter alia on 'illegal content Codes of Conduct for accessibility, Art 47 (2) designing, explaining, making accessible	
Comments	User friendly Exclusively electronically	User friendly Basis for litigation

89 P. Rott, New Liability of Online Marketplaces Under the Digital Services Act? European Review of Private Law, Volume 30, Issue 6 (2022) pp. 1039 – 1058

90 European Law Institute, Model Rules on Online Platforms, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf

dd) Providers of online platforms

Subsection 3 contains a whole set of elaborated obligations for providers of online platforms. Artt. 20–24 DSA may be read as a continuation of subsection 2 laying down the ground rules for the management of illegal content. They specify how the providers have to handle potential notices of individual recipients or trusted flaggers, the measures to be taken against misuse and the reporting duties to the recipients. Artt. 25–28 on the other hand lay down particular requirements on advertising, marketing and transparency.

Art. 25 DSA regulates the much-debated dark patterns[91] providing for a definition. Interfaces shall not deceive or manipulate the recipient. In theory, Art 25 DSA would have affected consumers. However, Art. 25 (2) DSA stipulates that Art. 25 shall not apply to practices covered by the UCPD. This exemption or reduction met strong resistance from BEUC but was integrated nevertheless into the final version of the DSA.[92] The DSA establishes special requirements for b2b advertising as far as they are covered by the DSA, thereby complementing Dir 2006/114 regulating misleading advertising in b2b relations. How Art. 25 DSA and Dir. 2006/114 fit together, will have to be clarified by the European Commission, which 'may issue' guidelines, even if Art. 25 (3) DSA seems to deal with selected issues only, which might come under the scope of Art. 25 (1) DSA. There is ample room though for the European Commission to engage with the broad debate on dark patterns and bring out clarification. The missing coordination with the UCPD could lead to contradictory results in that the business recipient is better protected than the consumer. The enforcement of Art. 25 DSA will be left to the competent national supervisory authorities, although the Member States might tend to entrust those which are competent for b2b advertising anyway.

Art. 26 DSA on the other hand addresses also the consumer. Art. 26 DSA overlaps with Art. 6 and 7 UCPD. The UCPD regulates potential omissions which could mislead the consumer, the DSA lays down positive obligations. The DSA should be read and interpreted in line with Art. 7 (5) UCPD. However, here a particular problem arises as both Art. 26 and Art. 28 DSA may be complemented through 'voluntary standards' in the meaning of Art. 44 DSA. These standards, if they reach beyond Art. 26 (1) DSA can only come under the scope of the UCPD if the rather narrow requirements of misleading codes of practices are met, Art. 6 (2) b). In practice, Art. 6 (2) b) UCPD does not play a role,[93] which sheds light on the possible impact of Art. 44 DSA. An additional problem arises about the potential addressee of an action for injunction. This could eventually also be the European Commission itself.[94]

Art 27 DSA requires that the transparency requirements on recommender systems must – Art. 27 says 'shall' – be set out in the terms and conditions. The 'main parameters' are submitted to judicial control under Directive 93/13 – provided they qualify as 'standard' terms – non-negotiated terms.

---

91 P. Rott, Dark Patterns im Verbraucherrecht, in: Maria Reiffenstein (ed.), *Konsumentenpolitisches Jahrbuch 2023* (Verlag Österreich 2023), 131–152; for attempt to categorise dark patterns, H.-W. Micklitz/ L. A. Reisch/ S. Bietz, Algorithmen und Verbraucher. Eine Studie im Auftrag des Ministeriums für Ländlichen Raum und Verbraucherschutz (MLR) Baden-Württemberg, Stuttgart. Friedrichshafen: Forschungszentrum Verbraucher, Markt und Politik | CCMP (Hrsg.), 2020; UCPD Guidance, OJ C 256/1, 29.12.2021, under 4.27. pp. 99; through the lenses of marketing research, J. Witte, P. Kenning, Ch. Brock, Consequences of User Manipulation through Dark Patterns, on file with the author.

92 Interview with BEUC and informal position paper on file with the author.

93 H.-W. Micklitz/M. Namyslowska, Art. 6 Rnr. 80 pp, Kommentar zum UWG, 3. Auflage 2020, at pp. 769.

94 For a discussion see M. Namyslowska, Future-Proofing the Unfairness Test in this report.

Artt. 20 and 21 DSA concern in-house complaint handling as well as online dispute resolution mechanisms. The scope is rather narrow. The ISO Standard 1002 Customer Satisfaction defines complaint handling systems. As the binding requirements contain only some specifications on the handling of notice, the EU rules can easily be integrated into the ISO standards. This would be different if Art. 20 DSA would interfere with the institutional setting and/or the procedural requirements. However, Art. 20 DSA does not contain a reference to ISO 1002 nor to standardization more generally.

Art. 21 DSA deals with ODR and is far more intrusive. It touches upon a field that the EU has paid particular attention to for decades, not only in b2c but also in b2b regulations at least in the EU rules governing regulated markets. The ODR Regulation 524/2014 is currently under revision. On the 17th of October, the European Commission proposed a revision of the Directive on Alternative Dispute Resolution, a withdrawal of the ODR Regulation, which should be replaced through a Recommendation.[95] The proposals are based on a study meant to evaluate their efficiency and effectiveness.[96] It remains to be seen what will happen to the three proposals and whether they will pass the legislative procedure until autumn 2024.

Art. 21 DSA requires that ODR systems are to be certified by the digital services coordinator – the national supervisory authorities of the Member States. The certification bodies can be either private or public, Art. 21 (6) DSA. The requirements the ODR have to respect are laid down in Art. 21 (5) DSA. They resemble the former Recommendations 98/257 and 2001/310,[97] which have later been translated into the current ADR Directive 2013/11. Art. 21 (4) DSA establishes the reporting duties of the certified bodies and Para 6 regulates who should bear the fees and under what conditions. Para 6 clarifies the relationship between the requirements laid down in Art. 21 (3) DSA for 'recipients of the service' and the ADR Directive 2013/11 on consumer dispute resolution. As the requirements are standing side-by-side the provider could in theory establish two ODR systems, one meeting the higher and more specific requirements of Dir. 2013/11 provided the recipient is a consumer and the more general and much vaguer requirements under Art. 21 (3) for b2b transactions. Whatever will happen in practice, the EU promotion of certified ODR systems forestalls a development which will quickly spread far beyond 'notices' and turn into the standard mechanism for online dispute resolution in both b2b and b2c relations of all sorts. Art. 21 DSA might function as a precedent to the upcoming revision of the ODR Regulation and maybe the ADR Directive. The DSA puts the certification into the hands of the Member States supervisory authorities and stays away from any attempt to harmonise the certification requirements. Art. 21 (3) DSA leaves enough space to expect major differences in the certification policies of the Member States. Amazingly the DSA does neither grant powers to the European Commission to adopt an implementing act on the necessary co-ordination nor to elaborate administrative guidelines. [98]At least the latter would not raise competence issues under the Treaty.

---

95 https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/resolve-your-consumer-complaint/alternative-dispute-resolution-consumers_en

96 COM (648) final 7 October 2023 Report on the application of Directive 2013/11/EU on alternative dispute resolution for consumer disputes and Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes, https://commission.europa.eu/system/files/2023-10/COM_2023_648_1_EN_ACT_part1_v3.pdf

97 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001H0310

98 On request, DG Connect confirmed that they do not want to take action, interview with an official on file with the author.

A last word on the rules specifying the role and function of trusted flaggers. Again there is a resemblance between the DSA rules and the consumer acquis. Directive 1828/2020 on Representative Actions lays down a similar mechanism for those 'qualified entities' which are given legal standing to go to court and ask for an injunction or even for collective compensation.[99] Trusted flaggers have to meet legitimacy requirements, they have reporting requirements of their activities towards the public and transparency requirements imposed on the European Commission. The latter has to make the list of trusted flaggers publicly available. As the illegality of content may result from infringements of consumer law, consumer associations qualify as trusted flaggers. Their recognition lies in the hands of the Member States. BEUC would need to be awarded the status of trusted flagger probably by the Belgian competent authorities. However, due to the underdeveloped elaboration of the relationship between illegal content and consumer law, it remains to be seen how the Member States react. Amazingly Art. 22 DSA does not deal with the procedure potential applicants have to set into motion, if they request the status of the trusted flagger, let alone if the Member States reject the application.

Subs. 3/type of obligations/ particularities					In addition to Art. 15				
Providers of online platforms	Art. 20 Internal complaint handling of notices	Art. 21 ODR on notice	Art. 22 trusted flaggers, independent experts	Art. 23 Protection against misuse	Art. 24 Reporting obligations of online platforms	Art. 25 online interface design (not manipulate or deceive)	Art. 26 advertising on online platforms	Art. 27 recommender systems	Art. 28 online protection of minors
SMEs Art. 19 (1) exempted Restrictions		No binding settlement, Art. 21 (2)				Not applicable to practices covered by Dir 2005/29	Art. 26 (3) on profiling Art. 4 (4) GDPR		Prohibition of profiling Art. 27 (2)
Addressee/ Major obligations	Art. 20 (1) recipients, + individuals or entities having provided a notice	Art 21 (1) same as (20) 1 Minimum requirements Art. 21 (2)-(8) Third-party certification	Art. 22 (3) publicly available, substance by Art. 16	Art 23 (1) Recipient, (2) individuals Suspension rules in terms and conditions (4)	Public at large (2), machine-readable (5) Detailed requirements	Art. 25 (1) Recipients	Art. 26 (1) Individual Recipients (2) minimum requirement	Art. 27 (1) Recipients (2)-(3) minimum requirements (1) Explain parameters in terms and conditions	Minors
Layers of regulation	ISO/IEC 10002 standards on in-house complaint handling		Voluntary Standard, Art. 44 (1) c)		Art 24 (6) EC implementing act template on reporting duties (3)-(5)	Art. 25 (3) EC may issue guidelines	Art. 26 (1) a) and (2) reference to Art. 44 Code of practice		Art 44 (1) g) standards for targeted measures + (4) EC may issue guidelines after consultation with the board
Particularities/ comments	User-friendly, qualified staff, not solely automated, Art. 20 (7)		Given priority over other notices		Additional obligation Art. 24 (1)			Set out in their terms and conditions	

99 P. Rott and A. Halfmeier, Reform of the Injunctions Directive and compensation for consumers, Study commissioned by BEUC, 2018, https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-022_reform_of_the_injunctions_directive_and_compensation_for_consumers.pdf.

ee) Providers of online platforms allowing for B2C contracts

Subsection 3 looks like an 'alien' in the DSA as it deals with distant contracts between traders and consumers, addressing and naming them explicitly. The three Articles impose obligations on the providers of online platforms in two different directions, the relationship between the provider and the (potential) online trader and the relationship between the provider and the consumer. Art. 30 DSA – traceability and 31 DSA – compliance by design, concern the pre-contractual stage and Art. 32 DSA – right to information – the post-contractual stage.

The rules on traceability deal with pre-contractual information that the trader should make available on himself, name, address and self-certification that they comply with the law. Art. 30 DSA defines the scope of information, the time – before the use of the service (which may lead to the conclusion of a contract) the potential addressees – the trader who shall deliver the information – and the consumer as the recipient of the information. Interestingly and somewhat in deviation from Art. 6 DSA, Art. 30 DSA obliges the provider to make 'best efforts' whether the information under (1) is correct,[100] Art. 30 (2) DSA and in case the provider discovers deficiencies, request the trader to remedy the infringement. If the trader is not willing to do so, the provider shall suspend the provision of the service, a decision against which the trader is entitled to complain, Art. 30 (4) DSA. The DSA is interfering in the contractual relationship – what else can it be – between the provider and the trader, regulating particular rights and duties regarding pre-contractual information. In that sense, the respective rules seem directly applicable.

The law is more complicated about the provider-consumer relationship. Art. 30 (7) DSA clarifies that the provider must inform the consumer of three selected items of information. Whilst the DSA addresses the provider, the para shall be read to grant the consumer an enforceable right against the provider, in case they do not get the information. Such a right cannot necessarily be regarded as a contractual right as there might often not be a contract between the consumer and the platform provider but a kind of factual relationship an 'as-if' contract.[101] The more delicate question is whether the consumer is entitled to sue the provider for non-compliance with the obligation to make best efforts and to eventually claim compensation provided they have suffered damage due to the non-compliance. Similar questions arise about the potential rights of the consumer against the trader to request compliance with the information requirements or to claim compensation in case of non-compliance. The relevant paras in Art. 30 (2)-(7) DSA clearly distinguish between the different relationships – provider vs. trader and provider vs. consumer. This makes it hard to integrate consumer rights into those sections which deal particularly with the provider-trader relationship. Liability issues are left to national private law orders anyway.

Art. 31 DSA equally deals with information – pre-contractual information, compliance (with pre-contractual information) and EU product safety information, Art. 31 (1), specified in Art. 31 (2) DSA. Art. 31 DSA addresses the provider to 'design' and 'organise' the 'interface' in a way that the trader may integrate the required information. Recto verso one might assume that the trader has a right to call for an appropriate interface. Art. 31 DSA does not deal with the

---

100 See P. Rott, Burden Of Proof in this report.

101 P. Pałka, Terms of Service Are not Contracts: Beyond Contract Law in the Regulation of Online Platforms, in European Contract Law in the Digital Age, S. Grundmann ed., Intersentia (2018).

potential rights of the consumer in case the design and organization of the interface are deficient. Art. 31 (3) requires the provider to make best efforts to check the information. In case the consumer has no rights, what about using Art. 7 (5) as a basis for taking action under the UCPD?[102]

The right to information concerns only the information on illegal content and has to be read in connection with Artt. 16 and 17 DSA. Being informed on the facts of illegal content, the reasons why the content is illegal and the laws which have been infringed is an indispensable prerequisite for the consumer to launch a complaint or eventually go to court. It remains to be seen what kind of information a potentially affected consumer might get from the provider. The first transparency report of the European Commission reveals that the providers are reducing the information to the minimum and that standard terms and compliance with them are taken as a yardstick.[103] Art. 32 DSA addresses consumers directly which implies that the illegal content may also result from an infringement of consumer law. So far Art. 32 DSA underpins the relevance of the consumer law acquis in the evaluation of 'illegal content'.[104] The position of the consumer, however, may be considerably weakened through the vague formula in Art. 32 (3) DSA, which grants the provider a large degree of discretion in substituting the obligation to inform all affected consumers through a broad announcement on their 'online interface' – the website. The information must be 'easily accessible' – whatever that might mean.

Subsection 4/type of obligations			
Providers of online platforms allowing B2C contracts	Art. 30 traceability of traders	Art. 31 Compliance by design	Art. 32 Right to information
SMEs exempted Art. 29 **Restrictions**	Art. 30 (3), setting limits to the exclusion of liability, Art. 6?	Art. 31 (3), setting limits to the exclusion of liability Art. 6?	
Addressee	Consumers and traders	Consumers and traders	Consumers
Particularities	Art. 30 mandatory prior information of the trader	Art 31 enables traders to comply with information requirements	The provider has to inform the consumer of illegal content

ff) VLOPs and VLSEs

To locate the consumer perspective in the extensive rules on VLOPs and VLSEs there is a word needed on the structure and the rationale behind subsection 5, which is by far the most elaborated one. The DSA starts from the premise that only the VLOPs and VLSEs can produce 'risks' which deserve to be regulated. The AIA does not regard them as 'high risk' but as 'low risk', subject to transparency requirements only, Artt. 52–54 AIA. The DSA induces from their size the potential to trigger 'systemic risks', which deserve to be 'mitigated' and even a 'crisis', legitimating regulatory intervention. Both systemic risks and crises are defined in the DSA. Art. 34 (1) DSA distinguishes four types of system risks: dissemination of illegal content, foreseeable negative effects on fundamental rights, on civil discourse, electoral process, public security and last but not least about *'gender-based violence, the protection of public health and minors and serious negative consequences in the person's physical and mental well-being'*. The wording raises many questions: is there a difference between 'foreseeable effects' and 'serious negative consequences'? The wording suggests that 'effects' are lighter than 'consequences'. If there is a difference, why are gender and minors higher ranked than physical and mental health? The 'crisis' means 'extraordinary circumstances (which) lead to a serious threat

102 See M. Namyslowska, Future-Proofing the Unfairness Test in this report.
103 https://transparency.dsa.ec.europa.eu/
104 See under 2 a) bb).

to public security or public health in the Union or significant parts of it', Art. 36 (2) DSA. There is considerable overlap between 'systemic risks' and 'crisis', which deserve to be solved in the implementation and enforcement of the DSA. How the DSA is conceived suggests that the European Commission after having consulted the Board has to decide whether the systemic risks must be regarded as a 'crisis' requiring regulatory action.

The basic information has to be provided by the VLOPs and VLSEs which are subject to extensive obligations in assessing risks and mitigating risks, Artt. 34 and 35 DSA. The DSA lays down several 'factors', which they have to take into account in assessing risks and determines a long list of measures tailored to specific systemic risks with due regard to their impact on fundament rights. To ensure that the VLOPs and VLSEs are not remaining an empty cell the DSA requires them to establish a two-layered compliance system on risk assessment and mitigation measures. The VLOPs and VLSEs have to take institutional precautionary measures to separate the organizational function of the companies from the compliance function, Art. 41 DSA. This is the *first* layer. Language is telling. The DSA uses legal concepts developed for public enforcement authorities. The VLOPs and the VLSEs have to designate a competent compliance officer, who must be independent, qualified, have the necessary resources at their disposal and cooperate with the European Commission. The *second* layer results from the obligation to mandate independent auditing at the expense of all Chapter III due diligence obligations, Art. 37 (1) a) DSA. Independent auditing is a functional equivalent to third-party certification bodies. However, the auditing companies are not accredited, although they have to fulfil several binding requirements on their qualification, their available resources, professional ethics, and objectivity as well as those aiming at avoiding conflicts of interest between the VLOPs and the VLSEs and the consultancies exercising the auditing.

The VLOPs and the VLSEs have reporting obligations on risk assessment and mitigation towards the European Commission, the DSC of establishment and the public at large subject to limitations, resulting from confidentiality requirements, Art. 42 (4) and (5) DSA. On **request** of the DSC of establishment or of the European Commission, they have to '*explain the design the logic, the functioning and the testing of their algorithms including recommender systems*', Art. 40 (3) DSA, on a **reasoned** request, they have to provide access to '*data necessary to monitor and assess compliance*', Art. 40 (1) DSA and on **reasoned** request to 'vetted researchers' who meet the requirements of independence laid down in Art. 40 (8) DSA by the national DSCs, subject to a '*duly substantiated application*'. Access to data is riddled with obstacles and vague legal terms that give VLOPs leeway to ward off or even prevent requests, this is true for the public authorities but also for vetted researchers who are dependent on the discretion of the national DSCs and the public at large.[105] Of particular practical relevance is the distinction between mere requests and reasoned requests. Reasoned requests require an initial suspicion of a possible infringement of the due diligence obligations.

The interests of consumers tend to get lost in the institutional, procedural and substantial design of the due diligence obligations of VLOPs and the VLSEs. This does not mean though that they do not exist, nor that the DSA does not deal with them. However, they have to be

105 For a deeper analysis on access for research purposes, L. Specht-Riemenschneider, Plattformregulierung – Plädoyer für ein funktionszentriertes Verkehrspflichtenmodell, Gutachten im Auftrag des vzbv (gemeinsam mit F. Hofmann), 01/2021, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2021/02/04/specht_hofmann_gutachten_plattformverantwortlichkeitdocx.pdf

dug out. Perhaps a telling metaphor could be the battle for information, to be generated by the VLOPs and the VLSEs based on the due diligence obligations.

Art. 34 (1) b) DSA explicitly refers to Art. 38 EUCFR, which begs the question of what kind of consumer interests are enshrined in Art. 38 EUCFR.[106] More telling and more precise are the 'factors' that the VLOPs and VLESs have to take into account. Art. 34 (2) a) c) d) DSA refer to algorithmic systems, the applicable terms and conditions and their enforcement, as well as to advertising. The measures taken to mitigate systemic risks mirror the relevance of the factors, Art. 35 (1) b) d) e) and adds trusted flaggers, g) DSA. This means that the VLOPs and the VLSEs store relevant information on compliance with Art. 38 EUCFR, on the role and function of standard terms and advertising in risk assessment and risk mitigation. The compliance to be exercised by the VLOPs and the VLSEs is then screened through independent auditing, which covers all Chapter III obligations, Art. 37 (1) a) DSA. Both the information generated by the VLOPs and the VLSEs as well as the reports developed by the independent auditing are of utmost interest for consumers to understand the degree to which their interests have been taken seriously.

However, access to the data for consumers is paved with legal barriers, first within the companies and then within the national enforcement authorities as well as the European Commission. That is why the role and function of vetted researchers who shall have access to internal data for independent research on systemic risks and mitigation of risks is crucial. It is certainly a step in the right direction that the DSA recognizes the importance of independent research and the need to regulate access to the internal data of the VLOPs and the VLSEs. It is plain that vetted researchers must ensure that they have the necessary competence, the skills to ensure data security and confidentiality and the obligation to make the results publicly available. Less convincing is the regulatory approach. The DSA does not design the role and function of the vetted researchers through their perspective, which would have required to grant them clearly defined rights and establish procedural safeguards. Instead, the DSA puts the DSCs into the role of a Cerberus which has to ask for 'substantiated requirements', Art. 40 (8) a) – g) DSA. The list is not exhausting 'meet all the following requirements' leaves room for discretion.

What remains for consumers is the publicly available data, which will be in practice thinned versions of the data filed in the public authorities as the VLOPs and the VLSEs may invoke confidentiality, Art 42 (4) and (5) DSA. The same is true about the research results to be made public by the vetted researchers. Much will depend on additional measures that the European Commission is entitled to take to concretise the various due diligence obligations under subs. 5. The European Commission is empowered to adopt delegated (sic) acts about independent auditing, Art. 37 (7) DSA and about data access and security in Art. 40 (13) DSA as well as guidelines on the mitigation of risks Art, 35 (3) DSA and online transparency Art. 39 (3) DSA. It deserves to be highlighted that in the sensitive field of online transparency, no further binding legislation is to be expected. There is a second source of information which might be relevant but it is limited to illegal content. Affected consumers have to be informed or the public at large. Interestingly neither the individual consumer nor consumer organisations have access to the data on explainability, Art. 40 (2) DSA.

106 See B. Kas Ensuring Digital Fairness in EU Consumer Law through Fundamental Rights: Is the EU Charter Fit for Purpose? in this report.

The DSA does not grant consumers and consumer organisations a particular standing or a set of rights if the due diligence requirements are under subs. 5 of the DSA are not met. There would have been several occasions where regulation of consumer interests would have been obvious. One is laid down in Art. 39 (2) DSA which obliges the VLOPs and VLESs to include in the advertising repository information on whether particular groups of recipients had been targeted and on the aggregated number of them, Art. 39 (2) e) and f) DSA. Here is the link to the vulnerabilities, which enjoy protection under Art. 5 (3) UCPD. Another crucial element is the accountability of the management body for institutionalizing the compliance function. Art. 41 (5) DSA insists on accountability, without specifying what this exactly means, thereby avoiding the language of liability.

Subs. 5									
Providers of VLOPs and VLSEs	Art. 34 risk assessment	Art. 35 Mitigation of risks	Art. 36 Crisis protocol	Art. 37 independent audits	Art. 38 Recommender systems	Art. 39 Online Advertising Transparency	Art. 40 data access and scrutiny	Art. 41 Compliance function	Art. 42 Transparency reporting obligation
Addressee	Gender, minors (1) b Public at large in connection with Art. 39	Addressees of fundamental rights Public at large in connection with Art. 38 (2) and Art. 39	Commission to take action			Art. 39 (2) e) f) particular groups of participants		Independent senior manager (2) (5) Management body accountable	Public at large, inter alia the audit report
Obligations	Systemic risks, foreseeable effects on Art. 38 EUCFR, Art. 40 (1) b)	In particular about fundamental rights, a long list of measures Art. 35 (a) to (k) i.a. terms and conditions	Crisis defined in Art. 36 (2)	(1) a) All obligations under chapter III. Subs. 1–6, b) codes Art. 45 and Art. 46 Art. 37 (3) minimum requirements for auditing organisations	A two-layer approach to profiling	Repository, based on minimum information	Art. 40 (4) upon a reasoned request from DSC-E to vetted researchers, condition – 'duly substantiated application' (8)	Compliance function, independent from organisational function (1	Art. 42 (2) minimum standards, (4) reporting requirements Making public (4)
Restrictions	Preserve documents for three years			Confidentiality (2)	One option not based on profiling		Access bound 'on request' and on 'reasonable request'		Confidentiality, (4) and (5)
Layers of regulation		Art. 35 (3) guidelines	(11) Report to the EP and the Council	(4) audit report, subject to detailed requirements Delegated act, (7)		Art. 39 (3) second para guidelines	(13) delegate acts		
Particularities	(2) a) c) d) factors, algorithmic system, standard terms, advertising Self-investigation of intentional manipulation (2) at the end		(6) Commission on its motion enters into a 'dialogue'.			Overlap with vulnerabilities, but not mentioned Art. 39 (3) special rules on advertising in terms and conditions		)	Key document for consumers, equivalent to the technical documentation in the AIA

gg) Standards, Codes and Protocols

Subs. 6 provides for rules on voluntary measures, to be promoted and facilitated by the European Commission. These measures can take various forms, voluntary technical standards, codes of practices or protocols. Two aspects are worth highlighting: the strong role of the European Commission in setting their elaboration into motion, not least through the involvement of civil society organisations and the tying of the voluntary measures to the fulfilment of certain minimum requirements. This is quite an unusual regulatory technique – the initiative is not left to the VLOPs and VLESs alone, instead the Commission takes the lead and sometimes even sets a clear timeframe. This is one particularity. The other one is the content requirements. The VLOPs and the VLESs have no choice in practice, they have to engage in the elaboration and they have to respect the minimum requirements. However, there is no general approach to monitoring and surveying their application in practice. Art. 45 (4) DSA stands out in the obligation of the Commission and the Board to 'assess' whether the codes of conduct on systemic risks and illegal content meet the requirements and evaluate whether the objectives have been achieved. The DSA thereby establishes a kind of ranking list. Systemic risks and illegal content require Commission supervision even if the measures taken are non-binding, whereas codes on advertising and accessibility should be monitored and surveyed by the VLOPs and the VLESs themselves. The same holds for standards in the meaning of Art. 44 DSA.

Voluntary measures affect consumer interests: the voluntary standards for targeted measures to protect minors online, Art. 44 (1) j); the code of conduct on systemic risks and illegal content, Art. 38 EUCFR (systemic risks) and the consumer acquis (Art. 3 h DSA), the Codes on online advertising Art. 16 DSA through the transmission of information affecting the 'recipients', the code on accessibility through the emphasis of persons with disabilities. The DSA provides for the inclusion of civil society organisations in their elaboration. This opens ways for consumer organisations to participate. However, the DSA does not grant a right to participation. That is why their involvement will depend in practice on the supervisory role of the European Commission in their elaboration, about their participation and whether the voluntary measures take full account of consumer interests. Such a role could only be identified about the codes on systemic risks and illegal content, Art. 45 DSA. The position of consumer organisations might be stronger if the codes come under the scope of application of the UCTD and/or the UCPD. So far, however, the protection against misleading advertising resulting from references to codes of practices has not played a bigger role.[107]

---

107 See under 2 j).

Subsec. 6					
other provisions on due diligence	Art. 44 standards	Art. 45 codes of conduct	Art. 46 codes of conduct	Art. 47 codes of conduct for accessibility	Art. 48 Voluntary crisis protocols
Mandate	Commission support and promotion after consultation of the board and de facto with the ESOs	Commission shall encourage and facilitate	Commission shall encourage and facilitate	Commission shall encourage and facilitate	The Board may recommend the Commission, the latter shall encourage
Addressee	No distinction between addressees But minors (1) j)	Civil society organisations may be invited by VLOPs VLSEs	Online platforms and other relevant service providers	Online platforms, other relevant services,	online search engines shall involve Member States and maybe Union bodies
Content	Ar. 44 (1) a-j minimum standards	Illegal content and systemic risks (3) key performance indicators	(1) further transparency in online advertising (2) substantive requirements to be met	Addressing the particular needs of persons with disabilities, (2) substantive requirements	Strictly limited to extraordinary circumstances affecting public health and public security
Particularities	Voluntary standards	Participation in civil society, (2)	(1) participation of civil society	(1) organisations representing the recipients, civil society organisations	(2) encourage participate participation of VLOPs/VLSEs, online platforms,

b) Due diligence under the AIA

The regulatory design of the AIA differs in various ways from the DSA which renders the access to the rather hidden impact of consumer law more difficult. The AIA does not deal with the obligations of the different addressees of the regulation broken down into subsections, but distinguishes between the different levels of risks 'prohibition', 'high-risk', and 'low risk' and then specifies the obligations along the line of the different risks. The bulk of due diligence obligations is to be found in Title III dealing with 'high risk', thereby distinguishing between 'Requirements for High-Risk Systems' in Chapter 2 and 'Obligations of Providers and Users of High-Risk AI Systems and Other Parties'. However, the two are closely interlinked through Art. 16 AIA and need to be analysed together. Here we find the same and similar language as in the DSA. Due diligence obligations focusing on 'low risk' are rather scarce and cover a few articles in Title IV under the notion of 'certain risks'.

The regulatory approach in the AIA calls for a different structure of analysis. *First* and foremost, there is the need to dive deeper into the different layers of high-risk regulation to disclose the degree of privatisation of the (consumer) law and the difficulties. A similar complexity does not exist about low risks. In the *second* step, the actors operating in the field of high-risk AI systems are identified about the scope and reach of obligations imposed on them. In a third step, we turn to the relationship between the due diligence obligations of high-risk AI systems providers and the consumer law acquis before the actors of low-risk AI systems and their obligations are described.

aa) Layers of Regulation of High-Risk Providers of AI Systems

The EU digital policy legislation operates with different layers of regulation, which range from binding, and semi-binding rules to all sorts of non-binding recommendations, guidelines, and standards. One might distinguish six layers, 1) mandatory binding legal requirements, 2) voluntary harmonized technical standards, 3) common specifications, 4) guidelines and recommendations from the European Commission, 5) non-binding guidance from the European

benchmarking authorities and last but not least 6) voluntary industry standards. Layers 2 to 5 come under the umbrella of co-regulation, the interaction between law and voluntary but harmonized rules, reflected in a sort of staggered legal effects. These effects are united by the philosophy that the binding rules and non-binding standards/guidelines/codes etc. reflect the 'generally acknowledged state of the art'. Thereby the EU digital policy legislation opts for the less stringent level of protection against risks, in the well-established hierarchy including 'the state of the science', the 'state of science and technology' and 'the generally acknowledged state of arts'.[108] This is rather astonishing in light of the exponential development of the new technology. Last but not least there are voluntary standards, technical standards but also codes of conduct, embedded into a regulatory frame, without, however, rewarding compliance.[109]

At each level, consumers' interests and the consumer law acquis might be affected. A full picture of the impact on consumer law requires analysing the six layers one by one, once all the additional measures are taken either by the European Commission, the European standardisation bodies or the AI systems providers. So far the framing remains rather anemic, as the lower levels of regulation have not yet been completed. It will take two to three years before the harmonised European standards are developed and approved by the European Commission.

108 There is a huge amount of literature on the classification and ranking of risks. The distinction, however, is well established.

109 Przemysław Pałka, Data Management Law for the 2020s: The Lost Origins and the New Needs, 68 Buff. L. Rev. 559 (2020)

	Provider, Art. 16-23, Art. 28 b) EP	Manufacturer Art. 24	Authorized representative Art. 25	Importer Art. 26	Distributor Art. 27	AI value chain providers, distributors, importers, deployers, third parties Art. 28	Provider foundational model, Art. 28 b EP	Deployer, Art. 29	Sandbox Art. 53 a) EP
Binding legal requirements **Implementing and delegated acts**	Art. 11 (3) delegated act,								
Harmonised standards	Art. 16 (1) e), Art. 17 (3) Art. 52 (2) and (3) EP						Art. 28 b) (2) g) EP		
Common specifications **To be complemented through implementing acts, Art. 41 (1)**	Art. 52 (2) and (3) EP						Art. 28 b) (2) g) EP		
Guidelines, recommendation codes of conduct	Art. 82 b) (1) a) Art. 8–15, 28 and 28 b) EP Art. 52 Art. 69 codes of conducts providers and business organisations						Art. 82 b) (1) a) EP		Art 53 (5)
Benchmarking							Art. 28 b) (2) g) EP		Art. 53 a) (2) h) EP
Voluntary standards	Art. 28 a) unilaterally imposed by an 'enterprise'	Art. 28 a) unilaterally imposed by an 'enterprise'	Art. 28 a) unilaterally imposed by an 'enterprise'	Art. 28 a) unilaterally imposed by an 'enterprise'	Art. 28 a) unilaterally imposed by an 'enterprise'	Art. 28 a) unilaterally imposed by an 'enterprise'	Art. 28 a) unilaterally imposed by an 'enterprise'	Art. 28 a) unilaterally imposed by an 'enterprise'	Art. 28 a) unilaterally imposed by an 'enterprise'

Binding legal requirements are ranked *first* in the AIA. The AIA establishes in Title III Chapter 2, multiple requirements for AI systems as well as obligations for providers, deployers and other third parties of AI systems. Such requirements and obligations are different according to the degree and kind of risks presented by each AI system: certain practices are prohibited (Art. 5); the core of the AIA provisions (Chapter 3) concern high-risk systems; some transparency requirements apply to certain non-high-risk systems, (Chapter 4), in general, non-high-risk systems are encouraged to adopt voluntary codes of conduct (Art. 69).

The requirements for AI systems may be understood as institutional safeguards on risk management, data governance, record keeping, transparency, human oversight, accuracy and robustness (Art. 8 – 15 AIA for high risks, Art 52 AIA for certain risks, Art. 69 AIA for all 'non-high-risk' systems). These institutional requirements are translated in Chapter 3 into obligations to be met by the relevant economic operators (to use a more neutral term which covers all potential addressees). The distinction between institutional – Chapter 2 – and personal requirements – Chapter 3 – is only maintained for high-risk systems and even there, on closer inspection, both dimensions are intertwined, through the direct connection of personal obligations to institutional requirements; the transparency for certain non-high systems are specified, by merging both dimensions, in a single rule, Art. 52 AIA. The European Commission is empowered to close

potential gaps in the binding legal requirements through delegated and implementing acts,[110] a residual power resulting from the full-harmonisation approach. Once these requirements have been adopted, there is no leeway for the Member States, unless it is explicitly foreseen in the AIA.[111]

The AIA (in Chapter 3) contains a whole range of obligations on providers of high-risk AI systems concerning: compliance with the institutional requirements, quality management systems, technical documentation, logs, conformity assessment, registration duties, corrective actions, notification and information to public authorities and notified bodies (certification bodies) as well as co-operation with public authorities. These obligations are further concretised in the subsequent rules of Art. 17–23. The institutional requirements and personal obligations on 'non-high-risk' AI systems are rather simple: besides the transparency requirement for the system in Art. 52, non-high-risk systems may be governed by voluntary codes of conduct.

The *second* layer is *harmonized European standards* to be elaborated by the European standardization organisations (ESOs) with the participation of stakeholder organisations, mandated and co-financed by the European Commission. References to harmonized European standards are omnipresent in the AIA. They form a constitutive building block of the AI regulatory framework, being meant to shape the often broadly worded binding legal requirements. Whilst their use is voluntary, the presumption of conformity in case of compliance sets a strong incentive to make use of the available harmonized standards, so that they may be de facto binding.[112] Harmonised technical standards – this is to be recalled – are meant to give shape to '*human-centric, secure, ethical and trustworthy AI*' (the standard formula of the AI legislation[113]) by concretising all obligations of Title III Chapter 2 and Chapter 3. Such standards may address substantive, institutional and personal requirements *as well as* the conformity assessment mechanisms to ensure compliance with such requirements. Therefore, to understand the co-regulatory requirements imposed on the AI systems providers and deployers, it does not suffice to look at the bombastic language of the binding legal requirements; it is also necessary to consider the AI harmonized technical standards existing in the form of ISO/IEC and IEEE standards or still under elaboration at the EU level.

The *third* layer is common specifications, enacted by the Commission to fill gaps left through delayed or insufficient harmonized technical standards, Art. 41 AIA. The fallback regulatory power may serve as the stick behind the door to push the European Standardisation Organisations into action. The EP requires the Commission to develop common specifications for the methodology to fulfil the reporting and documentation requirements on energy consumption of AI systems, without leaving room for harmonized standards, Art. 84 AIA. The European Standardisation Organisations are very critical of the residual power of the European Commission. They fear a downgrading of private standardization through the European Commission which might use this broadly worded competency to substitute private standards through legally binding common specifications. Civil society groups, on the contrary, tend to support

110 Referring to the distinction between Art. 290 and 291 TFEU, thereto M Chamon, The European Parliament and Delegated Legislation, An Institutional Balance Perspective, Hart 2021

111 N. Helberger/ O. Lynskey/ H.-W. Micklitz/ P. Rott/ M. Sax/ J. Strycharz, EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets, A joint report from research conducted under the EUCP2.0 project, BEUC, March 2021, 207 pages; https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf

112 ECJ Case C-171/11 Fra.bo ECLI:EU:C:2012:453

113 H.-W. Micklitz, The Role of Standards, loc. cit. pp. 98.

public regulatory powers, as they believe that public interests are better off in the hands of public authorities,[114] which is highly debatable.[115]

The *fourth* layer includes all sorts of non-binding guidelines, recommendations, voluntary standards or codes of conduct, promoted by the AIA and provided with some sort of public recognition. The EP is more outspoken on the role and function of soft law: it has broadened the potential areas for it, has specified requirements these rules need to fulfil, has strengthened the consultative functions of the newly proposed AI Office, which is supposed to function as a spider in the net of public enforcement authorities and which might even turn into a predecessor of a potential EU AI Agency.[116] Contrary to the EC proposal, the EP intends to grant the European Commission widely conceived powers to adopt guidelines for the implementation of the institutional requirements of high-risk AI systems (Art. 8–15 AIA), for the transparency of certain AI systems Art. 52 AIA, and the regulation of non-high-risk systems through codes of conduct, Art. 69. The original EC proposal is more targeted about special areas and, at the same time less specific about powers, which would give the European Commission more leeway.

The *fifth* layer concerns non-binding guidance on benchmarking, namely, determining the expected levels of performance of the AI system, particularly about accuracy and robustness. According to the EP Art. 58 (b), the AI Office, together with national and international metrology and benchmarking authorities, are assumed to address the technical aspects of measuring appropriate levels of accuracy and robustness in Art. 15, and more generally to provide cost-effective guidance and capabilities to measure and benchmark aspects of AI systems and AI components. Performance metrics and their expected level should be defined with the primary objective of mitigating risks and negative impact of the AI system Recital 49, and coordinating the work of the ESOs to establish a common level playing field for all technical standards involved and deal with measuring. The EP seems to start from the premise that a clear line can be drawn between EC recommendations/guidelines under Art. 82 b) AIA and the guidance on benchmarking under Art. 58b) AIA. The AIA provides for three institutions, at the EU level, tasked with determining the correct functioning of AI systems,

- the European Commission in Art. 82 b), with the task of adopting guidelines
- The benchmarking authorities, with the task to specify the relevant benchmarks, under the responsibility of the AI Office, as a self-standing independent legal body, where the European Commission participates, however, without voting rights
- the European Standardisation Organisations, with the task to elaborate the harmonized technical standards, on which the AIA is built.

The side-by-side of the three bodies with no delimited tasks and responsibilities implies that there are likely to be conflicts between the three actors on the competent and responsible authority.

---

114 This is the conclusion one of the authors got in interviews taken with civil society organisations.

115 H. Schepel, The Constitution of Private Governance (Oxford: Hart Publishing, 2005), with a recent revival, O Kanevsk AIA-P, The Law and Practice of Global ICT Standardization, CUP 2023, M. Gérardy, The 'Standards Effects': The Public Instrumentalisation of technical standards in EU law, PhD University of Luxembourg, 202; see also P Delimatsis (ed), The Law, Economics and Politics of International Standardisation, CUP 2015.

116 Recital 76 (fn 11).

The *sixth* layer is voluntary rules which the economic operators involved in making, deploying, distributing, importing AI systems or authorizing their use are developing out of their motion. Interestingly the AIA limits the private autonomy of economic actors in various ways. Where the AIA calls for harmonized standards, voluntary standards may only be used to fill gaps outside the scope of application of the AIA. We wonder whether AI operators or deployers may voluntarily commit to requirements for quality and performance going beyond what is required by the AIA.

Even more striking are the AIA rules on codes of conduct. Under Art. 69 AIA the European Commission, the Member States and the proposed AI Office shall 'encourage' and 'facilitate' the development of codes for 'non-high risk' AI systems, which shall meet minimum requirements. We may wonder whether Art. 69 AIA should be interpreted as a contrario as excluding that voluntary codes of conduct may be adopted in the area of high-risk AI systems or whether such codes are permissible under the condition that they go beyond the binding legal requirements, which seems to be the more reasonable consequence.

Codes of conduct intended to foster voluntary compliance with the principles underpinning trustworthy AI systems, Art. 69 (2) AIA 'shall' (sic!) comply with a long list of precisely defined requirements, which are even more specific in the EP proposal. Are these requirements mandatory? Does this mean that codes of conduct which do not meet the Art? 69 (2) AIA requirements are prohibited? Art. 69 (3) AIA makes clear that neither the provider nor the respective business organisations are obliged to develop such 'codes of conduct'. They 'may' do so or not. But are other economic operators excluded from the elaboration of codes of conduct? The AIA does not set any incentives for economic actors who are ready to engage in such an exercise and neither clarifies who will oversee controlling compliance with such voluntary codes of conduct which are 'encouraged' and 'facilitated' by public authorities. All in all, the purpose, of the regulation of voluntary codes of practice remains rather opaque: they are semi-binding in the sense the law recognises them and sets minimum standards for them but puts no mechanisms in place to ensure compliance and enforcement.

Standard terms, whether elaborated by business organisations or by companies come under the category of voluntary standards. However, Art. 28 (a) AIA EP regulates standard terms which 'an enterprise' unilaterally imposes on SMEs or start-ups, by stating that certain categories of terms are to be considered unfair, and therefore non-binding. This is the third time that the EU has regulated the fairness of standard terms in B2B relations, in value chains in the food sector,[117] in platform regulation[118] and now in AI systems. If the proposal is approved in the trialogue, freedom of contract would be considerably limited.[119]

bb) Actors and Responsibilities within High Risk AI systems

The EC proposal puts the provider of a high-risk AI system centre stage. The EP intends instead to upgrade the responsibilities of the deployer considerably through the extension of special obligations and most prominently through making them – alone – responsible for the

117 Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain *OJ L 111, 25.4.2019, p. 59–72*

118 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services *OJ L 186, 11.7.2019, p. 57–79*

119 This is the language of the Directive 93/13/EEC on unfair terms in consumer contracts, Art. 6 (1).

fundamental rights impact assessment of high-risk AI systems. In this sense, one might speak of a double-headed approach to the design of responsibilities.

The content of the various obligations follows the design of EU product safety regulation: in the scope as well as in the allocation of responsibilities to the various economic actors, according to their responsibilities in the AI value chain. The degree to which other economic operators are submitted to the same set of obligations as the provider has been subject to a battlefield ever since. Whilst the extension of public law responsibilities of other economic operators than the provider is obvious over the last decades, their infringement does not necessarily imply private liabilities. There is a considerable mismatch between EU product safety and risk-based EU AI legislation and product liability under Directive 85/374/EC. The proposed revision of the Directive as well as the newly proposed AI Liability Act are closing the gap to a rather limited extent only.[120] Therefore, the scope and reach of private liability remain governed by national tort law, which stands side by side with EU product liability or AI liability rules.

The table is structured in the following way: it breaks down the potential addressees and allocates to them the obligations laid down in Chapter 3.

120 Ph. Hacker, The European AI Liability Directives _ Critique of a Half-Hearted Approach and Lessons for the Future https://arxiv.org/abs/2211.13960; P. Machnikowski (ed), European Product Liability: An Analysis of the State of the Art in the Era of New Technologies (Intersentia, Cambridge 2016).

	Obligations Art. 16 **In line with Chapter 2**	**Quality management Art. 17** **Together with Art. 9 (risk assessment), 10 (data governance), 13 (transparency), 14 (human oversight), 15 (robustness)**	**Technical documentation Art. 18** **Together with Art. 11**	**Conformity Assessment, Art. 19**	**Automatically generated logs Art. 20** **Art. 12 (3) Reporting facilitate post-market monitoring**	**Corrective action, Art. 21**	**Duty of information, Art. 22**	**Co-operation with authorities, Art. 23** **and stakeholders + independent experts**	**Post-market monitoring duties Art. 61** **Reporting of serious incidents Art 62**
Provider, Art. 16–23,	Compliance with Chapter 2 Art. 61 and 62	h) Post-market monitoring i) Reporting incidents	By Annex VI	Art 43 in compliance with Chapter 2	Contractual arrangement with the deployer EP by industry standards	Inform distributor authorized representative importer EP Distr. Representative, national authority **not** importer, notified bodies, deployer	Authorities and notified bodies EC known risks EP is aware of the risks EP distributors importers deployers representative EP deployers	Chapter 2 compliance info and docu on request, on reasoned request logs	Providers actively systematically collect, document analyses relevant data by users (provided by deployers Art. 61 new) or collected through other sources throughout their lifetime, 61
Manufacturer Art. 24	Annex II Section A Same as provider								
Authorised representative, Art 25	Where an importer cannot be identified EP appointment mandatory		Have a declaration of conformity available Upon reasoned request EP specifications on the declaration	Upon reasoned request	Upon reasoned request			Upon reasoned request	
Importers, Art. 26			Ensure the provider has drawn up Make available upon a reasoned request	Ensure that the provider meets the requirement Make available upon a reasoned request	Upon reasoned request		Inform provider + authorities	Shall cooperate	
Distributor, Art. 27			Shall verify CE marking, documentation Make available upon a reasoned request	Shall verify compliance Make available upon a reasoned request			Inform the provider and authorities EP based on the information in its possession	Shall cooperate	

AI value chain, Art. 28	Any distributor, importer, user or third party shall be treated as a provider if.. EP **substantial** modification + further specifications along the AI value chain		The former provider shall make available to the new provider						
Deployers/ users, Art. 29	Shall use by instructions EP take technical and organizational measures to ensure compliance with instructions EP Inform natural persons on the use of AI system EP Consult worker representation for AI systems at the workplace	EP's particular management duties on human oversight and human control			Shall keep the logs for a limited time (EP 6 months by industry standards)		Notify serious incidents to provider and distributor EP also importer and relevant national authorities	Shall cooperate with the relevant authorities	EP Art. 29 (1) new Inform the provider by Art. 61
Art. 53 and 53 a) Sandboxes	Particular requirements Art. 51 a) new EP To be specified by implementing act			Art. 53 (1) e) achieve regulatory compliance Art. 53 a) (2) e) conformity assessment or voluntary application of codes of conduct					Maybe through implmentating act

The already complex picture is not yet complete though. The EP has proposed major amendments. First and foremost a need to initiate a fundamental rights impact assessment Art. 29a) AIA for high-risk AI systems. The EP proposal on the developers of a foundational model does not fit in the overall distinction between high-risk and low-risk and certainly not into Chapters 2 and 3 as they aim at identifying the degree of risk before making it available for commercial purposes. Somewhat in between ranks the 'provider of a foundational model' as proposed by the EP in Art. 28 b) AIA. The 'provider' – as the EP calls it – is equally obliged to conduct a particular kind of impact assessment. The requirements to be met are tailored to the explorative character of a foundational model. That is why Chapters 2 and 3 cannot be transferred to foundational models, as the degree of risk is not yet clear. Whilst there is a similarity between the respective requirements, Art. 28b) AIA introduces rules on the participation of independent experts and information duties to facilitate the use of downstream deployers in the development of foundational models. The impact assessment to be conducted is certainly the core of the large set of requirements. It aims to demonstrate compliance through appropriate design and testing to reduce and mitigate reasonably foreseeable risks to health, safety, fundamental rights, environmental protection, democracy and the rule of law.

cc) Due Diligence and Consumer Law in High-Risk AI Systems

The design of the obligations of providers of high-risk AI systems could be understood as a developed version of subsection 5 in the DSA on VLOPs and VLESs. On April 23 the Commission adopted the first designation decisions under the Digital Services Act (DSA), designating 17 Very Large Online Platforms (VLOPs) and 2 Very Large Search Engines (VLSEs) that reach at least 45 million monthly active users.[121] The basic elements are similar – quality management covering risk management, risk mitigation, data governance and logs – conformity assessment instead of compliance and auditing and – in addition, more sophisticated rules on the duties to information and co-operation with public agencies. From a consumer perspective, the post-market monitoring obligations of AI system providers, Art. 61 AIA are of particular relevance.

The overall structure is similar to the DSA with one major difference, the implementation is not left to the providers but is concretised not only through delegated acts but through omnipresent guidelines and in particular through harmonised European standards, which in case of compliance grant access to the Internal Market. Therefore, the leeway left to the providers of AI systems is narrower than the one left to the VLOPs and the VLESs, although a fully-fledged analysis requires the existence and availability of all supplementing documents – the delegated and implementing acts, the guidelines and the harmonised standards, which are not yet available and which are in the case of harmonised standards subject to copyright protection and therefore not fully available. These harmonised standards are playing a key role in the EU digital policy legislation, formally separated from EU rules governing b2b and b2c private law relations. However, the CISG in b2b as well as Art. 8 Directive 2019/770 on consumer sales contracts leave room for assessing whether a product is free of defects, thereby taking into consideration (harmonised) technical standards.[122]

---

121 https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413

122 H.-W. Micklitz, Soft Law, Technical Standards and European Private Law, Chapter 10 in: Mariolina Eliantonio/ E. Korkea-aho/ Ulrika Mörth (eds.), Research Handbook of Soft Law, Edward Elgar Publishing, 2023, 144–161

Contrary to the DSA, the AIA in Title III – High-Risk AI System does not provide for specific rules on consumer protection. There is no equivalent to subsection 4 dealing with contractual relations between the provider of an AI system and the consumer. In the EC proposal, there are no references to 'terms and conditions'. This is different from the EP proposal, which aims at protecting SMEs against the bargaining power of AI system providers. The proposal if adopted, could serve as a benchmark for testing whether the SMEs under the AIA are better and more effectively protected than the consumer under Dir. 93/13. Of particular interest could be Art. 28 b) (4) AIA declaring unfair a term which *(c) gives the party that unilaterally imposed the term the exclusive right to determine whether the technical documentation and information supplied are in conformity with the contract or to interpret any term of the contract (see below)*. The second major difference between the AIA-EC and the AIA-EP concerns the role and function of advertising. Art. 5 AIA-EP broadens the scope in two ways, it covers all the affected as well as '*subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm*'. The extension of the scope affects the relationship between Art. 5 AIA and the UCPD, which is subject to a separate analysis.[123]

There are, however, rules in the AIA which impose the obligation on the AI system provider to comply with due diligence obligations in a way that takes the consumer fully into consideration. One such reference is laid down in Art. 9 (4) AIA Risk Assessment: '*In eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used*.' The reference to the environment can hardly be limited to the narrow definition of the professional user, let alone the overall debate on whether the provider has to take the foreseeable use into account, a criterion which could easily build a bridge to the integration of the consumer perspective.[124] Another crucial element in the risk assessment is the obligation to protect children through an appropriate design, Art. 9 (8) AIA.

More important could become the amendments to Art. 13 AIA proposed by the EP on specifying 'information and transparency' of high-risk AI systems, although the wording leaves doubts on who the exact addressee of the obligation shall be. The EP proposes to take away 'user' in the heading, but then addresses providers and users in Art. 13 (1) AIA as those who shall '*reasonably understand*' the AI system's '*functioning*'. As the EP has replaced the user in the EC proposal through the deployer, Art. 13 (1) AIA might be read as if 'user' has to be understood in a much broader way. However, the EP does not speak of all those '*who are affected by the system*', which is the language applied by the EP to make sure that everybody shall be protected by the rules of AIA against risks to their health, safety and against '*signification harm*' (to their economic interests).[125] It seems as if the revised Art. 13 (1) AIA does not include a due diligence obligation of the AI provider in combination with Art. 16 a) AIA to design the system to make

123 M. Namyslowska, Future-Proofing the Unfairness Test in this report.
124 The debate on foreseeable use determines product safety regulation ever since and has been transferred to the EU digital policy legislation.
125 On the broadening of the scope through the AIA-EP under 2 a) and b).

it reasonably understandable to consumers, i.e. to 'all affected'. The potential gap, however, will be closed through the revised Art. 52 AIA, as explained below under 4.

Outside and beyond the bits and pieces which could be pulled together, the AIA obliges the providers of AI systems along the layers of regulation to pay due respect to the omnipresent charter of fundamental rights. This is true about Art. 38 EUCFR as well as about individual fundamental rights which embrace the consumer interest. The stock-taking of the case law of the CJEU and the ECtHR under the EUCFR and the ECHR insinuates a word of caution though. One might argue that the consumer is protected against manipulation at least under exceptional circumstances and against the lack of human oversight, in case the human does not have the last word. However, this seems to be much more wishful thinking than forthcoming reality. Art. 38 EUCFR, which is sometimes referred to implicitly, does not provide much help to compensate for the deficits of individual rights.[126]

The key document is the technical documentation, laid down in Artt. 10, 18 AIA together with Annex VI. Consumers and consumer organisations have no access to the technical documentation, which is or shall be available on request to the enforcement authorities. The EP proposes to call for a reasoned request which would make it even more difficult for the enforcement authorities. Whether and to what extent the provider of an AI system has fully considered the fundamental rights, here those enshrining the consumer interests depend on getting to know the measures the provider has undertaken to meet their requirements. The AIA does not foresee any remedy dealing with access to information, it does not even mention the importance of technical documentation for consumers and consumer organisations in contributing to the enforcement of the AIA. Here lies one of the major deficits within the AIA, which needs to be remedied. The search for appropriate tools for information in the hands of the AI systems providers is not without precedence, as the gap has been subject to controversy ever since due diligence obligations made their way into (EU) legislation.

The EP does not deal with the rights of the '*affected*' to get access to the technical documentation, but proposes to introduce a 'Right to the explanation of individual decision making, Art. 68 c) AIA which deserves to be quoted in full:

> Any affected person subject to a decision which is taken by the deployer based on the output from a high-risk AI system which produces legal effects or similarly significantly affects him or her in a way that they consider to adversely impact their health, safety, fundamental rights, socio-economic well-being or any other of the rights deriving from the obligations laid down in this Regulation, shall have the right to request from the deployer clear and meaningful explanation pursuant to Article 13(1) on the role of the AI system in the decision making procedure, the main parameters of the decision taken and the related input data.

This ruling, if adopted would establish a mandatory right as an integral part of the relationship between the 'deployer' (the user of an AI system) and the 'affected' (which could potentially be every citizen). A clear and meaningful explanation reaches far beyond the vague language proposed by the EC. The EP does not concretise what meaningful could mean, not even in the revised recitals. The term leaves room for interpretation.[127] Interestingly and somewhat

126 B. Kas, EU Consumer Law and Fundamental Rights, in this report.

127 On the right to meaningful information, M. Sax and N. Helberger, Digital Vulnerability and Manipulation in the Emerging Digital Framework in this report.

unsystematically, Art. 52 AIA contributes to a better understanding of the political objectives behind the new formula.

dd) Due Diligence and Consumer Law in Low-Risk AI systems

The potential impact of the AIA depends to a large degree on whether the trialogue will agree to the double extension proposed by the EP, the introduction of a new legal category 'affected person' and the integration of 'economic harm', even if narrowly limited to 'significant harm'. Such a double extension would transform the AIA into a universal legislation, whose scope of application *sedes personae* depends only on who is affected – which could be everybody and – whose scope of application *sedes material* would introduce a universal layer of protection against manipulative and misleading advertising. The implications for high and low-risk AI systems are discussed by Monika Namyslowska.[128]

The AIA contains in Title III one single rule on providers of low-risk AI systems. All that they must do is to meet the transparency requirements of Art.52 AIA. The scope is negatively defined. All risks which are not prohibited or categorized as high risk, are automatically classified as low risk. By now most of the services consumers are calling for are low risk. That is why the scope and reach of the DSA are of utmost importance. Art. 52 AIA complements the obligations of '*intermediary service*' under the DSA, the platforms, provided their service have to be regarded as an AI system in the meaning of Art. 3 (1) AIA.

The exact scope of Art. 52 AIA is subject to controversy between the EC and the EP. None of them questions, however, that low-risk providers of AI systems should bear limited due diligence obligations and that Art. 52 AIA should not address deployers/users of AI systems only. The EP aims at restricting the use of biometric recognition far beyond the standards proposed by the EC. This is one strand of conflict. There is also disagreement on what transparency could mean and there is uncertainty on the potential addressee. Art. 52 AIA-EC states that '*AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system unless this is obvious from the circumstances and the context of use*'. The EP proposes much more demanding requirements, in line with the 'Right to meaningful explanation': *'Where appropriate and relevant, this information shall also include which functions are AI-enabled, if there is human oversight, and who is responsible for the decision-making process, as well as the existing rights and processes that, according to Union and national law, allow natural persons or their representatives to object against the application of such systems to them and to seek judicial redress against decisions taken by or harm caused by AI systems, including their right to seek an explanation*. The addressees of Art. 52 AIA are natural persons who 'interact' with an AI system. Interaction, which comes clear from Recital 70, does not require the existence of a contract between the natural person and the AI system provider/deployer. Interaction is closer to communication before the conclusion of a contract or even without there being a contract.[129] Interaction might therefore be a mode of communication which comes potentially under the scope of application of the UCPD. Such an interpretation begs the question of where to draw a line between

128 See Chapter VI: M. Namyslowska, Future-Proofing the Unfairness Test.

129 P. Pałka, Terms of Service Are not Contracts: Beyond Contract Law in the Regulation of Online Platforms, in European Contract Law in the Digital Age, S. Grundmann ed., Intersentia (2018).

being 'affected' and 'interacting'. Affected suggests a passive attitude, whereas interaction insinuates some sort of activity on the side of the natural person.

Art. 52 (3) AIA lays down particular requirements for 'deep fakes'. The EP provides for a definition in Art. (3) (ff d)

> "Deep fake" means manipulated or synthetic audio, image or video content that would falsely appear to be authentic or truthful, and which features depictions of persons appearing to say or do things they did not say or do, produced using AI techniques, including machine learning and deep learning;

In line with the definition Art. 52 (3), AIA-EP calls for much more specific transparency obligations than the EC (in bold the amendments of the EP):

> 3. Users of an AI system that generates or manipulates ***text***, audio or ***visual*** content that would falsely appear to be authentic or truthful ***and which features depictions of people appearing to say or do things they did not say or do, without their consent*** ('deep fake'), shall disclose ***in an appropriate, timely, clear and visible manner*** that the content has been artificially generated or manipulated***, as well as, whenever possible, the name of the natural or legal person that generated or manipulated it. Disclosure shall mean labelling the content in a way that informs that the content is inauthentic and that is visible to the recipient of that content. To label the content, users shall take into account the generally acknowledged state of the art and relevant harmonised standards and specifications.***

Here is the link to Art. 68 c) and the missing concretisation of what exactly the right to meaningful explanation covers.

4. Privatisation of Consumer Law Enforcement through Compliance and Conformity

The analysis of the privatisation of consumer law through due diligence obligations sheds light on the substantive requirements, that the EU digital policy legislation imposes on the AI system providers and on the intermediary service providers with particular emphasis on disclosing the relationship and the interaction between the consumer law acquis and the DSA and the AIA. Speaking of privatisation of consumer law enforcement implies that the due diligence obligations embrace the consumer explicitly but or implicitly. Privatisation is inherent to the EU digital policy legislation through the overwhelming importance of self-regulation – within the regulatory frame marked out by broadly defined provisions, which despite all the efforts of the legislator via layered regulation – the AIA/DSA, delegated/implementing acts, Commission guidelines –, assigns the companies a decisive role in concretising not only the binding legal requirements but also in implementing these provisions – through compliance and conformity assessment. The providers of AI systems as well as the platforms are turning into regulators in a twofold dimension, they are drafting the rules within the limits of the binding legal requirements and they are enforcing them.

It is not within the scope of the report to engage with the enforcement of the AIA and the DSA via public supervisory bodies of the Member States, European agencies and the European

Commission.[130] However, seen through the lenses of public enforcement, compliance and conformity assessment mechanisms forestall and determine the role and function of national supervisory bodies. Supervising and monitoring compliance and assessment of the companies in charge of the due diligence obligations is one of the two elements of public enforcement. The other one is ex officio investigation. A full stock-taking would require an analysis of the deeper structure of private and public enforcement, the going together of compliance, conformity, supervision, monitoring and regulatory action. The following analysis may serve as an appetizer to point to the overwhelming relevance of self-regulation in organizing compliance and conformity and how the chosen approach affects the division of responsibilities, the competencies and the new dependencies, that the DSA and the AIA have or are going to establish.

The due diligence obligations their substance of the due diligence obligations and their implementation through self-regulation could best be reconstructed in the threefold distinction between institutional, procedural and substantive governance. We will begin with the DSA and then move to the much more sophisticated AIA. All in all, however, the common denominators are easy to identify.

a) Compliance with the DSA

Compliance is omnipresent in the DSA, particularly regarding due diligence duties, Chapter III. *Institutional* safeguards interfere with the inner organisation of the companies concerned. The DSA obliges the VLOPs – and these are the only ones contrary to LOPs and SMEs – to

> *'establish a compliance function, which is independent of their operational functions and composed of one or more compliance officers, including the head of the compliance function. That compliance function shall have sufficient authority, stature and resources, as well as access to the management body of the provider of the very large online platform or the very large online search engine to monitor the compliance of that provider with this Regulation'*, Art. 41 DSA.

The very same VLOPs are also obliged to execute an *independent auditing*. This means that another private company is involved in ensuring compliance. Auditing is functionally equivalent to third-party certification, although they do not have to be accredited and the regulatory impact is much softer than the one on certification bodies. Auditing comprises all Chapter III obligations, in between all those that are related to consumer protection generally and more specifically, Art. 37 (1) a) DSA. The management board is accountable for the implementation but not legally liable. The broad scope includes Art. 44 DSA which regulates compliance with voluntary standards, in contrast to harmonised European standards in the AIA. It is the European Commission which holds the exclusive power to supervise and enforce all obligations imposed on VLOPs. On top of Art. 37 (7) DSA grants the European Commission the power to adopt delegated acts which concretise *'the necessary rules on the procedural steps, auditing methodologies and reporting templates for the audits performed under this Article. Those delegated acts shall take into account any voluntary auditing standards referred to in Article 44(1), point (e) DSA.'* Consumers or consumer organisations are not involved.

All other rules address *procedural* arrangements. This includes the whole arsenal of requirements imposed by the legislator on the development of due diligence obligations, with or without the

130 H.-W. Micklitz/G. Sartor Compliance and Enforcement in the AIA in G. De Gregorio, O. Pollicino, P. Valcke (eds.) Oxford Handbook on Digital Constitutionalism, OUP upcoming 2024.

participation of consumers and other stakeholders; on access to the results of the compliance, and their dissemination and control (for example, by public supervisory bodies). The DSA puts much emphasis on reporting duties inter alia on due diligence obligations and thereby distinguishes between different providers, SMEs, LOPs and VLOPs. Two of the due diligence obligations deserve to be highlighted – the risk assessment due to the integration of the rights of minors and voluntary standards.[131] Art. 42 (4) a) DSA requires the VLOPs to report on the risk assessment, i.e. also on how they are weighing potential risks to minors in the design of the mitigation of risks. There is no such obligation for LOPs or SMEs. This is all the more amazing as Art. 45 DSA Codes of Conduct address all providers independent of their size. Art. 45 (5) DSA even obliges the European Commission and the Board to regularly monitor and evaluate the achievement of their objectives, having regard to the key performance indicators and publishing their conclusions. The involvement of consumers and consumer organisations is missing.

b) Compliance and conformity with the AIA

The AIA (Chapter 2) requires that the provider and the deployer of an AI system, on the one hand, adopt appropriate safeguards, and institutional, substantive and procedural measures[132] (on risk management and data governance, accuracy and robustness, human oversight, etc.); on the other hand engage in record keeping, transparency, and the preparation of documentation (Art. 8–15 AIA).[133] Based on the conformity assessment, providers obtain the EC mark, which gives them access to the internal market. The EC mark sends the message to the outside world that the responsible actor has taken all the necessary institutional, substantive and procedural safeguards. Self-certification is the dominant paradigm in the AIA, even about self-standing high-risk AI systems despite the strong resistance from civil society organisations.[134] The AIA suggests that harmonized European standards are the appropriate benchmark at both strands: the substance of the obligations imposed by law and concretised through standards as well as the demonstration of compliance, through appropriate procedures.

When it comes to the distinction between self-certification and third-party certification, different rules apply to high-risk AI systems which are safety components of products or standalone AI systems. In products with AI components, existing third-party certification provided for the types of products enlisted in Annex II is extended beyond product safety, to include protection against physiological and psychological harm[135] and respect for fundamental rights in the EC proposal[136] and in addition protection against economic harm under the EP proposal.[137] In

131 Art. 26 'Advertising of Online Platforms' is also referring to Art. 44 DSA. Art. 26 (1) and (2) include information on the reference to voluntary standards on advertising – here a link could be built to Art. 6 (2) UCPD. However, details are not relevant for the purpose of the study.

132 The distinction is in line with theories of governance St. Grundmann/ F. Möslein/ K. Riesenhuber (eds.), Contract Governance – Dimensions in Law and Interdisciplinary Research, OUP, 2015.

133 See above under 3 b).

134 Position paper BEUC AI AND GENERATIVE AI: TRILOGUE NEGOTIATIONS FOR THE AI ACT , BEUC recommendations, 25.7.2023, https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-101_AI_and_Generative_AI_trilogue_negotiations_for_the_AI_Act.pdf.

135 P. Pałka, AI, Consumers & Psychological Harm (July 15, 2023). "AI and Consumers," L. DiMatteo, C. Poncibò, Martin Hogg, G. Howells (Eds.), Cambridge University Press (2023/2024).

136 COM (2021) 206 final Proposal for the AIA; Explanatory Memorandum at 5 and rec 30, where the products are listed.

137 EP Art. 5 Amendment 215: 'a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that

standalone AI systems, where little to no experience exists, self-certification is the rule, Article 40 AIA-P. The only exceptions are remote biometric identification systems, Article 43 (1) Annex VII AIA. There is considerable disagreement between the EC and the EP on how to categorise biometric identification systems and the degree to which they should be allowed. However, there is agreement on the limited use of third-party certification. Insofar the EP has not expressed any reservations. Under EU law third-party certification can either be exercised by public or private bodies. The ultimate responsibility for the accreditation of certification bodies, however, lies with public authorities.

The reliance of the EU legislator on third-party certification has boosted the development of private certification bodies, such as the German TÜV. The PIP scandal (concerning defective silicone implants used for plastic surgery) disclosed the conceptual deficiencies of the EU third-party certification. Before the amendment of the medical device directive, certification bodies were neither obliged to monitor and survey compliance after the certification nor explicitly empowered to conduct on-site inspections without prior notification.[138] The impositions of such obligations on certification bodies (and the granting of corresponding powers), would turn such bodies into some sort of a post-market control entity. The AIA does not take a clear stand and thereby reiterates the uncertainties which led the CJEU to hold that the certification bodies were not liable in the PIP scandal.[139] Art. 43 AIA remains silent on the exact scope of obligations of such bodies. Details are laid down in Annex VII which contains a chapter on 'surveillance',[140] without, however, specifying what surveillance entails and without reference to Art. 61, which addresses the post-market monitoring duties of the provider.

The EP insists on the necessity for the certification bodies to get access to the source code but does not engage in a debate on the scope of the surveillance duties. Only public authorities should have the power of unannounced on-site inspections, according to the EP proposal in Art. 63 (3) AIA. However, there is a proviso: the post-market surveillance duties could in theory be complemented through implementing acts, Art. 51 (3) AIA. Systematically speaking, the self and third-party certification come close to a kind of premature outsourcing of public enforcement responsibilities to private parties – the private parties (AI system providers) who self-certify and are obliged to exercise post-market control as well as private certification bodies, which have at least 'surveillance duties' – whatever that might mean in practice. The private parties are indeed in the pole position, they are closer to the business practice, closer to discovering non-compliance, and closer to discovering potential infringements, the public authorities play a backstage role. However, to take any action, private parties need a particular reason, i.e., a strong enough motivation, which may indeed be missing in concrete cases.

The design of the different conformity requirements for AI systems as safety components and standalone systems leads to a paradoxical result: third-party assessment might have a role to play where technology is an 'add-on' to already existing products, whereas third-party assessment has practically no role in the world of the new risks – physiological and psychological harm and protection of fundamental rights. There is an obvious imbalance between the role of third-party assessment in product regulation and standalone technology. In the AIA approach,

---

person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm;'

138 H.-W. Micklitz/ N. Reich/ L. Boucon, L'Action de la victime contre l'assureur du producteur RIDE, 2015, 37–68

139 CJEU Case C-219/15 Schmitt ECLI:EU:C: 2017:128.

140 EC Proposal on AIA Annex VII under 5.

self-assessment is ideally to be compensated through appropriate enforcement mechanisms and the establishment of a European Commission-run European 'registry' (Article 51). Recital 15 sends a clear message jointly agreed by the EC and the EP [141]

> *A comprehensive ex-ante conformity assessment through internal checks, combined with **strong** ex-post enforcement, could be an effective and reasonable solution for those systems, given the early phase of the regulatory intervention and the fact the AI sector is very innovative and expertise for auditing is only now being accumulated. After the provider has performed the relevant conformity assessment, it should register those stand-alone high-risk AI systems in an EU database that will be managed by the Commission to increase public transparency and oversight and strengthen ex-post supervision by competent authorities.*

5. Observations and Recommendations

The title of the paper is 'dissolution' through 'fragmentation' and 'privatisation', the driver is the EU digital policy legislation. Consumer (contract) law is grounded in the distinction between the consumer and the supplier/trader, in the bilateral transaction focusing on sales transactions. The manufacturer comes in as the producer of risky products which might trigger product liability. The complexity of economic transactions is reduced to a triangular relationship. This is the core, the legislative reply to the consumption society of the 1950s/1960s – the development of the consumer law acquis where 'contract' and 'tort' (product liability) are the two pillars. Today's economy looks different. There are new commodities on the market, and new ways of consuming them. This is not just a matter of new digital products (such as computer games), but rather of focusing on buying "experience" and access to social relations, think of dating apps, like Tinder, or of social media platforms, like Instagram. Consumer law is not very well equipped to grasp this kind of problems. National courts are struggling in how and whether consumer law can be applied outside the original consumer context. A prominent examples is the tension between freedom of contract, consumer law and freedom of religion.[142] Whether the Digital Fairness Fitness Check[143] will lead to a revision of the consumer acquis and or the EU Digital Policy Legislation will have to be seen. Moreover, supply chains are omnipresent, upstream and downstream, rendered possible and promoted through electronic communication.[144] They bring all the actors within the supply chain to the limelight – the AI provider, the AI deployer, the dealers, the representative authorities, the importers, the platforms small and large, SMEs, regulatory sandboxes etc. and make them potential addressees of legal claims, no longer as consumers, but as customers, vulnerable persons, individuals, natural persons or simply as the affected.

The EU is relying on a 'risk-based' approach, which goes back to the New Approach/New Legislative Framework 1985/2012 – establishing a broad legal framework full of broad policy objectives which are then translated into equally broad legal principles to be filled out and concretised through private regulation, technical standards first and now ever more often codes

---

141 EC Proposal on AIA Explanatory Memorandum at 15.

142 M. Grochowski, Freedom of Speech, Consumer Protection and the Duty to Contract in. C. Mak and B. Kas (eds.) Civil Courts and European Polity, The Constitutional Role of Private Law Adjudication in Europe, 2023, 123.

143 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en.

144 R. Baldwin, The Great Convergence: Information Technology and the New Globalization, Harvard University Press, 2016.

of practices. What started in product safety has now been translated into the digital economy, thereby intermingling health, safety and economic harm. The de facto or de jure – depending on the outcome of the AIA trialogue – extension of the regulatory approach beyond health and safety into the economic sphere provides evidence for path dependency. The EU intends to transpose the 'success' of the internal market regulation from the old to the new economy. Whether this will work in practice, remains to be seen.[145]

a) Long Term Recommendations

What matters in our context is the dynamic function of public and private regulation which clashes with the rather static consumer law, mirrored in the straight jacket of the consumer vs. trader/supplier distinction. The legislature had to react to the multitude of actors operating within the supply chains and the diversity of all those who may come into contact with the different actors, no longer in their role of a consumer, but ever more often in the role of a citizen. The EU has no competence in private law, in contract and tort, and certainly not in b2b regulation. One option would theoretically be the elaboration of a new private law that fits the global value chains. The Treaty does not allow for such a regulatory model. The new approach – a new legal framework type of thinking has led to the establishment of a regulatory body which compensates for the lack of an EU private law on b2b transactions. Elsewhere I have argued that the traditional b2b private law is sandwiched between the public regulatory framework top down and the private regulation bottom up.[146] For nearly 50 years consumer law functioned as the spearhead of the modernization and transformation of private law relations, gradually affecting b2b relations. It seems as if the new private law in b2b the EU is promoting forcefully in EU digital policy legislation is now taking over the role of consumer law as the driver for change. One might even argue with Giovanni di Gregorio that *'business is the new consumer'*.[147] The DSA and the AIA establish a kind of superstructure, composed of meta-regulation and self-regulation.

Key elements of the new b2b private law are the going together of public and private regulation, the establishment of new modes of governance, the breaking up of traditional legal concepts and the deliberate bringing out of new legal figures. This is not the place to go into details. Building on established distinctions in governance one may distinguish between the institutional setting, the procedures of law/rulemaking and enforcement/compliance as well as the substance. All three forms of governance are most developed in the law of standards[148] and have now entered digital policy legislation. The EU legislature is taking a backstage role, it accepts and legitimises businesses as regulators of supply chains. The executive – the public supervisory authority which has to enforce the law – thereby turns into the supervisor of private regulation – both in the making of the rules and their private enforcement through

145 M. E. Kaminski, Regulating the Risks of AI (August 19, 2022). Forthcoming, Boston University Law Review, Vol. 103, 2023, U of Colorado Law Legal Studies Research Paper No. 22–21, Available at SSRN: https://ssrn.com/abstract=4195066 or http://dx.doi.org/10.2139/ssrn.4195066

146 H.-W. Micklitz, The European Transnational Private Law on Regulated Markets, in: A. Beckers/ H.-W. Micklitz/ R. Vallejo/ P. Letto-Vanamo (eds.), The Foundations of European Trans-national Private Law, Hart Publishing, forthcoming 2024.

147 Giovanni di Gregori from Nova Lisboa coined this term in an online lecture in November 2023, where the author was present.

148 H. Schepel The Constitution of Private Governance (Oxford: Hart Publishing, 2005), with a recent revival, O Kanevsk AIA-P, The Law and Practice of Global ICT Standardization, CUP 2023, M Gérardy, The 'Standards Effects': The Public Instrumentalisation of technical standards in EU law, PhD University of Luxemburg, 2023, R. Vallejo, The Private Administrative Law of Technical Standardization, Yearbook of European Law, Volume 40, 2021,172–229.

compliance and conformity assessments with the support of private third parties. This mechanism implies that the potential producers of laws/rules are extended that procedures have to be established in which the interaction between all the actors is organized and that substantive rules have to be generated matching the needs of the digitized supply chain economy.

Seen through the lenses of consumer advocacy the EU is about to develop a dense regulatory body which is not coordinated with the consumer law acquis and which therefore produces frictions. This new body of rules puts the EU consumer law acquis into a precarious situation – the meta-regulation reaches beyond the scope and reach of consumer law through the stretching of the scope *sedes personae* and the new modes of self-regulation – technical standards, codes of conduct or more broadly due diligence – tend to escape the regulatory grip of consumer law. Therefore consumer law and the consumer law acquis have to be re-thought at the two levels – the meta regulation and the self-regulation. So far consumer law is being understood as a task which should lie, and which lies in the hands of the public regulator alone, due to the full harmonization policy in those of the EU. Taking the co-regulatory approach seriously requires understanding private regulation as an integral part of consumer law, to accept that the new law in the age of digitization is not the product of state-made law alone but a co-product of public and private actors. The consequences are reaching far – consumers and consumer organisations or more broadly speaking civil society has to become the third actor in the production and the enforcement of (consumer) law. The consumer impact materializes at the level of self-regulation, the rules which are meant to concretise the meta-regulation. Here civil society has to operate on an equal footing with the EU and the businesses and their regulation to be able to provide input into the making of private regulation.

I have developed such a model as a revision of Reg. 1025/2012.[149] This regulation lays down the institutional and procedural framework for the development of European technical standards. The regulation could be understood as a blueprint for a mode of governance needed to react to the privatization of consumer law – provided it is completely overhauled in the spirit of a triangular relationship between the EU/Member States, business and civil society organisations. But this is not all, a similar exercise needs to be undertaken to break up the system of compliance and conformity assessment and to systematically integrate civil society. This strand of EU legislation is not yet in the limelight of consumer advocacy. Both the reconceptualisation of the law-rule-making procedure and the reconceptualisation of compliance and conformity given due regard to the interaction with public enforcement is the kind of long-term task that consumer policy and consumer advocacy face.[150] Otherwise, there is the risk that the consumer law acquis is gradually marginalized, except the two or three horizontal elements of the EU consumer law acquis – the Unfair Contract Terms Directive, the Unfair Commercial Practices Directive and the Consumer Data Protection Regulation[151] – the GDPR – as far as the new forms of governance – technical standards, codes of practices and due diligence are coming under their scope of application. The obvious gaps – the deficient judicial review of technical standards, codes of practices and due diligence obligations – cannot or hardly be closed through stretching concepts like 'standard terms' or 'commercial practices' or 'data privacy'. This is a good example for demonstrating the creativity of the EU legislation, now in

149 H.-W. Micklitz, The Role of Standards, loc. cit. pp. 172.

150 The parallel to the GDPR seems useful M. Pichlak, K. Gaczoł, Simple and advanced reflexivity in GDPR enforcement: empirical evidence from DPA activity International Data Privacy Law, ipad018, https://doi.org/10.1093/idpl/ipad018

151 F. Zuiderveen Borgesius, N. Helberger, A. Reyna, The perfect match? a closer look at the relationship between EU consumer law and data protection law, Common Market Law Review, Volume 54, 2017, pp. 1427–1465.

the field of B2B through laying down minimum standards for the elaboration of EU-promoted codes of practices.[152]

b) Short Term Recommendations

There is one single issue which stands out and requires utmost attention and a shorthand solution – this is access to the information which results from the implementation of the due diligence obligations through compliance and conformity assessment mechanisms. Without having access to this internally generated information, which is shared between private bodies, the auditing companies and/or the certification bodies and which is accessible even for public authorities only on request or even reasoned request, law enforcement through consumers and their organisations is doomed to fail. The key documents of interest are in the AIA the technical documentation, in the DSA the self-assessment reports and in the case of VLOPs and VLSEs those forwarded to the auditing bodies as well as the auditing reports. How to get access to these documents and if so under what conditions? How to balance out confidentiality trade secrets and the legitimate interests of private parties who are 'affected' or who are suffering from the 'interaction'?

The problem is not without precedence as it is inherent to due diligence. The most advanced discussions circulate Art. 22[153] on Corporate Sustainable Due Diligence focusing on civil liability.[154] Presumably, there is still a lot of political change to be made; the positions of the European Commission, the European Parliament and the Council are relatively far apart. Most of the academic discourse focuses on the Commission and the Proposal of February 2022, but it is also necessary to look at the EP's negotiating position of June 2023 and the Council's negotiating key points of November 2022.[155] The direction in the academic debate seems to be rather critical because Art. 22 is fault-based and also has to be incorporated into the different liability regimes of the member states. Seen through the lenses of this report, the discussion puts the cart before the horse. Litigants need to have access to the information that the potential defendant has on stock on what they have done to comply with the law.

The problem to be solved is not far away from the one discussed in Consumer Law 2.0., in the possible consequences to be drawn from digital vulnerabilities/digital asymmetries. The burden of proof has to be eased and transformed into a mechanism, where on reasoned request of the consumer and/or the consumer organisations the providers of AI systems or the providers of intermediary services have to gradually disclose the information needed to go to court and to have a realistic chance to provide evidence or the suggested infringement.[156]

---

152 See above 3 b) aa).

153 Proposal for a Directive on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937 COM/2022/71 final

154 See out of the blossoming literature A. M. Pacces, Civil Liability in the EU Corporate Sustainability Due Diligence Directive Proposal: A Law & Economics Analysis (March 16, 2023). European Corporate Governance Institute – Law Working Paper No. 691/2023, Amsterdam Law School Research Paper No. 2023-14, Amsterdam Center for Law & Economics Working Paper No. 2023-02, Forthcoming in Ondernemingsrecht (2023), Available at SSRN: https://ssrn.com/abstract=4391121 or http://dx.doi.org/10.2139/ssrn.4391121; S. Deva, Mandatory human rights due diligence laws in Europe: A mirage for rightsholders?, Leiden Journal of International Law (2023), 36, 389–414, doi:10.1017/S0922156522000802; K. Engsig Sørensen, 'Corporate Sustainability Due Diligence in Groups of Companies'. European Company Law Journal 19, no. 5 (2022): 119–130; C. Bright, A. Marx, N. Pineau and J. Wouters, "Towards a corporate duty for lead companies to respect human rights in their global value chains?". 22(4) Business and Politics (2020), 667–697.

155 https://commission.europa.eu/business-economy-euro/doing-business-eu/corporate-sustainability-due-diligence_en

156 See P. Rott, Burden of Proof in this Report.

V. Ensuring Digital Fairness in EU Consumer Law through Fundamental Rights: Is the EU Charter Fit for Purpose?

Betül Kas[1]

1 Visiting Fellow at the Private Law Department of Erasmus School of Law, Rotterdam, author of publications on the influence of EU fundamental rights on private law, EU civil justice and litigation. The Chapter to this report was concluded mid-October 2023.

1. Introduction

The references to fundamental rights are omnipresent in the EU digital policy legislation. The substantive protection offered by fundamental rights to consumers in the digital economy is however largely unexplored. This part assesses to what extent the protection of consumers in the digital sphere can be anchored in the EU Charter of Fundamental Rights and which consumer rights may thus enjoy constitutional standing in the EU legal order. Some explanations are required before embarking into an assessment of the actual and potential role of the fundamental rights set out in the EU Charter for ensuring digital fairness in EU consumer law.

The historical roots of the rhetoric that treats consumer rights as fundamental rights lies in the famous speech of President Kennedy in 1962, which focused on four consumer rights concerning safety, choice, information, and representation. In the EU this found its parallel at the Paris Summit of 1972, which launched a political commitment to construct more than mere economic integration on the foundation of the European Economic Community, and which resulted in a Council Resolution of 14 April 1975 on a preliminary programme for a consumer protection and information policy.[2] Point 3 of the Annex set out five basic consumer rights: (a) the right to protection of health and safety; (b) the right to protection of economic interests; (c) the right of redress; (d) the right to information and education; (e) the right of representation. While there was no explicit legislative competence in the field of consumer protection granted by the Treaty at that time, nowadays Article 169 Treaty on the Functioning of the European Union ('TFEU') provides for a legal basis, which is however of a more limited scope. Notably, the provision recognises the right to information. It remains however a subject of scholarly debate whether Article 169 TFEU can be treated as an individual legal basis for consumer claims and possesses direct (horizontal) effect.[3]

Article 38 of the EU Charter can be perceived as an important recognition of consumer rights and a signal that consumers are valued not only as market actors but also as human beings.[4] The provision does not however currently confer rights on individuals, nor does it extend the scope of the EU's legislative competence. The 'principle of consumer protection' in Article 38 enshrines currently merely a policy objective for Union policies.[5] Therefore, it remains vital to determine to what extent consumer rights can be realised through the application or interpretation of other individual fundamental rights contained in the Charter.[6] Specifically, the rights to human dignity (Article 1), personal integrity (Article 3), right to liberty (Article 6), respect for private life (Article 7), protection of personal data (Article 8), freedom of thought (Article 10), freedom to receive information (Article 11) and non-discrimination (Article 21) have been

2 Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy [1975] OJ C 92/1.

3 Affirming its nature as a subjective right with horizontal direct effect, Norbert Reich, Hans-Wolfgang Micklitz, Peter Rott and Klaus Tonner, *European Consumer Law* (2nd edn, Intersentia 2014), 22; denying this nature, Monika Jagielska and Mariusz Jagielski, 'Are consumer rights human rights?' in James Devenney and Mel Kenny, *European Consumer Protection. Theory and Practice* (Cambridge University Press 2012), 350; sceptical, Stephen Weatherill, 'Article 38' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Nomos, CH Beck, Hart Publishing 2021), 1068 ("It is fanciful to treat it as the basis for creating generally applicable and legally enforceable 'rights '.")

4 Iris Benöhr and Hans-Wolfgang Micklitz, 'Consumer protection and Human Rights' in Geraint Howells, Iain Ramsay and Thomas Wilhelmsson, *Handbook of Research on International Consumer Law* (Edward Elgar 2018), 22.

5 Benöhr and Micklitz, 'Consumer protection and Human Rights', 23–24; see also Weatherill, 'Article 38', 1076 ff.

6 Jagielska and Jagieslki, 'Are consumer rights human rights?', 352; see also Benöhr and Micklitz, 'Consumer protection and Human Rights', 18–20, who speak of "implicit consumer protection" by other fundamental/human rights.

chosen for a more detailed assessment as they may at least potentially unfold relevance in the area of consumer law. For the protection of vulnerable consumers, potential might also lie in using Article 38 EU Charter and/or the previously mentioned rights and freedoms in conjunction with the rights of the child (Article 24), of the elderly (Article 25) and of persons with disabilities (Article 26).

From a methodological perspective, it should be stressed that the assessment relies primarily on the case law of the Court of Justice of the European Union (hereafter 'CJEU'). The assessment is however at times hampered by the absence of sufficient case law by the CJEU. The case law of the European Court of Human Rights (ECtHR) may to some extent serve as an indication as to how the case law of the CJEU could develop in the future. According to Article 52(3) EU Charter, in so far as Charter rights correspond to rights guaranteed by the ECHR, the meaning and scope of those rights must be the same as those laid down by the Convention.[7] However, it is important to stress that the EU may provide for more extensive protection. In addition, the CJEU is not a human rights court, and the Charter protects rights or principles that are not contained in the ECHR (such as Articles 16 and 38 EU Charter), leading necessarily to different questions about the balancing of rights and interests.[8] Furthermore, the Charter's content is shaped and limited by existing secondary EU law. On the one hand, considering the extensive consumer law acquis, it is not inconceivable that the CJEU's interpretation of the Charter may give more room for the protection of consumers' economic interests than the ECHR. On the other hand, the Charter's protection may be more limited than the ECHR as it may not extend the scope of EU law beyond the competences of the EU (Article 51(2) of the Charter).

As a final point, it should not be forgotten that the sometimes rather broadly worded provisions of the EU Charter are subject to continuous judicial development by the CJEU. While scholarship can thus anticipate their adaptation to various phenomena in the quickly developing digital sphere, the case law is necessarily to some extent lagging behind. It is an instance of what Ackerman once strikingly described as judges sitting on the back of a train, looking backward from their caboose, and only seeing (technological) change after it occurred.[9] Therefore, it is necessary to carefully distinguish between developments suggested in scholarship and the status quo of the case law.

2. Article 38 EU Charter– Principle of Consumer Protection

The most straightforward provision of the Charter dealing with the protection of the consumer is Article 38 EU Charter. According to Article 38, "Union policies shall ensure a high level of consumer protection." 'Union policies' comprises policies adopted by the EU institutions. The Member States are addressed in so far as they are responsible for the implementation of those policies.[10] As described by Benöhr, the inclusion of consumer protection in the 'Solidarity'

7 The Explanations relating to the Charter of Fundamental Rights ([2007] OJ C 303/17) highlight these instances. According to Article 52(7) EU Charter, the explanations must be given due regard by the CJEU and the national courts.

8 Allan Rosas, 'The Court of Justice of the European Union: A Human Rights Institution?' (2022) 14 *Journal of Human Rights Practice* 204.

9 Bruce Ackerman, 'Constitutional politics/constitutional law' (1989) 99 *Yale Law Journal* 453, 546.

10 See Article 51(1) EU Charter.

chapter of the Charter was controversial. The initial draft Charter stated that EU policy should ensure a high level of protection on health, security, and consumer interests. In the following, various amendments were proposed, including the complete removal of consumer law from the Charter to the introduction of a subjective right for consumer protection. The final agreed version is a compromise.[11]

Although Article 38 EU Charter gives the appearance of a statement with significant constitutional weight, consumer protection is in fact already part of the constitutional order of the EU considering the provisions of the TFEU. As stated by the explanatory note to the Charter, "the principles set out in this Article have been based on Article 169 of the Treaty on the Functioning of the European Union."[12] Article 169(1) provides that "the Union shall contribute to protecting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests." An additional relevant provision is Article 12 TFEU, which requires that "consumer protection requirements shall be taken into account in defining and implementing other Union policies and activities." This cross-cutting provision requires that consumer protection is mainstreamed in the elaboration of all EU policies. Finally, Article 114 TFEU – the internal market legal basis – requires in its third paragraph adherence to a high level of consumer protection.

Considering that 'consumer protection' enjoys already constitutional standing in the TFEU, it is debated whether its inclusion in the Charter has brought about any significant changes. One crucial question is whether Article 38 Charter is merely of a programmatic character or may constitute a basis for creating generally applicable and legally enforceable rights. Article 52(5) of the Charter states that "the provisions of this Charter which contain principles may be implemented by legislative and executive acts (...) of the Union, and by acts of Member States when they are implementing Union law, in the exercise of their respective powers" and that they "shall be judicially cognisable only in the interpretation of such acts and in the ruling on their legality." The Agency of Fundamental Rights appears to take however the view that the Charter contains a right to consumer protection: "The Charter's supranational nature and its explicit wording make it an important tool for strategic litigation. The right to data protection, the right to consumer protection, and the right to a fair trial serve as examples."[13] So far, the CJEU has not taken a clear position on whether Article 38 EU Charter may constitute more than a principle.[14] While Advocate General Wahl in *Pohotovost' sro* advocated that Article 38 EU Charter has nothing to say about directly defined individual legal positions,[15] Advocate General Tanchev in *Walbusch Walter Busch* appears to have left it open whether the provision may confer subjective rights.[16]

Weatherill has examined the case law of the CJEU on Article 38 EU Charter and concludes that the provision reaffirms the existing normative structure by which consumer protection is considered in EU law, without having shown a transformative impact of its own on the outcome of particular debates or disputes. Advocate General Bobek stated in his Opinion in *TÜV Rheinland*

11 Iris Benöhr, *EU Consumer Law and Human Rights* (Oxford University Press 2013), 58.
12 Explanations relating to the Charter of Fundamental Rights, 28.
13 European Union Agency for Fundamental Rights, *Ten years on: unlocking the Charter's full potential* (2020), 14.
14 Weatherill, 'Article 38', 1076–1077.
15 Opinion of Advocate General Wahl delivered on 12 December 2013 in Case C-470/12 *Pohotovosť sro v Miroslav Vašuta* EU:C:2013:844, para 66.
16 Opinion of Advocate General Tanchev delivered on 20 September 2018 in Case C-430/17 *Walbusch Walter Busch GmbH & Co KG v Zentrale zur Bekämpfung unlauteren Wettbewerbs Frankfurt am Main eV* EU:C:2018:759, para 59.

that "Article 12 TFEU made consumer protection requirements transversally applicable, to be taken into account in defining and implementing other EU policies " and so "free movement must reflect and strive for a high level of consumer protection, as enshrined in Article 38 of the Charter."[17] Article 38 of the Charter did not however become the subject of express references in the CJEU's judgments in free movement cases. It appears that the Court considers its existing approach sufficient to take account of consume protection, which it has shown in such cases as *Buet*,[18] *Eyssen*[19] and *Citroën Belux*.[20] [21] In the legislative elaboration of EU consumer law, the Court' s reliance on Article 38 is seen as sporadic and merely confirming its longstanding approach of a consumer-friendly interpretation.[22] It seems that Article 38's added value is most pronounced where EU legislation is challenged for its interference with commercial freedom. Examples are the rulings in *McDonagh*[23] and *Airhelp*[24] concerning passenger rights. However, also in this respect, Weatherill concludes that this type of balancing is nothing new compared with the practice of the Court before the grant of binding status to the Charter and there is no routine invocation of Article 38 even where this is feasible.[25]

Finally, looking at EU legislative harmonisation and the role of Article 38 EU Charter therein, Weatherill concludes that the provision merely confirms the commitment to a high level of consumer protection in the setting of EU harmonised standards and "whether or not it is explicitly cited in the several legislative texts concerning the protection of the consumer does not appear to be of substantive significance."[26] The latter statement holds also truth for the proposal for an AI Act. The explanatory memorandum explains that the proposal will positively affect a high level of consumer protection as protected by the Charter.[27] As highlighted by BEUC: "Beyond the declarative non-binding layer in the recitals, consumer protection is lacking in the proposed AI Act. The proposal does not refer to protection of consumers from the adverse impact of AI among the legislative objectives of the AI Act. Consumers are not granted horizontal rights under the proposal and are excluded from the conceptual framework (...)."[28] In view of its vague wording, Article 38 EU Charter may not close this gap on its own.

---

17 Opinion of Advocate General Bobek delivered on 6 February 2020 in Case C-581/18 *RB v TÜV Rheinland LGA Products GmbH, Allianz IARD SA* EU:C:2020:77, para 106.

18 Case 382/87 *Buet and Others v Ministère public* EU:C:1989:198.

19 Case 53/80 *Officier van justitie v Koninklijke Kaasfabriek Eyssen BV* EU:C:1981:35.

20 Case C-265/12 *Citroën Belux NV v Federatie voor Verzekerings- en Financiële Tussenpersonen (FvF)* EU:C:2013:498.

21 Weatherill, 'Article 38', 1069–1072.

22 Ibid, 1079 ff.

23 Case C-12/11 *Denise McDonagh v Ryanair Ltd* EU:C:2013:43, para 60–63.

24 Case C-28/20 *Airhelp Ltd v Scandinavian Airlines System Denmark – Norway – Sweden* EU:C:2021:226, para 49.

25 Weatherill, 'Article 38', 1077–1079.

26 Ibid, 1074.

27 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, recital 28 ("The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. Those rights include the right to [...] consumer protection [...].")

28 BEUC, *Regulating AI to protect the consumer* (BEUC-X-2021-088, 7 October 2021), 3.

3. Article 3 EU Charter– Right to Integrity of the Person

Article 3 of the Charter enshrines the right to the integrity of the person. The first paragraph of the provision provides that "(e)veryone has the right to respect for his or her physical and mental integrity." While Article 3(1) is not related to a particular area of life, Article 3(2) concerns integrity in the fields of medicine and biology. It requires in particular (a) the free and informed consent of the person concerned; (b) the prohibition of eugenic practices; (c) the prohibition on making the human body a source of financial gain; (d) the prohibition of reproductive cloning. Under the ECHR, the right to physical and mental integrity is protected by Article 8(1) as part of the right to private life.[29]

It is recognised that the digital age poses new risks for the health and safety of consumers and changes the way that existing risks could materialise. The inherent characteristics of AI and of similar new technologies – such as autonomy, data dependency, connectivity, and opacity – have been found to negatively impact the safety of consumers.[30] An example is a product becoming dangerous by not possessing a sufficient level of cybersecurity, leaving it open to hacking by a malicious party. In the case of a passenger car, software security gaps exploited by a malicious party could cause a road accident. Similarly, a smartwatch for children can become a tool to have access to the location of the child and thus pose a risk to the child's personal security. In addition, there is evidence that new technologies can have an impact on the mental health of consumers. Connected products were related to depression, loss of sleep, altered brain function and myopia or early blindness in students and children.[31] Next to new technologies, also online sales channels were found to have created new challenges for the safety of consumers.[32] Article 3 of the Charter bears the potential of strengthening consumer safety by for instance conferring on consumers a right that AI-powered products do not harm their physical and mental integrity. While consumer safety would thus find a constitutional basis in the Charter, the case law of the CJEU does not currently provide a benchmark for 'physical and mental integrity'. The Court's case-law on Article 3 of the Charter is notably scarce.[33]

The ECtHR has not yet clearly sketched out its understanding of physical and mental integrity either.[34] Notably, it clarified in *Dordevic v Croatia* that the right to integrity not only encompasses a negative right to be free from interference, but also a positive duty to guarantee the individual's integrity in the form of providing protection from interferences by others.[35] It can be questioned whether threats to the individual stemming from digital surroundings can be equated to environmental issues. The ECtHR has decided that an individual's wellbeing may be negatively impacted by unsafe or disruptive environmental conditions.[36] However, an issue

29 *X and Y v the Netherlands* App no 8978/80 (ECHR, 26 March 1985), 22.
30 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final, 3–11.
31 Commission Staff Working Document, Impact Assessment, Accompanying the document, Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, SWD(2021) 168 final, 12, 13.
32 Ibid, 15–17.
33 Steve Peers, 'Article 3' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Nomos, CH Beck, Hart Publishing 2021).
34 Ibid, 45–46.
35 *Đorđević v Croatia* App no 41526/10, paras 141–143.
36 *Cordella and Others v Italy* App nos 54414/13 and 54264/15, paras 157–160.

under Article 8 only arises if individuals are directly and seriously affected by the nuisance in question and able to prove the direct impact on their quality of life.[37] Thus, the applicability of Article 8 has been determined by a severity test. As stated by the ECtHR: "The concept of threshold of severity has been specifically examined under Article 8. In environmental cases, in particular, an arguable claim under Article 8 may arise where an environmental hazard attains a level of severity resulting in significant impairment of the applicant's ability to enjoy his or her home or private or family life. The Court has ruled that the assessment of this minimum level in such cases is relative and depends on all the circumstances of the case, such as the intensity and duration of the nuisance and its physical or mental effects on the individual's health or quality of life."[38] [39]

Another interesting aspect is the need of free and informed consent by the person concerned. According to Article 3(2) EU Charter, this condition applies however only in the field of medicine and biology. The reference to 'informed' consent stems from Article 5 of the Oviedo Convention, which requires that a "person shall beforehand be given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks."[40] The adequacy of the provision of information and the use of traditional consent forms have become an issue in the context of nanomedicine and the uncertainties regarding the risks they pose. In its Opinion on the ethical aspects of nanomedicine, the European Group on Ethics in Science and New Technologies concluded in that respect that "attempts to provide adequate and understandable information and obtain consent ... cannot exclusively be met by informed consent forms signed by patients" and suggests that research is needed to develop improved methods of providing information and obtaining consent.[41] [42]

4. Article 6 EU Charter – Right to Liberty and Security

Article 6 EU Charter states that "(e)veryone has the right to liberty". In principle, the reference to 'liberty' could denote a broad concept of freedom that gives leeway to incorporate private autonomy and contractual freedom in the ambit of the provision. Personal autonomy plays a crucial role in consumer law. It enables consumers to make free choices. The digital sphere poses the question of how the consumer's own choices may be protected in a data-driven environment.[43] In the AI context, personal autonomy is understood as meaning "that humans interacting with AI systems must be able to keep full and effective self-determination over themselves" and prohibits that AI systems "unjustifiably subordinate, coerce, deceive, manipulate, condition or herd humans."[44]

---

37 *Çiçek and Others v Turkey* App no 44837/07, paras 32 and 22–29; *Fadeyeva v Russia* App no 55723/00, paras 68–69; *Chiş v Romania* App no 3360/03; *Thibaut v France* App nos 41892/19 and 41893/19.

38 *Denisov Ukraine* [GC] App no 76639/11, paras 111 ff.

39 See also the summary in Council of Europe/European Court of Human Right, *Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence* (2022) 46.

40 Peers, 'Article 3', 46–47.

41 European Group on Ethics in Science and New Technologies to the European Commission, Opinion on the ethical aspects of nanomedicine, Opinion no 21, 17 January 2007, paras 4.3.2 and 5.7.

42 Peers, 'Article 3', 48.

43 BEUC, *EU Consumer protection 2.0. Protecting fairness and consumer choice in a digital economy* (BEUC-X-2022-015, 10 February 2022), 2.

44 High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI* (2019), 12.

However, personal autonomy is not acknowledged as a self-standing fundamental right under the Charter.[45] The right to liberty in Article 6 EU Charter is merely understood as a right not to be subjected to arbitrary bodily restraint by for instance arrest or detention.[46] This reading is confirmed by the case law of the CJEU and complies with the wording and interpretation of the corresponding provision in Article 5 ECHR by the ECtHR.[47] Since Article 6 contemplates the physical liberty of the person, the provision is particularly relevant in the areas of criminal justice and immigration. The current restrictive meaning of the notion 'liberty' excludes any immediate potential for the anchoring of consumer rights in Article 6 EU Charter.

5. Article 7 and Article 8 EU Charter – Right to Respect of Private Life and Right to Protection of Personal Data

According to Article 7 EU Charter, "everyone has the right to respect for his or her private and family life, home and communications." The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR.[48] Prominently, the significance of the right to respect for one's home in Article 7 EU Charter for consumer disputes became evident in the aftermath of the *Aziz* case, in which the CJEU interpreted the Unfair Terms Directive 93/13 in order to improve the protection of particularly vulnerable consumers in the context of mortgage foreclosure and loss of the family home.[49] In *Kušionová*, the CJEU relied on two ECtHR's rulings[50] to give shape to the right to the home and emphasised with respect to Article 7 EU Charter "the consequences of the eviction of the consumer and his family from the accommodation forming their principal family home."[51]

When it comes to the protection of the private sphere and information technologies, Article 7 is mostly considered in conjunction with Article 8 of the Charter. Individually or in the aggregated collected data can reveal details about an individual's private life. Article 8 of the EU Charter sets out the right to the protection of personal data. There is no equivalent provision in the ECHR. Article 8(1) states that "everyone has the right to the protection of personal data concerning him or her." The second paragraph requires that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." In addition, "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." Paragraph 3 requires that "compliance with these rules shall be subject to control by an independent authority."

45 Differently to for example the German Basic Law, which enshrines the right to personal freedom in Article 2.
46 Daniel Wilsher, 'Article 6' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Nomos, CH Beck, Hart Publishing 2021), 126.
47 Explanations relating to the Charter of Fundamental Rights, 19; see also Council of Europe/European Court of Human Right, *Guide on Article 5 of the European Convention on Human Rights – Right to liberty and security* (2022).
48 Explanations relating to the Charter of Fundamental Rights, 20.
49 Case C-415/11 *Mohamed Aziz v Caixa d´ Estalvis de Catalunya, Tarragona i Manresa (Catalunyacaixa)* EU:C:2013:164, para 61.
50 *McCann v United Kingdom* App no 19009/04, para 50; *Rousk v Sweden* App no 27183/04, para 137.
51 Case C-34/13 *Monika Kušionová v SMART Capital, as* EU:C:2014:2189, para 66; see on this case law, Irina Domurath and Chantal Mak, 'Private Law and Housing Justice in Europe' (2020) 83 *Modern Law Review* 1188.

A decision that comingled Articles 7 and 8 EU Charter is for instance *TK v Asociatia de Proprietari bloc M5A-ScaraA*.[52] In that case, an individual challenged the legality of several video cameras set up in the common areas of the apartment building in which he owned a unit based on an interference with his private life. The cameras had been installed for the purpose of ensuring the safety of individuals and property and recorded all traffic within these areas without the consent of those recorded. The case was brought under the Data Protection Directive.[53] The CJEU found that the principles relating to data quality and the criteria for making data processing legitimate read in light of Articles 7 and 8 EU Charter did not preclude national law from authorising such a video surveillance system. The CJEU stressed the following three conditions: First, the data controller or the third party or parties to whom the data are disclosed must pursue a legitimate interest. The legitimate interests must be present and effective at the date of the data processing and must not be hypothetical at that date.[54] Second, derogations and limitations in relation to the protection of personal data must apply only insofar as is strictly necessary.[55] Third, the referring court must ensure that the fundamental rights and freedoms of the person affected do not take precedence over the legitimate interest pursued. Factoring in the seriousness of the infringement of the data subject's rights and freedoms, the referring court must assess whether the video surveillance system fulfilled the legitimate interests set out in the Data Protection Directive.[56]

Another example is *Google v Spain*, where the CJEU ruled that EU citizens have a right to request that commercial search firms, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant. The CJEU emphasised:

> *(P)rocessing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10 eDate Advertising and Others EU:C:2011:685, paragraph 45).*[57]

Importantly, establishing an interference with Article 7 does not require the individual to show the information on private life was sensitive or that individuals were inconvenienced.[58] Thus, the threshold for interference with Article 7 is not tied to incurring some form of harm. It is

52 Case C-708/18 *TK v Asociatia de Proprietari bloc M5A-ScaraA* EU:C:2019:1064.

53 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

54 Case C-708/18 *TK v Asociatia de Proprietari bloc M5A-ScaraA* EU:C:2019:1064, para 44.

55 Ibid, para 46.

56 Ibid, para 47.

57 Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317, para 80. The follow-up ruling in Case C-507/17 *Google LLC v CNIL* EU:C:2019:772 concerned the territorial scope of the right to be forgotten.

58 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238, para 33.

sufficient that an interference is demonstrated.[59] This aspect facilitates consumers' actions against excessive collection of personal data.[60]

It should be stressed that an individual consumer may also become a data processor as shown by *Ryneš*, where an individual committed a number of offences in relation to the protection of personal data by installing a surveillance camera under the eaves of his house which recorded not only his own home but also the public footpath and the house opposite. The Court found that the camera usage at stake fell outside of the scope of the exemption for domestic purposes of the Data Protection Directive because it covered a public space and is accordingly directed outwards from the private setting of the person processing the data. The narrow construction of the domestic purposes exemption was prompted by the activity being liable to infringe upon fundamental freedoms, in particular the right to privacy.[61]

6. Article 10 EU Charter – Freedom of Thought, Conscience and Religion

Article 10(1) EU Charter states that "everyone has the right to freedom of thought, conscience and religion", which "includes freedom to change religion or belief and freedom, either alone or in community with others and in public or in private, to manifest religion or belief, in worship, teaching, practice and observance." As stated in the explanatory note, this right corresponds to the right guaranteed in Article 9 of the ECHR and, in accordance with Article 52(3) of the Charter, has the same meaning and scope.[62]

Article 10's potential relevance for consumers may in principle lie in a 'right not to be manipulated'[63] that could derive from the right to freedom of thought. To determine the viability of this construction, it is necessary to examine the present scope of Article 10 EU Charter.

a) To assess the viability of anchoring consumer rights in Article 10, it is essential to determine first the scope of the beliefs or viewpoints that are covered by the provision. The wording of Article 10 makes clear that the provision applies to thought, conscience and religion. Non-religious beliefs are therefore also covered.[64] The CJEU has not yet clarified which non-religious beliefs or viewpoints Article 10 protects.[65] The organs of the Convention have recognised philosophical

59 David Mangan, 'Article 7' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Nomos, CH Beck, Hart Publishing 2021), 185.

60 On the interplay of data protection law and consumer protection law, see Frederik Zuiderveen Borgesius, Natali Helberger, Agustin Reyna, 'The perfect match? A closer look at the relationship between EU consumer law and data protection law' (2017) 54 *Common Market Law Review* 1427.

61 Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* EU:C:2014:2428, para 29.

62 Explanations relating to the Charter of Fundamental Rights, 21.

63 Cass R Sunstein, 'Manipulation as theft' (2022) 29 *Journal of European Public Policy* 1959.

64 Ronan McCrea, 'Article 10' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Nomos, CH Beck, Hart Publishing 2021), 315, 325.

65 McCrea notes that the CJEU has recognised a broad definition of religion in the Directive regulating asylum (Joined Cases C-71/11 and C-99/11 *Bundesrepublik Deutschland v Y and Z* EU:C:2012:518) and showed a commitment of treating expressions of religious and non-religious belief equally in discrimination cases (Cases C-157/15 *Samira Achbita and Centrum voor gelijkheid van kansen en voor racismebestrijding v G4S Secure Solutions NV* EU:C:2017:203, C-188/15 *Asma Bougnaoui and Association de défense des droits de l'homme (ADDH) v Micropole SA* EU:C:2017:204), see McCrea, 'Article 10', 325.

convictions such as pacifism,[66] principled opposition to military service,[67] veganism and opposition to the manipulation of products of animal origin or tested on animals,[68] opposition to abortion,[69] a doctor's opinions on alternative medicine,[70] the conviction that marriage is a lifelong union between a man and a woman,[71] and attachment to secularism.[72] According to the ECtHR, in order for a personal or collective conviction to benefit from the protection under Article 9 ECHR, it must attain a certain level of cogency, seriousness, cohesion and importance.[73]

b) The second step of the assessment requires determining whether the right to freedom of thought, conscience and religion contains a 'right not to be subjected to manipulation'. According to the case law of the ECtHR, Article 9 ECHR contains two rights, namely the right to hold a belief and the right to manifest that belief.[74] In our context, the interference with the right to hold a belief through for instance dictating what a person believes or taking coercive steps to make him change his beliefs is most relevant.[75] In *Mockutė v Lithuania*,[76] the ECtHR had to deal with the question whether the exertion of psychological pressure on a vulnerable person to abandon her beliefs could constitute a violation of the freedom of thought, conscience and religion. The Court confirmed an infringement of Article 9 in the case of a woman who practised meditation in the Osho religious movement, and who had been forcibly admitted to psychiatric hospital, diagnosed with acute psychosis and kept in hospital for 52 days, during which time the doctors attempted to "correct" her beliefs by disparaging them and encouraging her to "adopt a critical attitude" to meditation and the Osho movement. The Court emphasised in its ruling the applicant's position of inferiority, vulnerability and powerlessness vis-à-vis the medical staff who were responsible for both her diagnosis and her continued confinement in the hospital. Another possible relevant area that could be loosely related to the subject of 'manipulation' concerns the case law of the ECtHR on pejorative expressions against religious communities in official documents, which may amount to interference with the rights secured under Article 9.[77]

This two-step assessment leads to the conclusion that Article 10 EU Charter provides very limited scope for the translation of consumer rights into the fundamental right to freedom of thought. It is rather unlikely that the CJEU will interpret the term 'thought' in such broad terms that a consumer will be protected against all kind of manipulations in the digital sphere. The benchmark for non-religious beliefs to come within the protective scope of Article 10 EU Charter is high. This is also reasonable considering that non-religious beliefs falling within the scope of Article 10 will be granted the same standard of protection as religious beliefs. The ECtHR's case law provides limited guidance on a possible interference with Article 10 EU Charter by some kind of manipulation of one's beliefs. It is therefore difficult to predict to what

66 *Arrowsmith v the United Kingdom* App no 7050/75, Report of the European Commission of Human Rights adopted on 12 October 1978, para 69.
67 *Bayatyan v Armenia* [GC] App no 23459/03.
68 *W v the United Kingdom* App No 18187/91, Decision of the European Commission of Human Rights of 10 February 1993.
69 *Knudsen v Norway* App no 11045/84, Decision of the European Commission of Human Rights of 8 March 1985; *Van Schijndel and Others v the Netherlands* App no 30936/96, Decision of the European Commission of Human Rights of 10 September 1997.
70 *Nyyssönen v Finland* App no 30406/96, Decision of the European Commission of Human Rights of 15 January 1998.
71 *Eweida and Others v the United Kingdom* App nos 48420/10, 36516/10, 51671/10 et al.
72 *Lautsi and Others v Italy* [GC] App no 30814/06, para 58; *Hamidović v Bosnia and Herzegovina* App no 57792/15, para 35.
73 *Campbell and Cosans v United Kingdom* App nos 7511/76, 7743/76, para 36.
74 McCrea, 'Article 10', 326; Council of Europe/European Court of Human Right, *Guide on Article 9 of the European Convention on Human Rights – Freedom of thought, conscience and religion* (2022), 12.
75 *Ivanova v Bulgaria* App no 52435/99, para 79.
76 *Mockutė v Lithuania* App no 66490/09, paras 123–125.
77 *Leela Förderkreis eV and Others v Germany* App no 58911/00, para 84; *Centre of Societies for Krishna Consciousness in Russia and Frolov v Russia* App no 37477/11, para 38.

extent the CJEU might interpret the right to freedom of thought, conscience and religion as containing a 'right not to have one's beliefs manipulated'.

7. Article 11 EU Charter – Freedom of Expression and Information

According to Article 11(1) EU Charter, "everyone has the right to freedom of expression", which "include(s) freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." The second paragraph of Article 11 EU Charter requires respect for the freedom and pluralism of the media. Article 11 corresponds to Article 10 of the ECHR.[78]

From the perspective of the consumer, it is pertinent that Article 11 sets out a right to receive information. The question that needs to be assessed is to what extent the right to receive information is suitable for providing an anchor for consumer rights in the Charter and whether any requirements on the quality of the information can be derived from the provision. When it comes to AI, the right to information can be linked to the principles of explicability and the notion of explainability. The High Level Expert Group on Artificial Intelligence explains the principle of explicability in the following way:

> *Explicability is crucial for building and maintaining users' trust in AI systems. This means that processes need to be transparent, the capabilities and purpose of AI systems openly communicated, and decisions – to the extent possible – explainable to those directly and indirectly affected. Without such information, a decision cannot be duly contested. An explanation as to why a model has generated a particular output or decision (and what combination of input factors contributed to that) is not always possible. These cases are referred to as 'black box' algorithms and require special attention. In those circumstances, other explicability measures (e.g. traceability, auditability and transparent communication on system capabilities) may be required, provided that the system as a whole respects fundamental rights. The degree to which explicability is needed is highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate.*[79]

'Explainability' means the following:

> *Explainability concerns the ability to explain both the technical processes of an AI system and the related human decisions (e.g. application areas of a system). Technical explainability requires that the decisions made by an AI system can be understood and traced by human beings. Moreover, trade-offs might have to be made between enhancing a system's explainability (which may reduce its accuracy) or increasing its accuracy (at the cost of explainability). Whenever an AI system has a significant impact on people's lives, it should be possible to demand a suitable explanation of the AI system's decision-making process. Such explanation should be timely and adapted to the expertise of the stakeholder concerned (e.g. layperson, regulator or researcher). In addition, explanations of the degree to which an AI system influences and shapes the organisational*

78 Explanations relating to the Charter of Fundamental Rights, 21.

79 High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI* (2019), 13.

decision-making process, design choices of the system, and the rationale for deploying it, should be available (hence ensuring business model transparency).[80]

'The right to receive information' under Article 10 ECHR has been discussed in the case law of the ECtHR with respect to access to information held by public authorities. The Court ruled that Article 10 does not confer on the individual a right of access to information held by a public authority nor oblige the Government to impart such information to the individual.[81] However, such a right or obligation may arise, firstly, where disclosure of the information has been imposed by a judicial order which has gained legal force and, secondly, in circumstances where access to the information is instrumental for the individual's exercise of his or her right to freedom of expression.[82] The Court has further specified that the right to receive information is not only implicated where access to information is denied, but also where, whilst being under a statutory obligation to provide information, the relevant public authority provides information that is disingenuous, inaccurate or insufficient.[83]

The ECtHR has thus linked the right to access information to its importance for the exercise of speech rights. This link with the exercise of speech rights is reflected in the cumulative assessment criteria for accessing State-held information established by the Court.[84] Firstly, the purpose of the information request must be examined. The purpose of the person in requesting access to the information held by a public authority must be to enable his or her exercise of the freedom to receive and impart information and ideas to others. Thus, access to the information sought must be an essential element of the exercise of freedom of expression. Secondly, the nature of the information sought is relevant. It must meet a public-interest test to prompt a need for disclosure under the Convention. Thirdly, the role of the seeker of the information in 'receiving and imparting' it to the public assumes special importance. The Court has recognised that this role is or may be played by journalists, NGOs, academic researchers, authors of literature, bloggers and popular users of the social media. It is essential that the person requesting the information would contribute to enhancing the public's access to the requested information and facilitating its dissemination. Finally, the Court considers that the fact that the information requested is ready and available ought to constitute an important criterion in the overall assessment of whether a refusal to provide the information can be regarded as an 'interference' with the freedom to 'receive and impart information' as protected by that provision.[85]

The close connection between the freedom of expression and the freedom to receive information (see also the wording of Article 11(1) referring to the latter as being 'included' by the former) complicates the applicability to the individual consumer, whose interest in information is presumably rather of a private instead of a public nature. In addition, in the consumer context, the right to receive information is rather constructed as a positive obligation on traders to provide consumers with certain prescribed information. With respect to Article 10 ECHR, the ECtHR clarified however that "the right to receive information cannot be construed

80 Ibid, 18.
81 Sarah Eskens, Natali Helberger and Judith Moeller, 'Challenged by news personalisation: five perspectives on the right to receive information' (2017) 9 *Journal of Media Law* 259, 263.
82 *Magyar Helsinki Bizottság v Hungary* [GC] App no 18030/11.
83 *Association BURESTOP 55 and Others v France* App nos 56176/18, 56189/18, 56232/18, 56236/18, 56241/18, 56247/18, paras 85 and 108.
84 *Magyar Helsinki Bizottság v Hungary* [GC] App no 18030/11.
85 Council of Europe/European Court of Human Right, *Guide on Article 9 of the European Convention on Human Rights – Freedom of thought, conscience and religion* (2022), 75–79.

as imposing on a State positive obligations to collect and disseminate information of its own motion",[86] thus requiring the information seeker to become active by making a request.

The CJEU has no established line of case law on the right to receive information. In *Sky Österreich*, the Court recognized that the freedom to receive information is a component of Article 11 EU Charter. However, also in this context, the *public interest* in the dissemination of information on certain events has been a crucial aspect of the ruling, as well safeguarding the freedom and pluralism of the media.[87] A report on the implications of AI-driven tools in the media for freedom of expression notes that one important implication of the use of AI-driven tools is that news users can be targeted in terms of precise groups, or even on an individual level, which can affect the exercise of an individual's right to receive information based on personal characteristics and preferences. This may lead to a situation in which certain parts of the population or users with particular characteristics are structurally excluded from accessing information. On the other hand, from a more positive perspective, the ability to design media products that are more interactive and more responsive to individual users' information needs can potentially open up new opportunities for users to exercise their right to receive information. Such efforts may be required in some circumstances to ensure that the Article 10 ECHR rights of users are adequately protected.[88]

While current case law provides no indication on the viability of anchoring the consumer's right to information in Article 11 EU Charter, the CJEU held that the freedom of expression applies – in line with the interpretation of the ECtHR of Article 10 ECHR[89] – to the circulation by an entrepreneur of commercial information in particular in the form of advertising.[90] This is reflected in *Walter Walbusch*, where the Court observed with respect to the information obligations under the Consumer Rights Directive:

> *The obligation to provide information set out in Article 8(1) and (4) of Directive 2011/83 means that the consumer receives, in an appropriate way, before the distance contract is concluded, the information needed to enable him to decide whether or not to conclude the contract, thereby meeting the legitimate objective in the public interest of consumer protection, in accordance with Article 169 TFEU, recalled in recital 3 of that directive, without, however, affecting the essence of the entrepreneur's freedom of expression and information, or its freedom to conduct a business, as enshrined in Articles 11 and 16 of the Charter.*[91]

86 *Magyar Helsinki Bizottság v. Hungary* [GC] App no 18030/11.

87 Case C283/11 *Sky Österreich GmbH v Österreichischer Rundfunk* EU:C:2013:28, paras 51, 52.

88 Natali Helberger, Sarah Eskens, Max van Drunen, Mariella Bastian and Judith Moeller, *Implications of AI-driven tools in the media for freedom of expression* (Council of Europe, Artificial Intelligence – Intelligent Politics Challenges and opportunities for media and democracy, Background Paper, Ministerial Conference, Cyprus 2020), 22, 23.

89 *Casado Coca v Spain* App no 15450/89, paras 35 and 36; *Krone Verlag GmbH & Co KG (No 3) v Austria* App no 39069/97, paras 19 and 20.

90 Case C-157/14 *Société Neptune Distribution v Ministre de l'Économie et des Finances* EU:C:2015:823, paras 64, 65; Case C-547/14 *Philip Morris Brands SARL and Others v Secretary of State for Health* EU:C:2016:325, para 147.

91 Case C-430/17 *Walbusch Walter Busch GmbH & Co KG v Zentrale zur Bekämpfung unlauteren Wettbewerbs Frankfurt am Main eV* EU:C:2019:47, para 42.

8. Article 21 EU Charter – Right to Non-Discrimination

Article 21 of the Charter safeguards the fundamental right to non-discrimination. It encompasses two paragraphs: Article 21(1), which is modelled on Article 14 of the ECHR, prohibits "any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation." Article 21(2) states that "within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited."

Considering the scope of the Charter as set out in Article 51(1), the prohibition of discrimination applies to EU institutions and bodies and the Member States when they are implementing Union law. The EU has therefore a comprehensive obligation to refrain from any form of discrimination based on all grounds listed in Article 21. The obligations of the Member States are however more limited: Article 21 applies when there is a 'direct link' with EU law.[92] The EU's four anti-discrimination directives (Directives 2000/43/EC,[93] 2000/78/EC, 2004/113/EC[94] and 2006/54/EC[95]) prohibit discrimination on grounds of race or ethnic origin, sexual orientation, disability, religion or belief, age and sex or gender. Article 21 of the Charter applies within the specific framework defined by these directives. The CJEU has repeatedly underlined that the directives constitute an expression, in the areas that they cover, of the general prohibition of discrimination laid down in 21 Article of the Charter.[96] Even though the Directives cannot, in principle, apply directly to private parties, the CJEU has recognised horizontal direct effects to Article 21(1) of the Charter.[97]

Looking at the EU anti-discrimination legislation, non-discriminatory access to the consumer market (specifically 'access to goods and services, which are available to the public') is only safeguarded when it comes to race or ethnic origin[98] and gender.[99] A proposal for a new anti-discrimination directive that would extend Directive 2000/78 covering sexual orientation, disability, religion or belief and age to access to goods and services which are available to the public, including housing, has been pending since 2008.[100] The case law on the intersection between anti-discrimination and consumer law is rare. A prominent example is *CHEZ* dealing in broad terms with the supply of electricity and, specifically, with the right of consumers to control their electricity consumption. The ruling of the CJEU clarified that not only the provision of the service per se is covered by 'access', but also the general conditions under which a

92 Case C-617/10 *Åklagaren v Hans Åkerberg Fransson* EU:C:2013:105, para 26.
93 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L 180/22.
94 Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation [2000] OJ L 303/16.
95 Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) [2016] OJ L 204/23.
96 See, for instance, Case C-83/14 *"CHEZ Razpredelenie Bulgaria" AD v Komisia za zashtita ot diskriminatsia* EU:C:2015:480, para 58 with further references to the case law.
97 Case C-414/16 *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV* EU:C:2018:257, para 81.
98 Article 3(1)(h) of Directive 2000/43/EC.
99 Article 3(1) of Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L 373/37.
100 COM (2008) 426 final.

service is supplied.[101] In line with that, also pricing is subject to the duty of non-discrimination. In *Test-Achats*, the CJEU made clear that insurers may not use gender as a proxy (an actuarial factor) to calculate risks and thus estimate premiums in the absence of granular information about individuals.[102]

What does this mean for algorithmic stereotyping in advertising or algorithmic price discrimination? Xenidis and Senden argue that the protective scope of EU non-discrimination law is limited. Advertising is excluded from the scope of Directive 2004/113/EC according to its Article 3(3), thus allowing for gender-targeting advertisements. The Race Equality Directive remains silent on this matter and may thus potentially prohibit race-based discriminatory advertising for goods and services in the EU. When it comes to the employment sphere, the CJEU has indeed interpreted the notion of "conditions for access to employment" to encompass recruitment advertising (Case C-54/07, Feryn EU:C:2008:155). As shown, other grounds are however not protected at all in the ambit of the consumption market.[103] In addition, it has been questioned whether highly personalized goods or services may fall at all under the definition of 'goods and services which are *available to the public*'.[104]

9. Article 1 EU Charter – Human Dignity

Article 1 of the EU Charter states that "(h)uman dignity is inviolable" and that "it must be respected and protected". As clarified by the explanatory note to the Charter, "the dignity of the human person is not only a fundamental right in itself but constitutes the real basis of fundamental rights." Dignity is considered as one of the most difficult concepts to fathom in law.[105] It has been related to such notions as "(self-)respect, autonomy, privacy, integrity and self-determination."[106]

Although 'human dignity' remains conceptually open, it has been put forth as a key foundational value to guide the governance of new technologies. There is a strong concern that new technologies such as AI may compromise core values of being human. According to the European Data Protection Supervisor, dignity could be the counterweight to the pervasive surveillance and asymmetry of powers which confronts the individual in the digital sphere and should be thus at the centre of digital ethics.[107] The Fundamental Rights Agency states that: "AI-driven processing of personal data must be carried out in a manner that respects human dignity. This puts the human at the centre of all discussions and actions related to AI. Rather than the technology, the 'human being' creating and affected by the new technology needs

101 Case C-83/14 *"CHEZ Razpredelenie Bulgaria" AD v Komisia za zashtita ot diskriminatsia* EU:C:2015:480, para 43.
102 Case C-236/09 *Association Belge des Consommateurs Test-Achats ASBL and Others v Conseil des ministers* EU:C:2011:100.
103 Raphaële Xenidis and Linda Senden, 'EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination' in Ulf Bernitz et al (eds), *General Principles of EU law and the EU Digital Order* (Kluwer Law International, 2020).
104 Philipp Hacker, 'Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law' (2018) 55 *Common Market Law Review* 1143.
105 Opinion of Advocate General Stix-Hackl delivered on 18 March 2004 in Case C-36/02 *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn* EU:C:2004:162, para 74.
106 Catherine Dupré, 'Article 1' in Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights. A Commentary* (2nd edn, Nomos, CH Beck, Hart Publishing 2021), 16–17.
107 European Data Protection Supervisor, *Towards a New Digital Ethics* (Opinion 4/2015), 12.

to be the focus."[108] The High-Level Expert group on AI reflects the need for respect of human dignity in its call for 'human-centric AI'. This approach "strives to ensure that human values are central to the way in which AI systems are developed, deployed, used and monitored, by ensuring respect for fundamental rights, including those set out in the Treaties of the European Union and Charter of Fundamental Rights of the European Union, all of which are united by reference to a common foundation rooted in respect for human dignity, in which the human being enjoy a unique and inalienable moral status."[109] In concrete terms, 'human-centric AI' includes 'human agency' and 'human oversight'. The former requires that users should be able to make informed autonomous decisions regarding AI systems.[110] The latter should ensure that an AI system does not undermine human autonomy through oversight by governance mechanisms such as human-in-the-loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC) approaches.[111]

Sue Anne Teo notes that when it comes to the relationship between AI and human rights, human dignity is used loosely as a placeholder expression or ideas that cluster around human autonomy and agency, including the need for human control over the development and deployment of new technologies.[112] Sue Anne Teo has identified four main ways in which human dignity has been substantively fleshed out in case-law and treaty interpretations:

First, inspired by the philosophy of Immanuel Kant, human dignity has been interpreted as the non-instrumentalisation of the human being. It stresses "the capacity for autonomy of the human agent which can only be displaced, if at all, through an exercise of these very autonomous capacities themselves, for example through individual consent."[113] The non-instrumentalisation conception was the dominant position assumed in the German Peep-Show case[114] and the German Airliner case.[115]

The second conception of human dignity focuses upon protecting classes of persons which the law deems to be vulnerable and hence as deserving of heightened degrees of protection. An example is the 'dwarf throwing' case in France where the Conseil d'Etat held that banning dwarf throwing activities in a local discotheque was done to respect public order which in turn consists of the respect for human dignity. Notably, the plaintiff in the dwarf-throwing

---

108 European Union Agency for Fundamental Rights, *Getting the Future Right – Artificial Intelligence and Fundamental Rights* (2020), 60.

109 High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI* (2019) 37.

110 Ibid, 16.

111 Ibid ("HITL refers to the capability for human intervention in every decision cycle of the system, which in many cases is neither possible nor desirable. HOTL refers to the capability for human intervention during the design cycle of the system and monitoring the system's operation. HIC refers to the capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the system in any particular situation. This can include the decision not to use an AI system in a particular situation, to establish levels of human discretion during the use of the system, or to ensure the ability to override a decision made by a system.").

112 Sue Anne Teo, 'Human dignity and AI: mapping the contours and utility of human dignity in addressing challenges presented by AI' (2023) *AI, Law, Innovation and Technology* 244; see also Lucia Vesnic-Alujevic, Susana Nascimento, Alexandre Poolvora, 'Societal and ethical impacts of artificial intelligence: Critical notes on European policy frameworks' (2019) *Telecommunications Policy* 6.

113 Sue Anne Teo, 'Human dignity and AI', 246.

114 'Peep-Show' Case, BVerwGE 64, 274 of 15 Dec 1981.

115 Aviation Security Act Case, BVerfG, 1 BvR 357/05 of 15 Feb 2006.

cases claimed that it was this dwarf-throwing work that brought him dignity, in that it would be undignified of him to be without work.[116]

The third conception of human dignity stresses the expression and recognition of individual self-worth. According to that conception, "the individual has inherent worth in her (human) existence, one that is independent of class, social standing, financial status, age or other contingent qualities."[117]

The final conception is the protection of humanity as a species concern, premised upon the idea of human exceptionalism. It recognises the uniqueness of human beings and that it is this unique status that justifies its protection. For instance, the CJEU in *The Netherlands v The European Parliament* has confirmed the need to preserve the uniqueness of humankind by prohibiting patenting rights over human genetic modifications and other biotechnological modifications.[118] This conception of human dignity may further the need for alignment of AI with human values and human involvement and control in AI.[119]

10. Conclusions

Taking stock of the Charter rights that may unfold relevance for the area of consumer law and looking at the wording of the provisions has shown that the Charter provides considerable potential for translating consumer rights into fundamental rights and for countering harms and injustices that manifest in the digital sphere. However, the potential of the Charter still needs to be realised in practice. The Charter is a 'living instrument' whose relevance for the digital transformation will depend on its future interpretation by the CJEU. For now, the case-law on the Charter is insufficient to provide a clear indication on the substantive level of protection offered by Charter rights to consumers in the digital economy. Judicial law-making requires time and – in the meantime – rears legal uncertainty. Considering the current stage of judicial development, it is uncertain to what extent the reliance on fundamental rights may compensate for the absence of well-defined consumer rights and substantive standards of protection in secondary EU law. It is important to underline that this conclusion does not render current efforts to prevent and mitigate negative impacts on fundamental rights through requiring impact assessments futile. With many policymakers, academics, national and international organizations and advocacy organizations endorsing the significance of fundamental rights impact assessments where AI systems are developed and deployed, future efforts will have to move towards an inclusive and transparent standard setting process.

---

116 Sue Anne Teo, 'Human dignity and AI', 248.
117 Ibid, 249.
118 Case C-377/98 *Netherlands v Parliament and Council* EU:C:2001:523; see Sue Anne Teo, 'Human dignity and AI', 251–254.
119 Ibid, 256.

VI. Future-Proofing the Unfairness Test[1]

Monika Namysłowska

1 The research leading to this Chapter was partly supported by the National Science Centre (*Narodowe Centrum Nauki*) in Poland based on decision No. 2018/31/B/HS5/01169.

I. At the outset: Conclusions

1. Exploring the unfairness test in the digital age

This Chapter **addresses a gap** in the research shared in the 'EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets' (hereinafter: 'EU Consumer Protection 2.0')[2] report commissioned by BEUC. This study introduced fundamental concepts to contemporary consumer law discussions: digital asymmetry and digital vulnerability. Insights presented in the report influenced legal debates and literature, serving as cornerstones for the present analysis. However, some key areas went unexplored due to the report's focus on structural asymmetries in digital consumer markets. Recognising the importance of these areas for consumer protection in the digital realm, this study delved into them.

The research presented in this Chapter examined the two components of the current unfairness test in Article 5(2) UCPD: the **concept of professional diligence** (Section II) and **consumer harm** (Section III). Previous research studies, literature, and numerous behavioural studies commissioned by the European Commission[3] confirm the unique characteristics of commercial practices in the digital environment. This analysis adopted the findings of these studies, assuming that complex algorithmic and data-driven business models and commercial practices influence consumer autonomous decision-making on an unprecedented scale. The detrimental effects of digital commercial practices were confirmed in the latest Consumer survey conducted by BEUC: only 43% of respondents reported feeling in full control of their online decisions. Almost half of respondents (46%) believed that a company violated their consumer rights[4]. This result is alarming when considering that many consumers are unaware of the influence exerted on them. Therefore, the concepts of professional diligence and protected consumer interests must also be examined in the new digital realm. Based on the hypothesis that the general clause does not sufficiently address consumer risks in the digital environment, the research question was whether Article 5(2) UCPD should transform, and if so, to what extent.

The research sought to enhance the comprehension of professional diligence and consumer harm facing the digital revolution and offer new insights in light of its evolving dimensions. The core of the analysis rested primarily on the framework provided by **the UCPD**, where the unfairness test is enshrined. However, the study also examined other traditional consumer pieces of legislation and recent legal developments within the **EU digital policy legislation**. This approach ensured a complex assessment of the current unfairness test.

2. From the new general clause to the horizontal safety net

Since Article 5(2) is already referred to as a 'safety net',[5] drawing from insights of the concepts of professional diligence and consumer harm, this Chapter also delved into the potential of crafting within consumer law a holistic protective mechanism against unfair digital commercial practices. The '**horizontal safety net**' is envisioned to counteract the fragmentation of consumer protection in EU digital policy regulations. Its objective is to encompass and pre-emptively

2 Helberger et al., 2021.
3 Mocanu and Sibony, 2023, footnote 32.
4 BEUC, 2023c, pp. 4, 8–9.
5 Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021/C 526/01), 2021, p. 8.

address a range of risks that may be overlooked or insufficiently tackled in other legislative frameworks. This approach aimed to provide a tight shield for consumers, ensuring that no consumer thread in the digital era remains outside the purview of consumer law, no matter how novel or unforeseen.

This part of the research, contained in Section IV, addressed the questions posed at the end of 'The Regulatory Gap: Consumer Protection in the Digital Economy' (hereinafter: 'The Regulatory Gap')[6] report, also commissioned by BEUC, regarding whether closing the regulatory gap requires **upgrading EU digital policy legislation** or **consumer *acquis***.

3. Dual-faceted research outcomes

The research outcomes in Section V can be divided into **two phases**. Following the initial and main phase of conceptualising the 'digital unfairness' paradigm, the concept of 'digital fairness' was subsequently introduced. Both paths highlight the urgent need for legislation that addresses the unique challenges present in the digital space as opposed to offline transactions.

3.1 Addressing digital unfairness & introducing new concepts

In the initial stage, addressing digital unfairness centred around introducing a novel concept: '**digital professional diligence**.' Accommodating digital unfairness within a new general clause via digital professional diligence required a recalibration of the scope of consumer interests protected under the UCPD. Additionally, accompanying measures essential for operationalising the new general clause were emphasised, including the need to define unfair commercial practices, introduce a general prohibition of unfair commercial practices, and complement the general clause with other legislative tools, notably an extended black list.

These considerations led to **conceptualising a horizontal safety net**, linking various laws protecting consumers against unfair digital commercial practices. The horizontal safety net is manifested in the new general clause. The general clause may also be based on the 'breach of law' concept inspired by German and Polish legislation. With the simultaneous adoption of a general prohibition against unfair digital commercial practices into the UCPD, consumer law will be better positioned against digital unfairness. This holistic approach fills the existing regulatory gap and offers the prospect of more frequent deployment of the general clause as a self-standing test. With this framework in place, the UCPD has the potential to effectively bridge the regulatory gap, serving as a fundamental building block for regulating the digital economy and digital society.[7]

3.2 Crafting digital fairness & proactive paradigm shift

The second phase highlighted the need to craft the **digital fairness** paradigm. This concept may evolve into '**digital fairness by design**' – a proactive approach that encourages the integration of the fairness principle right from the outset. Rather than waiting for issues of digital unfairness to arise and addressing them ex-post, this approach urges businesses to incorporate fairness

6 See Helberger et al., 2021.
7 See Scheuerer, 2021, p. 845.

considerations from the inception of their digital projects. The emphasis moves from merely responding to issues as they emerge to preventing potential unfairness through thoughtful and anticipatory design choices. This stage recognises the transformative potential of a shift in mindset.

3.3 The twin pillars of digital recalibration

These two phases, encompassing both the response to digital unfairness and the promotion of digital fairness, mark a crucial transition in adapting consumer law for the increasingly digitalised era. Rather than seeing these **two strategies** as distinct entities, viewing them as interwoven strands of a broader strategy is more apt. They can be initiated concurrently, each informing and strengthening the other. Alternatively, they can be approached sequentially: beginning by addressing the glaring issues of digital unfairness, laying down the groundwork, and then constructing upon that by integrating the principles of digital fairness. This phased approach ensures a comprehensive evolution of consumer law, making it more resilient to the challenges of the digital age.

4. Beyond the horizon

While this Chapter touched upon a series of prevailing problems, its primary intent was to chart potential future directions for the UCPD and its general clause in the digital age. The insights provided are merely the tip of the iceberg, emphasising the ever-evolving nature of the digital landscape. Further studies are imperative to capture the complexities inherent in the subject. These analyses should not overlook **B2B relationships** and the potential interaction between B2B and B2C concepts of (un)fairness. This exploration may pave the way for a unified approach in B2B and B2C transactions. This challenge is another issue that has been recognised since analogue times and has become particularly significant in the digital environment, where digital asymmetry between big players and smaller businesses mirrors the gap between businesses and consumers.[8]

This exploration is a **starting point**, inviting further research studies and a clear path to robust solutions. Yet, this should not deter us from enacting essential legislative reforms immediately. Aware of the pressing need for a change in perspective, let us not slow but rather, with unwavering determination, recalibrate the consumer law compass for the digital age.

II. Professional diligence

1. Professional diligence at the crossroads of continuity and disruption

Previous research study presented in the 'EU Consumer Protection 2.0' report has introduced and conceptualised terms vital to the recent consumer law debate, namely digital asymmetry and digital vulnerability. While these notions have not yet been incorporated into legislative texts, they have become central to the scholarly discourse and academic literature on consumer law, serving as the foundation of this analysis. The prior research placed a particular

8 See Namysłowska, 2022b.

emphasis on these emerging concepts, leaving other significant issues relatively unexplored. Among them is the enduring **notion of professional diligence**, a pivotal yardstick that helps delineate the contours of unfair commercial practices. Given its importance, it became apparent for this project to focus on exploring the professional diligence concept within and beyond the framework of the UCPD.

In essence, this Section explores the tension between the new paradigms introduced by digital transformation and the enduring principles of consumer protection enshrined within established legal frameworks. In this context, we face the age-old question about the **need to recalibrate existing laws**: Does the digital age demand a reform of the concept of professional diligence, which serves as a foundation for determining unfairness? This reflection raises fundamental issues at the intersection of tradition and adaptation in the legal landscape.

Historically, professional diligence has been a cornerstone of ethical conduct, guiding professionals across diverse industries in their dealings with competitors, clients, and consumers. The concept of professional diligence can be traced back to the 19th century, with Article 10bis of the Paris Convention for the Protection of Industrial Property, adopted in 1883, emphasising the need for effective protection against acts of unfair competition, referring to an act contrary to honest industrial and commercial practices (*un acte de concurrence déloyale tout acte contraire aux usages honnêtes en matière industrielle ou commerciale*). The German law of 1909 prohibited acts of competition conflicting with good morals (*gute Sitten*). More recently, a direct reference to the professional diligence concept was made in Article 5(2) UCPD in 2005, defining the general prohibition of unfair commercial practices as laid out in Article 5(1) UCPD. Despite nearly a century separating these pieces of legislation, similar concepts remain in use.

At the beginning of the 20th century, the landscape of unfair conduct vastly differed from what we witness today. While undoubtedly significant within their contexts, the scope and impact of unfair practices in the past were inherently limited due to the constrained reach, simpler market structures, and the absence of the technological advancements present in today's globalised commerce. It is the digital revolution that has ushered in **transformative changes**. The dynamics of commercial practices have undergone a metamorphosis. Modern times have opened the door to a myriad of large-scale, technologically-driven manipulative tactics that exploit consumers on an unprecedented scale. As technology redefines the boundaries of interaction between traders and consumers, new challenges to fair B2C relationships emerge. They demand careful legal scrutiny.

From an initial perspective, the enduring relevance of the professional diligence concept appears to withstand the **test of time**, encapsulating the duty to care across various professional capacities. Nevertheless, despite its expansive scope, this traditional concept might not adequately address the complexities of the digital ecosystem. Consequently, the broadness of the professional diligence concept should not deter nuanced discussions crucial for safeguarding consumers and fostering trust in the digital consumer marketplace.

At the heart of this study lies the unveiling of the **digital renaissance** – a reawakening of the established principles governing the trader-consumer relationship. As we grapple with the complexities of the digital era, we face new hurdles necessitating a critical re-evaluation of consumer law paradigms. While the digital landscape transforms, the relevance of the traditional protection framework against B2C unfairness must evolve in tandem. An opportunity to propose new solutions has emerged through the ongoing 'Digital fairness – fitness check on

EU consumer law', which focuses on evaluating three key consumer law Directives: the UCPD, CRD, and UCTD. The overarching question of the fitness check is whether specific digital areas require a more tailored legislative approach. One question in the public consultation survey was whether the trader's professional diligence towards consumers should be further clarified in the digital context.

The paramount question now is: How can we ensure that the core principles of professional diligence endure in the digital era? As the digital realm permeates every facet of commercial interactions, we must reflect on the values that have guided commerce throughout history and **breathe new life** into them in the context of the digital environment. We should foster a thoughtful and adaptive conceptualisation of professional diligence that acknowledges current dilemmas. The legal framework must respond to the dynamic realities of the digital era and promote a resilient and equitable digital consumer marketplace for the benefit of all stakeholders involved.

In addressing the issue of whether the concept of professional diligence requires adjustment for the digital economy, it is essential to understand its current application. Through an analysis of its scope across various domains of consumer law, areas needing refinement and enhancement to better align with the rapidly evolving digital landscape can be identified. Evaluating the **current state** and associated risks is the foundation for determining whether changes or modifications are warranted and, if so, how they should be conceived and executed.

2. Professional diligence in the UCPD

2.1 The concept of professional diligence vs. the concept of unfairness

The notion of professional diligence (*berufliche Sorgfalt*, *diligence professionnelle*) forms a **key component** within the framework of the protection against unfair commercial practices in the European Union, as established by the UCPD. As the UCPD pertains solely to business-to-consumer relationships, the definition of professional diligence at the European level only concerns the conduct of traders towards consumers.

The UCPD builds upon the **principle of not trading unfairly**,[9] achieved through the prohibition of commercial practices in Article 5(1), as defined in Article 2(d).[10] The negative aspect of this narrative implies that anything not explicitly prohibited is deemed permissible. Advocate General Trstenjak argued that the UCPD 'presupposes that commercial practices are fair as long as the precisely defined conditions for a prohibition are not fulfilled'.[11] Or as Siciliani, Riefa, and Gamper observed: 'what is not unfair is therefore fair by default'.[12] Thus, from a linguistic perspective, the UCPD does not establish the positive duty to trade fairly but rather the duty not to act unfairly. This negative formulation is interpreted as promoting a trader's

9 Abbamonte, 2006, p. 699.

10 Article 2(d) UCPD: 'business-to-consumer commercial practices' (hereinafter also referred to as commercial practices) means any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers.

11 Cases C-261/07 and C-299/07, VTB-VAB NV and Galatea BVBA, ECLI:EU:C:2008:581, para. 81.

12 Siciliani, Riefa and Gamper, 2019, p. 187.

commercial freedom and aligns with the principle of *in dubio pro liberate*, which applies in the case of the UCPD.[13]

A **three-fold UCPD architecture** operationalises the prohibition of unfair commercial practices:

1. the general prohibition of unfair commercial practices in Article 5(1) with the general clause in Article 5(2) and further clarification in Article 5(3);
2. specific provisions in Articles 6 to 9 on misleading and aggressive commercial practices;
3. Annex I, which prohibits 35 unfair commercial practices *per se*.

The concept of professional diligence forms the prohibition of unfair commercial practices. According to Article 5(2), an unfair commercial practice is a practice that is contrary to the requirements of professional diligence (Article 5(2)(a)), and that 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 (Article 5(2)(b)). Therefore, professional diligence establishes a **superior concept** – the unfairness of commercial practices – as one of two cumulative criteria. Commercial practices that run counter to the requirements of professional diligence and materially distort consumer economic behaviour are indicative of unfairness. Conversely, commercial practices adhering to the requirements of professional diligence are considered fair, provided they do not materially distort the consumer's economic behaviour. Both concepts, professional diligence and material distortion of consumer's economic behaviour, are defined by the UCPD.[14]

From the above, it is clear that a breach of the professional diligence requirements is **not synonymous with unfairness**. Merely violating professional diligence requirements does not constitute unfair conduct under the UCPD. Unfairness only arises when consumers' economic interests are harmed. While a breach of the consumer's economic behaviour could be theoretically seen as a violation of professional diligence, the former condition explicitly underscores two points: the necessity of an impact from breaching the professional diligence requirements and the UCPD's exclusive focus on safeguarding economic interests.

Article 5 is a **self-standing prohibition**[15] but can be applied as a last resort. First, an assessment is necessary to determine if the commercial practice is included in the black list in Annex I. If not, one has to evaluate whether it falls under the prohibitions of misleading (Articles 6 and 7) and aggressive practices (Articles 8 and 9). Only if a given commercial practice is not prohibited under these provisions can it be assessed against the general clause in Article 5.[16] That is why Article 5 serves as a safety net for the assessment of commercial practices that are neither misleading nor aggressive, closing regulatory gaps. While the majority of commercial practices fall into one of the two forms of unfairness prohibited by the UCPD (misleading and aggressive commercial practices), Article 5 is rarely applied.[17]

---

13 Cases C-261/07 and C-299/07, VTB-VAB NV and Galatea BVBA, ECLI:EU:C:2008:581, para. 81. See Durovic, 2016, p. 69.
14 Articles 2(h) and 2(e).
15 Case C-435/11, CHS Tour Services GmbH, ECLI:EU:C:2013:574; Case C-388/13, UPC Magyarország kft, ECLI:EU:C:2015:225, para. 61–63.
16 Guidance on the interpretation and application of the UCPD, 2021, pp. 25–26.
17 Durovic, 2016, p. 69; Trzaskowski, 2021, p. 81.

Does this make Article 5 and the professional diligence concept redundant? No, it does not. The general clause represents **policy determination** and the **philosophical foundation** of the UCPD.[18] Specific provisions within the UCPD must align with the overarching concept of unfairness. It is assumed that Articles 6 to 9, along with the prohibitions listed in Annex I, adhere to the requirements stipulated under Articles 5(1) and 5(2). This assumption holds for Annex I, as these commercial practices are prohibited in all circumstances. This rule applies not only to currently proscribed practices but also to future amendments. Any new prohibitions of unfair commercial practices should also incorporate the criteria of being contrary to the requirements of professional diligence and materially distorting consumers' economic behaviour. Despite this central role in protecting consumers against unfair commercial practices, the operationalisation of the professional diligence concept presented in this Chapter aims to make the general clause a direct self-standing test to determine unfairness.

2.2 The definition of professional diligence

As mentioned above, the concept of unfairness provided by the UCPD builds upon the concept of professional diligence, or – more precisely – of the commercial practice being contrary to the requirements of professional diligence. Professional diligence is **defined** in Article 2(h) UCPD as:

'the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity'.

The definition of professional diligence consists of **two parts**:

1. it is the standard of special skill and care, which a trader may reasonably be expected to exercise towards consumers;
2. it is the standard of special skill and care commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity.

Firstly, professional diligence is the standard of **special skill and care**. Reference to the special skill implies that a competent trader is concerned.[19] It denotes a level of diligence that exceeds that of 'an ordinary person or non-specialist'.[20] The standard of special skill and care is a standard of due care that a trader is expected to exercise towards consumers.[21] The intention or negligence is irrelevant.[22]

Secondly, the standard of special skill and care is clarified by the notions of honest market practice and the general principle of good faith. These concepts are recognised in national regulations and EU law.[23] As previously mentioned, the term '**honest market practices**' originates from the Paris Convention for the Protection of Industrial Property and is commonly

18 Durovic, 2016, p. 71; Abbamonte, 2006, p. 391.
19 Abbamonte, 2006, p. 705.
20 Abbamonte, 2006, p. 706.
21 See Trzaskowski, 2016 .
22 Case C-388/13, UPC Magyarország kft, ECLI:EU:C:2015:225, para. 48.
23 First Report on the application of the UCPD, 2013, p. 12.

used in intellectual property law. The concept of '**good faith**,' which might be considered either in conjunction with or separately from honest market practices, is known from Article 3(1) of the Unfair Commercial Practices Directive (UCTD) adopted in 1993. Despite the moral connotations of these concepts, the UCPD does not encompass legal requirements related to taste and decency. As set out in Recital 7 UCPD, 'Member States should (...) be able to continue to ban commercial practices (...) for reasons of taste and decency even where such practices do not limit consumers' freedom of choice.'[24]

The concepts of honest market practice and the principle of good faith pertain to the **trader's field of activity**. As such, they are evaluated in relation to the specific industry sector to which the trader belongs,[25] taking into account rules derived from **national and international standards** and codes of conduct.[26] Recital 20 UCPD states: 'In sectors where there are specific mandatory requirements regulating the behaviour of traders, it is appropriate that these will also provide evidence as to the requirements of professional diligence in that sector.' Nevertheless, the precise role of standards in establishing industry-specific benchmarks of diligence still requires a thorough analysis.[27] While the importance of standards in this context is growing, delegating regulatory responsibility to entities lacking experience in this field may raise concerns.[28]

2.3 A deeper dive into the professional diligence concept

A) The beauty of the professional diligence concept

The professional diligence concept did not simply become the magic potion of the UCPD, considering the ongoing disputes about its label as a general clause. The general clause can be understood either broadly as the **entire legal provision** that allows to base decisions on extra-legal criteria or, more narrowly, as an **indefinite term** referring to an extra-legal criterion.[29] This distinction is evident in the Commission's Guidance on the interpretation and application of the UCPD, where the term 'general clause' refers both to the entire Article 5(2) UCPD,[30] and to the term 'professional diligence' within this provision.[31] However, whether one adopts any of these definitions or uses them synonymously does not impact the analyses dedicated to the general clause.[32] In fact, much of the praise for the professional diligence concept arises precisely from the advantages it offers as a general clause. General clauses are often regarded as the central standard, serving as a reference point for regulations whose regulatory content heads in the same direction, and are even seen as the **royal standard** of a legislative act.[33]

---

24 See more Micklitz, 2006, pp. 87 et seq.
25 Durovic, p. 78.
26 Guidance on the interpretation and application of the UCPD, 2021, p. 37; Galli, 2022, pp. 171–174
27 See e.g. Micklitz, 2023.
28 See in this context about the draft AIA Veale and Borgesius, 2021, para. 108.
29 Leszczyński and Maroń, 2013, p. 83.
30 Guidance on the interpretation and application of the UCPD, 2021, p. 20.
31 Guidance on the interpretation and application of the UCPD, 2021, p. 20. The prohibitions of misleading and aggressive commercial practices are also called general clauses (e.g. Anagnostaras, 2010) or small general clauses (e.g. Keirsbilck, 2011, p. 311).
32 Leszczyński and Maroń, 2013, p. 83.
33 Henning-Bodewig, 2015, p. 530.

Pointing out vague terms in the definition of professional diligence does not have to carry a pejorative meaning. Ambiguous concepts are a characteristic feature of general clauses, providing **flexibility** and the ability to function as a **safety net**. The definition of professional diligence set out in the UCPD is inherently flexible, employing concepts such as 'honest market practices' and 'good faith'. These notions, anchored in moral considerations, allow it to be versatile, making the general clause applicable across various sectors, both offline and online. As a result, one of its primary advantages is the capacity to prohibit practices that the original legislators did not anticipate. This feature makes a general clause particularly valuable for new legislative acts when potential infringements are hard to predict. They can, therefore, be viewed as future-proofing the legislation.[34]

As mentioned, the general clause's leading role stems from reflecting the UCPD's policy and philosophical foundation. Its specific provisions, including Articles 6 to 9 and Annex I, must align with the **central unfairness concept**. This function of the general clause is crucial for current and future updates to the UCDP, as it determines what is fair and what is not.

From the perspective of the EU legislator, the absence of a general clause in a legislative act aimed at regulating unfairness undermines its **harmonising effect**, as Member States can retain differing national general clauses.[35] Such an omission allows Member States to persist with their own unique general clauses, which can lead to varied interpretations and applications across borders, potentially creating inconsistencies in how fairness is approached and implemented throughout the Union.

Additionally, the incorporation of general clauses serves a dual purpose in the realm of regulatory frameworks. On the one hand, they can prevent **overregulation** by providing a flexible, overarching principle that adapts to changing circumstances without requiring constant legislative amendments. On the other hand, they help in averting **underregulation** by ensuring that even if specific situations are not enumerated in the legislation, the general clause can still be applied, offering a safety net against potential legislative gaps.[36]

B) Questioning the bedrock

Is the concept of professional diligence in UCPD a beauty, or is it the **beast**? After all, not everyone is thrilled with the general clause as the legislative tool for protection against unfairness. For instance, shortly after the adoption of the UCPD, Howells argued that the UCPD: 'would have been better advised creating a common framework so that the legal regimes evolved towards a common conceptualisation of fairness'.[37]

The definition of professional diligence may seem comprehensive with its two lengthy components. However, does it help determine what constitutes unfairness towards consumers? This question is crucial, particularly when applying Article 5 as an independent test and where the professional diligence standard is a benchmark for future prohibitions of unfair commercial

---

34 Twigg-Flesner, 2016, point 3.

35 Proposal for a Directive of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the Internal Market and amending directives 84/450/EEC, 97/7/EC and 98/27/EC (the Unfair Commercial Practices Directive) COM(2003)356, Explanatory Memorandum, para. 48; See Glöckner, 2013, pp. 225–226.

36 Larouche and de Streel, 2021, p. 556.

37 Howells, 2006, p. 85.

practices. The main challenge of a general clause lies in adopting vague notions to define a broad term. Defining the content of the terms used in the professional diligence definition poses dilemmas for traders, consumers, and law enforcement authorities. Such indeterminate concepts increase market participants' uncertainty.[38] The **discretionary latitude** in interpreting general clauses is extensive, even if it was the legislator's intention.[39] Therefore, the choice of the **interpretation method** is essential. Grammatical and logical interpretation often fall short when applied to a general clause.[40] Given today's rapidly changing commercial landscape, driven by the advent of new technologies, historical interpretation has become obsolete. While teleological interpretation can be effectively applied, ethical and moral evaluations should not serve as the sole basis for interpretation, even when dealing with concepts with a strong axiological charge. Instead, an economic-functional interpretation should be prioritised.[41]

Even though Micklitz claims that the UCPD does not 'reinvent the wheel',[42] assistance is needed in interpreting the professional diligence concept. Interestingly, however, the **UCPD's Recitals** do not touch upon the concept of professional diligence at all. This omission is particularly striking, especially when considering the professional diligence concept's overarching function and the significant role of the preamble in this legislative act, manifested, among others, in introducing the definition of the 'average consumer.' **Specific provisions** of the UCPD that exemplify professional diligence include the prohibitions of misleading commercial practices detailed in Articles 6 and 7, as well as Nos. 1–23 in Annex I, and the prohibitions of aggressive commercial practices outlined in Articles 8 and 9, along with Nos. 24–31 of Annex I. Still, these examples do not particularly facilitate the interpretation of other factual scenarios not covered by these provisions. The **Commission's Guidance 2021** devotes just three sentences to professional diligence, even though this is the third guidance and spans 129 pages.[43]

The term 'professional diligence' is mentioned in a few **CJEU judgments**.[44] However, in cases like UPC Magyarország,[45] where the judgment states that determining a misleading practice is not dependent on intent or negligence, one could argue that this also pertains to the interpretation of professional diligence.[46] Only in the Deroo-Blanquart judgment does the CJEU go beyond quoting Article 5(2)(b). Nevertheless, the CJEU ultimately states in this judgment that 'it is for the national court to take them into account in the context of its overall assessment of all the circumstances of the case in the main proceedings in light of the respect for the requirements of professional diligence'.[47] Some voices even suggest the CJEU is not competent to concretise general clauses, partly due to the lack of consistency in legal traditions.[48]

---

38 Manteuffel and Piaskowski, 2017, p. 37.
39 See Polish Supreme Court III CZP 82/13 Centrala Handlowo-Usługowa E. S.A. w W. v P. C.
40 Patti, 2014, p. 613.
41 E.g. Podszun, 2009, p. 509.
42 Micklitz, 2006, p. 87.
43 Section 2.7: 'The notion of 'professional diligence' encompasses principles which were already well-established in the laws of the Member States before the adoption of the UCPD, such as 'honest market practice', 'good faith' and 'good market practice'. These principles emphasise normative values that apply in the specific field of business activity. It may include principles derived from national and international standards and codes of conduct.'
44 Case C-428/11, Purely Creative Ltd and Others, ECLI:EU:C:2012:651; Case C-310/15, Deroo-Blanquart, ECLI:EU:C:2016:633.
45 Case C-388/13, UPC Magyarország kft, ECLI:EU:C:2015:225.
46 In this direction: Koch et al., 2022, p. 29.
47 Case C-388/13, UPC Magyarország kft, ECLI:EU:C:2015:225, para. 37.
48 Grundmann, 2022, p. 255; Patti, 2014, p. 616.

Others believe that if the CJEU starts to provide too strong material guidance, this would 'disallow self-regulation and crush social initiatives and freedom of market parties to innovate'.[49]

Guidance could be provided by **case law in EU Member States**. Although the professional diligence concept is subject to an autonomous interpretation to achieve the goal of harmonising national provisions,[50] it is challenging to maintain a similar interpretation of general clauses rooted in Union law across the EU.[51] Member States often refer to their national traditions, and some of them even maintain the old terms, like good customs (*dobre obyczaje*) in Poland.[52] Consequently, those opposed to EU general clauses argue they are ineffective tools for harmonising national regulations.[53]

The interpretation of the general clause occurs **ex-post**. Therefore, since traders find it hard to predict how the interpretation of the general clause will look in a specific factual situation, it is difficult for them to shape their behaviour in a certain way.

Nevertheless, this research study primarily criticises the difficulty of applying the professional diligence concept in Article 5 UCPD in the **digital age**.

The rapid transformation of business models, driven by evolving technical and technological innovations, constantly **redefines commercial practices**. These advancements pose particular challenges for those interpreting the general clause.[54] The dilemma becomes more pronounced when considering the role of general clauses within legal frameworks. General clauses, designed to be overarching and adaptable, intersect with the broad realm of legal interpretation and specific intricacies of modern commerce. In an environment where the specifics of a technology-driven business model can change in months, interpreting a general clause becomes a balancing act. It requires understanding the facts of the case, current state and possible future directions of technological advancements.

The conceptual approach, specifically the formulation that 'the standard of special skill and care is to be **reasonably expected** to be exercised by a trader towards consumers', is problematic. This phrasing also faced criticism in the analogous era. It introduces an overly subjective criterion, and it is unclear who should set these expectations for the trader's appropriate behaviour. Is it a regulatory authority or consumers who might not be equipped to define honest market practices?[55] In the digital age, a court could struggle to grasp new business models, while consumers might remain unaware that they have been subjected to unfair digital commercial practices.

The criteria of honest market practice and the general principle of good faith refer to the **trader's field of activity**. Initially, this approach was criticised for its close connection with factual standards established by traders.[56] The Commission acknowledged that 'business practices which conform with custom and usage will not be caught' by the UCPD even if they

49 Tjong Tjin Tai, 2015, p. 12.
50 E.g. Glöckner, 2004, p. 943; Schmidt, 2009, pp. 43 et seq.
51 Micklitz and Namysłowska, 2020b; Anagnostaras, 2010, p. 170.
52 See also First Report on the application of the UCPD, 2013, p. 12.
53 E.g. Cafaggi, 2007, p. 22; Bakardjieva Engelbrekt, 2017, p. 124.
54 Willis, 2020, pp. 188–190.
55 Micklitz, 2006, p. 99.
56 Köhler, Lettl, 2003, p. 1036.

influence consumer's economic behaviour.[57] There is a concern that traders might use simple compliance with common industry practices as a defence.[58] At present, two problems arise from this approach. First, it is unclear what constitutes honest market practices in emerging business models, especially in markets with only a few actors. Second, some digital consumer markets might have subpar[59] or non-existent market practice standards, leaving no clear guidance for proper behaviour. These standards might also never develop. A potential solution could be crafting a definition of professional diligence that takes into account the digital environment's specificity.

The challenge is also rooted in the **conceptual misalignment** of the current general clause with the digital age's demands. While there are detailed, even meticulous, analyses in the literature regarding the compliance of digital commercial practices with the UCPD,[60] most authors acknowledge some need for legislative changes. This conceptual disparity becomes especially pronounced as we move forward since the general clause will increasingly serve as a self-standing test. This is especially relevant for commercial practices that don't align with the definitions of either misleading or aggressive.

One might also question the functions of the reference to professional diligence or, more broadly, the general clause in the UCPD in the digital era. Is it a **higher standard of professional diligence** than before, or just a different one? The digital space is characterised by structural asymmetry, which gives rise to new professional duties and obligations of professional diligence in the sense of Article 5(1) and (2) UCPD.[61] Elevating the standard of professional diligence to bridge this gap between traders and consumers seems inevitable to close the digital divide. Furthermore, for effective consumer protection a safety net is now needed, such as the general clause, provided that it captures the specificity of digital commercial practices. Its effectiveness will also be greater if it is possible to identify a common denominator in the form of a similar concept of professional diligence for B2C relations in various EU digital policy legislations.

3. Professional diligence beyond the UCPD

3.1. Once again: The concept of professional diligence vs. the concept of unfairness

To operationalise the conclusions derived from this Chapter, it is worth considering whether **a common standard of professional diligence** exists across various areas of consumer or even economic law. Discussions about a common standard may pertain to a shared standard for commercial practices and other business activities concerning consumers.

---

57 Proposal for a Directive of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the Internal Market and amending directives 84/450/EEC, 97/7/EC and 98/27/EC (the Unfair Commercial Practices Directive) COM(2003)356, Explanatory Memorandum para. 53. See more Köhler, Lettl, 2003, p. 1036.

58 Howells, 2006, p. 80.

59 See also Siciliani, Riefa and Gamper, 2019, p. 195.

60 Hacker, 2021; Grochowski 2021; Galli 2022; Mocanu and Sibony, 2023.

61 Sax, Helberger, and Bol, 2018, p. 26.

This task is challenging, and the difficulty starts at the **linguistic level**. As mentioned earlier, within the scope of Article 5(2), the concepts of 'unfair commercial practices' and 'acting contrary to professional diligence' are not synonymous. Acting contrary to professional diligence is one of the two criteria for recognising commercial practices as unfair. One could argue, therefore, that the problem of a clear distinction between fairness and professional diligence only arises outside of the UCPD. However, this is inaccurate as the distinction between these concepts is not always clear-cut, even within the UCPD, beyond Article 5(2). The distinctiveness of these notions is also highlighted by various research studies focusing on either fairness[62] or professional diligence,[63] even though their close, almost synonymous nature appears evident.

We should examine the approach to a common professional diligence standard from the perspective of EU legislation: from the **standpoint of the UCPD** and **other legal acts**. The answer to the question of whether a common standard of professional diligence is needed will be addressed in Section IV in the context of a horizontal safety net. In this Section, the answer allows for further reflection on the definition of the professional diligence standard in the digital environment.

3.2 Professional diligence beyond the UCPD through the lenses of the UCPD

Despite the maximum harmonisation of provisions concerning unfair commercial practices by the UCPD, the Directive does not create a legislative void. Even the UCPD itself recognises the existence of other provisions on unfair commercial practices in EU law. **Article 3(4) UCPD** states: 'In the case of conflict between the provisions of this Directive and other Community rules regulating specific aspects of unfair commercial practices, the latter shall prevail and apply to those specific aspects.' Therefore, the UCPD acknowledges regulating unfair commercial practices by other legal acts. From this, one can infer the existence of a common standard of unfairness or professional diligence.

Article 3(4) expresses the collision rule ***lex specialis derogat legi generali*** in the event of a conflict between two provisions. The term 'conflict' is understood not only as a situation where two norms are contradictory but also, more broadly, encompassing scenarios where the content of another EU law provision overlaps with the content of the UCPD provision. This overlap can occur when the other provision regulates the conduct in question in greater detail or applies to a specific sector.[64] The UCPD itself states in Recital 10 that it 'accordingly applies only in so far as there are no specific Community law provisions regulating specific aspects of unfair commercial practices, such as information requirements and rules or the way the information is presented to the consumer. It provides protection for consumers where there is no specific sectoral legislation at Community level and prohibits traders from creating a false impression of the nature of products.'

The **CJEU confirmed this interpretation** of Article 3(4) and ruled that Directive 2001/83/EC contains specific rules regarding the advertising of medicinal products. Therefore, in the event of a conflict between the provisions of the UCPD and Directive 2001/83/EC, the latter takes precedence over the provisions of the UCPD and applies to these specific aspects of unfair

62 E.g. Scheuerer, 2023.
63 E.g. Tjong Tjin Tai, 2015.
64 Guidance on the interpretation and application of the UCPD, 2021, pp. 8–10.

commercial practices.[65] A similar argument was presented in the judgment C-476/14, Citroën Commerce, concerning Directive 98/6/EC, which regulates specific aspects of unfair commercial practices, especially those related to indicating the selling price of products in advertising.[66] In the judgement C-102/20, StWL Städtische Werke Lauf a.d. Pegnitz, the UCPD was analysed together with Directive 2002/58/EC,[67] as explicitly allowed by point 26 of Annex I by a non-preclusion clause.[68] However, the CJEU also does not rule out the possibility of simultaneous application of the UCPD and another legal act if there is no clear contradiction between them.[69]

Given that Article 3(4) UCPD indicates the existence of Union legal acts that regulate specific aspects of unfair commercial practices, the question of how to identify these acts. The first hint comes from the UCPD itself. **Annex II to the UCPD** contains a non-exhaustive list of information requirements established by the EU law in relation to commercial communication, including advertising or marketing, which must be regarded as material. Their omission in a commercial practice indicates its unfairness.[70]

In the **Explanatory Memorandum**, the Commission stated that *lex specialis* provisions do not apply to references in sectoral Directives to broad principles such as the 'general good' or 'fair trade'. Still, this statement is not particularly helpful because it refers to concepts related to especially broad notions.[71]

A possible solution may be to focus on acts that regulate commercial practices, as defined in Article 2(d) UCPD, such as legal acts that specifically address advertising-related issues. Nevertheless, based on the wording of Article 3(4), it becomes evident that this pertains not to all legislative acts but to those that govern matters related to unfair commercial practices. Unfair commercial practices are defined as acts that contradict the requirements of professional diligence and significantly distort the economic behaviour of consumers. Herein lies the problem because, as the UCPD indicates, 'this Directive consequently complements the Community *acquis*, which is applicable to commercial practices harming consumers' economic interests.' Nonetheless, in cases like Abcur, the CJEU dealt with Directive 2001/83, designed to protect consumers' health. On the other hand, **health-related matters** are explicitly excluded from the scope of the UCPD under Article 3(3).

Yet, the UCPD does not use the term 'commercial practices contrary to the requirements of professional diligence' but 'unfair commercial practices.' This **logical error** has practical consequences, as it allows practices that do not fall under the definition of Article 2(d) to be associated with unfair commercial practices. Focusing on professional diligence would be justified as it does not specify the type of harm protected by the relevant provisions. Nevertheless, 'unfair commercial practices' is a catchier phrase and is easier to use than formulating a provision like Article 3(4).

---

65 Cases C-544/13 and C-545/13, Abcur AB, ECLI:EU:C:2015:481, para. 70–81
66 Case C-476/14, Citroën Commerce GmbH, ECLI:EU:C:2016:527, para. 44–46.
67 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.
68 Case C-102/20, StWL Städtische Werke Lauf a.d. Pegnitz GmbH, ECLI:EU:C:2021:954, para. 32–63.
69 Micklitz and Namysłowska, 2020a, No. 36.
70 Article 7(5) UCPD.
71 See Wilhelmsson, 2006, p. 77.

In that case, it is necessary to emphasise again that under Article 5(2) UCPD, **professional diligence** is **not synonymous with fairness**. Acting contrary to professional diligence requirements alone is insufficient for a commercial practice to be considered unfair. There must also be a causal link between this violation and consumer harm. However, according to Article 3(4), equating these concepts is justified. In many of these specific provisions, there is no mention of the infringement of consumer interests, particularly economic interests. Therefore, they exemplify professional diligence and, more precisely, what is contrary to professional diligence.

Yet, due to Article 3(4), a common standard of professional diligence regarding commercial practices must be assumed ***a priori***; otherwise, it would never be applied.

3.3 Regulatory alignment with the UCPD: Insights from other legal acts

Not only does the UCPD recognise in Article 3(4) and Annex II the existence of other legal acts related to unfair commercial practices, but other EU legal acts also directly reference the UCPD. Furthermore, there are legal acts whose connection with the UCPD is evident but **not explicitly mentioned** in the provisions. Prominent examples are Articles 6 to 9 UCPD, where these concepts do not appear explicitly. Additionally, the DSA builds upon the concept of unfair commercial practices. Nevertheless, in some provisions, such as Article 25(1) DSA ('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.'), the concepts of fairness and professional diligence are not explicitly mentioned.

The list of legal acts related to the UCPD is impressive and will be presented in the following table in reverse chronological order.

Table 1, List of legal acts referring to the UCPD

	Legal act	Reference to the UCPD
1.	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on **markets in crypto-assets**, OJ L 150, 9.6.2023, pp. 40–205	Recital 29: Even though some offers of crypto-assets other than asset-referenced tokens or e-money tokens are exempt from various obligations of this Regulation, Union legislative acts that ensure consumer protection, such as **Directive 2005/29/EC** (...), Directive 93/13/EEC, including any information obligations contained therein, **remain applicable** to offers to the public of crypto-assets where they concern business-to-consumer relationships.
2.	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (**NIS 2 Directive**), OJ L 333, 27.12.2022, pp. 80–152	Article 6(28): 'online marketplace' means an online marketplace **as defined in Article 2**, point (n), of **Directive 2005/29/EC** (...).
3.	Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (**Digital Services Act**), OJ L 277, 27.10.2022, pp. 1–102	Recital 73: Providers of online platforms allowing consumers to conclude distance contracts with traders should design and organise their online interface in a way that enables traders to **comply** with their obligations under relevant Union law, in particular the **requirements set out** in (...) **Article 7** of **Directive 2005/29/EC** (...). Article 25(2): The prohibition in paragraph 1 shall not apply to practices covered by **Directive 2005/29/EC** (...).
4.	Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (**Digital Markets Act**), OJ L 265, 12.10.2022, pp. 1–66	Recital 12: This Regulation should also apply **without prejudice** to the rules resulting from other acts of Union law regulating certain aspects of the provision of services covered by this Regulation, in particular (...) and **Directives** 2002/58/EC, **2005/29/EC** (...).
5.	Directive (EU) 2021/2167 on **credit servicers and credit purchasers**, OJ L 438, 8.12.2021, pp. 1–37	Recital 21: (...) Moreover, this Directive is **without prejudice** to the protection of consumers guaranteed by **Directive 2005/29/EC** (...). Recital 52: In order to ensure a high level of consumer protection, Union and national law provide for a number of rights and safeguards related to credit agreements granted to a consumer. Those **rights and safeguards apply** in particular to the negotiation and conclusion of the credit agreement, to the use of unfair business-to-consumer commercial practices as laid down in **Directive 2005/29/EC** and to the performance or default of the credit agreement.
6.	Regulation (EU) 2021/690 establishing a programme for the internal market, competitiveness of enterprises, including small and medium-sized enterprises, the area of plants, animals, food and feed, and European statistics (**Single Market Programme**), OJ L 153, 3.5.2021, pp. 1–47	Recital 48: **Directives** (...) **2005/29/EC** have been adopted to ensure, inter alia, the **equal treatment of consumers** (...). In view of that fitness check, **supporting the full implementation of those Directives** and actions and promoting their cross-border enforcement should therefore be a priority.
7.	Directive (EU) 2019/770 on certain aspects concerning **contracts for the supply of digital content and digital services**, OJ L 136, 22.5.2019, pp. 1–27	Recital 35: The commercial practice of bundling offers of digital content or digital services with the provision of goods or other services is **subject** to **Directive 2005/29/EC** (...).
8.	Regulation (EU) 2017/2394 on cooperation between national authorities responsible for the **enforcement of consumer protection laws**, OJ L 345, 27.12.2017, pp. 1–26	Annex: Directives and Regulations referred to in point (1) of Article 3 (...) 9. **Directive 2005/29/EC** (...).
9.	Directive (EU) 2016/97 on **insurance distribution** (recast), OJ L 26, 2.2.2016, pp. 19–59	Article 17(2): Without **prejudice** to **Directive 2005/29/EC**, Member States shall ensure that all information related to the subject of this Directive, including marketing communications, addressed by the insurance distributor to customers or potential customers shall be fair, clear and not misleading.
10.	Directive (EU) 2015/2366 on **payment services in the internal market**, OJ L 337, 23.12.2015, pp. 35–127	Recital 55: Consumers should be **protected** against unfair and misleading practices in **accordance** with **Directive 2005/29/EC** (...).
11.	Directive 2014/40/EU on the approximation of the laws, regulations and administrative provisions of the Member States **concerning the manufacture, presentation and sale of tobacco** and related products, OJ L 127, 29.4.2014, pp. 1–38	Recital 24: (...) The provisions on misleading information will **complement** the general **ban** on misleading business to consumer commercial practices **laid down** in **Directive 2005/29/EC**.
12.	Directive 2014/17/EU on **credit agreements for consumers relating to residential immovable property**, OJ L 60, 28.2.2014, pp. 34–85	Article 10: Without **prejudice** to **Directive 2005/29/EC**, Member States shall require that any advertising and marketing communications concerning credit agreements are fair, clear and not misleading.

13.	Regulation (EU) No. 1169/2011 on the **provision of food information to consumers**, OJ L 304, 22.11.2011, pp. 18–63	Recital 5: **Directive 2005/29/EC** (...) **covers certain aspects** of the provision of information to consumers specifically to prevent misleading actions and omissions of information. The general principles on unfair commercial practices should be **complemented** by specific rules concerning the provision of food information to consumers.
14.	Directive 2011/83/EU on consumer rights, OJ L 304, 22.11.2011, pp. 64–88	Article 6(n): the existence of relevant codes of conduct, as defined in point (f) of **Article 2 of Directive 2005/29/EC**, and how copies of them can be obtained, where applicable.
15.	Regulation (EU) No. 1007/2011 on **textile fibre names and related labelling and marking of the fibre composition of textile products**, OJ L 272, 18.10.2011, pp. 1–64	Recital 19: **Misleading commercial practices**, involving the provision of false information that would cause consumers to take a transactional decision that they would not have taken otherwise, are **prohibited** by **Directive 2005/29/EC** (...).
16.	Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (**Audiovisual Media Services Directive**), OJ L 95, 15.4.2010, pp. 1–24	Recital 82: Apart from the practices that are covered by this Directive, **Directive 2005/29/EC** (....) **applies to unfair commercial practices**, such as misleading and aggressive practices occurring in **audiovisual media services**.
17.	Regulation (EC) No. 1223/2009 on **cosmetic products**, OJ L 342, 22.12.2009, pp. 59–209	Recital 51: The consumer should be protected from misleading claims concerning efficacy and other characteristics of cosmetic products. In particular **Directive 2005/29/EC** (...) is **applicable**.
18.	Regulation (EC) No. 1221/2009 on **the voluntary participation by organisations in a Community eco-management and audit scheme** (EMAS), OJ L 342, 22.12.2009, pp. 1–45	Article 40(2): **Provisions** put in place in accordance with **Directive 2005/29/EC** (...) may be used.
19.	Directive 2008/122/EC on the protection of consumers in respect of certain aspects of **timeshare, long-term holiday product, resale and exchange contracts**, OJ L 33, 3.2.2009, pp. 10–30	Recital 9: **Directive 2005/29/EC** (...) **prohibits** misleading, aggressive and other unfair commercial business-to-consumer practices.
20.	Directive 2006/123/EC on **services in the internal market**, OJ L 376, 27.12.2006, pp. 36–68	Recital 32: This Directive is **consistent** with Community legislation on consumer protection, such as **Directive 2005/29/EC** (...).
21.	Directive 2006/114/EC **concerning misleading and comparative advertising**, OJ L 376, 27.12.2006, pp. 21–27	Article 4(a): (...) it is not misleading **within the meaning** of Articles 2(b), 3 and 8(1) of this Directive or Articles 6 and 7 of **Directive 2005/29/EC** (...).
22.	Directive 2002/65/EC concerning the **distance marketing of consumer financial services**, OJ L 271, 9.10.2002, pp. 16–24	Article 9: Given the prohibition of inertia selling practices laid down in **Directive 2005/29/EC** and without prejudice to the provisions of Member States' legislation on the tacit renewal of distance contracts, when such rules permit tacit renewal, Member States shall take measures to exempt the consumer from any obligation in the event of unsolicited supplies, the absence of a reply not constituting consent.

From the list provided above, it is evident that the UCPD is referenced for a variety of reasons, which are defined inconsistently: establishing the UCPD as the *lex generalis*,[72] non-preclusion,[73] applicability of the UCPD provisions to the subject matter of the regulatory act[74], exemptions from the applicability of certain or all UCPD provisions,[75] compliance with the UCPD provisions,[76] cross-reference of a definition.[77] Importantly, however, the primary purpose of these legal acts is not to combat unfair commercial practices. Nevertheless, they support this goal despite no direct reference to fairness. Therefore, using a **specific term** is not crucial for determining whether they are connected with the UCPD.

Nonetheless, some legal acts explicitly **employ the concepts** of 'professional diligence' and 'fairness.'

'Professional diligence' is defined solely in the UCPD. Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property only refers to this term. The references therein are, in fact, intriguing. According to Recital 31: 'A key aspect of ensuring

72 Table 1, points 11, 13.
73 Table 1, points 1, 4, 5, 9, 12.
74 Table 1, points 6, 15, 16, 17, 19, 20.
75 Table 1, points 3, 21.
76 Table 1, points 3, 5, 7, 8, 10, 20.
77 Table 1, points 2, 14.

consumer confidence is the requirement to ensure a high degree of fairness, honesty and professionalism in the industry', and 'Member States shall require that when manufacturing credit products or granting, intermediating or providing advisory services on credit and, where appropriate, ancillary services to consumers or when executing a credit agreement, the creditor, credit intermediary or appointed representative acts honestly, fairly, transparently and professionally, taking account of the rights and interests of the consumers',[78] whereby a high level of professionalism of creditors, credit intermediaries and appointed representatives is achieved through adequate level of knowledge and competence.[79] Meanwhile, 'the creditor's actual knowledge of the costs should be assessed objectively, taking into account the requirements of professional diligence.'[80] In this Directive, therefore, 'professional diligence,' almost equated with professionalism, reflects **possessed knowledge**. A similar solution is adopted in the twin Directive on consumer credit.[81]

'Professional diligence' is also mentioned in the DSA. Each time, it does so in the same context: service providers should make their best efforts in accordance with **high industry standards** of professional diligence.[82]

Besides, in various legal acts, the term '**due diligence**'[83] is often used. The relationship between the concept of professional diligence and due diligence must be examined separately in further research studies.

The term '**fairness**' often appears in legal documents. Two of the most notable instances are in the UCTD and the GDPR. There has been extensive discussion on the relationship between these legal instruments and the UCPD, as documented in the 'EU Consumer Protection 2.0' report and the Commission's 2021 Guidance.[84] These instruments help to safeguard consumers against unfair commercial practices, with the UCTD targeting imbalances in consumer contracts and eliminating unfair terms. In turn, the GDPR establishes comprehensive data protection principles and fairness, as enshrined in Article 5(1)(a) GDPR, is an overarching principle of European data protection law, along with lawfulness and transparency.[85]

These analyses need not be repeated in this Chapter to underscore the argument that a common standard of professional diligence or a unified principle of fairness can be distilled from laws tackling consumer issues. In the B2C context, this common standard of professional diligence is characterised by actions grounded in relevant competence and expertise, encompassing both **passive measures** (to avoid harm) and **active steps** (to protect consumer interests).[86]

---

78 Article 7(1) of Directive 2014/17/EU.
79 Recital 32 of Directive 2014/17/EU.
80 Recital 50 of Directive 2014/17/EU.
81 Recital 20 of Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC OJ L 133, 22.5.2008, pp. 66–92.
82 E.g. Recital 66, Article 17(4)(b) DSA.
83 E.g. the DSA; Regulation (EU) 2023/1115 of the European Parliament and of the Council of 31 May 2023 on the making available on the Union market and the export from the Union of certain commodities and products associated with deforestation and forest degradation and repealing Regulation (EU) No 995/2010, OJ L 150, 9.6.2023, pp. 206–247.
84 Helberger et al., 2021, pp. 27 et seq.; Guidance on the interpretation and application of the UCPD, 2021, pp. 8–10; See also e.g. Helberger, 2017; Trzaskowski 2021, pp. 104 et seq.
85 Galli, 2022, p. 249; Scheuerer, 2023, p. 5. It is also important to discuss the necessity of moving away from silo-based thinking and, instead, adopting a more holistic approach towards consumer protection based on consumer law, competition law, and data protection law. See: Koolen, 2023.
86 See e.g. Tjong Tjin Tai, 2015, pp. 6, 8; Durovic, 2016, p. 73.

While one must consider the specificities of each sector, the actions guided by professional diligence or fairness standards also hinge on shared values. Acknowledging and strengthening these values offers a blueprint for understanding the evolving nature of professional diligence in the digital era.

Suppose fairness (or professional diligence) is the guiding paradigm for regulating the digital economy, functioning as a substantive benchmark in statutory law and case law and a meta-principle extending beyond codified provisions.[87] In that case, it is worth considering within this report whether this common standard of professional diligence **differs in the digital environment** compared to the analogue world. To address B2C relations, let us adopt the previously mentioned definition, which asserts that professional diligence encompasses passive measures, like preventing consumer harm, and active engagement, involving proactive steps to guarantee a high level of consumer protection. When examining EU digital policy legislation, a noticeable shift towards emphasising active engagement becomes evident. An illustrative example is Article 25(1) DSA, which mandates appropriate design, organisation, and operation of online interfaces for online platform providers and the obligation for gatekeepers, as defined by the DMA, to ensure DMA compliance through design.[88]

The concept of professional diligence is most comprehensively developed in legislation addressing unfair commercial practices. However, it extends beyond the UCPD. Many consumer-oriented laws, both predating the digital era and specifically tailored to the digital environment, rely on this standard. This universal benchmark establishes expectations and guides businesses across various platforms and sectors. As digital commerce expands, adherence to and recognition of this standard will be crucial. The implications of a common professional diligence standard are far-reaching for the topics discussed in this Chapter. They suggest a need to consider the **rationale for altering the scope of the professional diligence** definition. Shifting the focus towards the active actions of businesses also sparks discussions about introducing a general duty to act fairly.

4. What next: Tried and True or Cutting Edge?

4.1 A common standard of professional diligence as a starting point

While shaped by historical practices, the current standard of professional diligence must **adapt** to contemporary challenges and technological shifts to ensure that traders do not operate unfairly, irrespective of their business model and the medium they operate within. Only some legal acts concern exclusively the digital market. Thus, the concept of professional diligence found in horizontal legal acts now must face threats from digital commercial practices and protect against digital unfairness, as technological innovations have reshaped the landscape of commerce, marketing, and communication. The digital environment poses difficulties particularly, but not exclusively, in B2C relationships that are not present or as pronounced in offline settings. It has its dynamics, characterised by rapid technological advancements, new business models, and evolving consumer behaviours. Interactions in the digital realm are mediated through technology. This introduces differences in speed, scale, and the nature of interactions. The continuous integration of AI and data analytics in commercial activities further intensifies

87 Scheurer, 2023, p. 1.
88 Recital 65 DMA.

the complexities of ensuring fair dealings. A minor grievance can quickly escalate into a **viral issue**. As much has already been written about the emergence of new threats to consumers in the digital environment, referring to the 'EU Consumer Protection 2.0' report is particularly beneficial due to the conceptualisation of digital asymmetry and digital vulnerability.

The analysis of professional diligence in consumer law raises several questions, the answers to which are crucial for the future development of consumer law. Given the above diagnosis, the core question is whether there is a **need to formulate new provisions**. Is there a need for consumer law amendments, including the redefinition of professional diligence, or can an appropriate interpretation be achieved using general concepts to protect against digital commercial practices? Do we have to consider all consumer protection legislation, or should we focus on this piece of legislation having the safety net function of the UCPD? Many arguments can justify the correctness of each of these options. What will be the impact of the new regulations on the supposed common standard of professional diligence?

4.2 Maintaining the status quo?

Several arguments can be raised to justify why, despite the digital revolution and the threats to consumers that arise from it, one might consider **retaining the legal *status quo***, primarily by maintaining the definition of professional diligence in Article 2(h) UCPD, and not seeking a new definition for digital contexts.

Firstly, the general prohibition on unfair commercial practices and the general clause of professional diligence are comprehensive. They are intentionally broad to ensure the ability to interpret every situation and maintain their relevance over time. This feature was recognised shortly after the adoption of the UCPD. The general unfairness prohibition was introduced to provide a safety net by making the UCPD **future-proof**[89] and enabling its adaptation to market evolution.[90] Trusting in the robustness of such wording can be more effective than continually creating new definitions for evolving contexts. The broad nature of the current concepts provides **flexibility** and addresses emerging and unforeseen developments without the need for constant legislative amendments. The current definition of professional diligence is characterised by its inherent inclusivity – it can already encompass digital nuances when interpreted in light of contemporary standards of good faith and honest market practices. Activities in the digital internal market are sanctionable under the UCPD.[91] The principles of honest market practices and good faith are universal and timeless. By maintaining the current standard, the universality of these values across all forms of trade is emphasised. The traditional definition withstood the test of time and various market fluctuations. These principles were tested and interpreted in various legal contexts. Modifying or specifying them might negate the existing body of jurisprudence.

Technologically neutral laws often prove more resilient over time. By not anchoring the definition to specific technologies or digital practices, it remains relevant as technologies advance. By avoiding a tech-specific definition, the law accentuates its neutrality and relevance across diverse technological scenarios. Overly specific regulations might quickly become outdated,

89 Abbamonte, 2006, p. 704.
90 Anagnostaras, 2010, p. 152.
91 Goanta, 2023, section 1.

leading to confusion and potential mismatches between the intended purpose of the regulation and its real-world application.

Additionally, arguments related to regulatory techniques should be considered. Introducing a second standard for digital contexts might muddle the legal landscape. The **regulatory siblings**, a concept introduced by Goanta, namely legal rules used across regulatory instruments which bear a striking resemblance, may lead to potential overlaps and contradictions.[92] Diverse definitions might pave the way for **fragmentation** in comprehension and application. Establishing specific definitions for various sectors or contexts might cause a divide in offline and online consumer protection standards, potentially bewildering consumers and traders. A singular, overarching definition promotes a consistent approach to professional diligence. This consistency benefits traders operating in digital and traditional markets by ensuring uniform practices and diminishing the administrative challenges of complying with varying standards. Furthermore, many business models now integrate both digital and traditional elements. A broad definition can tackle the intricacies of such hybrid models without requiring separate evaluations for their digital and non-digital components.

Proposing specific definitions for the digital arena may lead to **inconsistencies** with more expansive legal principles set in other legal areas. Introducing another standard of professional diligence could create ambiguities concerning the interplay between the UCPD and other legal measures in consumer protection.

By avoiding the anchoring of legal definitions strictly to certain technologies or digital practices, legislators can ensure they do not unintentionally **hamper technological progress**. This approach instils confidence in businesses to innovate, understanding that the legal structure remains flexible and will not morph into an obstruction due to excessive specificity. Rather than encouraging the exploration of new technologies, overregulation might deter companies from trying them out, fearing potential regulatory backlash.

Regularly updating or establishing specific definitions in reaction to technological advancements could result in **regulatory fatigue** for legislators and businesses. A singular, comprehensive definition covering both traditional and digital realms lessens the frequency of legislative revisions, thus ensuring a stable and predictable legal framework. This method sidesteps the potential pitfalls of reactive legislation, which could perennially lag behind the actual developments in the digital sphere.

This consistency benefits businesses, allowing them to **streamline compliance procedures** without incessantly adjusting to shifting legislation: familiarising new rules, checking compliance, and adjusting business practices. While large corporations might have the resources to navigate a complex regulatory landscape, start-ups and small-to-medium enterprises (SMEs) could struggle. Having to ensure compliance with stringent regulations could result in higher operational costs. Overregulation can be a barrier to entry, preventing innovative start-ups from getting off the ground. Each time a new standard or definition emerges, the legal community and businesses are challenged to grasp, adapt, and comply.

92 See more in Goanta, 2023, section 1 et seq.

Technological advancement has been a constant throughout history, and the legal systems have invariably adapted. Undoubtedly, not every novel development engenders legal dilemmas[93] making legal amendments inevitable. Many new regulations focusing on the digital realm will quickly become outdated due to rapid market shifts and regulatory decision-making cannot suffer under **time pressure**.[94]

Finally, as Article 5 UCPD is **seldom invoked** because most unfair practices fall under the prohibition of misleading and aggressive practices, it might remain untouched.

In summary, while the digital revolution presents new challenges, there are compelling reasons to retain the existing legal definition of professional diligence in Article 2(h) UCPD without crafting a separate digital counterpart. One may claim that the current framework's breadth and adaptability allow it to address evolving situations, ensuring its relevance as technology advances. By emphasising technological neutrality, the law can remain pertinent across purely digital and hybrid business models, fostering consistent consumer expectations across platforms. There is a risk that introducing digital-specific definitions could suppress innovation, complicate regulation, and create legal inconsistencies. Moreover, constant updates to match technological changes can lead to regulatory fatigue and increase complexity for all stakeholders. Instead of making frequent amendments, businesses can seek **guidelines**, like those from the Commission, for clarity. Given the rare application of Article 5 UCPD, major changes might be excessive. Overregulation risks becoming counterproductive.

4.3 Towards the concept of digital professional diligence

Despite the reasons to retain the current legal *status quo*, there are opposing views to consider. Several arguments **challenge the adequacy** of the definition of professional diligence in Article 2(h) UCPD in addressing the unique concerns of the digital era. Therefore, as digital technologies continue to permeate every facet of our lives, traditional legal frameworks must be re-evaluated for their relevancy and applicability. While the general clauses depend on jurisprudential interpretations, these interpretations may be slow to catch up with fast-paced digital changes and might leave gaps in consumer protection. A specific definition can provide immediate clarity without waiting for relevant case law to develop.

(87) The significance of the differences between the analogue and digital worlds, as well as their varying impacts in the realm of rights and freedoms, was even noted by the **European Court of Human Rights**, particularly in the context of online press archives. The Court emphasised that traditional services transitioned to the internet exhibit functional specificity, pointing, for example, to the capabilities for storing and transmitting information and a higher risk of harm caused by content and messages posted online.[95] For these reasons, as the Court highlighted, the rules governing this domain compared to traditional forms might differ. The latter must

---

93 Bennett Moses, 2007, p. 246.
94 Twigg-Flesner, 2016, section 3.
95 Application no. 33846/07, Węgrzynowski and Smolczewski v. Poland, ECLI:CE:ECHR:2013:0716JUD003384607; Applications no. 23676/03 and 3002/03, Times Newspaper Ltd v. the United Kingdom, ECLI:CE:ECHR:2009:0310JUD000300203; Applications no. 60798/10 and 65599/10, M.L. and W.W. v. Germany, ECLI:CE:ECHR:2018:0628JUD006079810; Application no. 57292/16, Hurbain v. Belgium, ECLI:CE:ECHR:2023:0704JUD005729216.

be adapted to the specific requirements of technology to ensure the protection of relevant rights and freedoms.[96] This ultimately influences the proper interpretation of the principle of proportionality, which underlies the assessment of whether a legislative intervention is justified.

Moreover, the emergence of a new legal issue does not automatically lead to the conclusion that the law must change. On the contrary. Upon identifying a new issue, it should be determined first whether the application of existing regulations suffices or if there is a need to enact new ones. However, the pace and scope of technological development have been unprecedented in recent years. It influences business models, relations between traders, and their commercial practices. Specifically, the technological superiority of certain traders over others leads to the employment of unfair commercial practices against weaker businesses, not only against vulnerable consumers. Emerging commercial practices associated with hitherto unseen business models, their approaches, scale, and scope, as well as the technologies they employ, give rise to novel challenges necessitating distinct legislative actions.[97] The enactment of new regulations is also warranted concerning emerging market phenomena, especially since the **increasing complexity** and **decreasing clarity** of technologies augment the ambiguity of the law, stemming primarily from uncertainties related to the classification of new behaviours.[98] Traditional legal structures such as general clauses, are not suited to modern world concerns.

A pivotal concern that merits attention is the existence of **digital asymmetry**. The digital environment places consumers in positions of power disparity compared to businesses. Many digital platforms and services are characterised by complex algorithms beyond the comprehension of the average user. Consumers do not understand how their data is being used, manipulated, or monetised, which can lead to potential exploitation. Furthermore, the depth and breadth of data collected digitally surpass traditional means, making consumer protection in this digital age imperative. While businesses have access to vast amounts of data and sophisticated tools to analyse consumer behaviour, individuals often lack the necessary tools or knowledge to safeguard their interests in the digital space. Such imbalance necessitates re-evaluating the definition of professional diligence to ensure it caters specifically to these digital disparities, fostering a more equitable digital ecosystem. This re-evaluation can be the key to establishing a digital playing field that respects consumers' rights and promotes fair commercial practices.

Further amplifying the urgency of this issue is the concept of **digital vulnerability**. Unlike traditional markets, where vulnerabilities might be more apparent, digital vulnerabilities are multifaceted. Digital platforms have an unparalleled reach, making the impact on such vulnerabilities exponentially more significant. Examples include persuasive design techniques like dark patterns or default settings that are not in the user's best interest. These tactics can particularly affect vulnerable groups in the traditional meaning of Article 5(3) UCPD, such as the

96 The interpretation of the European Convention on Human Rights, which constitutes the primary common foundation for the protection of fundamental rights in the EU, made by the ECtHR, affects both the interpretation of analogous rights and freedoms in the CPC and national constitutions, as well as the interpretation of specific provisions. See the decisions of the European Court of Human Rights in the cases: Application no. 12268/03, Hachette Filipacchi Associés v. France, ECLI:CE:ECHR:2009:0723JUD001226803, para. 41; and also the Court of Justice of the European Union, which, in its interpretation, relies on the case law of the European Court of Human Rights, in accordance with Article 52(3) of the Charter of Fundamental Rights: Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238, para. 54 i 55; Case C-398/13 P, Inuit Tapiriit Kanatami and Others, ECLI:EU:C:2015:535, para. 46; Case C-157/15, G4S Secure Solutions NV, ECLI:EU:C:2017:203, para. 27; Case C-157/15, Policie ČR, Salah Al Chodor and Others, ECLI:EU:C:2017:213, para. 37 i 38).

97 Cox, 2021, p. 153.

98 See more Bennett Moses, 2007, p. 269.

elderly or children, amplifying the risk of exploitation. Moreover, with the growing number of digital natives, the magnitude of these vulnerabilities is set to increase. In the age of digital reliance, recognising and addressing this heightened vulnerability through tailored legal provisions becomes paramount. A one-size-fits-all approach, as currently embodied in the professional diligence definition, might fall short of safeguarding the rights and interests of digitally vulnerable consumers.

The assertion that the existing ban on unfair commercial practices is sufficiently broad **ignores the characteristics of digital commerce**. While general clauses might be designed for adaptability, the rapid evolution of the digital realm can render these clauses due to the conceptual misalignment observed above. Digital platforms and services often present unique scenarios that a general clause might not adequately cover. The contemporary dynamics of the digital market, including technological advancements and evolving consumer behaviours, demand definitions tailored to their specificity. Relying solely on honest market practices and good faith might prove inadequate in addressing the sophisticated manipulations and novel challenges that the digital space presents. However, in any case, the new general clause should allow for assessments of the present world but needs to focus on the fact that the infringement occurred, not how it occurred. Courts cannot understand this since even businesses using artificial intelligence-driven machines to design and target digital interactions often do not know what their machines did to cause a sale.[99]

Technological neutrality, while commendable, might not be feasible given the fast-paced developments in the digital sphere. Though broadly applicable, general laws might not have the **specificity** required to tackle unique hurdles presented by digital technologies. The blurring lines between the physical and digital realms further complicate the application of general laws. The era of big data and machine learning calls for more focused legislation. **Hybrid business models**, which merge digital and traditional components, could exploit the gaps in general definitions, potentially leading to consumer harm. Additionally, emerging technologies like virtual and augmented reality make the distinction between digital and physical commerce even more nuanced. Furthermore, consumers' increased reliance on digital platforms for essential services further underscores the need for specific safeguards.

Arguments based on regulatory techniques favouring a unified standard may underestimate the potential pitfalls of overgeneralisation. Instead of complicating the legal landscape, a digital-specific standard could offer clarity by addressing the characteristics of digital commercial practices, thus ensuring robust consumer protection. Moreover, a tailored approach to regulating digital commerce might inspire greater **consumer confidence**. Distinct standards, especially for emerging technologies, can provide clearer pathways for industry innovation while safeguarding user rights. This can foster a harmonious environment where businesses can thrive and consumers are protected. The risk of overregulation can be mitigated through consultation with industry stakeholders and the iterative refinement of regulations. Given the dynamism of the digital world, a customised approach offers better protection for consumers and stronger support for businesses. The legal framework remains in step with modern realities by recognising and distinguishing the nuances between digital and traditional practices.

99 Willis, 2020, pp. 188–189.

While introducing specific definitions for the digital space might challenge established legal principles, it reflects the realities of modern commerce. Such definitions can **bridge the gap** between legacy legal principles and modern digital practices, ensuring a seamless transition and adaptation for businesses of all scales. From an idealistic perspective, this approach can foster an environment where innovation flourishes without compromising consumer rights.

Reacting to technological advancements is not necessarily a symptom of regulatory fatigue but might reflect **responsive and responsible legislation**. A robust legislative framework should be agile, evolving with technological and market developments. The legal framework remains relevant and applicable in all contexts by keeping pace with advancements. A forward-thinking approach that anticipates digital trends can empower businesses to innovate confidently and clearly. By creating a digital-specific definition, the legal framework can stay ahead of the curve, setting clear business guidelines and ensuring consumer protection. In a rapidly shifting digital landscape, timely adaptability in legislation is not preferable but essential.

Creating a distinct definition of professional diligence does more than just address the unique nuances of the digital sphere; it serves as a **powerful statement** on the evolving priorities of consumer protection. By establishing a separate category, regulators signal that the complexities and challenges of the digital world are not merely an extension of traditional commerce but are unique and deserving of separate, nuanced consideration. This action draws a clear line, ensuring that stakeholders – whether businesses, consumers, or intermediaries – recognise the heightened significance of diligence in digital transactions.

Moreover, in an era where digital transactions are becoming the norm rather than the exception, emphasising the importance of tailored regulation reflects a **forward-thinking regulatory approach**. It can encourage businesses to prioritise best practices, knowing that there is an established standard to which they are held. Consumers are reassured that their rights are at the forefront of regulatory considerations. Highlighting the significance of a novel standard of professional diligence becomes an integral component in fostering trust. Trust, after all, is the cornerstone of any sustainable digital ecosystem. By underlining this importance through a separate definition, the regulatory framework acknowledges the current digital reality and paves the way for a more secure and equitable digital future.

The Commission's 2021 Guidance offers practical insights into the application of the UCPD in the digital context. Still, it cannot replace a legislative framework that anticipates and addresses the digital age. While the Guidance can serve as a supplement and provide interim solutions, the foundation of consumer protection relies on well-defined and future-proof legislation. The European legislator has recognised this and has issued laws regulating the digital market. Still, core consumer law remains outdated with established but obsolete provisions. With the European Union's aspirations for a **cohesive Digital Single Market**, the need for a digital-specific definition of professional diligence becomes even more pronounced.

It is, of course, possible to identify equally important issues that require legislation, such as a black list. However, new unfair digital commercial practices will emerge tomorrow. This is why we need a resilient standard concurrently. Integrating the digital-specific definition of professional diligence at the core level ensures that the legal framework remains cohesive and comprehensive. Addressing digital nuances directly in the core definition leads to a tailored and, therefore, more effective regulatory approach. To achieve this goal, the nature and focus of the new concept must be clearly reflected in both **language** and **substance**.

4.4 Navigating the digital professional diligence concept

Based on the above considerations, it becomes clear that a **new definition of professional diligence** is necessary to enhance consumer protection in the digital age against digital commercial practices. This definition should exclusively address digital concerns. Accordingly, professional diligence in the digital environment would be referred to as 'digital professional diligence,' aligning with the language and scope of digital commercial practices and unfairness. These linguistic and substantive innovations position the concept of professional diligence in the digital realm. The decision to create a distinct definition separate from traditional professional diligence also underscores the urgent need for legislation addressing the unique challenges of digital transactions as opposed to offline transactions. This would establish a dichotomy of standards for the online and offline worlds. The concept of digital professional diligence should, in turn, be an integral part of a new general clause that specifies a fresh general prohibition of unfair commercial practices.

Crafting the content of the digital professional diligence notion requires initial consideration of the **characteristics** it should possess.

Above all, the new definition of digital professional diligence must **focus on the digital environment** and address the difficulties posed by digital commercial practices. The digital environment is not merely an extension of the physical world. For example, an algorithm-driven recommendation system on a platform operates differently from a salesperson's advice in a brick-and-mortar store. By specifying the digital context, such a definition ensures its scope is precisely targeted at the unique issues of the online world. Only in this way can it hope to be effective and relevant.

As we operate within a general clause, the definition of digital professional diligence should be **flexible** and establish broad principles in the digital context to accommodate technological advancements and emerging infringements. The flexibility of the terms used in the definition of digital professional diligence must endure over time to address unforeseen ways in which consumers may be harmed. The emergence of AI, augmented reality, or quantum computing may introduce novel legal challenges that are not yet anticipated.

Last but not least, considering the legislative technique's impact on a legal tool's effectiveness, the definition of digital professional diligence should be **concise**[100] yet **comprehensive**. Conciseness reduces ambiguity, facilitating understanding, compliance, and enforcement for those involved. Shorter definitions also reduce the risk of inconsistencies within the text or with other related laws. In the EU context, a concise definition simplifies its incorporation into national legal systems. Stakeholders find it easier to remember a succinct definition, and using catchy phrases in discussions and debates can aid comprehension. However, this conciseness should not come at the expense of comprehensiveness; the definition must accurately capture the essence of the term. Incomplete definitions could potentially allow for the evasion of obligations. A complete definition ensures seamless integration with other terms and concepts in the text. The goal is to strike a balance between a comprehensive representation of the term and maintaining clarity and manageability.

---

100 See the critique of too complex new laws in Savin, 2022, p. 15.

Does the current **definition of professional diligence** in Article 2(h) UCPD ('Professional diligence means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity.') possess the characteristics mentioned above?

The current definition is **generic**; it does not explicitly reference the digital environment. While the UCPD originates from the pre-digital era, it does not surprise and theoretically allows it to be applied to both offline and online worlds. This universality can be assessed as a strength in the absence of other solutions. On the other hand, considering the previously mentioned arguments about the unique characteristics of the digital realm, this broad applicability becomes a drawback. The definition is only comprehensive for the needs of the offline world but fails to capture the digital world's particularities without a clear focus on digital aspects.

The definition is not as clear or concise as it could be. It is **lengthy** and might lead to interpretational challenges, especially when determining the standard of special skill and care that can be reasonably expected from traders, especially in the ever-evolving digital domain. None of the concepts used in the definition are explained elsewhere in the UCPD, including its Recitals. However, studies in behavioural economics have shown that we have an intuitive understanding of standards of fair dealing. Even an intuitive view provides a starting point for self-reflection by businesses about whether a proposed course of conduct is likely to offend community values and the statutory safety net prohibitions.[101] This assumption may hold in the offline world. Nevertheless, there is no clear understanding of what constitutes a standard and what does not in the digital environment. So, operating with old concepts will not help effectively combat digital unfairness. Therefore, a mere reference to the digital context in the definition (e.g. 'Digital professional diligence means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers in the digital environment, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity.') will not dramatically change the current interpretation of Article 2(h) or make the definition more useful when applied to digital infringements. Instead, all its components need to be **rejected**.

Rejecting all elements of the current definition means that the definition of digital professional diligence needs to be formulated from the ground up. This effect is not disadvantageous, considering that the definition of digital professional diligence must **differ** from the definition of professional diligence while still being based on the same values underlying the fight against B2C unfairness and being crafted with a nod toward ethical considerations. The need for distinct phrasing arises from expectations of a higher standard of professional diligence that aligns with the nature of unfair digital commercial practices and the risks they present. At the same time, using different terminology prevents the overapplication of non-digital interpretations from the existing definition of professional diligence to digital scenarios and underapplication where digital nuances are evident. The definition's specificity significantly influences the outcomes of the assessment. Differing concepts mean that the regulations will not become regulatory siblings, which might even 'risk disrupting the systematisation and coherence of European law as attributes of legal certainty.'[102]

---

101 Akerlof and Shiller, 2009, see Paterson and Brody, 2015, p. 352.
102 Goanta, 2023, Section 5.

When considering the definition of digital professional diligence, the operationalisation of which will be presented in Section V, it is important to remember that, under the current general clause, commercial practice must always be examined concerning its **impact on consumers**. Acting contrary to the requirements of professional diligence does not automatically determine unfairness, which only occurs when such actions' impact on consumers' economic behaviour is demonstrated. Therefore, the issue of consumer harm must be evaluated as it holds similar importance for any potential new general clause and the functioning of consumer law as a safety net in the digital environment.

III. Consumer Harm

1. 'Consumer harm' vs. 'consumer interests'

Fostering a redefinition of the professional diligence concept, which results in an amendment of the general clause, necessitates a simultaneous analysis of whether the second criterion of unfairness under Article 5(2) UCPD – **distortion of consumers' economic behaviour** – can remain unchanged in the digital era. As observed in Section II, the profound digital transformation raises questions about re-evaluating established norms. Assessing whether the UCPD should still confine itself to solely safeguarding the economic interests of consumers becomes increasingly vital. For this reason, this section analyses the requirement of distorting the economic behaviour of consumers when facing digital unfairness. The primary focus of this analysis is whether, in the world of unfair digital commercial practices, the UCPD should broaden its scope to encompass a spectrum of consumer harm. The digital era has expanded the horizons of consumer harm, extending beyond traditional economic dimensions to include psychological and societal aspects. This expansion presents the UCPD with the question of how to address these multifaceted dimensions of consumer harm effectively.

'Harm' is, however, not the language of the **traditional European consumer law**, unlike EU competition law.[103] 'Harm' does not appear in the UCTD and the CRD. In the UCPD, 'harm' is used only as a verb when referring to 'harming the economic interests.'[104] The use of the term 'economic interests' clearly resonates with Article 169(1) TFEU, according to which the protection of the economic interests of consumers is a means to promote the interests of consumers and to ensure a high level of consumer protection.

More recently, the Omnibus Directive refers to consumer harm in its recitals but without providing further details or relevant context.[105] In contrast, 'harm' in the sense of 'harm caused by digital services' is the language used in **new legislative acts** regulating the digital market, such as the DSA, the DMA, and the draft AIA.

---

103 E.g. Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union Text with EEA relevance, OJ L 349, 5.12.2014, pp. 1–19.

104 E.g. Article 1 UCPD.

105 E.g. Recitals 7, 11 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7–28.

The terms '**harm**' and '**consumer harm**' will be used throughout this Chapter. Even a preliminary analysis suggests that the concept of 'consumer harm' is broader than 'harming the consumers' interests' in core consumer law. Therefore, employing the term 'harm' might better capture the various infringements characteristic of the digital age. Using the term 'harm' is also essential for operational reasons; this can streamline the discussion about consumer protection in the digital realm, which is particularly vital if consumer law should function as a horizontal safety net.[106]

First to consider in this Section are the nature of digital commercial practices and the types of consumer harm they generate. Furthermore, the current state of consumer protection regarding economic interests under the UCPD should be examined. This assessment will be conducted in light of the new **EU digital policy legislation**. Determining the current state is the basis for asking whether amending consumer law, particularly the UCPD, is necessary to protect consumers against harm arising in the digital realm. Such an inquiry challenges the paradigms of the UCPD and consumer law, potentially paving the way for a thoughtful reimagining of the consumer harm concept that comprehensively addresses the intricacies of the digital era.

2. The nature of consumer harm in digital realms

2.1 The digital shift in consumer harm

The core principles of consumer law have **traditionally** centred around safeguarding consumers' economic interests. Consumer harm was primarily understood in tangible terms, such as financial loss when consumers purchased products with characteristics different from those advertised. The focus on infringements related to economic interests is not surprising when considering the historical development of the market and the establishment of European consumer protection in the 1960s as a fundamental principle of the welfare state.[107] At the EU level, consumer's right to protect their economic interests was introduced in 1975.[108] Emphasising the safeguarding of economic interests also aligns with the broader EU goal of ensuring the proper functioning of the internal market and the economic integration of its Member States. The aim is to instil confidence in consumers participating in the internal market, thereby reinforcing the EU's vision of a unified economic space.[109] This commitment is evident in Article 169(2)(a) TFEU, which states that the Union contributes to the attainment of consumer protection objectives through measures adopted under Article 114 in the context of the completion of the internal market.

Certainly, the Union's competencies are not limited to safeguarding consumers' economic interests but also extend to protecting the **health and safety** of consumers, as well as promoting their **right to information**, **education**, and the ability to **organise themselves** to protect their interests.[110] Hence, provisions related to areas such as product safety, food, and pharmaceutical law. In the traditional commercial environment, the assessment of commercial

---

106 See Section IV.
107 Grochowski, 2020, p. 392.
108 Preliminary Programme of the European Economic Community for a Consumer Protection and Information Policy, OJ C 92, 25.4.1975. See also Valant, 2015, p. 4.
109 See more in e.g. Reich, 1992.
110 Article 169(2)(a) TFEU.

practices for their unfair nature, however, was conducted solely in terms of their impact on economic interests. The UCPD even explicitly excludes the protection of consumers' health and safety from its scope.[111]

In the digital environment, business models and commercial practices **look different**. Admittedly, even in the traditional brick-and-mortar model, traders influenced consumers to make one decision rather than another, consumers were consistently pressured, their emotions capitalised on, and brand loyalties subtly instilled. They were introduced to desires they never knew they had. With digital business models becoming increasingly complex, it is not just about being misled or aggressively persuaded into buying goods or services anymore. Today, the very nature of commerce has shifted, offering a vast array of opportunities and channels. We face unprecedented dimensions of influence and potential exploitation. Operating in real-time, with instant gratifications, feedback loops, and 24/7 engagement cycles, can distort consumers' perceptions of time, value, and urgency, making them more susceptible to impulsive decisions. With a global audience at their fingertips, traders use **advanced digital marketing techniques**, leveraging big data and analytics to tailor their approach to individual consumer preferences.[112] Social media platforms, for-profit mobile apps, online retail platforms and others increasingly mediate our transactions, interactions, and experiences. Digital business models, underpinned by sophisticated algorithms, can subtly influence consumer choices in ways they may not understand or even notice.

In the digital age, personal assistants and chatbots are not just tools but extensions of ourselves, interpreting our needs and desires. As we transition from the Internet of Things (IoT) to the Internet of Behaviours (IoB), each consumer emerges as a separate market.[113] In today's brave new world, businesses no longer simply sell: they predict and **tailor experiences** so intimately that the line between user and technology becomes almost indistinguishable. We are approaching a future where individualism extends beyond self-expression in the universe to self-programming within the vast expanse of the metaverse. We spend our days on digital marketplaces and online platforms,[114] our reality is virtual or augmented. Products are 'free', contracts – smart, twins – digital[115], and our life is on subscription. Relationships with consumers are not limited to economic transactions; they extend into ecosystems where consumers **engage, share,** and **participate**. This ongoing interaction fosters deeper brand loyalty and affiliations. The prolonged engagement increases the potential for emotional and psychological impact.

The evolution of business models is influencing the **changes in consumer behaviour**.[116] Consumers had to adapt their traditional buying routines, which involved clear exchanges of money for goods or services, to the digital space. In today's digital consumer marketplace, transactions often involve more cryptic exchanges, such as data for access or attention for entertainment. These invisible transactions make it hard for consumers to assess the true cost of their online

111 Article 3(3) UCPD.
112 See e.g. Duivenvoorde, 2023, p. 177.
113 BEUC, 2023b.
114 In the recent BEUC Consumer survey, over half of respondents (52%) said they spend three hours per day or more on the internet, which includes responses declaring they spent between three and six hours per day online (32%) and those saying they spent more than six hours online (20%). BEUC, 2023c, p.8.
115 See e.g. Mocanu and Sibony, 2023, pp. 229–257.
116 Durovic, 2016, p. 71.

engagements. Every click, preference logged, and interaction with chatbots and personal assistants contributes to a digital narrative and a dataset that can be exploited. Unseen scripts predict, influence, and manipulate choices, challenging the very core of consumer autonomy. Consumers are no longer choosing; they are being chosen. The digital shift is not solely about devices but about decisions. It is not merely technological; it is deeply personal. As consumers shape their digital identities, they must grapple with the unsettling reality that in an era of hyper-personalisation driven by mind-reading technologies,[117] **autonomous choices** are becoming a luxury.[118]

Distinct from conventional paradigms, where the primary concern of consumer law was economic harm, the digital environment introduces multidimensional risks that extend beyond economic interests and market vulnerability in classic terms.[119] The nature and scope of potential consumer detriment evolved dramatically and led to the phenomenon of **digital vulnerability**, described in-depth in the 'EU Consumer Protection 2.0' report. While consumer vulnerability in offline contexts might be linked to factors like age or health, in the digital realm, it revolves around digital asymmetry and the overwhelming analytical capabilities of traders and platforms vis-à-vis individual consumers. Beyond the palpable economic pitfalls, the digital age presents subtler yet profound threats, including data privacy breaches, psychological distress, issues like digital dependency, and the rampant spread of misinformation. Advanced manipulation techniques can impact consumers' self-worth, induce anxiety, and foster addiction. Digital practices can induce stress, anxiety, and depression. The potential for harm is ever-present, with an increasing dependency on digital platforms for various aspects of life, from work to entertainment to socialisation. This evolution of consumer harm has already been extensively documented, and various taxonomies have been used to analyse and categorise these harms.[120]

2.2 Blurring the lines

Along with changes in the very nature of commercial practices and their impact on consumer behaviour, the digital age has blurred the lines between the economic and the emotional, safety, and privacy. Traders' actions in the digital space often appear to have no commercial intent, or the services are offered 'for free'. While **non-commercial in appearance**, they foster the platform's economic interests. The value derives from our data or attention.[121] From social media feeds designed to evoke strong reactions to products that create viral moments, our emotions are now a primary resource being tapped and traded. Quasi-non-commercial actions may ultimately influence our economic decisions. In the digital environment, we all are consumers, even if we think we are not. What is more, we are constantly nudged to become more compliant consumers.[122]

Changes in consumer impact and blurred lines between commercial and non-commercial result in many legal and societal problems. The main legal problem boils down to the fact that

---

117 Hacker, 2021, pp. 2–3.
118 See e.g. Mik, 2016, pp. 1–38; Gal, 2018, pp. 58–104; Galli, 2022, pp. 214–217; Wertenbroch et al., 2020, pp. 429–439.
119 See Grochowski, 2020, p. 388.
120 E.g. Siciliani, Riefa and Gamper, 2019; Trzaskowski, 2021, p. 19 et seq.; Department for Digital, Culture, Media and Sport (2023).
121 Trzaskowski, 2021.
122 Trzaskowski, 2016, p. 18.

traditional consumer law focuses primarily on economic harm. When the lines blur, it becomes challenging to determine which laws apply. Moreover, the exploitation of emotional or cognitive weaknesses may be an unintentional side-effect of contractual optimisation through machine learning.[123] The digital realm also allows consumers to adopt multiple identities, persons, and avatars. While this can empower self-expression, it also creates a landscape where marketers target a myriad of digital selves, each with its vulnerabilities and desires. The line between consumer and product, between genuine choice and engineered outcomes, has become ever more tenuous. The digital age does not just present novel goods or services; it reshapes the very essence of consumption. The line between personal space and market space is diminishing. Our behaviours, preferences, sentiments, and even values, once inherently personal, are now shaped by online giants. We live in a world where not only products but also perceptions are packaged, priced, and peddled. This entwining of the private and commercial realms necessitates us to reconsider not just our **role as consumers** but also the **role of consumer law**. This constant exposure means the stakes are higher, and the law must reflect this new reality. In such a landscape, the onus is on academia and policymakers to reassess, redefine, and reinforce new parameters of consumer protection.

The basis for further work is the analysis of how consumer law addresses consumer harm in traditional and more digitally-focused pieces of legislation. Due to the scope of core consumer law, the study maintains the basic distinction between economic and non-economic consumer harm. However, the **apparent nature of this division** was presented above.

3. Addressing the wallet and psyche by EU law

3.1 Economic consumer harm

A) The UCPD

The protection of consumer economic interests is the **primary goal of the Directives** subject to the Digital Fairness Fitness Check: the UCPD, the UCTD and the CRD. The UCPD leaves no doubt about the aim it intends to achieve. According to Article 1, the purpose of the UCPD is 'to contribute to (...) achieve a high level of consumer protection by approximating the laws, regulations and administrative provisions of the Member States on unfair commercial practices harming consumers' economic interests.' As the UCPD focuses on harm resulting from the violation of consumers' economic interests, it excludes from its scope commercial practices that are unrelated to the infringement of their economic interests, such as purely personally and subjectively perceived loss[124], protection of privacy, health or personal safety.[125] However, according to the CJEU, the UCPD applies even if national legislation has other objectives. Still, one must be the protection against unfair commercial practices,[126] including the protection of economic interests.

---

123 Hacker, 2021, p. 10.
124 Alexander, 2023, p. 328.
125 Guidance on the interpretation and application of the UCPD, 2021, p. 6.
126 C-540/08 Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG v „Österreich"-Zeitungsverlag GmbH ECLI:EU:C:2010:660, para. 15.

The fact that the UCPD 'is guided by economics'[127] is evident. Article 5(2), specifying the general prohibition of unfair commercial practices in Article 5(1), in addition to the requirement of contradicting professional diligence requirements, considers a commercial practice unfair if '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.' Therefore, the infringement of economic interests manifests itself in the form of violating the consumer's economic behaviour. This is the **most complex concept** in the UCPD: the notion of materially distorting the economic behaviour of consumers is defined in Article 2(e), and additionally, an element of this definition, 'transactional decision,' is further defined in Article 2(k).

Based on Article 2(e), we can distinguish **two parts of the definition** of 'the material distortion of the economic behaviour of consumers: (1) using a commercial practice to significantly impair the consumer's ability to make an informed decision and (2) thereby causing the consumer to take a transactional decision that he would not have taken otherwise. Since each provision in the directive must align with Article 5(2), we should examine how these aspects are reflected in the detailed provisions, depending on the characteristics of the unfair commercial practice.

As for the first requirement – impairing the consumer's ability to make an informed decision – Article 6(1) associates this prerequisite with deceiving the consumer, Article 7(1) links it to omitting material information that is necessary for the consumer to make an informed transactional decision and Article 8 to significantly impairing the consumer's freedom of choice or conduct regarding the product. Therefore, the first criterion encompasses the consumer's **autonomous decision-making**, whether it is hindered by the inability to make an informed decision or infringed upon in terms of freedom of choice or conduct. However, since Article 5(2) serves as a self-standing test and acts as a safety net, other forms of infringements on autonomous decision-making may also be considered. In this regard, various aspects of psychological harm influence the consumer,[128] but the subsequent part of the definition redirects towards the primary economic focus of the UCPD.

Economic interests are evident in the second part of Article 2(e). The requirement of 'causing the consumer to take a **transactional decision** that he would not have taken otherwise' is repeated in all specific provisions of the UCPD on misleading and aggressive practices (Articles 6 to 8).

Article 2(k) UCPD defines the term 'transactional decision' as any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting. This concept encompasses **nearly any choice** a consumer makes in the market[129] but raises questions about how strict this causal link should be.[130] A well-known example of recognising entering a shop as a transactional decision comes from the CJEU.[131] According to German jurisprudence, a transac-

127 Siciliani, Riefa and Gamper, 2019, p. 193.
128 Goanta, 2023, Section 4.3.
129 Alexander, 2023, p. 328.
130 See also on the transactional decision test in case of Howells, 2006, p. 80.
131 Case C-281/12, Trento Sviluppo srl and Centrale Adriatica Soc. coop. Arl, ECLI:EU:C:2013:859.

tional decision includes visiting a website, an online shop or a shopping platform,[132] but not the decision to take a closer look at an offer in an advertisement.[133] Such an assessment, however, seems inconsistent with the need for a broad understanding of the concept of transactional decision, also advocated by the European Commission.[134]

There is no doubt that the current wording of the UCPD requires a violation of economic interests. The distortion of consumers' economic interests must have a certain **qualitative significance** – it must be material. This *de minimis* rule acknowledges that a certain degree of manipulation is even tolerated.

The nuances of the digital context make the traditional evaluation of 'transactional decision' ill-suited. Even in a simple and well-known example, it is clear that such an approach to the scope of the UCPD is **insufficient**. Currently, dark patterns are not directly regulated by the UCPD. Depending on their form, Articles 6 to 9, or possibly Article 5, can be applied to them, but it should be remembered that a violation of economic interests must occur for the prohibition to apply. In other cases, such as the addictive design of dark patterns, the UCPD cannot be considered. Interestingly, from the perspective of consumer protection consequences and regulatory technique, the European Parliament has recently proposed new point 7a(i) of Annex I: 'giving more prominence to certain choices when asking the recipient of an online service for a decision should be prohibited in all circumstances.'[135] This means that, in the specified scope, dark patterns will be prohibited *per se*, regardless of the type of harm caused. As mentioned, every specific provision in the UCPD also contains the criterion of materially distorting consumers' economic behaviour. Only 35 *per se* prohibitions in Annex I do not specify this. They are deemed to inherently contain both criteria of unfairness (being contrary to the requirements of professional diligence and having the potential to materially distort consumers' economic behaviour with regard to the product). This indicates that, in terms of causing consumer harm by digital commercial practices, the black list is an optimal legislative choice as it bans specific practices regardless of the harm caused, although theoretically, *per se* prohibitions should meet the criteria of Article 5(2).

B) Other examples

Looking at the second pillar of European consumer law – **the UCTD** – it does not extensively refer to protected interests. **The UCTD** Recitals referer to Community programmes for consumer protection and information policy, pointing to the heading 'Protection of the economic interests of the consumers'. In the normative part, the UCTD mentions **consumer detriment**: Article 3(1) serves as the basis for protection against unfair contract term that has not been individually negotiated if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer. When applying this Article, the economic impact of the transaction is considered. However, it cannot be the sole criterion in assessing whether the imbalance in the

132 Federal Supreme Court of Germany I ZR 23/15 Geo-Targeting; Federal Supreme Court of Germany I ZR 184/17 Energieeffizienzklasse.
133 Federal Supreme Court of Germany I ZR 129/13 Schlafzimmer komplett.
134 Guidance on the interpretation and application of the UCPD, 2021, pp. 30–33.
135 Proposal for a Directive of the European Parliament and of the Council amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and better information, COM/2022/143 final.

rights and obligations to the consumer's detriment is significant. This is the case when there is a 'sufficiently serious impairment of the legal situation in which the consumer (...) is placed by reason of the relevant national provisions.'[136]

The **GDPR** recognises a broad range of harm. While it is not yet typical EU digital policy legislation, it is also not traditional consumer law. However, due to data-driven commercial practices, the GDPR is frequently used against unfair digital commercial practices. Article 82 GDPR is particularly significant here, using the concept of **material** and **non-material damage** as the result of an infringement of the Regulation. Recital 75 is more specific and merits citation:

> 'The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.'

Similarly, Recital 85 states:

> 'A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.'

3.2 Beyond economic consumer harm

A) Before the digital transformation

The narrative in legal acts changes along with the legal acts that regulate the **digital market**, addressing issues relevant to consumers. Nonetheless, discovering different forms of harm is not unique to our times. Advocate General Trstenjak explained her views in case Plus, crucial for interpreting the UCPD, on the grounds that 'the use of games of chance in advertising is very likely to arouse the human pleasure in gambling'. Therefore, games of chance 'can arouse the attention of prospective customers and direct them to certain ends by means of the chosen advertising strategy'.[137] Nevertheless, as mentioned above, the provision transposing the

---

136 Case C-226/12, Constructora Principado SA, ECLI:EU:C:2014:10, para. 22–23.

137 Opinion of Advocate General Trstenjak, case C-304/08, Zentrale zur Bekämpfung unlauteren Wettbewerbs eV v Plus Warenhandelsgesellschaft mbH, ECLI:EU:C:2009:511, para. 93.

UCPD may take into account other interests. The decision in this regard is left to national legislators. A general solution, however, should be made at the EU level.

B) EU digital policy legislation and possible legislative initiatives

Among the legal acts mentioned in this subsection, **the DSA** is the most consumer-oriented,[138] even defining a consumer for its specific purposes.[139] The Regulation acknowledges potential harm, such as societal and economic harm, stemming from the design of services by very large online platforms and very large online search engines.[140] Still, while it refers to 'damage', it does not specifically address consumer harm. Additionally, the DSA amends Article 90 of Annex I to Directive (EU) 2020/1828 on representative actions by adding the DSA as point 68.

The DMA recognises the possibility of harm caused to consumers by gatekeepers, particularly acknowledging the potential for harmful effects resulting from unfair practices by gatekeepers[141] without specifying the harm. Gatekeepers are required to comply with legislation on consumer protection by design.[142] Furthermore, the DMA refers to Directive 2020/1828 on representative actions, which can be used to address violations by gatekeepers of provisions in the DMA that harm or have the potential to harm consumers.[143]

The draft AIA[144], as approved by the Coreper on 2 February 2024, makes a similar reference to Annex I to Directive 2020/1828.[145] Furthermore, the draft AIA delves more deeply into consumer-related issues. It is indisputable that the Regulation will significantly influence consumer protection, as 'in the digital world, the consumer is the potential addressee of an endless chain of potential uses of an AI systems.'[146] However, references to consumer law and consumers only appear in the Explanatory Memorandum of the draft,[147] while the normative part of the draft AIA does not even employ the term 'consumer.'

The draft AIA uses the term 'harm' in the broadest sense among the presented legal acts. In the original Commission proposal, there was already mention of 'harm,' which could be material or immaterial.[148] The version approved by the Coreper further defines harm as follows:

> '(...)depending on the circumstances regarding its specific application, use, and level of technological development, artificial intelligence may generate risks and cause harm to public or private interests and fundamental rights of natural persons that are protected by Union law. Such harm might be material or immaterial, including **physical, psychological, societal** or **economic harm**.'[149]

---

138 See more Micklitz, 2023, pp. 84 et seq.
139 Article 3(d) DSA.
140 Recital 70 DSA.
141 Recital 65 DMA.
142 Recital 65 DMA.
143 Article 42 DMA.
144 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.
145 Article 68d of the draft AIA.
146 Micklitz, 2023, pp. 15–16.
147 Explanatory Memorandum, 1.4.2., 2.4, 3.5; Recital 28 of the draft AIA.
148 Recital 4 of the draft AIA.
149 Recital 4 of the draft AIA.

This amendment is crucial, especially considering that initially, the Commission included physical and psychological harm, excluding consumers' economic interests. Jabłonowska aptly observes that it remains uncertain whether the legislative intent was to allow the placement of similar systems on the market when only economic interests were at risk, or if it aimed to delegate the safeguarding of economic interests to consumer law specifically.[150]

Although numerous provisions of the AIA pertain to consumers, Recital 4 stands out in the context of the harm. This is especially true for **Article 5 of the draft AIA**, which lists prohibited practices related to artificial intelligence. Goanta views Article 5 of the draft AIA as a regulatory sibling of Article 5 UCPD.[151] However, the character of this provision is not straightforward. Indeed, it contains elements similar to Article 5 UCPD – some practices are only prohibited when the use of an AI system causes harm. Yet, some of them are *per se* prohibitions, like Annex I to the UCPD, as they prohibit certain practices related to AI systems in all circumstances.

At first, Article 5 of the draft AIA prohibited four practices.[152] This list has been extended due to the amendments proposed by the European Parliament. The prohibitions will be quoted below, with the **amendments approved by the Coreper** in bold and italics. Requiring the occurrence of harm, the following artificial intelligence practices shall be prohibited under Article 5(1):

- (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness ***or purposefully manipulative or deceptive techniques, with the objective to or the effect of*** materially ***distorting*** a person's ***or a group of persons'*** behaviour ***by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken*** in a manner that causes or is likely to cause that person***,*** another person ***or group of persons significant*** harm;
- (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective to or the effect of materially distorting the behaviour of a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

In these provisions, harm is not defined as 'material or immaterial, including physical, psychological, societal, or economic harm,' but a criterion of **significance** has been proposed: harm must be significant.

In the context of harm, Article 5(1)(c) also deserves attention. Regarding the prohibition of social scoring, the occurrence of at least one of the following criteria is required: '**detrimental** or **unfavourable** treatment of certain natural persons or whole groups thereof in social contexts ***that*** are unrelated to the contexts in which the data was originally generated or collected' (point i) or 'detrimental or unfavourable treatment of certain natural persons or groups thereof that is unjustified or disproportionate to their social behaviour or its gravity' (point ii).

150 Jabłonowska, 2022, p. 71. See also e.g. Ebers et al., 2021, p. 592.
151 Goanta, 2023.
152 Article 5(1) points a) to d) of the draft AIA.

The remaining provisions prohibit practices regardless of the harm caused. In these cases, it can be assumed that the occurrence of harm is **presumed**, and this presumption cannot be overruled:

- (ba) ***the placing on the market or putting into service for this specific purpose, or use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. This prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;***
- (d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces (...);
- (da) ***the placing on the market, putting into service for this specific purpose, or use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person to commit a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics. This prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;***
- (db) ***the placing on the market, putting into service or use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;***
- (dc) ***the placing on the market, putting into service or use of AI systems to infer emotions of a natural person in the areas of law enforcement, border management, in workplace and education institutions.***

Considering the broad definition of harm in Recital 4, the content of the recent **European Parliament resolution on addictive design** of online services and consumer protection in the EU single market is not surprising.[153] The resolution, using strong phrasing such as '[the EP] is alarmed,' highlights the surge in design features that induce addictive behaviours in users of digital services, leading to various harms to consumers. The document specifically identifies physical, psychological and material harm caused by addictive design[154] and lists numerous examples without categorising them as such. Additionally, examples of societal harm are evident.[155] Below is a classification of some of the examples provided by the European Parliament. The categorisation of certain manifestations of harm is somewhat arbitrary, as they could also fit into another category.

The resolution lists the following **psychological harms** caused by addictive design:

- lower life satisfaction and mental health symptoms such as depression, low self-esteem, body-image disorders, eating disorders, anxiety, high levels of perceived stress, neglect

153 European Parliament, IMCO, Resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market, P9_TA(2023)0459.
154 Resolution on addictive design, point 3.
155 Resolution on addictive design, point B, where the European Parliament observes that digitalisation and social media pose new challenges to society.

of family and friends, loss of self-control, lack of sleep and obsessive-compulsive symptoms, such as compulsive buying among young adults;[156]
- mental-health issues, including risk factors for suicide and self-harm;[157]
- particular risk to children and young people being even more vulnerable and their mental-health conditions established in childhood will shape their subsequent life course;[158]
- problems with daily obligations, declining grades, poor school and academic performance;[159]
- poor job performance;[160]
- links to attention deficits, shorter attention spans, impulsiveness and attention deficit hyperactivity disorder (ADHD) symptoms;[161]
- risks to neurodevelopment, learning and memory, increased risk of early neurodegeneration;[162]
- social pressure to be permanently online and connected, increasing the risk of stress and burnout;[163]
- information overload and excessive sensorial stimuli throughout the day, constraining cognitive ability, and user interfaces offer only limited control over their data.[164]

Physical harm mentioned by the resolution is:

- not spending time being active, moving, being outside, which is associated with physical well-being.[165]

Societal harms caused by addictive design include:

- addictive design can have a 'negative impact on everyone';[166]
- societal harms are discussed as a side effect of recommender systems,[167] both based on personalisation and interaction like clicks and likes.

Also **economic harms** are mentioned, such as:

- maximising extraction of money alongside engagement;[168]
- incentivising compulsive buying, consuming more than needed;[169]
- spending more time than intended.[170]

The resolution does not categorise infringement of **fundamental rights** as harm, although this would be possible, especially considering the increasing references in legal acts that also impact consumers, emphasising the need to protect fundamental rights.[171]

---

156 Resolution on addictive design, point D.
157 Resolution on addictive design, point D.
158 Resolution on addictive design, point D.
159 Resolution on addictive design, point D.
160 Resolution on addictive design, point D.
161 Resolution on addictive design, point F.
162 Resolution on addictive design, point F.
163 Resolution on addictive design, point G.
164 Resolution on addictive design, point G.
165 Resolution on addictive design, point G.
166 Resolution on addictive design, point G.
167 Resolution on addictive design, point M.
168 Resolution on addictive design, point A.
169 Resolution on addictive design, point D.
170 Resolution on addictive design, point A.
171 See more Micklitz, 2023, 69–70, 81, 82–89, 90.

It appears challenging to depart from such a broad understanding of harm, given the comprehensive nature of harm and the need to consider the real impact of digital commercial practices on consumers. In this context, the position of the European Parliament to **intervene legislatively** if the issue of addictive design remains unresolved is noteworthy.[172]

4. What next: Same old song or a new tune?

4.1 Point of no return

Business activities in the digital realm, characterised by their innovative commercial strategies, have fundamentally reshaped the dynamics of consumer interactions. Gone are the days when consumers were gently persuaded into purchasing overpriced organic apples, subpar televisions, or unnecessary collections of antique teapots. In the digital environment, the relationships between businesses and consumers take on a different dimension. They often have a **continuous** and **long-lasting** character. It is not just about enticing the consumer to make a one-time purchase but about keeping their **attention** for as long as possible. Brand loyalty now has an entirely different dimension. Furthermore, the lines between commercial and private domains are becoming increasingly blurred, ushering in a new era of consumer relations. Consumer autonomy is diminishing, and this shift is intentional.

The primary concern is that the harm caused by commercial practices extends far **beyond consumers' economic interests**. Furthermore, it is essential to acknowledge that without experiencing such commercial practices, a person may not even transition into the role of a consumer. Recognising and addressing these broader harms in legal frameworks is not just progressive but imperative. Consumer protection laws must evolve to address this shift, moving beyond traditional paradigms to safeguard consumers effectively in this digital age. This shift challenges the foundational principles of consumer law, necessitating a thoughtful and reflective **reconceptualisation** of how we define and address consumer harm.

Considering the varied interpretations of consumer harm, one must ponder the necessity of harmonising this concept within consumer law. Can digital policy legislation alone sufficiently address this matter? Can regulations like the DSA and AIA effectively cleanse the market of predominant practices that harm consumers, preventing harm in its most expansive definition? The simple answer is no, it cannot. These legal acts **do not contain a safety net**, and their regulatory gap in consumer protection is enormous. Additionally, enforcement issues may make it impossible for consumers to pursue claims based on them. Therefore, we must turn to consumer law.

Additional empirical research on harms might be necessary to prevent the risk of overregulation,[173] although substantial evidence already exists. The suggested amendments are based on concrete data and studies concerning consumer harm, providing a strong foundation.[174] Meanwhile, the European Parliament applies political pressure.

---

172 Resolution on addictive design, point 4.
173 On game design see Sørensen, Sein and Rott, 2023, p. 22.
174 Mocanu and Sibony, 2023, footnote 32.

4.2 Harmonising the consumer harm concept through consumer law

How should consumer law address **non-economic concerns**, and to what extent? This also relates to the current allocation of emphasis within consumer law between individualistic (consumer as a human being who deserves protection merely for the sake of being a market actor) and EU integration-oriented (consumer confidence and harmonisation of law as vehicles for closer economic integration) rationales for consumer protection.[175]

The answer is not clear-cut for every piece of consumer legislation. Consumer laws often specialise in narrow issues, focusing on specific consumer risks. Not all of them pertain to the digital environment; in any case, the nature of digital commercial conduct does not change the extent of damage inflicted on consumers. However, in many cases related to the digital environment, it is necessary to consider the strong influence of traders on consumers, which results in violating consumers' interests not addressed in a given piece of legislation. Therefore, the **evolving nature** of consumer threats underscores the pressing need to adapt and modernise consumer law.

How should consumer regulation, traditionally centred on safeguarding economic interests, cope with its intrinsic scope limitation? While many consumer protection laws could technically be amended from a regulatory standpoint, doing so may not be practical. Such changes risk **excessive legislative efforts**, leading to inconsistencies and overregulation.

Once again, we must reference **the UCPD** due to its function as a horizontal safety net, as detailed in Section IV, though this is not the only argument. The UCPD was once considered a 'comprehensive regulatory regime applicable to all types of commercial practices that may impact on the economic interests of consumers.'[176] Now, this is no longer sufficient. Given the central role of the UCPD within consumer law, it is crucial to understand how it can address both economic and non-economic consumer harms in the context of the digital environment. There is no doubt that the current UCPD solely protects consumers' economic interests, even though the 2021 Guidance creates the impression that it can be applied to combat any type of digital consumer rights infringements.[177]

Incorporating **all forms of harm** to consumers into the UCPD is justified by numerous reasons. The proposed amendments to the UCPD will introduce a more holistic approach to addressing consumer harm. Shifting from a narrow focus on the distortion of economic interests to a broader understanding of harm demonstrates a deeper appreciation of how unfair digital commercial practices can impact consumers and ensures that consumer protection remains robust. By expanding the scope to encompass all forms of harm, the revised UCPD will provide a comprehensive safety net for consumers in various scenarios. It will be flexible enough to adapt to future challenges that may arise with the advancement of digital technology and market practices, ensuring that the legislation does not become outdated or irrelevant.

---

175 Grochowski, 2021, p. 30; Reich and Micklitz, 2014, pp. 17–21.

176 Anagnostaras, 2010, p. 147.

177 In this direction Leahy, 2022, p. 586: 'the UCPD, as evidenced by the updated Guidance, offers an existing and flexible legislative solution which can tackle exploitative game design, use of psychological manipulation techniques to drive spending, use of aggressive game mechanics and industry targeting of vulnerable players.'

Expanding the UCPD's scope of application could lead to **greater consistency**, aligning it with the nature of consumer harm in the digital environment and other EU digital policy legislation. This harmonisation is essential given the UCPD's role as a horizontal safety net and as a central piece of legislation in consumer protection.

Expanding the scope of the UCPD to encompass other forms of harm will not lead to the cessation of regulating 'economic unfairness,' as Howells described it.[178] There will be **no overlap** with other policy sectors as it will always involve an assessment of a (digital) commercial practice, which inherently includes a commercial element. The new regulation will merely respond to the extensive harm that can currently be inflicted on consumers through commercial activities.

Incorporating more digital commercial practices into Annex I can address various types of harm. What are the implications of this? Eliminating these practices from the market can mitigate the potential for multifaceted harm. However, given the current legislative challenges, including every type of exceptionally harmful commercial practice **within Annex I is impossible**. The most effective approach will be a blend of regulations, namely, a new general clause coupled with a new section of Annex I.[179] Adjusting the general clause becomes even more pertinent, given the proposal to introduce the concept of 'digital professional diligence' and to establish a new general clause based on this idea. The operationalisation of ideas about expanding the scope of the UCPD will be discussed in Section V, following an essential analysis of the UCPD's role as a horizontal safety net in the subsequent Section.

IV. Consumer Law as the Horizontal Safety Net

1. Confronting the regulatory gap

In 2021, Natali Helberger, Hans-W. Micklitz, and Peter Rott analysed the regulatory gap concerning consumer protection in the digital environment. Their report, titled **'The Regulatory Gap'**, was published during the draft stages of the Digital Governance Act (DGA), Digital Markets Act (DMA), Digital Services Act (DSA), and the Artificial Intelligence Act (AIA) – collectively referred to as 'the Four'. The study delved into the 'regulatory underground,' which pertains to the reliance on standardisation, conformity assessment, and certification. Moreover, the research aimed to determine the extent to which the proposed rules of the Four might fall short in addressing issues related to unfair digital commercial practices.

The adoption of the DGA, DMA, and DSA has not changed their insightful diagnosis. The regulatory gap, stemming from fragmented protection measures in new digital law, the lack of legislation, or insufficient legislation, still exists. What has shifted is the **perspective.** Previously, the European Commission seemed to believe that the existing consumer *acquis* was adequate to address consumer challenges in the algorithm-driven economy and that 'the Four' offered comprehensive regulation for all relevant areas, including potential consumer issues.[180] Now,

178 Howells, 2006, p. 80.
179 See Section V.
180 Helberger, Micklitz and Rott, 2021, p. 2.

perhaps due to political pressure,[181] the Commission appears more willing to recognise this regulatory gap and seems inclined to reconsider the core consumer protection legislation.

2022 marked a significant turning point. In December 2021, the Commission issued new Guidance on the interpretation and application of the UCPD. As its nature suggests, this **Guidance** avoided deep dives into conceptual debates surrounding the direction of consumer policy-making. While it did not pinpoint regulatory gaps in the UCPD, it did illustrate how the existing rules might encompass certain digital commercial practices or sectors.[182] By May 2022, the Commission had initiated a '**Digital fairness – fitness check on EU consumer law**', which covered three pivotal consumer law Directives: the UCPD, CRD, and UCTD. This move emphasised the need for a thorough re-evaluation of numerous prevailing issues. Even though the survey's questions are not revolutionary and do not promise a drastic shift in consumer protection, essential in today's digital age, preliminary feedback indicates a strong inclination among stakeholders towards legislative amendments.[183] Additionally, the European Parliament's dedication to moulding digital consumer legislation is unmistakable. This commitment is evident in its recent proposals to amend the UCPD and the **resolution on addictive design** of online services and consumer protection in the EU single market. As highlighted in Section III, should discussions on addictive design remain at an impasse, the European Parliament has hinted at its willingness to employ its legislative prerogative.[184] Consequently, this research resonates with the wind of change from Brussels.

The regulatory gap analysis in this research study **is distinct from** its predecessor. While the earlier study predominantly identified the regulatory gaps in digital sector legislation (the Four), the current analysis delves into the potential for closing these gaps from the perspective of consumer *acquis*.

When seeking the optimal legislative solution, we must remember that creating a **fully tight system** responsive to all consumer rights infringements is impossible. In the context of digital law, one of the most significant reasons for regulatory gaps is the rapid pace of innovation. **Regulatory gaps emerge** when new technologies or business practices do not fit neatly within the confines of existing legislation. Regulatory bodies struggle to keep up with the complexity of new business models and technology. The inability to adapt quickly and adequately leads to areas where no regulation applies. Moreover, when laws are crafted, they are based on the current understanding of the new challenges. Legislation crafted for past dilemmas might not address new ones effectively. As new scenarios emerge that were not foreseen at the time of drafting, further gaps can appear.

It would, however, be **overly simplistic** to attribute all regulatory challenges solely to the rapid evolution of the digital market. Obstacles also emerge from inherent legislative complexities. Regulators intentionally leave gaps, opting for a lighter regulatory touch with the belief that the market or the sector can achieve self-regulation or out of concern that excessive regulation could inhibit innovation. Additionally, some interests resist specific legislation. Regulatory gaps frequently result from subpar legislative quality and the limitations imposed

---

181 Micklitz, 2023, p. 14.
182 Narciso, 2022, p. 148.
183 Digital fairness – fitness check on EU consumer law, 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en.
184 Resolution on addictive design, point 4.

by language. When laws are formulated imprecisely or when the terms used are ambiguous or open to multiple interpretations, they may fail to provide a high level of consumer protection. Further gaps and inefficiencies stem from various enforcement mechanisms, interpretations and implementations across EU Member States.

Closing regulatory loopholes in the digital realm goes beyond mere legal technicalities. It is not only pivotal for future-proofing consumer protection but also for upholding the values of **European society** for the **digital society**.[185]

The proposals outlined in the 'Regulatory Gap' paper primarily distinguish between upgrading EU digital policy legislation and enhancing the consumer *acquis*. It is worth examining the arguments in favour of these options to determine the most fitting solution to ensure that consumer law can serve as a horizontal safety net. Referring to the title of the concluding section of the 'Regulatory Gap' paper – 'Upgrading the Four Regulations or Consumer *Acquis*?' – **exploring the potential consumer law** in closing regulatory gaps is essential.

2. Upgrading the EU digital policy legislation or consumer acquis?

2.1 Two roads, one horizon?

A few years ago, the answer to whether upgrading EU digital policy legislation or consumer *acquis* might have looked different. If the ongoing fitness check on digital fairness had been conducted before the beginning of legislative work on, for instance, the DMA, DSA, DGA, DA, AIA, and CRA, this question could have been seriously taken as a starting point for an in-depth policy discussion. Yet, the Commission did not initiate a serious debate on addressing consumer digital issues.[186] Most of these legal acts are already in place and address consumer issues on a case-by-case basis. However, **EU digital policy legislation** regulates the digital economy and digital society.[187] Legislative acts such as the DMA, DSA, DGA, or the forthcoming AIA are not primarily designed for consumer protection and, as a result, do not systematically connect to consumer matters.[188] Therefore, it is unsurprising that their provisions concerning consumer protection are criticised for, among other things, leaving regulatory gaps.[189]

Looking at it short-term, or perhaps realistically – there is no turning back from the transformation of consumer rights through EU digital policy legislation. Thus, the decision of whether to upgrade EU digital policy legislation or enhance consumer rights is **not a true alternative**. We can only console ourselves with slogans about the superiority of EU digital policy legislation over consumer law in addressing consumer harm caused by digital unfairness and vice versa.

So, it can be assumed that EU digital policy legislation is better equipped to address the rapidly evolving and digitally specific challenges posed by unfair digital commercial practices. This legislation is **specifically designed** for the digital environment, offering more detailed and tailored provisions, technically sound and capable of addressing intricacies of digital practices

185 Scheuerer, 2021; Micklitz, 2022.
186 Micklitz, 2023, p. 67.
187 Micklitz, 2023, p. 63 and in this report.
188 See Helberger et al., 2021.
189 See e.g. resolution on addictive design, points I, M, P.

that may be beyond the scope of traditional consumer law. Consequently, one can argue that it provides consumers with a more comprehensive set of protections in the digital sphere.

While tailored to particular industries or technologies, digital sector legislation might overlook or underestimate the interplay between them and consumer *acquis*, leading to potential gaps or overlaps.[190] Exceptionally complex relationships between legal acts are emerging. For example, the DSA introduces provisions against the use of 'dark patterns' but these are limited to the choice architecture and influencing choices and do not address addictive behavioural design. Moreover, they are limited in scope as they only apply to online platforms, not all online services. Nevertheless, Article 25(3) DSA excludes the possibility of applying the UCPD and the GDPR concerning deceptive online interfaces to the extent that they cover this practice. It should be noted here that the DSA should be without prejudice to both,[191] and the UCPD does not explicitly tackle the issue of dark patterns. As an overarching negative consequence of the EU digital policy legislation facing consumer issues, one can point to the phenomenon of the **dissolution of EU consumer law**[192] and the dismantling of the consumer notion through the introduction of new categories: customer, user, natural person, the individual or consumer-citizen or businesses: economic operator, provider, small-scale provider, user, operator, large online platform, very large online platform, etc.[193]

One could also present the opposite argument. A compelling thesis is that consumer protection in the digital environment, when rooted in core consumer law, is **more comprehensive and holistic** than relying on EU digital policy legislation. While the latter approach addresses specific facets of the digital landscape, core consumer law provides a framework that encompasses a broader range of protection tools. A well-constructed core consumer law understands its interplay with the digital realm. Furthermore, grounding consumer protection in core consumer law guarantees taking into account the comprehension of consumers' particular needs and provides greater clarity.

Even if many of these cursory arguments are accurate, the discussion about forward-looking solutions has not been seriously undertaken, and ultimately, we need political will for it to happen now. Of course, one can still hope for comprehensive changes within consumer law. Hence, this Chapter advocates for a profound **recalibration** of consumer law. However, the future will reveal how feasible this will be, considering that the fitness check on digital unfairness only covers three Directives: the UCPD, UCTD, and CRD. This starting point alone seems insufficient for the needed changes.

Considering the current state of affairs, we should adopt a **dual approach**: the concurrent enhancement of both EU digital policy legislation and consumer law. It is important to recognise that various methodologies can potentially strengthen protective measures within consumer protection. These strategies should not be viewed in isolation. Ideally, they would provide consumers with a layered, multi-dimensional protective shield.

From this perspective, continuous improvement of consumer law is essential. The decision to update the consumer *acquis* requires continuous monitoring of whether consumer law is still

---

190 See more on regulatory gaps in the DSA, e.g. Cauffman, Goanta, 2021; on the draft AIA, e.g. Veale and Borgesius, 2021.
191 Articles 2(4)(f) and (g), and Recital 10 DSA.
192 Hans-W. Micklitz in this report.
193 Micklitz, 2023, pp. 16–17.

fit for purpose, which carries the risk of **underregulation**. Subsequent amendments should be bolder than those introduced by the Omnibus Directive and entirely focused on digital consumer concerns. Some of the proposals will be presented in Section V.

As for EU digital policy legislation, ignoring consumer issues is currently not an option. Such a stance would entail complete reliance on core consumer law and likely result in underregulation of consumer issues in the digital environment. Imperfect as it may be, each **additional layer of protection** can contribute to consumer safety. It is essential, though, that EU digital policy legislation serves as an extra layer, meaning it should not hinder further refinements of consumer law.

Therefore, it is crucial to incorporate provisions that prevent **any preclusionary effects** within EU legislation. Provisions like Article 25(3) DSA mentioned above are not easily understandable, hinder discussion on further-reaching consumer protection, blur the lines between consumer law and consumer-oriented provisions in digital laws, and impede the establishment of a horizontal safety net. However, there is room and necessity to go further, as non-preclusion alone does not guarantee that consumer law captures risks not addressed in other legislation.

The reasons for a dual approach do not diminish the need for a more profound **reflection on consumer law**. New legislation and adjustments to current legal frameworks alone will not redefine B2C relationships in the digital era. The implementation of additional legislative instruments and innovative standards that uphold the values of fairness, transparency, and accountability is imperative. European consumer law is the hero of our times, albeit not a perfect one.[194]

2.2 A bridge over troubled water

The organic development of consumer law, whether in EU digital policy legislation or traditional consumer law, will not close regulatory gaps. Although the UCPD is already referred to as a safety net in the realm of unfairness, albeit without a focus on digital unfairness, digital sector regulations do not yet incorporate safety nets. A more streamlined approach would ensure that consumer law fulfils the role of a **horizontal safety net**, understood as an overarching legal framework that applies uniformly across various sectors and commerce domains. While EU digital policy legislation may delve deeply into the intricacies of digital actors, business models, types of transactions, or technologies, a horizontal safety net will provide a consistent foundation for consumer protection.

One of the primary and obvious strengths of a horizontal approach is its **broad coverage**. A horizontal safety net serves as a catch-all, ensuring that a baseline level of consumer protection applies in the digital environment, regardless of how unique or novel a digital practice may be or if traders attempt to circumvent existing rules. It acts as a safeguard against the known and a shield against the unknown, as it anticipates the unanticipated. For example, one can envision the need for a horizontal safety net related to a given system that does not meet the definition of an AI system, which would result in consumers not being covered under Article

194 Goanta, 2021, pp. 177-179.

5 AIA or arising from the DMA's limitation to a narrow category of gatekeepers, as defined in Article 3 DMA.[195]

While revising and updating digital sector rules and consumer law to address specific consumer protection issues is essential, a horizontal safety net regulation is generally **more adaptive**, ensuring that consumer protection remains relevant as new challenges emerge. A horizontal safety net can act as a **feedback mechanism** for sectoral rules. By observing the obstacles and remedies invoked under the horizontal safety net, lawmakers can better understand where digital sector legislation may need amendments or expansion.

How do we structure consumer law as a horizontal safety net? While embedding catch-all safeguards within each piece of consumer legislation is theoretically possible, such an approach neither appears the most practical to implement nor the most transparent. A more straightforward solution involves utilising an existing legal framework or drafting a new one. In the continental legal system, a cornerstone legal instrument enabling the legislative act to function as a safety net is a general clause.[196] General clauses appear in **various areas of law** and may cover B2C or B2B relations, or both. They are best known as a legal tool for combating unfairness. By defining unfair conduct, a general clause sets a standard of behaviour referencing extra-legal concepts such as good morals, good faith, fair practices in industry and commerce, and professional diligence.[197] The concept of professional diligence in the UCPD, with its benefits and drawbacks, was analysed in Section II. The subsequent part of the report will advocate for consumer law to become the horizontal safety net for digital consumer concerns, as this appears to be the area to which the EU legislator pays the least attention.

3. What next: Retracing Steps or Forging Ahead?

3.1 Tackling the regulatory gap with the UCPD

It is not surprising to propose the UCPD as a horizontal safety net. According to the Commission, 'the UCPD works as a 'safety net', ensuring that a high common level of consumer protection against unfair commercial practices can be maintained in all sectors, including by complementing and filling gaps in other EU law.'[198] **The UCPD** also seems aptly suited to act as a horizontal safety net in the digital environment. While other legal tools are available, the inherent qualities of the UCPD, coupled with its track record of adapting to new commercial environments, its extensive scope, and a considerable body of case law at the national and EU levels, mark it as a preferred tool to offer comprehensive protection to consumers. Moreover, the UCPD already functions as a horizontal mechanism – the general prohibition of unfair commercial practices[199] with the underlying general clause based on the principle of professional diligence[200] covers all B2C commercial practices across different sectors. According to the Commission, the general clause of Article 5(2) UCPD even serves as an 'additional safety

195 Veale and Borgesius (2021), Demystifying the Draft EU Artificial Intelligence Act, Computer Law Review International, 4, para. 12; Helberger, Micklitz and Rott, 2021, p. 29.
196 R. Sack, 1985, pp. 1 et seq.
197 See e.g. S. Grundmann, 2006, pp. 141 et seq.
198 Guidance on the interpretation and application of the UCPD, p. 8.
199 Article 5(1) UCPD.
200 Article 5(2) UCPD.

net to capture any unfair practice which is not caught by other provisions of the UCPD (i.e. that is neither misleading, aggressive or listed in Annex I).'[201]

Given the UCPD's cross-sectoral reach, the label 'horizontal safety net' is fitting and self-explanatory. Nevertheless, the UCPD's role as a horizontal safety net for a vast range of digital activities involving consumers is not entirely evident, and not all consumer concerns can be effectively captured by a horizontal safety net. As elaborated in Section II, it is essential to acknowledge that professional diligence and, by extension, fairness serve as the **common denominator** for consumer protection in the digital environment. This research suggests that fairness emerges as a central principle of both consumer law and consumer-focused EU digital policy legislation. This insight naturally leads to deeper contemplation about the potential for a consumer's right to fairness.

It is widely recognised that the UCPD is **context-independent**, making it one of the most effective tools for addressing various challenges brought about by digitalisation and the rise of digital players.[202] Given that the UCPD already functions as a horizontal safety net, is there still a need for further refinement in this direction? The answer is a resounding yes, and legislative amendments at the EU level are inevitable. Prior research, specifically the 'EU Consumer Protection 2.0' and 'The Regulatory Gap' reports, highlighted significant difficulties in applying the UCPD to the digital sphere. Drawing from the insights presented in those papers, this study aims to adapt the UCPD to the digital context. Thus, any recommendations regarding its role as a horizontal safety net stem from this foundational premise: there is a need to mould the digital market with tailored regulation, taking into account the unique aspects of B2C commercial practices in the digital realm.

3.2 More than a horizontal safety net?

Defining digital professional diligence and incorporating it into the UCPD should enable its functioning as a horizontal safety net for digital consumer concerns. However, it is worth considering strengthening this mechanism, given the weaknesses associated with relying on this inherently vague term. Paradoxically, a source of inspiration for the digital environment in the ongoing 21st century can be found in century-old German and Polish legislation. This model revolves around the concept of '**breach of law**' (*Rechtsbruch*), which would serve as the basis for recognising a digital commercial practice as unfair. Admittedly, the question of whether a commercial action is unfair because it violates a legal provision has been and remains one of the most challenging and controversial aspects of fair trading law.[203] Nevertheless, the 'breach of law' concept enhances protection against unfair commercial practices by providing direction and illustrating the relationships between legal acts addressing this issue.

Referring to national solutions with a nearly 100-year history does not aim at perpetuating **tradition** but rather the opposite. Given the digital age, it is important to examine the reasons behind introducing the requirement 'against the law' into the Polish Act of 1993. At that time, the prevailing belief was that the political, economic, and legal situation following regaining independence and the transition to a market economy played a crucial role in designating

201 Guidance on the interpretation and application of the UCPD, p. 75.
202 Narciso, 2022, p. 148.
203 Köhler, 2021, section 1.1.

acts contrary to the law as a form of unfair competition. In these circumstances, there was a clear lack of well-established domestic jurisprudence which defined what constituted unfair competition. In such a landscape, indicating that behaviours contrary to existing law could also be considered unfair competition provided some clarity for the courts, at least to some extent. These assumptions hold particularly true considering the vague boundaries and disputes surrounding the essence, as well as the evolving views on good morals. Compared to them, existing legal provisions appeared more specific and unambiguous. It was also easier to determine which regulations are in force than which customs are considered good.[204]

The arguments referencing the historical situation in Poland during the 1990s can easily be **related to** the contemporary challenges concerning consumer protection in the digital environment. There is also a significant shift toward a digital economy without firmly established jurisprudence defining unfair digital commercial practices. As in the past, pinpointing behaviours that contravene existing laws can provide clarity to courts when determining what constitutes unfair digital practices. Indeed, it is often simpler to identify which regulations are in place than to discern practices that deviate from professional diligence. While several more arguments support this viewpoint, which will be discussed subsequently, they require careful consideration.

When conceptualising a potential solution for the UCPD, it is worth examining how the concept of 'breach of law' developed in **Germany and Poland** and how it evolved differently.

The precursor to today's **German regulation** was the category of 'competition infringement through breach of law', which was developed by the Reichsgericht (*Imperial Court of Justice*). Even within the old general clause of § 1 UWG 1909 (*Gesetz gegen den unlauteren Wettbewerb*, Act Against Unfair Competition), breaches of law could have been penalised as contrary to good morals. While jurisprudence generally did not attribute unfairness to a mere breach of the law, it was easily affirmed. The Reichsgericht and later the **Bundesgerichtshof** (BGH, Federal Court of Justice) differentiated between value-neutral and value-related norms. Value-related norms were those that expressed a basic moral perception. Such morally grounded norms included, for example, criminal law provisions or those for the protection of minors. On the other hand, a norm was merely value-neutral if it had been enacted solely for reasons of orderly expediency and did not represent an expression of a moral command or serve a particularly important common good. In this case, there had to be a deliberate and systematic disregard of the law for it to be deemed unfair.[205] Since 1997, the BGH has upheld the norm purpose theory (*Normzwecktheorie*) – the violation of a norm, even one that is value-related, does not meet the requirements of § 1 UWG if the norm does not have a secondary competition law protective function.[206]

The breach of law concept was explicitly introduced to the UWG only in 2008 as Section 4, point 11, and in 2015, it was moved to Section 3a.[207] According to **Section 3a UWG**, unfairness is deemed to have occurred where a person violates a statutory provision that is also intended to regulate market conduct in the interest of market participants, and the breach of law is capable

---

204 Jasińska, 2019, para. 49.
205 Köhler, 2021, section 1.1.
206 Schaffert, 2022, section 10.
207 Act against Unfair Competition in the version published on 3 March 2010 (Federal Law Gazette I, p. 254), as last amended by Article 20 of the Act of 24 June 2022 (Federal Law Gazette I, p. 959).

of significantly harming the interests of consumers, other market participants or competitors (*Unlauter handelt, wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln, und der Verstoß geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen.*).[208] The regulation is based on the premise that anti-competitive behaviour is not necessarily equivalent to violating the law, so the violation of the law should not automatically imply anti-competitive behaviour, as the UWG is not designed to penalise all types of legal violations.

The jurisprudence of German courts served as an inspiration for the Polish legislator. As early as in the first Act on Combating Unfair Competition in 1926, acts 'contrary to applicable regulations or good morals (merchant honesty)' were prohibited. A similar provision can be found in the subsequent **Polish Act on Combating Unfair Competition** (*Ustawa o zwalczaniu nieuczciwej konkurencji, UZNK*) of 1993. This technology-neutral legislation was designed to address unfair competition in B2B and B2C relationships.

Originally, Article 3(1) – a general clause similar to Article 5(2) UCPD – stated: 'An act of unfair competition is an action contrary to the law or **good morals** (*dobre obyczaje*), if it threatens or violates the interest of another trader or customer, especially consumer.' After implementing the UCPD into a separate legislative act in 2007 – the Act on Counteracting Unfair Market Practices – consumer protection was transferred to this act by removing the phrase 'especially consumer' from Article 3(1). However, the dual criteria of action contrary to the law or good morals – constituting a general clause to the concept of professional diligence – remained intact. Nevertheless, the breach of law concept does not have its counterpart in the law implementing the UCPD. The structure of the UZNK, which currently addresses B2B commercial practices, is similar to that of the UCPD, but it lacks a general prohibition equivalent to Article 5(1) UCPD. The Act has a two-tier structure: it includes the general clause in Article 3(1) and specific provisions but does not contain a black list.

One can argue that the **infringement of the law** can, as such, already fall under the prohibition of acting contrary to the (digital) professional diligence, rendering the addition of the breach of law concept redundant. However, this argument is oversimplified. The CJEU did not exclude a **parallel application** of the UCPD and the UCTD.[209] The Court held that a contractual practice violating the UCPD does not automatically qualify as unfair under the UCTD. Still, provided the contracting practice is to be regarded as an unfair commercial practice, this assessment must be considered one of the elements in the fairness test under the UCTD. German courts consider a violation of unfair contract terms law concurrently with a breach of unfair commercial practices law.[210] The Pereničová and Perenič doctrine is equally relevant when examining the interplay between the GDPR and the UCPD, and may be extended to other pieces of legislation, such as EU competition rules.[211] As the 'EU Consumer Protection 2.0' paper indicates, 'the overall purpose should be to seek a common denominator between the various fairness tests'.[212] Taking the UCPD as a benchmark, which is the case in this proposal, the assessment

208 Act against Unfair Competition, 2022, https://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html.
209 Case 109/17, Jana Pereničová and Vladislav Perenič, ECLI:EU:C:2018:735, para. 49, see Keirsbilck, 2021; Helberger et al., 2021, p. 60.
210 See Helberger et al., 2021, p. 61.
211 Guidance on the interpretation and application of the UCPD, pp. 8–10; Keirsbilck, 2021, pp. 247 et seq.; Alexander, 2012, pp. 515 et seq.
212 Helberger et al., 2021, p. 61.

is also not automatic. Instead, it should begin by determining whether a particular practice is a digital commercial practice. Furthermore, it is necessary to determine the impact of the practice on the consumer. Still, the assessment remains somewhat simplified, as it omits the test for inconsistency with digital professional diligence.

In the literature, there is a question about the inconsistency of the 'breach of law' concept with the UCPD and going beyond the **full harmonisation principle** on which the UCPD is based.[213] However, it loses its *raison d'être* if this concept is included in the Directive.

The **operationalisation** of a horizontal safety net for digital consumer concerns from the UCPD will be discussed in Section V as part of the broader concept of recalibrating the UCPD in the digital environment.

V. Concepts unleashed

1. Recalibration of the UCPD: Digital unfairness

1.1 Operationalisation of the digital unfairness concept

The proposals outlined in this Section form a comprehensive **package of changes** designed to shield consumers from digital unfairness. They necessitate a re-examination of the conventional understanding of consumer protection within the digital domain. These proposals do not necessitate discarding all existing principles. In fact, they draw partial inspiration from the UCPD. The UCPD already functions as a safety net, as highlighted by Article 5. Given the earlier discussion about the need to adjust the UCPD to the digital environment, it seems clear that introducing the proposed amendments into the UCPD is a logical initial step. This could eventually lead to the creation of the Digital Fairness Act as an independent piece of legislation.

From a regulatory technique perspective, the proposed solutions could be **incorporated into the UCPD** as new provisions with a new general clause. Alternatively, they could be categorised as new prohibitions listed in Annex I or placed under a separate section, for example, 'Digital commercial practices which are in all circumstances considered unfair.'[214] Due to the number of amendments, a separate chapter in the UCPD could also be considered, titled 'Unfair Digital Commercial Practices.' This chapter could follow a structure similar to Chapter 2 of the UCPD titled 'Unfair Commercial Practices,' including definitions and a new general clause to clarify the new general prohibition of unfair digital commercial practices.

A worthy consideration is a division into two levels of prohibitions: 1) a general prohibition with a general clause and 2) *per se* prohibitions of unfair commercial practices. The idea of a 2-tier structure was presented by the European Commission in 2012 for B2B relations within Directive 2006/114/EC, which would then consist of a general clause and a black list.[215] Thanks to

---

213 E.g. Köhler, 2021, sections 1.7 et seq.
214 Helberger et al., 2021, p. 79.
215 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Protecting businesses against misleading marketing practices

this solution, the general prohibition with a general clause would become a self-standing test, which is justified in the digital environment due to the difficulties in applying prohibitions of misleading and aggressive commercial practices to more complex digital commercial practices.[216] Looking further into the future, one can envision a separate legal act: the **Unfair Digital Commercial Practices Directive** (the UDCPD), the **Digital Fairness Act**, or even a new regulatory framework – EU Fair Trading Law 2.0 – as suggested by Galli.[217] As technological changes accelerate, the need for a systematic approach to new problems becomes increasingly urgent.[218]

It is worth adding that, unlike the sector-specific regulations, the UCPD should remain a **symmetric law** applying equally to all categories of traders.[219]

1.2 Digital commercial practices

Incorporating the paradigm of protection against unfair digital commercial practices into the UCPD first requires analysing whether the current definition of commercial practices is **sufficient** for addressing consumer interests' violations in the digital environment.

Due to the UCPD's focus on commercial practices, it has a broader scope than the CRD and UCTD, which focus on contracts and contract terms, respectively. The definition of commercial practice is also **extensive** and refers to 'any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers.'[220] Furthermore, the UCPD encompasses all commercial practices before, during, and after a commercial transaction, which the consumer may make or potentially make. The UCPD addresses commercial practices directly influencing consumers' transactional decisions regarding products.[221] The concept of transactional decision is broader than that of a contract, as it covers any decision directly related to the contracting decision.

The definition of a commercial practice is extensive but **not endless**.[222] Within a digital sphere, numerous activities of traders can be classified as commercial practices and evaluated for underlying unfairness. However, the distinction between the concept of commercial practices and digital services monetised not directly through remuneration paid by consumers is often blurred. Likewise, the classification of addictive designs or provision of a personalised experience by social media platforms,[223] or exploitation practices being a side-effect of contractual optimisation through machine learning[224] remain unclear.

---

and ensuring effective enforcement — Review of Directive 2006/114/EC concerning misleading and comparative advertising' COM(2012) 702 final.

216 See Trzaskowski, 2021, p. 83.
217 Galli, 2022, pp. 261 et seq.
218 Bennett Moses, 2007, p. 285.
219 See more on symmetric and asymmetric laws in Savin, 2022, pp. 7–8.
220 Article 2(d) UCPD.
221 Recital 7 of the UCPD.
222 Jabłonowska, 2022, p. 69.
223 Jabłonowska, 2022, p. 69.
224 Hacker, 2021, p. 10.

Consequently, refining the definition of commercial practice to incorporate characteristics specific to commercial practices in the digital realm may be unavoidable. This revision is particularly necessary as the main proposal involves modifying the general clause by adding the criterion of digital professional diligence. This would constitute one of the new provisions of the UCPD addressing digital unfairness, rendering them more operational. While expanding the current definition in Article 2(d) UCPD is conceivable, it may lead to a less transparent definition due to the amalgamation of technologically neutral elements and those unique to the digital environment. Therefore, a more effective solution entails introducing a new definition of **digital commercial practice**.

Yet, the definition of digital commercial practices may incorporate some elements from the current definition in Article 2(d) UCPD. In this situation, avoiding regulatory twins becomes challenging because some commercial practices share the same character, online and offline. To tailor the definition to the digital environment, it is worth adding that among the forms of digital commercial practices, there are also **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 but can also be connected indirectly.

1.3 General prohibition of unfair digital commercial practices

The idea proposed in Section 2 of introducing the concept of 'digital commercial practices,' which would change the scope of the general clause, requires enacting a general prohibition of unfair digital practices. This prohibition could be analogous to Article 5(1) UCPD, stating that '**Unfair digital commercial practices are prohibited**.' This prohibition would need to be specified similarly to Article 5(2) but taking into account the specificity of the digital environment, as will be discussed in the next subsection.

1.4 New general clause

As discussed throughout this Chapter, Article 5(2) UCPD defines unfair commercial practices using two criteria. An unfair commercial practice is a practice 1) that is contrary to the requirements of professional diligence and 2) that materially distorts or is likely to materially distort the consumer's economic behaviour. The research undertaken in this project underscores the need to **revise Article 5 UCPD** to address in a new general clause the concept of digital professional diligence,[225] accommodate the multifaceted nature of consumer harm,[226] and ensure it functions as a horizontal safety net.[227] Each of these elements will be presented below.

A) Digital professional diligence

Section II proposes introducing the concept of digital professional diligence into the UCPD. Considering the previously cited statement from the 'EU Consumer Protection 2.0' report that structural asymmetry **creates new professional duties and obligations** of professional

225 Section II.
226 Section III.
227 Section IV.

diligence in the sense of Article 5(1) and (2) UCPD[228] and the desire to avoid the pitfalls of regulatory twins, the definition of digital professional diligence may not simply replicate the definition of professional diligence in Article 2(h) ('Professional diligence means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity.'). Instead, it should refer to 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.

The definition of digital professional diligence refers to the fundamental characteristics of digital B2C relationships: **digital asymmetry** and **digital vulnerability**, explored by the 'EU Consumer Protection 2.0' paper. As a result, the definition directs persons and entities applying the UCPD to distinctive features of the digital world. These terms immediately convey the inherent power imbalances and potential areas of exploitation in digital B2C relations, and their definitions should also be introduced to the UCPD. They are not just terminologies; they resonate with the very ethos of the digital consumer marketplace, spotlighting areas where fairness is most at risk. The definition explicitly states what action (exploiting one or both elements) is considered a breach of digital professional diligence.

This proposal is also consistent with the European Parliament's resolution on **addictive design** of online services and consumer protection in the EU single market, in which the European Parliament demands that a revision of the UCPD takes into account 'consumers' susceptibility to the exploitation of the unequal power in the trader-consumer relationship resulting from internal and external factors beyond the consumer's control'.[229]

The definition of the new digital professional diligence concept sets clear responsibility benchmarks by emphasising the trader and their duty of **'not exploiting'**. The term 'exploiting' is heavily negatively loaded[230] and undeniably powerful. The notion carries a profound moral implication, discouraging behaviours that might disadvantage the consumer. This underlines the trader's responsibility not to take advantage of these digital specificities. Such a stance proactively advocates for consumer rights by setting clear limits for traders.

Furthermore, 'not exploiting digital asymmetry and/or digital vulnerability' echoes **the same traditional values** as 'being contrary to honest market practices and/or good faith'. The new definition weaves traditional values with contemporary challenges, establishing a solid foundation for equitable digital B2C interactions. Considering the trader's professional status, the standard of professional diligence may encompass anticipating how consumers are expected to react to specific commercial practices based on their expertise.[231] However, as new concepts, digital symmetry and digital vulnerability should be defined in the UCPD.

The definition follows a **prohibitive structure**, specifying what should not be done rather than what should be done. Combined with the general prohibition of unfair digital commercial

---

228 Helberger et al., 2021, p. 26.

229 European Parliament's Resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market, P9_TA(2023)0459.

230 According to Cambridge Dictionary, to exploit means to use someone or something unfairly for your own advantage. Exploit https://dictionary.cambridge.org/dictionary/english/exploit.

231 See in traditional offline context in Trzaskowski, 2016, pp. 43–44.

practices, which should be adopted concurrently, it becomes evident that digital commercial practice is unfair if it exploits digital asymmetry and/or digital vulnerability.

The definition is **concise** and avoids delving into extraneous details, making it more impactful and less prone to misinterpretation. It omits unnecessary legal jargon, making it understandable and applicable for stakeholders. While brevity is an advantage, as a general clause, it still allows for diverse interpretations. It offers flexibility to address various potentially unfair digital commercial practices, even as the digital landscape evolves.

In the proposed definition, there is **no mention of the commercial context**. This reference is achieved through the unfair digital commercial practices' notion, defined by the breach of digital professional diligence requirements. Moreover, the definition does not refer to 'not establishing digital asymmetry and/or digital vulnerability'. There is no consensus in the literature regarding the significance of 'establishing digital asymmetry and digital vulnerability,' specifically whether 'establishing' carries greater semantic weight.[232] In the context of the general clause, 'exploiting' appears more appropriate, as it suggests a connection with the violation of consumer interests. Instead of regulating specific processes or methods, the focus should be on the outcomes.

B) Consumer harm

Adjusting the UCPD to address consumer harms caused by unfair digital commercial practices is the next step to enhance consumer protection against digital unfairness. The lens of **economic behaviour is too narrow**.

Let us re-examine how the requirement for a commercial practice to impact consumer interests is currently shaped: 'A commercial practice is unfair if (...) it materially distorts or is likely to materially distort the economic behaviour with regard to the product (...).'[233] It is the **second requirement** in the unfairness test, besides being contrary to the requirements of professional diligence. So, how should the digital unfairness test be designed when it already concerns digital commercial practices, and the first condition is based on actions contrary to digital professional diligence?

Different options reflecting the need to consider non-economic interests are possible. **Four proposals** will be presented in the table and discussed below:

1. Table 2, Proposals

	De minimis **rule**	**Impact**	**Additional requirement**
Article 5(2)	A commercial practice is unfair if (...) it materially distorts or is likely to materially distort	the economic behaviour	with regard to the product
1.	A digital commercial practice is unfair if (...) it materially distorts or is likely to materially distort	consumer's behaviour	-
2.	A digital commercial practice is unfair if (...) it materially distorts or is likely to materially distort	consumer's behaviour	in a manner that it causes or is likely to cause harm

232 Simony, 2023, p. 250.
233 Article 5(2)(a) UCPD.

3.	A digital commercial practice is unfair if (...) it materially distorts or is likely to materially distort	consumer's autonomous decision-making	-
4.	A digital commercial practice is unfair if (...) it materially distorts or is likely to materially distort	consumer's autonomous decision-making	in a manner that it causes or is likely to cause harm

The above proposals divide the criterion of harming consumer interests into **three parts**:

1. They introduce a de minimis rule in each of the options;
2. As an impact, they specify either the distortion of consumer's behaviour or the consumer's autonomous decision-making;
3. They require or do not require causing harm to the consumer.

The **first part** consists of the ***de minimis* rule**, which remains unchanged from its current wording. This is an important requirement because every commercial practice somehow affects consumer decision-making in the trader's interest. Therefore, a balance of the different involved interests must be struck to determine which type of influence breaches professional diligence.[234] In this case, it is not just about any distortion but a significant one, which implies a substantive alteration in consumer behaviour or autonomous decision-making that would not have occurred in the absence of the said practice. Minor or negligible shifts in consumer behaviour that do not have profound implications will not qualify.

The **second part** of the criterion replaces the current requirement of impacting the consumer's economic behaviour. This criterion currently directly points to the economic focus of the UCPD. Its two versions should be considered.

The first one directly refers to the current wording and changes the scope of the UCPD solely by **removing 'economic,'** making it possible to encompass various changes in consumer behaviour caused by unfair digital commercial practices. The advantage of this solution is minimal linguistic interference with the current provision while simultaneously introducing a powerful change in the meaning. The relationship is not limited to a consumer's purchasing decisions or the economic behaviours of a consumer. It may also pertain to how consumers navigate an app, the time they spend on a platform, and their sharing of personal data. Moreover, some digital commercial practices may have a cumulative effect, subtly shaping consumer behaviours over extended periods. The new wording of this requirement takes it into account.

At the same time, the minor linguistic amendment is a **drawback** of the proposed solution. Firstly, removing only the word 'economic' may tempt the application of the current interpretation of Article 5(2)(a) UCPD. Secondly, as mentioned earlier, greater linguistic changes signal a paradigm shift in protection.

The second proposal is based on a significant linguistic change: replacing 'the economic behaviour' with the phrase '**autonomous decision-making**.' However, the advantage of this solution is not only a linguistic change. Such a designation precisely indicates the violated element of behaviour. Importantly, as demonstrated in Section III, even in the current requirement, 'distortion of economic behaviour' includes harm that violates the consumer's autonomous

234 Hacker, 2021, p. 12.

decision-making – currently in the form of the inability to make an informed decision (Articles 6 and 7) or violating freedom of choice or conduct (Article 8).

When considering this option, it should be noted that the concept of autonomy of consumer choice is **central to EU consumer law**.[235] Even so, the concept of autonomy has never been clearly defined.[236] Therefore, adopting this concept in the amended general clause would confirm the importance of this concept for consumer protection and initiate a thorough examination of its specification.

As for the **third part** of the requirement, it is optional. The proposed versions can either be self-standing or include an additional criterion related to the **necessity of causing harm** ('in a manner that it causes or is likely to cause harm'). This requirement implies a causal link between the distortion of behaviour or autonomous decision-making and the resulting harm. While distortion of behaviour and autonomous decision-making already cause harm, this phrasing highlights that it must lead to an adverse consequence.

In the above proposal, there is **no *de minimis* requirement** for harm, partly because harm can build up without a specific event surpassing a critical severity level, making it challenging to substantiate. These cumulated harms become increasingly reinforced over time.[237]

The main **advantages** of including harm violation in the UCPD are the proper filling of regulatory gaps and the harmonisation of concepts in various legal acts protecting consumers, whose diversity weakens this protection. As an example, we can mention the draft AIA, which was, in fact, a direct source of inspiration when it comes to including consumer harm in the UCPD, especially Article 5(1)(b) of the draft AIA. This provision concerns the exploitation of vulnerabilities by an AI system, a situation to be covered by the UCPD amendments aimed at adapting this legal act to the digital environment. Moreover, this provision is based on terminology known from the UCPD and takes into account a broad understanding of harm, not just economic harm. This provision aligns closely with option No. 2. However, the AIA does not mention autonomous decision-making, which is justified by the broader scope of the AIA, covering more than just consumer-related aspects.

The **drawback** of including harm infringements is using the concept of harm itself. The requirement to prove that consumers have suffered harm carries the risk of diminishing the current level of consumer protection.[238] This is an important argument in favour of the previous option. Nevertheless, the concept of harm will be present in other legal acts, so addressing it will be necessary.

C) Breach of law

The proposed legislative package aims to ensure the UCPD serves as an effective horizontal safety net in the digital environment. In other words, it should **close regulatory gaps** resulting from the fragmentation of protection measures in the new digital law, the lack of legislation, or inadequate legislation. This objective will be achieved by implementing a general clause

---

235 See more Jabłonowska et al., 2018, pp. 12–14; Fassiaux, 2023.
236 See Sax, Helberger and Bol, 2018, pp. 103, 130.
237 Veale and Borgesius, 2021, para. 12.
238 Abbamonte, 2006, p. 706.

based on the digital professional diligence concept. However, it will be fortified by incorporating the concept of a 'breach of law' into the general clause.

The proposal for this change to the UCPD can be based on a solution similar to the Polish one outlined in Section IV. The phrase 'and/or the law' could be introduced alongside the prohibition of actions contrary to digital professional diligence. Meeting the criteria of being contrary to the requirements of digital professional diligence and/or the law does not automatically render a digital commercial practice unfair. The **second requirement** – materially distorting a consumer's behaviour – must also be met.

As discussed in Section IV, the proposed revision of point a) is based on the assumption of a **common standard for (digital) professional diligence** in B2C relationships. While consumer concerns often fall under digital sector legislation beyond core consumer law, the new provision guarantees that businesses operating in the digital environment are equally accountable under the UCPD. Maintaining the relevance of the UCPD and its alignment with the broader legislative framework provides a dual-layered protection mechanism. The provision encompasses a wide range of actions and behaviours, referencing both the law and the new concept of digital professional diligence. The use of 'and/or' terminology 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.

The dual criterion of infringement of digital professional diligence and the law offers several advantages for consumer protection in the digital environment:

1. Referencing 'and/or the law' **directly points to other laws** addressing consumer harm caused by digital commercial practices. It provides an additional safeguard for appropriately addressing digital unfairness alongside the digital professional diligence concept. When any law is breached, it simplifies the application of the general clause, as there is no longer a need to prove the infringement goes against digital professional diligence, a new concept open to interpretation without sufficient precedent or detailed understanding. This reduces overreliance on jurisprudence, significantly strengthening consumer protection.
2. The proposed solution will enhance consumer protection when a particular legal act does not directly protect the **consumer's economic interest** against unfair commercial practices, such as the Audiovisual Media Directive.[239]
3. If an action does not violate other laws, this dual standard prompts us to consider the potential contradiction of **digital professional diligence**. This is where the horizontal safety net starts, ensuring that consumers are protected, even when existing laws do not specifically cover an issue or when it is not adequately addressed. It also ensures that no digital commercial practice in any sector can bypass the UCPD's protective measures, effectively closing regulatory gaps.
4. Shifting the emphasis to the UCPD allows for a solid foundation of the concepts of digital asymmetry and digital vulnerability – the **main concepts** for digital unfairness. Simultaneously, it avoids the necessity of interpretation within the context of the

239 BEUC, 2013, p. 8.

regulatory underground, as described in 'The Regulatory Gap' paper.[240] Certainly, this does not exempt one from necessary deliberations within the context of other legal instruments, notably the Four. Still, it allows the adoption of a more direct strategy within the UCPD.

5. Introducing the breach of law concept **simplifies the assessment** of unfairness, which is particularly important in the digital environment.
6. This solution can help **interpret newer digital laws**, offering guidance on fairness and consumer expectations. The references to established interpretations and prior cases make justifying any breach relatively straightforward.
7. The proposed solution allows for a **more consistent application** of various legislation addressing B2C digital unfairness across the EU Member States, benefiting both traders (by providing predictability) and consumers (by ensuring comprehensive consumer protection).
8. Such a solution is an additional layer of consumer protection, abstracting from different **enforcement methods** established by various legal acts, whose violation could constitute an unfair digital commercial practice, and from the doctrinal discussions about them.[241] National authorities already have experience enforcing the UCPD, which may be more favourable for consumers, although individual and collective enforcement still raise many doubts. Moreover, a potential limitation of this approach lies in the enforcement principles under the UCPD, particularly when juxtaposed against the more centralised enforcement elements found in digital sector legislation, such as the DSA and the DMA. The UCPD's enforcement mechanisms might appear demanding when confronting major market players. However, several considerations are worth noting. Firstly, many consumer protection authorities, such as the Italian Competition Authority (AGCM), have managed to navigate these challenges effectively, imposing fines on big players.[242] Secondly, not every infringement in the digital environment is an act of a big player, although their actions have the most significant impact on consumers.
9. The proposed wording of the new general clause will ensure that this provision can function as a **self-standing test** more frequently than the current Article 5.

Upon closer examination of the new general clause, it is noteworthy that the reference to 'the law' encompasses all B2C legislation that meets the criteria for regulating digital commercial practices. There is no need to **narrow** the term 'the law' to specific areas such as Union law, EU digital policy legislation, or consumer law. Such a limitation could be unjustified, resulting in claims that a specific legal act does not fall within the defined scope. Moreover, relevant provisions in EU Directives require transposition into national law. In the broad context of consumer law, we deal with both European and national laws.

Examples of 'the law' would include, among others, the GDPR, the DSA, the DMA, the DGA, the UCTD, and the CRD. These legal acts have **varying objectives** that neither need to be nor can be harmonised in any other manner. Adding 'the law' finally breaks down the boundaries between different consumer pieces of legislation, and between consumer law and other areas

240 Helberger, Micklitz and Rott, 2021, p. 37.
241 See Helberger, Micklitz and Rott, 2021, pp. 16–17.
242 In 2018, Facebook was fined 10 million EUR for withholding information about its data-sharing practices from consumers. In 2021, they were fined another 7 million EUR for not complying with the previous decision. Facebook fined again in Italy for misleading users over what it does with their data, 2021, https://techcrunch.com/2021/02/17/facebook-fined-again-in-italy-for-misleading-users-over-what-it-does-with-their-data/.

such as competition law or data protection law. This solution does not amend these pieces of legislation but address consumer issues. However, it is important to note that not every breach of the law will be considered unfair. Since we are dealing with unfair commercial practices law, the trader's action must constitute a digital commercial practice and must materially distort or be likely to materially distort the behaviour of a consumer.

The competent national authority responsible for evaluating unfair commercial practices should assess law infringement under the new general clause. **No prior evaluation** of law infringement under the relevant provisions is required. This principle is fundamental due to the different enforcement systems (public/private, individual/collective). Inspiration cannot be drawn from the regulatory technique in Article 1(7) DMA to enable national authorities to operate without conflicting with the EU level by prohibiting making decisions that 'run counter' to Commission decisions. Article 1(7) DMA relates to applying a single legal act by various bodies. Therefore, such an obligation is inappropriate when assessing two pieces of legislation. A single behaviour may be subject to multiple legal regimes, and there should be no chronological order in the application of these provisions.[243] The relevant provision must be included in EU digital policy legislation.

Using the UCPD as a horizontal safety net aligns with the principle of **proportionality** – it is appropriate for achieving the legitimate objectives pursued by the UCPD and does not go beyond the limits of what is necessary to achieve those objectives.[244] It does not expand the scope of regulation beyond what existing law stipulates. Unfair commercial practices are already prohibited under the UCPD. Still, a recalibration of this framework is essential.

1.5 Accompanying measures

The new concept of digital professional diligence can offer a robust framework for combating digital B2C unfairness as it stands out as a strong step in recognising and codifying the nuanced aspects of digital commercial practices. However, its implementation in real-world scenarios will greatly depend on **auxiliary provisions** such as the general prohibition of unfair commercial practices, definitions of digital asymmetry and digital vulnerability, the reformulation of the material distortion of economic behaviour of consumers being the second criterion of the general clause, and the expansion of the black list.

A) Black list of unfair digital commercial practices

When considering the need to enact regulations concerning unfair digital commercial practices, it is evident that one should not only contemplate a general prohibition with a general clause but also specific provisions in the form of prohibitions for various circumstances. The question pertains, among other things, to the justification for **expanding Annex I** to the UCPD, for example, in the form of a section within Annex I under the heading 'Digital commercial practices which are in all circumstances considered unfair.'

---

243 In relation to the Polish Act: Jasińska, 2019, para. 52.

244 Case C-547/14, Philip Morris Brands SARL and Others v Secretary of State for Health, ECLI:EU:C:2016:325, para. 165.

After the amendments introduced by the Omnibus Directive, Annex I to the UCPD includes four new commercial practices applicable in all circumstances, totalling **35 prohibitions**. These four new *per se* prohibitions address digital unfairness.[245] However, to put it plainly, the effectiveness of the black list in combating unfair digital practices is still limited,[246] even though the CJEU does not rule out applying prohibitions intended for the offline world to the digital environment.[247] For the reasons discussed above, this is not an optimal solution. The question arises whether expanding the black list for the digital environment should be proposed to enhance consumer protection.

The general clause and the black list are **contrasting legal tools** in terms of precision. The distinctions between them boil down to the fact that the general clause defines standards of behaviour, whereas a black list establishes rules.[248]

The black list as a regulatory technique is often criticised. Despite its goal to safeguard consumer interests, its rigid nature often garners negative feedback. The most serious criticism is based on the argument that the black list is an extreme form of **interference with the autonomy of will**, tying the hands of judges, enforcement authorities, and legislators in the EU Member States.[249] Milder critics argue that ambiguous formulations of prohibitions weaken the benefits of the black list. Thus, the more detailed the regulation, the easier it is to apply.[250] At the same time, the literature presents arguments criticising excessive detail in legislation.[251] The risk of circumventing detailed provisions is also highlighted, which can, however, be impeded by meticulous legislative techniques, ensuring clarity and comprehensiveness of the prohibition.[252] The length of the black list in the UCPD is ambiguous in its assessment – it is easier to adapt to a shorter list. A longer list increases the market-cleansing effect but can lead to critique due to **overregulation**[253] and the arbitrary selection by the legislator of prohibited practices.[254] This argument, though, only means that arbitrariness occurs at the stage of creation, not the application of the law, meaning that the assessment of the fair nature of the practice is transferred to the legislator, not the enforcing bodies, as in the case of general clauses requiring concretisation.[255] Nevertheless, the strong harmonising effect of the black list is reduced by differing transposition into national laws.[256]

---

245 No. 11a: 'Providing search results in response to a consumer's online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of products within the search results.'; No. 23a: 'Reselling events tickets to consumers if the trader acquired them by using automated means to circumvent any limit imposed on the number of tickets that a person can buy or any other rules applicable to the purchase of tickets.'; No. 23b: 'Stating that reviews of a product are submitted by consumers who have actually used or purchased the product without taking reasonable and proportionate steps to check that they originate from such consumers.'; No. 23c: 'Submitting or commissioning another legal or natural person to submit false consumer reviews or endorsements, or misrepresenting consumer reviews or social endorsements, in order to promote products.'

246 See Helberger and al., 2021.

247 Case C-371/20, Peek & Cloppenburg KG, v Peek & Cloppenburg KG, ECLI:EU:C:2021:674, para. 43.

248 E.g. Ehrlich and Posner, 1974, p. 258; Kaplow, 1992, pp. 557 et seq. See also Cafaggi, 2013, pp. 10–11.

249 Caruso, 2013, pp. 292–293. See also Oechsler, 2019, p. 138.

250 Naudé, 2007, p. 133.

251 Wadlow, 2012, p. 5.

252 Howells, Twigg-Flesner and Wilhelmsson, 2018, p. 55.

253 Keirsbilck, 2011, p. 387.

254 de Vrey, 2006, p. 70.

255 See Ehrlich and Posner, 1974, p. 261.

256 See more Namysłowska, 2022a.

The UCPD mentions **one reason justifying** this legal tool. According to Recital 17, the advantage of the black list is to provide greater certainty, which results from its harmonising effect. Enhancing legal certainty, in turn, contributes to the proper functioning of the internal market. However, the UCPD does not specify whose legal certainty would be increased. The UCPD mentions in the context of all its provisions the legal certainty of businesses, as both consumers and businesses can benefit from 'a single regulatory framework based on clearly defined legal concepts,'[257] reconciling the objectives of legal certainty and regulatory elasticity.[258]

And indeed, both sides of the B2C relationship **benefit** from the list of *per se* prohibitions. Businesses can relatively easily perform **ex-ante** assessments using the black list, which cannot be achieved with the vague terms of the general clause,[259] thus avoiding legal inconsistencies. The black list is significant for new markets where the line between fairness and unfairness is unclear. Businesses gain confidence that their competitors are in a similar situation.[260] Additionally, consumers benefit by knowing which practices directed towards them are prohibited. It provides harmonisation through examples.[261] Since the black list results in *ex-ante* action, allowing for the removal of banned commercial practices from the market, there is a likelihood that consumers will not encounter some unfair actions. The Commission also acknowledges law enforcement authorities as beneficiaries of the black list.[262] *Per se* prohibitions free them from assessing unfairness based on a hard-to-interpret general clause, limiting interpretation errors[263] and reducing the costs of applying the law, especially due to less frequent and shorter court proceedings, which is significant from an economic perspective.[264]

Considering the advantages of the black list, particularly in the digital age, the issue of **adapting** Annex I to the current realities is essential.[265] The Commission seems to increasingly appreciate *per se* prohibitions, judging by the proposal for a Directive amending the UCPD and the CRD as regards empowering consumers for the green transition.[266] It proposes the expansion of Annex I by ten prohibitions. For strengthening protection in the digital environment, two amendments by the European Parliament are significant: new point 7a '(i) giving more prominence to certain choices when asking the recipient of an online service for a decision' and '(ii) making the procedure of terminating a service significantly more burdensome than signing up to it'.[267] Advocating for further *per se* prohibitions, such as those indicated in the 'EU Consumer Protection 2.0' paper,[268] thus fit into the regulatory trend. The adaptability of the UCPD will determine their effectiveness in safeguarding interests in the digital age.

Theoretically, the entire legal system could be based on a general clause. Even so, regarding the UCPD, caution should be exercised regarding **overreliance** on the (digital) professional

257 Recital 12 of the UCPD.
258 Anagnostaras, 2010, p. 147.
259 Naudé, 2007, pp. 131–132; Stumpff, 2016, p. 666.
260 Naudé, 2007, p. 133. See in relation to a grey list Beale, 1995, p. 246.
261 H. Collins, *Harmonisation by Example*..., p. 110.
262 Guidance on the interpretation and application of the UCPD, 2021, pp. 60–71.
263 Ehrlich and Posner, 1974, p. 267.
264 Ehrlich and Posner, 1974, pp. 265–266; Kerber, 2021, p. 29; Larouche and de Streel, 2021, p. 556.
265 See also Galli, Algorithmic Marketing, 2022, pp. 272–273.
266 Proposal for a Directive of the European Parliament and of the Council amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and better information, COM/2022/143 final.
267 See Rosca (2023).
268 Helberger and al., 2021, p. 79.

diligence concept as a tool for defining (digital) unfairness. Faced with difficult-to-understand technological changes, both for businesses and decision-making, it is unclear what constitutes fair behaviour and what does not.[269] Given the latest market challenges, provisions of the most detailed nature need to take precedence, even though it is impossible to enact new laws for every situation,[270] and the more detailed a provision is, the more often it will need to be changed.[271] General clauses should be accompanied by specific provisions, especially *per se* prohibitions. A **mixed normative approach** best serves those applying the law.[272] At the time of enacting the UCPD, such a hybrid concept was innovative.[273] After 18 years, it has stood the test of time. However, striking a balance between the flexibility of the general clause arising from the use of vague concepts and legal certainty is one of the most significant issues in the discussion about the appropriate legislative technique to be employed when regulating the market,[274] especially concerning consumer protection.[275]

Aside from the relatively easy ways to circumvent the overly prescriptive black list, the most significant criticism is the **lengthy legislative process** that hinders the introduction of new commercial practice prohibitions that have only recently emerged and pose the greatest threat to consumer autonomy. As the digital landscape changes rapidly, Annex I to the UCPD may become obsolete. The next subsection presents a possible solution – amendments through a comitology procedure, already briefly mentioned in the 'EU Consumer Protection 2.0' paper.[276]

B) Comitology procedure

The proposed (r)evolution of the UCPD brings the risk that specific provisions, particularly *per se* prohibitions, could quickly become outdated. Given the ever-changing nature of the market, certain commercial practices requiring regulatory oversight may soon be rendered obsolete or give way to newer commercial practices. The legislative process is lengthy and may struggle to keep pace with such rapid market changes. Creating an agile legislative framework that can respond promptly is significant. Hence, there is a discernible need for more streamlined legislative procedures **beyond the conventional amendments** of EU legal acts.[277]

A potential solution to the time-intensive legislative process is the Commission's use of delegated acts under Article 290 TFEU. **Delegated acts** can offer a more agile and responsive mechanism to address emergent issues without requiring a complete legislative overhaul. It can bridge the gap between static legislative provisions and dynamic market evolutions. According to Article 290(1) TFEU, a legislative act may delegate to the Commission the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act. Legal literature mooted this approach, especially in discussions around the draft P2B Regulation.[278] In the areas under current review, the EU's legislative approach has recognised this regulatory instrument in the DSA, the DMA and the draft AIA.

---

269 Ehrlich and Posner, 1974, p. 261.
270 Stumpff, 2016, p. 650.
271 Ehrlich and Posner, 1974, p. 278.
272 Ohly, 2018, pp. 91–92.
273 Anagnostaras, 2010, p.147.
274 Grundmann, 2006, pp. 158 et seq.
275 Paterson and Brody, 2015, pp. 352–353.
276 See Helberger et al., 2021.
277 See also Savin, 2022, pp. 13–14.
278 de Streel, 2021, p. 22.

A point of contention remains regarding whether modifying or supplementing the list constitutes an alteration of non-essential elements of the legislative act. The distinction between **essential** and **non-essential** elements is vague. Recent regulatory shifts suggest a broadened interpretation of 'non-essential'. Elements categorised as 'non-essential' can undergo both modifications and enhancements. This solution allows the Commission, operating within its granted discretion, to amend existing provisions and introduce new stipulations that augment the Union legislator's partial regulation of specific sectors.[279]

The DMA proposes issuing delegated acts after conducting a thorough market analysis, which leads to the critics of this procedure as too time-consuming.[280] Nevertheless, the key lies in finding an optimal **balance between comprehensive analysis** and **swift action**. Applying the comitology procedure carefully and thoughtfully to the UCPD would significantly enhance the effectiveness of the protective framework[281] while preserving legal certainty.[282]

C) Others

The abovementioned changes related to digital unfairness necessitate numerous **modifications within the UCPD and beyond**. Some of these issues, such as digital vulnerability, have been addressed in the 'Consumer Protection 2.0' report. Others require additional research, especially those on enforcement, which is partly the subject of this report. Within the scope of this chapter, one can point to the problem concerning compensation for damage suffered in the case of broadening the scope of consumer harm protected under the UCPD. However, even with solely economic interests being protected, such a problem arises.[283] In the transposition of Art. 11a(1) UCPD, it is possible but not obligatory to provide compensation for immaterial loss in domestic law.[284] Additionally, among other things to consider is the clarification of Article 3(4) UCPD, and the introduction of a provision stating: 'In the absence of specific provisions on digital commercial practices, the provisions on commercial practices should apply accordingly.'

The proposed amendment requires **amendments in other legal acts** to avoid preclusionary effects. For instance, the already contentious Article 25(3) DSA, establishing the principle that the prohibition of deceptive online interfaces in Article 25(1) does not apply to practices covered by the UCPD and the GDPR, would have to be repealed. An explicit provision such as 'This Regulation/Directive should be without prejudice to Union law on consumer protection, in particular....' should be included in the normative part of a Regulation/Directive, like in Article 2(4)(f) DSA.

---

279 COM(2009) 673 final Communication from the Commission to the European Parliament and the Council Implementation of Article 290 of the Treaty on the Functioning of the European Union, p. 5.
280 Podszun, Bongartz and Langenstein, 2021, point III; Monti, 2021, pp. 10–11.
281 In relation to the DMA see Kerber, 2021, p. 30
282 In relation to the DMA see Chirico, 2021, p. 497.
283 Alexander, 2023, pp. 327–336.
284 Alexander, 2023, p. 330.

2. Beyond the UCPD: Digital fairness

2.1 From digital unfairness to digital fairness

The analysis undertaken in this Chapter, coupled with the ideas put forth, centres on the operationalisation of the prohibition of digital unfairness. This endeavour has shed light on the myriad challenges inherent to our digital epoch. In confronting this complex landscape it becomes apparent that a sole, albeit comprehensive, focus might not be adequate for an all-encompassing reform. The foundational principles we adhere to today might necessitate **re-evaluation** soon. This calls for more than mere adaptability; it demands a forward-looking perspective that surpasses the scope of the above proposals on digital unfairness.

In parallel or as a subsequent step, our emphasis must, therefore, pivot to the redefinition of consumer law, ushering in the paradigm of **digital fairness**. This concept could be manifested, among others, as **digital fairness by design**. This paradigmatic shift encourages a broader interpretation of fairness, transcending mere regulatory compliance. The metamorphosis of consumer law should not only grapple with the current difficulties posed by the digital age but also preempt potential future obstacles. Adopting such a proactive approach could ensure that our legal framework keeps pace with the ever-evolving contours of technology and digital practices.

2.2 The concept of digital fairness

In previous reports commissioned by BEUC, the term 'digital fairness' appeared only two times.[285] This lack of focus is understandable because the UCPD, which serves as a starting point for discussions on consumer law, speaks of unfairness. Unfair commercial practices are prohibited. What is not prohibited by the UCPD is considered fair and, as a result, allowed. This stance is justifiable as consumer law introduces limitations on the freedom of economic activity. Therefore, there needs to be a justification for consumer law and a balance between consumer rights and business activities, especially considering the assurance of fostering innovation nowadays.

Digital fairness is a concept that is gaining popularity as a standard of fairness in the digital environment. This is especially the case thanks to the Fitness check on EU consumer law, which includes the term 'digital fairness' in its title. The need to ensure 'a fair digital environment' has also been emphasised in the **European Declaration on Digital Rights and Principles for the Digital Decade** issued by the European Commission.[286]

Before delving into the content of digital fairness, it is essential to consider the relationship between digital fairness and digital unfairness. As repeatedly stated in this Chapter, the prohibition of unfairness demands abstaining from acting unfairly. The positive obligation to act fairly elevates expectations towards traders.[287] In this context, traders are obliged to proactively seek ways to act fairly. Thus, without further ado, it can be asserted that digital fairness is **not a simple opposite of digital unfairness**.

---

285 Helberger, Micklitz and Rott, 2021, p. 26.
286 European Declaration on Digital Rights and Principles for the Digital Decade, OJ C 23, 23.1.2023, pp. 1–7.
287 Siciliani, Riefa and Gamper, 2019, p. 188.

There may be arguments against operationalising the digital fairness concept, deeming it highly controversial. Opponents could argue that this principle intrudes more into traders' rights than the prevailing emphasis on digital unfairness. This Chapter, however, has presented arguments highlighting the stark differences between the offline and digital worlds and the negative effects of current commercial practices on consumers. These discussions underscore the need for differing legal regulations for the analogue and digital realms, which the European Court of Human Rights supports. As such, there is a clear justification for increased intervention to ensure digital fairness. This embodies the balance of interests between traders and consumers. If the digital asymmetry surpasses the asymmetry seen between businesses and consumers in the offline world, it provides grounds for **more significant legislative intervention** against unfair digital commercial practices. A secondary but noteworthy point is that in the digital sphere, there is no risk of interventions perpetuating consumers' moral hazard – that is, hindering them from learning from past mistakes.[288] The complexities of unfair digital commercial practices prevent such an outcome.

In other words, the digital environment justifies introducing the digital fairness principle. However, it would be more challenging to justify the proportionality of such an obligation in B2C relationships in the **offline world,** although it is also advocated.[289]

Filling the concept of digital fairness with content is as complex a task as defining what digital unfairness is. There are many solutions, and the following suggestions are merely a **starting point** for further research studies. The only certainty is that the appropriate interpretation of existing regulations is out of the question, so new regulations are necessary. Consideration should be given to the positive duty to trade fairly in the digital environment. This will change the perspective and result in a move away from the double negative obligation not to trade unfairly.[290] A broad definition may challenge traders to think critically about what professional diligence means in their specific context, encouraging them to elevate their standards continuously.

More specifically, one can begin defining the obligation for digital fairness by negating the current prohibition against unfair actions. Such a mandate could be based on the need to act according to **digital professional diligence**, meaning not exploiting digital asymmetry and digital vulnerability. For reasons extensively discussed earlier, referring to concepts known from pre-digital unfair practices law is not advisable.[291]

Regarding the placement of such a change, an optimal solution would be the introduction of the **Digital Fairness Act**, emphasising the shift in perspective already in its name. Amendments to existing legislation, especially the UCPD, are not recommended. While one can imagine a dual standard of unfairness for the analogue and digital worlds, as proposed earlier, legislation maintaining a dichotomy of a standard of digital fairness for the digital environment and a prohibition of unfairness for the analogue world would not be an effective legislative tool.

---

288 Such a risk can occur in analogous context. See Siciliani, Riefa and Gamper, 2019, p. 182.
289 Siciliani, Riefa and Gamper, 2019, pp. 179 et seq.
290 Siciliani, Riefa and Gamper, 2019, p. 187.
291 Regarding such proposals, for example, the reference to acting in accordance with the principle of good faith and fair dealing see Siciliani, Riefa and Gamper, 2019, p. 188.

There is also a need to address the question of whether the obligation of digital fairness should vary based on the size of the enterprise. In a horizontally-focused act concerning fairness, such as the Digital Fairness Act, **differentiation based on company size** is not recommended, as will be elaborated below.

However, the question of whether digital fairness might require a common standard of care that applies even beyond consumer-facing services cannot be answered within this report, as it requires further research into the relationship between **B2B and B2C** unfairness, the necessity of which was pointed out in Section I.

2.3 Overarching principle: Digital fairness by design

The standard digital fairness can also be operationalised by introducing the concept of **fairness by design**. Proposals for 'by design' regulation against unfair commercial practices have already appeared, such as 'non-manipulation by design',[292] 'fair marketing by design',[293] 'fair design obligation',[294] 'consumer protection by design'[295] and, indeed, as 'fairness by design'.[296]

Introducing the principle of fairness by design represents a groundbreaking step in protecting consumers from unfair digital commercial practices. It signifies a departure from the traditional ex-post regulatory model where prohibited behaviour is followed by sanctions.[297] Without listing all the benefits of this solution, it can be pointed out that it would encourage a proactive approach in anticipating and addressing potential harm to consumers, thus fostering a fair and trustworthy digital consumer marketplace. Fairness by design would be a horizontal obligation with a broad scope. Examining the evolution of the **'by design' concept is worthwhile** to support this idea.

The regulatory concept of 'by design' in the context of challenges related to new technologies in the area of fundamental rights concerning privacy was developed by Ann Cavoukian as **privacy by design**. This concept results from efforts aimed at embedding the practice of considering privacy in new projects as both a philosophical and practical response to the difficulties in ensuring adequate privacy protection in the face of rapidly evolving technology. It is based on seven principles: 1) a proactive approach, not reactive: preventive, not remedial; 2) privacy as the default setting; 3) privacy embedded into the design; 4) full functionality understood as achieving a positive-sum, not a zero-sum; 5) privacy protection throughout the entire lifecycle of the data involved; 6) transparency and visibility; and 7) respect for user privacy.[298]

This is a horizontal concept of a procedural nature aimed at aligning protective requirements with business objectives and embedding assessment as a constant evaluation element when creating and using new solutions. This approach allows for placing the human being at the centre of attention when designing, for example, new solutions, processes, and tools using modern technologies. Focusing the assessment perspective on the human allows for the

---

292 Hacker, 2021, pp. 29–31.
293 Willis, 2020, pp. 187 et seq.
294 Resolution on addictive design, point 8.
295 See Lubasz, Jabłonowska and Namysłowska (forthcoming).
296 E.g. BEUC, 2023, pp. 4 et seq.
297 Savin, 2022, p. 5.
298 Cavoukian, 2011.

simultaneous realisation of the postulate of striving for technology to regain trust and incorporating mechanisms to ensure this into the design (**trust by design**).[299]

Cavoukian modified the original concept, pointing to the need for ethical construction of tools utilising AI mechanisms (**AI ethics by design)**. The fundamental elements of this concept became: 1) transparency and accountability of algorithms; 2) ethical principles applied to the treatment of personal data; 3) algorithmic oversight and responsibility; 4) respect for privacy as a fundamental human right; 5) data protection/personal control via privacy as the default; 6) proactive identification of security threats, thereby minimising harms; 7) strong documentation facilitating ethical design and data symmetry.[300] The basic procedural approach of integrating compliance objectives into the process remained unchanged, and in this sense, this concept is functionally universal.

The 'privacy by design' concept was implemented as a regulatory instrument in Article 25(1) GDPR. **Data protection by design** exhibits some specificity arising from the scope of protection related to the application of its provisions. However, the procedural approach presented by Cavoukian is also present in the GDPR. The analytical process underlying the discussed obligation is multi-stage, starting from determining organisational needs, i.e., the purpose of the project, defining assumptions and determining circumstances, scope, the layer of tools, through specifying requirements, including regulatory ones, which the project must meet, and ending with an assessment of the impact of the above factors on rights and freedoms. This is the basis for properly developing and implementing the project.

Effectiveness is a central element of this concept. The requirement for effective implementation means that every measure should achieve the intended results from the perspective of assessing compliance with regulatory requirements. Therefore, whether specific measures are effective will depend on the context of a given situation. Thus, compliance assessment is shifted from the level of regulation (moving away from rigid, uniform requirements for all entities on the market or groups of entities) to the level of a specific case of a particular entrepreneur. This also means that the addressees of the norms bear the burden of proving that they have ensured adequacy and that the implemented measures and safeguards produce the desired effect.[301]

The implementation philosophy of the data protection by design requirement is fundamentally based on Deming's cycle, which organises implementation actions in the logical order of successive activities **P-D-S-A** (Plan-Do-Study-Act), taking into account the accountability principle at each stage. This concept assumes a deep reflection on the key elements of the project, including the testing and verification phases before implementation, followed by continuous improvement of the implemented solution.

Such an approach is present in other legal acts, for example, in the draft AIA. The European Parliament proposed the introduction of an impact assessment for fundamental rights for high-risk AI systems (FRIA – fundamental rights impact assessment).[302] The solution approved in the trilogue is also a horizontal obligation for a contextual assessment of the use of AI, encapsulated in a multi-stage analytical process.

---

299 Chomiczewski and Lubasz, 2020, pp. 67 et seq.
300 Cavoukian, no date.
301 European Data Protection Board, 2020, p. 7.
302 Article 29a of the draft AIA.

All these models, apart from the one used in the DMA,[303] have a **horizontal character** and apply regardless of subjective criteria. The key to them is a contextual approach, i.e., the assessment and measures implemented depend on the situation of the specific obligated entity. This best reflects the principle of proportionality shifted from the level of more or less arbitrary regulation to the level of individual players.

The 'by design' concept should be applied to fairness in the next legislative step. Most importantly, fairness by design should be introduced as a horizontal principle. Traders will not use the same measure but one adequate for the threats to consumer rights arising from traders' market behaviours. **Proportionality** is fully applied – different compliance measures will be applied for small and large enterprises. This solution fits into European policy and the risk-based approach extended to more and more areas. It also allows for a full assessment of the context of action, in this case, the digital specificity that changes over time, as it is a continuous process (Deming cycle) and not a one-time event.

The arguments **against horizontal fairness by design** are predictable: lack of understanding and knowledge to choose the right analytical method, lack of tools, implementation costs, and a shortage of experts. However, it is hard to understand why these would outweigh the need to ensure consumer protection in the digital reality.

In concluding this Section it is clear that the legal landscape must adapt dynamically to mirror the complexities of the digital era. As we stand at this crossroads, balancing historical standards and future necessities, we must advocate for principles ensuring effective consumer protection. Some of these were proposed in this Chapter – from innovative solutions such as defining 'digital professional diligence' to groundbreaking ones like introducing the principle of 'fairness by design.' Yet, there are still many issues to analyse, including the need for establishing a consumer right to fairness by design.[304] In the evolving landscape of legal discourse, we may refer again to the Deming cycle, this time metaphorically – regulating fairness is a continual process, not a one-time achievement.

303 Rectial 65 DMA.
304 BEUC, 2023, p. 26.

VI. Final conclusions: Like Phoenix from the ashes

The adoption of the UCPD in 2005 was regarded as a revolutionary step in the development of consumer protection law.[305] At that time, it was even described as 'one of the most significant pieces of legislation to emanate from Brussels'.[306] Five years later, the taste of the UCPD was only bittersweet.[307] The Directive, which had the potential to become the most important piece of consumer law, is languishing in **obsolescence**, albeit not a planned one. After 18 years since the UCPD's enactment, the world looks entirely different. The issues related to the digital age presented in this Chapter are not intended to provide a dystopian view into the consumers' future. However, balancing the benefits and harms of digitalisation is not straightforward within the context of today's consumer law.[308] The UCPD could be rescued by meticulously interpreting digital consumer rights infringements, but it is an increasingly challenging intellectual journey. Facing the rapid digital transformation, it is no longer akin to navigating a maze but more like traversing a road with no exit.

This chapter is based on the assumption that a holistic and teleological interpretation of existing laws is not sufficient.[309] It includes a proposal for the **redefinition of the general clause**. In particular, it is necessary to:

1. Introduce a general prohibition of unfair digital commercial practices along with the definition of 'digital commercial practices.'
2. Create a definition for 'digital professional diligence.'
3. Establish a general clause similar to Article 5 UCPD, based on the contradiction with the requirements of digital professional diligence.
4. Expand the scope of consumer interests protected by the UCPD.
5. Introduce the concept of 'breach of law' into the new general clause.
6. Create a black list of unfair digital commercial practices.
7. Implement the comitology procedure.

The recommendations can be summarised as tailoring the UCPD to the digital environment. In the second place, we should consider the conceptualisation of **digital fairness** and the operationalisation of **fairness by design**.

This Chapter offers a preliminary analysis of just one issue pivotal for restarting consumer law. Yet, as the entire report and previous research studies indicate,[310] several other challenges await to be addressed. The UCPD indeed requires a reinvention, signalling a **paradigm shift**. We also need a shift in our mindset regarding consumer law. Just as the Phoenix is reborn from its ashes, the unfair commercial practices law can redefine its future. The imperative for this transformation is voiced by consumers, championed by the market, and echoed by the digital society.

---

305 Anagnostaras, 2010, p. 148.
306 Howells, Micklitz and Wilhelmsson, 2006, p. 13.
307 Anagnostaras, 2010, p. 170.
308 Wagner, Eidenmüller, 2019, in particular pp. 607–608.
309 This concept is advocated by e.g. Trzaskowski, 2016, p. 12.
310 See Helberger et al., 2021; Helberger, Micklitz and Rott, 2021.

VII. References

1. Abbamonte, G. B. (2006) 'The Unfair Commercial Practices Directive: An Example of the New European Consumer Protection Approach', *Columbia Journal of European Law*, 12, pp. 695–713.
2. Alexander, Ch. (2012) 'Vertragsrecht und Lauterkeitsrecht unter dem Einfluss der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken', *Wettbewerb in Recht und Praxis,* 5.
3. Alexander, Ch. (2023) 'Unfair Commercial Practices and Individual Consumer Claims for Damages – The Transposition of Art. 11a UCP Directive in Germany and Austria', *Gewerblicher Rechtsschutz und Urheberrecht International,* 72(4), pp. 327–336.
4. Anagnostaras, G. (2010) 'The Unfair Commercial Practices Directive in Context: From Legal Disparity to Legal Complexity?', *Common Market Law Review*, 47(1), pp. 147–171.
5. Bakardjieva Engelbrekt, A. (2017) 'The Impact of the UCP Directive on National Fair Trading Law and Institutions: Gradual Convergence or Deeper Fragmentation?' in: Bernitz, U., Heide-Jørgensen C. (eds.), *Marketing and Advertising Law in a Process of Harmonisation*, Oxford: Hart Publishing.
6. Beale, H. (1995) 'Legislative control of fairness: The Directive on Unfair Terms in Consumer Contracts' in: Beatson, J., Friedmann, D. (eds.), *Good Faith and Fault in Contract* Law, Oxford: Clarendon Press.
7. Bennett Moses, L. (2007) 'Recurring Dilemmas: The Law's Race to Keep up with Technological Change', *University of Illinois Journal of Law, Technology and Policy*, 21.
8. BEUC (2013) 'European Commission's report on the application of the Unfair Commercial Practices Directive BEUC position paper', Available at: https://www.beuc.eu/sites/default/files/publications/2013-00457-01-e.pdf
9. BEUC (2023a) 'Towards European Digital Fairness BEUC. Framing response paper for the REFIT consultation', Available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf (Accessed: 20 September 2023).
10. BEUC (2023b) 'Each Consumer a Separate Market? BEUC position paper on personalised pricing', Available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-097_Price_personalisation.pdf (Accessed: 20 September 2023).
11. BEUC (2023c) 'Connected but unfairly treated. Consumer survey results on the fairness of the online environment', Available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.pdf (Accessed: 20 September 2023).
12. Cafaggi, F. (2007) 'Which Governance for European Private Law?', *EUI Working Papers. Law.* Available at: https://ssrn.com/abstract=1024110 (20 September 2023).
13. Caruso, D. (2013) 'Black Lists and Private Autonomy in EU Contract Law' in: Leczykiewicz, D., Weatherill, S. (eds.) *The Involvement of EU Law in Private Law Relationships*, Oxford: Hart Publishing.
14. Cauffman, C., Goanta, C. (2021) 'A New Order: The Digital Services Act and Consumer Protection', *European Journal of Risk Regulation*, 12(4), pp. 758–774.
15. Cavoukian, A. (2011) 'Privacy by Design. The 7 Foundational Principles', Available at: https://www.torontomu.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf (20 September 2023).
16. Cavoukian, A. 'AI Ethics by design', Available at: https://www.torontomu.ca/content/dam/pbdce/papers/AI_Ethics_by_Design.docx (20 September 2023).

17. Chirico, F. (2021) 'Digital Markets Act: A Regulatory Perspective', *Journal of European Competition Law & Practice*, 12(7), pp. 493–499.
18. Chomiczewski, W., Lubasz, D. (2020) 'Privacy by design a sztuczna inteligencja', *Monitor Prawniczy*, 20, pp. 86–95.
19. Cox, M. 'Activating EU Private Law in the Online Platform Economy' in: Tridimas, T., Durovic, M. (eds.) *New Directions in European Private Law,* Oxford: Bloomsbury Publishing.
20. Department for Digital, Culture, Media and Sport (2023) 'Digital consumer harms – A taxonomy, root cause analysis and methodologies for measurement', Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1129431/DCMS_consumer_harms_research_01-Jan-22.pdf (20 September 2023).
21. Digital fairness – fitness check on EU consumer law (2022) Available at; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en (20 September 2023).
22. Duivenvoorde, B. (2023) 'Redesigning the UCPD for the Age of Personalised Marketing', *Journal of European Consumer and Market Law*, 5, pp. 177–184.
23. Durovic, M. (2016) *European law on unfair commercial practices and contract law*, Oxford: Hart Publishing.
24. Ebers, M., Hoch, V.R.S., Rosenkranz, F., Ruschemeier, H., Steinrötter, B. (2021) 'The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)', *Multidisciplinary Scientific Journal,*4(4), pp. 589–603.
25. European Data Protection Board (2020) 'Guidelines 4/2019 on Article 25 Data Protection by Design by Default', Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (20 September 2023).
26. Ehrlich, I., Posner, R.A. (1974) 'An Economic Analysis of Legal Rulemaking', *The Journal of Legal Studies*, 3(1), pp. 257–286.
27. *Exploit, Cambridge dictionary*. Available at: https://dictionary.cambridge.org/dictionary/english/exploit (20 September 2023).
28. *Facebook fined again in Italy for misleading users over what it does with their data* (2021) Available at: https://techcrunch.com/2021/02/17/facebook-fined-again-in-italy-for-misleading-users-over-what-it-does-with-their-data/ (20 September 2023).
29. Fassiaux, S. (2023) 'Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A Long-Term Approach', *European Journal of Risk Regulation*, 1, pp. 1–21.
30. Gal, M.S. (2018) 'Algorithmic Challenges to Autonomous Choice', *Mitchigan Technology Law Review*, 25(1), pp. 58–104.
31. Galli, F. (2022) *Algorithmic Marketing and EU Law on Unfair Commercial Practices*, Cham: Springer.
32. Glöckner, J. (2004) 'Richtlinienvorschlag über unlautere Geschäftspraktiken, deutsches UWG oder die schwierige Umsetzung von europarechtlichen Generalklauseln', *Wettbewerb in Recht und Praxis*, 8, pp. 936–945.
33. Glöckner, J. (2013) 'Über die Schwierigkeit, Proteus zu beschreiben – die Umsetzung der Richtlinie über unlautere Geschäftspraktiken in Deutschland', *Gewerblicher Rechtsschutz und Urheberrecht,* 115(3), pp. 224–238.
34. Goanta, C. (2021) 'European consumer law: the hero of our times', *Journal of European Consumer and Market Law,* 10(5), pp. 177–179.

35. Goanta, C. (2023) 'Regulatory Siblings: The Unfair Commercial Practices Directive Roots of the AI Act', Available at: https://ssrn.com/abstract=4337417 (20 September 2023).
36. Grochowski, M. (2021) 'European Consumer Law after the New Deal: A Tryptich', *Max Planck Private Law Research Paper,* 21/24, pp. 387–422.
37. Grundmann, S. (2006) 'The General Clause or Standard in EC Contract Law Directives – A Survey on Some Important Legal Measures and Aspects in EC Law' in Grundmann, S., Mazeaud, D. (eds.), *General Clauses and Standards in European Contract Law. Comparative Law, EC Law and Contract Law Codification*, Hague: Kluwer Law International, pp. 141–161.
38. Hacker, P. (2021) 'Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law', *European Law Journal*, pp. 1–34.
39. Helberger, N. (2017) 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law', *Common Market Law Review*, 54(5), pp. 1427–1465.
40. Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M., Strycharz, J. (2021) 'EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets', *BEUC*, Available at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection 2.0.pdf (20 September 2023).
41. Helberger, N., Micklitz, H.-W., Rott, P. (2021) 'EU Consumer Protection 2.0 The Regulatory Gap: Consumer Protection in the Digital Economy', *BEUC,* Available at: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-116_the_regulatory_gap-consumer_protection_in_the_digital_economy.pdf (20 September 2023).
42. Henning-Bodewig, F. (2015) 'Lauterkeit im B2B-Verhältnis – „anständige Marktgepflogenheiten", nicht „fachliche Sorgfalt"!', *Gewerblicher Rechtsschutz und Urheberrecht International,* 64(6), pp. 529–534.
43. Howells, G. (2006) 'The Rise of European Consumer Law Whither National Consumer Law?', *Sydney Law Review*, 28, pp. 63–88.
44. Howells, G., Micklitz, H.-W., Willhelmsson T., (eds.), *European Fair Trading Law: The Unfair Commercial Practices Directive*, London: Routledge.
45. Howells, G., Twigg-Flesner, C., Wilhelmsson, T. (2018) *Rethinking EU Consumer Law*, London: Routledge Taylor & Francis Group.
46. Jabłonowska, A., Kuziemski, M., Nowak, A.M., Micklitz, H.-W., Pałka, P., Sartor, S. (2018) 'Consumer law and artificial intelligence: Challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence. Final Report of the ARTSY Project', *EUI Working Paper LAW 2018/11*, Available at: https://cadmus.eui.eu/handle/1814/57484 (20 September 2023).
47. Jabłonowska, A. (2022) 'Consumer Protection in the Age of Data-Driven Behaviour Modification', *Journal of European Consumer and Market Law*, 11(2), pp. 67–71.
48. Jasińska, K. (2019) 'Komentarz do art. 3 ZNKU' in: Szwaja (ed.), Warsaw: C.H. Beck.
49. Kaplow, L. (1992) 'Rules Versus Standards: An Economic Analysis', *Duke Law Journal*, 42(3), pp. 557–629.
50. Keirsbilck, B. (2011) *The New European Law of Unfair Commercial Practices and Competition Law*, Oxford and Portland, Oregon: Hart Publishing.
51. Keirsbilck, B. (2013) 'The interaction between consumer protection rules on unfair contract terms and unfair commercial practices: Perenicova and Perenic', *Common Market Law Review,* 50(1), pp. 247–263.
52. Kerber, W. (2021) 'Taming Tech Giants with a Per-Se Rules Approach? The Digital Markets Act from the 'Rules vs. Standard' Perspective', *Concurrences,* 3, pp. 28–34.

53. Koch, B.A., Borghetti, J.-S., Machnikowski P., Pichonnaz, P., Rodríguez de las Heras Ballell, T., Twigg-Flesner, C., Wendehorst, C. (2022) 'European Commission's Public Consultation on Civil Liability Adapting Liability Rules to the Digital Age and Artificial Intelligence', *European Law Institute*. Available at: https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Public_Consultation_on_Civil_Liability.pdf (20 September 2023).
54. Koolen, Ch. (2023) 'Consumer Protection in the Age of Artificial Intelligence: Breaking Down the Silo Mentality Between Consumer, Competition, and Data', *European Review of Private Law*, 2 & 3, pp. 427–468.
55. Köhler, H. (2021) 'Kommentar zu § 3a UWG' in: Köhler, H., Bornkamm, J., Feddersen, J., *Gesetz gegen den unlauteren Wettbewerb*, Berlin: C.H. Beck.
56. Köhler, H., Lettl, T. (2003) 'Das geltende europäische Lauterkeitsrecht, der Vorschlag für eine EG-Richtlinie über unlautere Geschäftspraktiken und die UWG-Reform', *Wettbewerb in Recht und Praxis,* 9, pp. 1019–1057.
57. Larouche, P. de Streel, A. (2021) 'The European Digital Markets Act: A Revolution Grounded on Traditions' *Journal of European Competition Law & Practice*, 12(7), pp. 542–560.
58. Leahy, D. (2022) 'Rocking the Boat: Loot Boxes in Online Digital Games, the Regulatory Challenge, and the EU's Unfair Commercial Practices Directive', *Journal of Consumer Policy*, 45, pp. 561–592.
59. Leszczyński, L. Maroń, G. (2013) 'Pojęcie i treść zasad prawa oraz generalnych klauzul odsyłających. Uwagi porównawcze', *Annales Universitatis Mariae Curie-Skłodowska* 60(1), pp. 81–91.
60. Lubasz, D., Jabłonowska, A., Namysłowska, M. (forthcoming) 'Protected by Design: The Case of Personalised Advertising' in: Poncibò, C., Howells, G., di Matteo, L., Hogg, M. (eds.) *AI and Consumers*, Cambridge: Cambridge University Press.
61. Manteuffel, K., Piaskowski, M. (2017) 'Relacja klauzuli generalnej do przykładowego katalogu nieuczciwych praktyk w ustawie o przeciwdziałaniu nieuczciwemu wykorzystywaniu przewagi kontraktowej w obrocie produktami rolnymi i spożywczymi', *internetowy Kwartalnik Antymonopolowy i Regulacyjny*, 1(6), pp. 35–46.
62. Micklitz, H.-W. (2023) 'The Role of Standards in Future EU Digital Policy Legislation', *BEUC,* Available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf (20 September 2023).
63. Micklitz, H. (2022) 'Discussion Society, Private Law and Economic Constitution in the EU' in: Grégoire, G., Miny, X. (eds.), The Idea of Economic Constitution in Europe, Leiden: Brill | Nijhoff, pp. 380–424.
64. Micklitz, H.-W., Namysłowska, M. (2020a) 'Article 3 UGP-RL' in: Heermann, P.W., Schlingloff, J. (eds.) *Münchener Kommentar zum Lauterkeitsrecht*, München: C.H. Beck.
65. Micklitz, H.-W., Namysłowska, M. (2020b) 'Article 5 UGP-RL' in: Heermann, P.W., Schlingloff, J. (eds.) *Münchener Kommentar zum Lauterkeitsrecht*, München: C.H. Beck.
66. Micklitz, H.-W., Reich, N., Rott, P. (2009) *Understanding EU consumer law*, Antwerp; Portland: Intersentia.
67. Mik, E. (2016) 'The erosion of autonomy in online consumer transactions', *Law, Innovation and Technology*, 8(1), pp. 1–38,
68. Mocanu, D. Sibony, A.-L. (2023) 'EU consumer law meets digital twins', *European Journal of Consumer Law, Revue Européenne de Droit de la Consommation,* 1, pp. 229–257.
69. Monti, G. (2021) 'The Digital Markets Act – Institutional Design and Suggestions for Improvement', *TILEC Discussion Paper No. 2021-04*, Available at: https://ssrn.com/abstract=3797730 (20 September 2023).

70. Namysłowska M. (2022a) 'Zawrotna kariera czarnej listy nieuczciwych praktyk handlowych przedsiębiorców wobec konsumentów' in: Byczko, S., Kappes, A., Kucharski, B., Promińska, U. (eds.), *Non omne quod licet honestum est. Studia z prawa cywilnego i handlowego w 50-lecie pracy naukowej Profesora Wojciecha Jana Katnera*, Łódź: Wolters Kluwer Polska, pp. 576–586.
71. Namysłowska, M. (2022b) *Zwalczanie nieuczciwych praktyk handlowych między przedsiębiorcami w prawie Unii Europejskiej. W poszukiwaniu modelu ochrony,* Warsaw: Wolters Kluwer Polska, 2022.
72. Narciso, M. (2022) 'The Unfair Commercial Practices Directive – Fit for Digital Challenges? An Analysis of the European Commission's Guidance (C/2021/9320)', *Journal of European Consumer and Market Law,* 11(4), pp. 147–153.
73. Naudé, T. (2007) 'The use of black and grey lists and grey lists in unfair contract terms legislation in comparative perspective', *South African Law Journal*, 124(1), pp. 128–164.
74. Oechsler, J. (2019) 'Die Schwarze Liste im Wettbewerbsrecht als negativer Safe Harbor', *Gewerblicher Rechtsschutz und Urheberrecht*, 2, pp. 136–142.
75. Ohly, A. (2017), 'A Fairness-Based Approach to Economic Rights' in: P.B. Hugenholtz (ed.) *Copyright reconstructed: rethinking copyright's economic rights in a time of highly dynamic technological and economic change,* Alphen aan den Rijn: Wolters Kluwer, pp. 83–119.
76. Paterson, J.M., Brody, G. (2015) '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models', *Journal of Consumer Policy,* 38(3), pp. 331–355.
77. Patti, S. (2014) 'Interpretation of the General Clauses Public Policy and Good Morals in European Contract Law', *European Review of Private Law,* 22(5), pp. 611–617.
78. Podszun, R. (2009) 'Der "more economic approach" im Lauterkeitsrecht', *Wettbewerb in Recht und Praxis*, 55(5), pp. 509–518.
79. Podszun, R., Bongartz, P., Langenstein, S. (2021) 'Proposals on How to Improve the Digital Markets Act' Available at: https://ssrn.com/abstract=3788571 (20 September 2023).
80. Reich, N., (1992) 'Protection of Consumers' Economic Interests by the EC', *Sydney Law Review*, 14(23), pp. 23–61.
81. Rosca, C. (2023) 'Destination 'dark patterns': On the EU (digital) legislative train and line-drawing', *Maastricht University*, Available at: https://www.maastrichtuniversity.nl/blog/2023/04/destination-%E2%80%98dark-patterns%E2%80%99-eu-digital-legislative-train-and-line-drawing (20 September 2023).
82. Sack, R. (1985) 'Die lückenfüllende Funktion der Sittenwidrigkeitsklauseln', *Wettbewerb in Recht und Praxis*, 1.
83. Savin, A. (2022) 'Designing EU Digital Laws', *Copenhagen Business School Law Research Paper No. 22–13*, Available at: https://ssrn.com/abstract=4293314 (20 September 2022).
84. Sax, M., Helberger, N., Bol, N. (2018) 'Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices', *Journal of Consumer Policy,* 41, pp. 103–134.
85. Schaffert, W. (2022) 'Kommentar zu § 3a UWG' in: *Münchener Kommentar. Lauterkeitsrecht*, Berlin: C.H. Beck.
86. Scheuerer, S. (2019) 'Artificial Intelligence and Unfair Competition – Unveiling an Underestimated Building Block of the AI Regulation Landscape', *Gewerblicher Rechtsschutz und Urheberrecht International*, 70(9), September 2021, pp. 834–845.
87. Scheuerer, S. (2023) 'The Fairness Principle in Competition-Related Economic Law', Available at: https://doi.org/10.1093/grurint/ikad081 (20 September 2023).
88. Schmidt, M. (2009) *Konkretisierung von Generalklauseln im europäischen Privatrecht*, Berlin: De Gruyter.

89. Siciliani, P., Riefa, C., Gamper, H. (2019) *Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement and Policy Making*, Oxford: Hart Publishing.
90. Sørensen, M.J., Sein, K., Rott, P. (2023) 'European Commission's Public Consultation on Digital Fairness – Fitness Check on EU Consumer Law Response of the European Law Institute', *European Law Institute,* Available at: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Response_of_the_ELI_to_the_European_Commission_s_Public_Consultation_on_Digital_Fairness_.pdf (20 September 2023).
91. Stumpff, A.M. (2013) 'The Law is a Fractal: The Attempt to Anticipate Everything', *Loyola University Chicago Law Journal*, 44(3), pp. 649–681.
92. Tjong Tjin Tai, E. (2015) 'Professional Diligence as a Standard in European Private Law', *Tilburg Private Law Working Paper Series No. 01/2015*, Available at: https://ssrn.com/abstract=2565877 (20 September 2023).
93. Trzaskowski, J. (2016) 'Lawful Distortion of Consumers' Economic Behaviour – Collateral Damage Under the Unfair Commercial Practices Directive', *European Business Law Review*, 27(1), pp. 25–49.
94. Twigg-Flesner, C. (2016) 'Disruptive Technology – Disrupted Law? How the Digital Revolution affects (Contract) Law' in: De Franceschi, A. (ed.), *European Contract Law and the Digital Single Market*, Antwerp; Portland: Intersentia.
95. Valant, J. (2015) 'Consumer protection in the EU. Policy overview. In-depth analysis', *European Parliamentary Research Service,* Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565904/EPRS_IDA(2015)565904_EN.pdf, (20 September 2023).
96. Veale, M. and Borgesius, Z. (2021) 'Demystifying the Draft EU Artificial Intelligence Act' *Computer Law Review International*, 22(4), pp. 97–112.
97. de Vrey, R.W. (2006) *Towards a European Unfair Competition Law. A Clash Between Legal Families*, Leiden; Boston: Martinus Nijhoff Publishers.
98. Wadlow, C. (2012) 'The Emergent European Law of Unfair Competition and its Consumer Law Origins', *Intellectual Property Quarterly*, pp. 1–24.
99. Wagner, G., Eidenmüller, H. (2019) 'Down by Algorithms? Siphoning Rents, Exploiting Biases and Shaping Preferences – The Dark Side of Personalized Transactions', *The University of Chicago Law Review*, 86(2), pp. 581–609.
100. Werten Broch, K., Schrift, R. Y., Alba, J. W., Barasch, A., Bhattacharjee, A., Giesler, M., Knobe, J., Lehmann, D. R., Matz, S., Nave, G., Parker, J. R., Puntoni, S., Zheng, Y., Zwebner, Y. (2020). 'Autonomy in consumer choice', *Marketing letters*, 31(4), pp. 429–439.
101. Willis, L. E. (2020) 'Deception by Design', *Harvard Journal of Law & Technology*, 34(1), pp. 116–190.

Judgments:

1. Case C-371/20, Peek & Cloppenburg KG, v Peek & Cloppenburg KG, ECLI:EU:C:2021:674, (2 September 2021).
2. Applications no. 23676/03 and 3002/03, Times Newspaper Ltd v. the United Kingdom, ECLI:CE:ECHR:2009:0310JUD000300203, (10 March 2009).
3. Cases C-261/07 and C-299/07, VTB-VAB NV v Total Belgium NV and Galatea BVBA v Sanoma Magazines Belgium NV, ECLI:EU:C:2008:581, (29 April 2009).
4. Application no. 12268/03, Hachette Filipacchi Associés v. France, ECLI:CE:ECHR:2009:0723JUD001226803, (23 July 2009).
5. Opinion of Advocate General Trstenjak, Case C-304/08 Zentrale zur Bekämpfung unlauteren Wettbewerbs eV v Plus Warenhandelsgesellschaft mbH, ECLI:EU:C:2009:511, (3 September 2009).

6. Case C-540/08, Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG v "Österreich"-Zeitungsverlag GmbH, ECLI:EU:C:2010:660, (9 November 2010).
7. Application no. 48009/08, Mosley v. the United Kingdom, ECLI:CE:ECHR:2011:0510JUD004800908, (10 May 2011).
8. Case C-453/10, Jana Pereničová and Vladislav Perenič v SOS financ spol. s r. o., ECLI:EU:C:2012:144, (15 March 2012).
9. Case C-428/11, Purely Creative Ltd and Others v Office of Fair Trading Reference for a preliminary ruling from the la Court of Appeal, ECLI:EU:C:2012:651, (18 October 2012).
10. Application no. 33846/07, Węgrzynowski and Smolczewski v. Poland, ECLI:CE:ECHR:2013:0716JUD003384607, (16 July 2013).
11. Case C-435/11, CHS Tour Services GmbH v Team4 Travel GmbH, ECLI:EU:C:2013:574, (19 September 2013).
12. Polish Supreme Court, Case III CZP 82/13, Centrala Handlowo-Usługowa E. S.A. w W. v P. C., (18 December 2013).
13. Case C-281/12, Trento Sviluppo srl and Centrale Adriatica Soc. coop. arl v Autorità Garante della Concorrenza e del Mercato, ECLI:EU:C:2013:859, (19 December 2013).
14. Case C-226/12, Constructora Principado SA v José Ignacio Menéndez Álvarez, ECLI:EU:C:2014:10, (16 January 2014).
15. Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238, (8 April 2014).
16. Federal Supreme Court of Germany, I ZR 129/13, Schlafzimmer komplett, (18 December 2014).
17. Case C-388/13, Nemzeti Fogyasztóvédelmi Hatóság v UPC Magyarország kft, ECLI:EU:C:2015:225, (16 April 2015).
18. Joined Cases C-544/13 and C-545/13, Abcur AB v Apoteket Farmaci AB and Apoteket AB, ECLI:EU:C:2015:481, (20 September 2023).
19. Case C-398/13 P, Inuit Tapiriit Kanatami and Others v European Commission, ECLI:EU:C:2015:535, (3 September 2015).
20. Case C-547/14, Philip Morris Brands SARL and Others v Secretary of State for Health, ECLI:EU:C:2016:325, (4 May 2016).
21. Case C-476/14, Judgment of the Court (Fourth Chamber) of Citroën Commerce GmbH v Zentralvereinigung des Kraffahrzeuggewerbes zur Aufrechterhaltung lauteren Wettbewerbs eV (ZLW), ECLI:EU:C:2016:527, (7 July 2016).
22. Case C-310/15, Vincent Deroo-Blanquart v Sony Europe, ECLI:EU:C:2016:633, (7 September 2016).
23. Case C-157/15, Samira Achbita and Centrum voor gelijkheid van kansen en voor racismebestrijding v G4S Secure Solutions NV, ECLI:EU:C:2017:203, (14 March 2017).
24. Case C-157/15, Policie ČR, Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie v Salah Al Chodor and Others, ECLI:EU:C:2017:213, (15 March 2017).
25. Federal Supreme Court of Germany, I ZR 23/15, Geo-Targeting, (27 October 2017).
26. Federal Supreme Court of Germany, I ZR 184/17, Energieeffizienzklasse, (7 March 2019).
27. Applications no. 60798/10 and 65599/10, M.L. and W.W. v. Germany, ECLI:CE:ECHR:2018:0628JUD006079810, (28 June 2018).
28. Case C-102/20, StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH, ECLI:EU:C:2021:954, (25 November 2021).
29. Application no. 57292/16, Hurbain v. Belgium, ECLI:CE:ECHR:2023:0704JUD005729216, (4 July 2023).

VII. Burden of proof

Peter Rott

A. Introduction

Unfair commercial practices may or may not be easily recognisable. Take the example of dark patterns. 'Deceptive design patterns (also known as 'dark patterns') are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something'.[1] Many of them are well-hidden. That does not only make it difficult for consumers to detect them, but also for enforcers, such as consumer organisations, to explain their (deceptive) functioning to a public authority or a court. The algorithms that determine, for example, the functioning of a website have often been described as a 'black box'.[2]

Dark patterns may constitute unfair commercial practices under the Unfair Commercial Practices Directive (UCPD), as implemented in the Member States, and some certainly do.[3] Where they do not come under the UCPD, they can be prohibited under Article 25(1) of the Digital Services Act (DSA), within the scope of application of that provision, which is narrower than the scope of application of the UCPD.[4] In both regimes, consumer organisations can play a major role as enforcers, where they are registered as qualified entities in the terms of the Representative Actions Directive (EU) 2020/1828.[5]

When initiating legal proceedings against traders that are suspected to use dark patterns, or unfair commercial practices in general, consumer organisations as claimants will have to show that the trader applies an unfair commercial practice. This may require knowledge of what the trader actually does; which may be difficult if that is exactly what is hidden in the 'black box'. Burden of proof has therefore been identified as a major obstacle in the fight against digital unfairness. Consequently, the European Commission has, in its public consultation on digital fairness, asked stakeholders to comment on the following thesis:

'The burden of proof of compliance with legal requirements should be shifted to the trader in certain circumstances (eg when only the company knows the complexities of how their digital service works).'[6]

In the following, this thesis is discussed in the light of the general principle of effectiveness of EU law and of comparable situations in which alleviations of the burden of proof have been introduced in the past or are currently discussed, in one way or another.

---

1 See H. Brignull, Deceptive design, https://www.deceptive.design. For similar descriptions, see M. Martini, C. Drews, P. Seeliger and Q. Weinzierl, Dark Patterns – Phänomenologie und Antwort der Rechtsordnung, Zeitschrift für Digitalisierung und Recht (ZfDR) 2021, 47, 49.

2 See, for example, the European Commission's proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final, 1.

3 For analysis of dark patterns as unfair commercial practices, see, for example, Martini et al. (n 1), 64 ff.; P. Rott, Dark Patterns im Verbraucherrecht, in M. Reiffenstein and B. Blaschek (eds.), Konsumentenpolitisches Jahrbuch 2023, Verlag Österreich, 2023, 181 ff

4 On the relationship between both regimes in relation to dark patterns, see Rott (n 3).

5 See Annex I nos 14 and 68 of Directive (EU) 2020/1828, as amended.

6 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/public-consultation_en.

B. Burden of proof – an element of effectiveness

Proving a breach of law is a fundamental problem of all enforcement efforts. This is why burden of proof is one element of the principle of effectiveness, as the Court of Justice has confirmed in a number of decisions. The principle of effectiveness prohibits Member States to frame the conditions for the enforcement of individual rights in such a way that it makes it virtually impossible or excessively difficult to obtain reparation.[7] The same applies, of course, to the rights of consumer organisations.

In *San Giorgio*, the Court applied the principle of effectiveness to issues of proof. The case concerned a reimbursement claim of an enterprise against the Republic of Italy for fees that the enterprise had been charged without a valid legal basis. The Republic of Italy argued that San Giorgio had passed the fees on to its customers and therefore had not suffered any damage. Thus, San Giorgio was supposed to prove that it had not passed the fees on to its customers; which Advocate General Mancini qualified as 'calling for proof of a diabolically high standard'.[8] The Court held that 'any requirement of proof which has the effect of making it virtually impossible or excessively difficult to secure the repayment of charges levied contrary to Community law is incompatible with Community law'.[9]

Generally speaking, the principle of effectiveness, however, only marks the outer limit of what lies otherwise in the competence of the Member States. According to the principle of procedural autonomy, it is for the domestic legal system of each Member State to designate the courts having jurisdiction and to determine the procedural conditions governing actions at law intended to ensure the protection of the rights which citizens have from the direct effect of Community law.[10]

Nevertheless, in individual cases, the principle of effectiveness may even require certain alleviations to the burden of proof, as the Court of Justice first held in the famous case of *Danfoss* in relation to equal payment between men and women.[11] The Employees' Union had first brought Danfoss A/S before the Industrial Arbitration Board, basing its case on the principle of equal pay for the benefit of two female employees, one of whom worked in the laboratory and the other in the reception and despatch department. In support of its action it had shown that in these two wage groups a man's average wage was higher than that of a woman's. In its decision, the Industrial Arbitration Board had however considered that in view of the small number of employees on whose pay the calculations had been based the Employees' Union had not proved discrimination. The Employees' Union thereupon brought fresh proceedings in which it produced more detailed statistics relating to the wages paid to 157 workers between 1982 and 1986 and showing that the average wage paid to men is 6.85% higher than that paid to women.

---

7 See ECJ, Case 33/76 Rewe-Zentralfinanz eG and Rewe-Zentral AG v. Landwirtschaftskammer für das Saarland, ECLI:EU:C:1976:188, para. 5, and Case 45/76 Comet BV v Produktschap voor Siergewassen, ECLI:EU:C:1976:191, paras 11–18.

8 AG Mancini, 27.9.1983, Case 199/82 Amministrazione delle Finanze dello Stato v Societa San Giorgio s.p.a., ECLI:EU:C:1983:247.

9 ECJ, 9.11.1983, Case 199/82 Amministrazione delle Finanze dello Stato v Societa San Giorgio s.p.a., ECLI:EU:C:1983:318. For an overview of confirming decisions, see P. Rott, Effektivität des Verbraucherrechtsschutzes: Rahmenfestlegungen des Gemeinschaftsrechts, 2006, http://download.ble.de/04HS033.pdf, 44 ff.

10 See ECJ – Rewe (n 7), para. 5.

11 ECJ, 17 October 1989, Case C-109/88 Danfoss, ECLI:EU:C:1989:383.

The Court of Justice found that 'the issue between the parties to the main proceedings has its origin in the fact that the system of individual supplements applied to basic pay is implemented in such a way that a woman is unable to identify the reasons for a difference between her pay and that of a man doing the same work. Employees do not know what criteria in the matter of supplements are applied to them and how they are applied. They know only the amount of their supplemented pay without being able to determine the effect of the individual criteria. Those who are in a particular wage group are thus unable to compare the various components of their pay with those of the pay of their colleagues who are in the same wage group.'12 The Court continued that 'in a situation where a system of individual pay supplements which is completely lacking in transparency is at issue, female employees can establish differences only so far as average pay is concerned. They would be deprived of any effective means of enforcing the principle of equal pay before the national courts if the effect of adducing such evidence was not to impose upon the employer the burden of proving that his practice in the matter of wages is not in fact discriminatory.'13 Thus, '(to) show that his practice in the matter of wages does not systematically work to the disadvantage of female employees the employer will have to indicate how he has applied the criteria concerning supplements and will thus be forced to make his system of pay transparent.'[14]

In the area of consumer credit law, in the case of CA Consumer Finance, the question arose whether and how the consumer could prove that the creditor has breached his obligation to assess the consumer's creditworthiness. The Court of Justice noted that 'compliance with that principle would be undermined if the burden of proving the non-performance of the obligations laid down in Articles 5 and 8 of Directive 2008/48 lay with the consumer. The consumer does not have the means at his disposal to enable him to prove that the creditor, first, did not provide him with the information required under Article 5 of that directive and, secondly, did not check his creditworthiness.'[15]

Burden of proof, as an element of effectiveness, has been discussed in a number of areas of law, including antidiscrimination law (the equal pay principle), tax law, product liability law and consumer law. The following analysis draws on legislative acts or proposals, and on case law of the Court of Justice, in these various areas of law and shows approaches that help claimants in proving their case.

C. Relevant legal issues

At the outset, it should be clarified that the burden of proof does not relate to breach of or compliance with the law but to the elements of a legal provision that determine the breach of or compliance with the law. In the above-mentioned example of the creditworthiness assessment, it is not for the creditor to show that he has complied with the law but to show what exactly he has done. The court will then judge on whether what the creditor has done satisfies the requirements of the legal provision, here: Article 8 of the Consumer Credit Directive. In other words, when we talk about burden of proof, we need to determine what exactly it relates to.

12 ibid., para. 10.
13 ibid., para. 13.
14 ibid., para. 15.
15 See CJEU, 18.12.2014, Case C-449/13 CA Consumer Finance SA v Ingrid Bakkaus and others, ECLI:EU:C:2014:2464, para. 27.

There will be instances in unfair commercial practices law where burden of proof is not an issue. Let us take the example of a cookie consent banner, which provides for two buttons: a big button in bright green showing the word 'accept' and a small button in light grey, nearly invisibly showing the word 'reject'.[16] The facts lie on the table. Whether or not this cookie banner complies with the law, is merely a question of law. There is no difference to, for example, misleading advertisement where courts base their decision on a screenshot.

Importantly, the unfairness test of the UCPD is an objective test. According to Article 5(1) UCPD, a commercial practice is 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. Similarly, under Article 6(1) UCPD, a commercial practice is misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise (...). Thus, the consumer or consumer organisation does not need to prove any kind of subjective element, and in particular no intention to manipulate the consumer. Nor needs the consumer or consumer organisation provide evidence of what the average consumer is like, or would think or do, by way of an empirical study or a poll, as the concept of the average consumer is normative rather than empirical.

Slightly more burdensome, but still feasible, is the documentation of a certain visible reaction of websites. For example, one could take screenshots of or film a website to demonstrate that whenever the consumer clicks on a product, the previously shown price is increased by 10 %; which should qualify as an unfair commercial practice.

In contrast, when it comes to, for example, personalised pricing, the first question is whether or not prices are personalised. Clearly, individual consumers will hardly be able to prove personalised pricing, or the use of prohibited criteria in personalised pricing. One could therefore consider to shift the burden of proof to the trader, perhaps provided that there are indications of personalisation.

Finally, Article 11a UCPD (as amended by the Modernisation Directive (EU) 2161/2019) provides for a damage claim. The provision implies that there is a causal link between an unfair commercial practices and damage suffered by consumers. Moreover, Article 11a UCPD leaves some leeway to Member States as for the details of the claim. For example, the damage claim can be designed as fault-based, as Germany has done.[17] Again, the issue of the burden of proof arises.

Looking more closely, the 'burden of proof' debate includes a variety of legal issues that are related to each other. As a starting point, the *burden of proof* is normally on the claimant, who has to prove those elements of a legal provision that act in their favour, whereas the burden of proof for defences is normally on the defendant. Of course, there are exceptions from this principle, as will be discussed below.

---

16 For a similar cookie banner design, see LG Rostock, 15.9.2020 – 3 O 762/19, Zeitschrift für Datenschutz (ZD) 2021, 166, 167.

17 See § 9 para. 2 of the Unfair Commercial Practices Act (Gesetz gegen den unlauteren Wettbewerb; UWG).

A different, however related issue is the *standard of proof*, thus what a party must do to provide sufficient evidence.

Finally, *accessibility of evidence* needs to be taken into account, which includes information rights of one party but also documentation obligations of the other party, which secures information to be available in the first place.

D. Burden of proof in unfair commercial practices law *de lege lata*

The Unfair Commercial Practices Directive does not comprehensively deal with the above-mentioned issues around burden of proof. Under Article 11(1) UCPD, Member States shall ensure that adequate and effective means exist to combat unfair commercial practices in order to enforce compliance with the provisions of this Directive in the interest of consumers. This codification of the principle of effectiveness implicitly touches on the burden of proof and the standard of proof, as set out above.

As a starting point, it is then, according to recital (25) of the UCPD, for national law to determine the burden of proof, although the EU legislator regards it as appropriate to enable courts and administrative authorities to require traders to produce evidence as to the accuracy of factual claims they have made. In that latter regard, Article 12 UCPD specifies that Member States shall confer upon the courts or administrative authorities powers enabling them (...) (a) to require the trader to furnish evidence as to the accuracy of factual claims in relation to a commercial practice if, taking into account the legitimate interest of the trader and any other party to the proceedings, such a requirement appears appropriate on the basis of the circumstances of the particular case and (b) to consider factual claims as inaccurate if the evidence demanded in accordance with (a) is not furnished or is deemed insufficient by the court or administrative authority.

Even Article 12 UCPD only seems to place a power on national courts or administrative bodies without requiring them to make use of them. Outside the scope of application of Article 12 UCPD, Member States appear to be free to introduce alleviations of the burden of proof. An outer limit to that would seem to be primary EU law, in particular the provisions on the free movement of goods and services, which could come into play where national provisions relating to the burden of proof become obstacles to trade.

When it comes to the current situation under the UCPD, analysed in relation to dark patterns in particular, the following questions arise:

1. Which situations does Article 12 UCPD cover?
2. In which other situations is it inappropriate to ask the consumer, or consumer organisation, to provide full evidence of the elements of a provision that constitute an unfair commercial practice?
3. What kind of facilitation could and should the law provide for?

I. Article 12 UCPD

1. Scope of application

Article 12 UCPD only relates to statements on facts. Thus, it applies to certain dark patterns that deal, for example, with time pressure. For example, under Annex I no. 7, it is prohibited to falsely state that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice. A statement related to the availability of the product is a statement on facts, and the national court or authority can ask the trader to furnish evidence of the particular times when a product was actually available.

In contrast, Article 12 UCPD does not deal with, for example, manipulative web design, or with personalised pricing (unless of course the trader claims not to apply personalised pricing). At best, one could discuss whether silence is a statement of fact where the trader is under an obligation of disclosing a certain fact. For example, under new Article 6(1)(ea) of the Consumer Rights Directive, the trader must inform the consumer, 'where applicable, that the price was personalised on the basis of automated decision-making'. Thus silence on this issue could be interpreted as a statement of the fact that no such price personalisation is applied. This is, however somewhat stretching the wording of Article 12 UCDP, and it may not even be necessary (see infra, D. II.).

2. Concretisation of facts

In many cases, a statement is not clearly incorrect but leaves room for interpretation. This applies, for example, where products are attributed certain characteristics, such as environmentally friendly, climate friendly, healthy or safe. Whether or not such a characterisation is accurate, depends on standards. The problem here is the concretisation of the standard.

In EU law, the solution in relation to particular statements lies in placing the burden of proof on the trader who has to demonstrate that a certain pre-defined standard is met. Thus, in relation to 'health claims', the EU has adopted Regulation (EC) No 1924/2006 on nutrition and health claims made on foods.[18] The rules of the Regulation apply to nutrition claims (such as 'low fat', 'high fibre') and to health claims (such as 'Vitamin D is needed for the normal growth and development of bone in children'). Any claim made on a food's labelling, presentation or advertising in the EU must be clear, accurate and based on scientific evidence, which is for the trader to supply.

The same concept is currently pursued with the proposed Directive amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and better information.[19] For example, according to the proposed Annex I no. 4a, traders would be prohibited to make a generic environmental claim for which he is not able to demonstrate recognised excellent environmental performance relevant to the claim.

---

18 [2006] OJ L 404/9.
19 COM(2022) 143 final.

3. External control

A further step towards ensuring the truthfulness and accuracy of factual statements lies in the integration of an external control mechanism. This is the system that the EU Commission has proposed for 'green claims', with the proposed Directive on substantiation and communication of explicit environmental claims (Green Claims Directive).[20] The proposed Directive provides for *ex-ante* verification of environmental claims as well as environmental labels carried out by independent accredited bodies, similar to the system that has been applied for a long time in EU product safety law.

II. Reversed burden of proof outside Article 12 UCPD?

As mentioned above (supra, C. I.), there are unfair commercial practices that do not work with (openly) visible or otherwise recognisable unfair features, such as the undisclosed personalisation of prices. In such a situation of digital asymmetry, the principle of effectiveness as codified in Article 11(1) UCPD may apply. The situation is comparable to the ones in *Danfoss* and in *CA Consumer Finance*: The consumer, or the consumer organisation, has no chance to find out what happens within the sphere of the trader.

It should be noted though that the employer's obligation to lay open the criteria for distinguishing salaries in *Danfoss* was not unconditional but it was triggered by indicators that demonstrated the possibility of unequal pay for men and women. This case law was later codified in anti-discrimination law.[21] Similarly, in *CA Consumer Finance* there was an indication that the creditworthiness assessment had not been performed at all, or insufficiently, as the consumer actually was not able to meet her obligations arising from the credit contract.

In the case of unfair commercial practices law, it would thus be necessary to show some sort of anomaly that indicates the potential presence of a breach of law. For example, in case of the suspected personalisation of prices, indication of an infringement could simply consist of two screenshots taken at the same time concerning the same product with different prices.[22]

Moreover, EU law takes into account the defendant's position, in the sense that it wants to achieve a fair balance between the legitimate interests of – in this case – traders and consumers.[23] Thus, it would not shift the burden of proof in such a way that it is virtually impossible or excessively difficult for the trader to prove compliance with the law. This is, however, not a problem in the case at hand, as the trader merely would have to show and explain the algorithm applied, which he is well able to do. Indeed, it is for the same reason that in Article 12(2) and (3) of the Digital Content and Digital Services Directive (EU) 2019/770, the burden of proof for the conformity of digital content and digital services with the contract falls largely on the trader.

---

20 COM(2023) 166 final. For detailed analysis, see S. Jung and M. Dowse, Die Eckpfeiler des europäischen Green-Claims-Richtlinienvorschlags, Verbraucher und Recht (VuR) 2023, 283, 286 ff.

21 See Art. 8(1) of Directive 2000/43/EC and Art. 9(1) of Directive 2004/113/EC.

22 See also A. Gleixner, Personalisierte Preise im Onlinehandel und Europas „New Deal for Consumers", Verbraucher und Recht 2020, 417, at 420.

23 See, for example, Proposal for an AI Liability Directive (n 2), 6.

E. Possible facilitation of proof below the reversal of the burden of proof

As we have already seen, facilitation of proof can be constructed in different ways.

I. Rebuttable presumption

The strongest form (below the reversal of the burden of proof) is the rebuttable presumption. We can find this instrument, for example, in the Sale of Goods Directive (EU) 2019/771. According to its Article 11(1), any lack of conformity which becomes apparent within one year of the time when the goods were delivered *shall be presumed* to have existed at the time when the goods were delivered, unless proved otherwise or unless this presumption is incompatible with the nature of the goods or with the nature of the lack of conformity. In other words, the trader must prove that the lack of conformity did not exist at the time of delivery. The reason for this rule is that the consumer will normally not avail of the expertise to demonstrate the defectiveness of a good that worked initially but failed to do so after some time.

A similar rule can be found in the European Commission's proposal for a new Product Liability Directive. According to Article 9(2)(b), the defectiveness of the product shall be presumed if the claimant establishes that the damage was caused by an obvious malfunction of the product during normal use or under ordinary circumstances.

In the context of the UCPD, one could think of a rule, according to which there is a rebuttable presumption of an unfair commercial practice where there is an indication of such a practice, based on factual evidence. For example, there could be a presumption that different prices for different persons at the same time are prompted by price personalisation unless the trader proves otherwise.

Rebuttable presumptions are also sometimes used for the proof of causation. According to Article 9(3) of the proposed new Product Liability Directive, the causal link between the defectiveness of the product and the damage shall be presumed, where it has been established that the product is defective and the damage caused is of a kind typically consistent with the defect in question.

A rebuttable presumption may also be used where a legal provision only applies if the claimant has reacted to a breach in a certain manner. For example, in German law it is presumed that the insured person would have taken the right decision (and therefore not suffered damage) if he or she had been correctly informed.[24] In the context of the UCPD, a rebuttable presumption could apply to the damage claim under Article 11a UCPD in the sense that the consumer would be presumed to have made a different decision had he or she not been misled, harassed, coerced or unduly influenced.

24 BGH, 22.5.1985 – IVa ZR 190/83, Neue Juristische Wochenschrift 1985, 2595. See also BGH, 08.05.2012 – XI ZR 262/10, Neue Juristische Wochenschrift 2012, 2427, for investor protection law.

II. Lowering the standard of proof

As mentioned above, the standard of proof determines what a party must do to provide sufficient evidence. Typically, the standard of proof is not regulated in EU law and, therefore, its regulation has remained within the competence of the Member States even if EU law regulates the burden of proof as such.[25] For example, in the case of *Sanofi Pasteur*, the Court of Justice held that it is for the national legal order of each Member State to establish the ways in which evidence is to be elicited, what evidence is to be admissible before the appropriate national court, or the principles governing that court's assessment of the probative value of the evidence adduced before it and also the level of proof required.[26] The only limitation of the Member States' leeway is that the rules on the standard of proof must not undermine the distribution of the burden of proof.[27]

Traditionally, Member States apply different formulas for the establishment of proof. Germany, for example, is particularly strict in requiring the full persuasion of the court of the facts. According to § 286 para. 1 of the Civil Procedural Code, the court is to decide, at its discretion and conviction, and taking account of the entire content of the hearings and the results obtained by evidence being taken, if any, whether an allegation as to fact is to be deemed true or untrue. German courts require, at least, a very high degree of likelihood, whereas 'mere likelihood' has explicitly been ruled out as insufficient.[28]

English law, in contrast, traditionally applies the balance of probabilities test in the area of causation, which means that the claimant only needs to show that what he or she claims is 'more likely than not'.[29]

However, we can also see that Member States may adjust the standard of proof where a strict standard is (too) difficult to meet in a particular area of law or life. Indeed, Advocate General Bobek indicated in *Sanofi Pasteur*, related to product liability law, that given the very different nature of the products covered by the Product Liability Directive 85/374/EEC, the type of damage they could cause and the way that damage might be caused, detailed rules on proof and evidence may not be identical in all cases.[30] In the case at hand, his statement aimed at the particular difficulties of proving vaccination damages but it would equally apply to opaque algorithms.[31]

One example from German law is indeed the area of social law concerning compensation for vaccination damage. As it is very difficult to establish with a high degree of certainty that a

25 See ECJ, 20.11.2014, Case C-310/13 Novo Nordisk Pharma GmbH, ECLI:EU:2014:2385, paras 25 ff.
26 See ECJ, 21.6.2017, Case C-621/15 N.W., L.W., C.W. v Sanofi Pasteur MSD SNC and others, ECLI:EU:C:2017:484, para. 25.
27 ibid., para. 27.
28 See BGH, 19.2.1970 – III ZR 139/67, NJW 1970, 946, 948.
29 See, for example, Court of Appeal, *In re H (Minors)[1996] AC 563, 586:* 'The balance of probability standard means that a court is satisfied an event occurred if the court considers that, on the evidence, the occurrence of the event was more likely than not.'
30 AG Bobek, 7.3.2017, Case C-621/15 N.W., L.W., C.W. v Sanofi Pasteur MSD SNC and others, ECLI:EU:C:2017:176, para. 22.
31 See P. Rott, Rechtspolitischer Handlungsbedarf im Haftungsrecht, insbesondere für digitale Anwendungen, 2017, https://www.vzbv.de/sites/default/files/downloads/2018/05/04/gutachten_handlungsbedarf_im_haftungsrecht.pdf28.

certain health issue was caused by a particular vaccination, the victim merely has to show that causation is more likely than not.[32]

An example from (future) EU law is Article 9(4) of the proposed Product Liability Directive. Where the claimant faces excessive difficulties, due to technical or scientific complexity, to prove the defectiveness of the product or the causal link between its defectiveness and the damage, or both, the defectiveness of the product or causal link between its defectiveness and the damage, or both, shall be presumed where the claimant has demonstrated, on the basis of sufficiently relevant evidence that a) the product contributed to the damage; and b) it is likely that the product was defective or that its defectiveness is a likely cause of the damage, or both.

Unfair commercial practices law could generally establish the standard of balance of probabilities ('more likely than not'), thus making sure that national courts do not apply an excessively high standard of proof, or at least do so when it comes to website architectures that are certainly beyond the expertise of the average consumer.

III. Accessibility of evidence

Due to digital asymmetry, evidence may be inaccessible for consumers or consumer organisations, and the success of litigation may depend on the right to obtain information and meaningful explanations from the defendant (or from a third party), as a first step. The UCPD does not touch upon that issue, and it is therefore in the competence of the Member State.

As a starting point in general civil procedural law, it is for the claimant to produce evidence, whereas the defendant is under no obligation to help the claimant with this exercise. German courts, for example, have often emphasised that German law prohibits pre-trial discovery. Thus, in the context of the breast implant scandal around the French producer Poly Implant Prothèse (PIP), the claimant could not ask for TÜV Rheinland's monitoring reports and therefore was not able to show what TÜV Rheinland has done or has failed to do.[33]

Again, however, we find exceptions to that rule in EU law and in national law where it was deemed appropriate to grant the claimant access to information. For example, Article 3 of Directive 2004/48/EC on the enforcement of intellectual property rights provides for an information right in favour of the claimant, under certain circumstances (although this only applies to a 'justified and proportionate request' of the claimant, which leaves the Member States some leeway).

Germany has introduced a right of information in the Pharmaceuticals Act (Arzneimittelgesetz; AMG), responding to the fact that it is very difficult for the claimant, who has no insights into the development and the manufacturing of the pharmaceutical product, to prove the existence of a design defect or a manufacturing defect. Thus, according to § 84a AMG, the victim can request information related to effects, side-effects and interaction of medical products that are known to the producer and to suspected effects, side-effects and interaction of medical products that were brought to the producer's attention and all further knowledge which

32 See § 61 of the Act on Protection against Infections (Infektionsschutzgesetz; IfSG). See also P. Rott, Compensation for Vaccination Damage under German Social Security Law, Otago Law Review 2020, 199, 211.

33 See OLG Karlsruhe, 27.6.2018 – 7 U 96/17, Beck-Rechtsprechung (BeckRS) 2018, 25317.

could be of significance in assessing the justifiability of harmful effects, provided that facts exist that justify the assumption that a medical product has caused the damage in question. This special right of disclosure aims to improve the claimant's procedural position[34] and to re-establish equal terms between the parties.[35]

As a recent example, the EU Commission has proposed a provision on disclosure of evidence in its proposal for a new Product Liability Directive.[36] According to Article 8(1) of the proposal, Member States shall ensure that national courts are empowered, upon request of an injured person claiming compensation for damage caused by a defective product ('the claimant') who has presented facts and evidence sufficient to support the plausibility of the claim for compensation, to order the defendant to disclose relevant evidence that is at its disposal. In the following, the Commission is committed to strike the balance between the interests of the victim and the producer. According to Article 8(2) Member States shall ensure that national courts limit the disclosure of evidence to what is necessary and proportionate to support the disclosure claim. When determining whether the disclosure is proportionate, national courts shall, according to Article 8(3), consider the legitimate interests of all parties, including third parties concerned, in particular in relation to the protection of confidential information and trade secrets. Finally, Member States shall ensure that, where a defendant is ordered to disclose information that is a trade secret or an alleged trade secret, national courts are empowered, upon a duly reasoned request of a party or on their own initiative, to take the specific measures necessary to preserve the confidentiality of that information when it is used or referred to in the course of the legal proceedings (Article 8(4)).

IV. Documentation duties

Accessibility of evidence often requires that relevant information has been collected and stored in the first place. Where the burden of proof lies with the defendant trader, he would be well advised to collect and store relevant evidence anyway. For example, as the creditor has to prove that he performed a creditworthiness assessment before giving out credit, according to the decision of the Court of Justice in *CA Consumer Finance*, he would surely document what he has done.

Documentation duties can also be stated in legislation. In the context of 'black boxes', the German legislator has introduced the duty for automated cars to store the position and time information determined by a satellite navigation system when there is a change in vehicle control between the driver and the highly or fully automated system. The same applies if the vehicle driver is asked by the system to take over control of the vehicle or a technical malfunction occurs in the system.[37] This shall allow, after an accident, to find out whether the accident was the fault of the driver or of the car and therefore its producer.[38]

---

34 See BGH, 12 May 2015 – VI ZR 328/11, Neue Juristische Wochenschrift (NJW) 2015, 2502.
35 See A. Spickhoff, Medizinrecht, 2nd ed,, CH Beck 2014, § 84a AMG para 1.
36 COM(2022) 495 final.
37 See § 63a para. 1 of the Road Traffic Act (Straßenverkehrsgesetz; StVG).
38 See also C. Armbrüster, Automatisiertes Fahren – Paradigmenwechsel im Straßenverkehrsrecht?, Zeitschrift für Rechtspolitik (ZRP) 2017, 83, 85; J.-E. Schirmer, Augen auf beim automatisierten Fahren! Die StVG-Novelle ist ein Montagsstück, Neue Zeitschrift für Verkehrsrecht (NZV) 2017, 253, 256 f.

In the same way, German case law on medical malpractice has triggered the need for doctors and hospitals to document closely what they have done. This documentation duty has in the meantime been codified in § 630f BGB:

'1. For the purpose of documentation, the treating party is obliged to keep medical records in paper form or as electronic documentation in close time with the treatment. (...).
2. The treating party is obliged to record all measures in the medical records that are relevant in medical terms for the current and future treatment and its results, in particular the establishment of the medical history, diagnoses, examinations, results of examinations, findings, therapies and their effects, procedures and their impact, consent and information. Physicians' letters are to be included in the medical records.
3. The treating party is to keep medical records for a period of 10 years following the conclusion of the treatment unless other periods for their retention govern in accordance with other provisions.'

A breach of this documentation duty is, among others, sanctioned by the reversal of the burden of proof. According to § 630h para. 3 BGB, where the treating party has not recorded a medically required major measure and its result in the medical records, contrary to what is stipulated in section 630f (1) or (2), or where, contrary to section 630f (3), they have not retained the medical records, it is to be presumed that they have not carried out this measure.

In the same way, the German Supreme Court has decided in relation to documentation duties of insurance intermediaries. Disregard of those duties can lead to the alleviation of the burden of proof of a breach (that is otherwise on the insured person), and even to the reversal of the burden of proof.[39]

A prominent area where documentation obligations will be introduced is certainly the regulation of artificial intelligence in the forthcoming Artificial Intelligence Act, which relies heavily on technical documentation. According to its Article 11(1) AI Act, technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date. Details are set out in Annex IV. That documentation is of course first of all meant to allow public authorities to exercise *ex-ante* market control. It could, however, also be used in private litigation to show, for example, the unfairness or otherwise of a commercial practice.

V. Combination

Finally, different of the above-mentioned elements can be combined. In particular, the failure to supply information or to provide documentation can be sanctioned with disadvantages in the burden of proof.

Thus, according to Article 9(2)(a) of the proposed new Product Liability Directive, the defectiveness of the product shall be presumed if the defendant has failed to comply with an obligation to disclose relevant evidence at its disposal in accordance with Article 8(1).

39 See BGH, 13 November 2014 – III ZR 514/13, NJW 2015, 1026.

F. The ignorant trader and the players behind

As set out by *Laurens Naudts*, *Natali Helberger*, *Marijn Sax* and *Michael Veale* in this study,[40] it is often, or usually, not the final trader alone that designs a website and its functionalities but there are one, or often more, layers behind. The final trader may not even be aware of all the functionalities, which may ultimately trigger the unfairness of his own commercial practices.

I. No exclusion of liability

1. Unfair practices

First of all, we should remember that unfair commercial practices law is not fault-based. Thus, for a commercial practice to be unfair, it does not matter whether the trader knew of its unfair functionalities but only that, as Article 5(2) UCPD puts it, the practice is contrary to the requirements of professional diligence and 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.

In the same vein, if there is an indication that a commercial practice is unfair and the burden is on the trader to explain why the website produces a certain result, the responsibility to be able to do so rests on the trader. If he cannot explain the functionality because it is hidden in a deeper layer of the website, which he has not designed, he will not be able to rebut any assumption of unfairness. Certainly, he cannot be 'excused' simply by not knowing what he is doing or using.

2. Individual rights

In relation to remedies of individual consumers based on (now) Article 11a UCPD, this may be different if the national implementation has based the remedies on the trader's fault and the trader had no reason to believe that there was an unfair commercial practices embedded in the website design as supplied by another player. As soon as the trader is made aware of such suspicion though, he would be required to investigate the potential unfair design. By not doing so, he would act negligently.

II. Remedies against other players?

1. Remedies of the trader

The only one that could help the trader in such a situation is the player that is responsible for the website design. This could be, in the first place, a contracting partner, for example, the operator of a platform that the trader uses, or a service provider who designed the website for the trader.

---

40 See part 3, Toward Accountable Optimisation: a new perspective on the regulation of recommender systems and the rights of users and society.

Of course, the trader could include a contractual term into such contracts, according to which his contracting partner would have to explain the functionality of the website design if the trader is approached by a consumer, a consumer organisation or a public authority, due to an indication of an unfair commercial practice, ideally accompanied by a redress mechanism in case the trader has to pay damages, or a fine. Not all traders will be in the position though to achieve the inclusion of such a term if they lack the necessary bargaining power.

In sales law, EU law tries to help the final seller, who is ultimately liable for any lack of conformity of a good with the contract, with a right of redress enshrined in Article 18 of the Sale of Goods Directive (EU) 2019/771. Likewise, if digital content or digital services are not supplied at all, or lack conformity with the contract, as a result of an act or omission by a person in previous links of the chain of transactions, the supplier of digital content or digital services has a right of redress against the person or persons liable in the chain of commercial transactions. In the same way, the UCPD could be amended with a provision that provides for such an internal solution, leaving the trader as the only person responsible for the unfair commercial practice towards consumers.

2. Remedies of consumers or consumer organisations

Alternatively, those that are truly responsible for an unfair commercial practice in terms of having designed the trader's website in a particular manner, or having infiltrated an unfair element into the website, could be made additional addressees of claims by consumers or consumer organisations.

This is already true for online platform operators that are themselves traders in the terms of Article 2(b) UCPD. Moreover, additional duties have just been imposed on online platforms by the Digital Services Act, including the prohibition under Article 25 DSA to 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.

Other players that may have added unfair elements to a deeper layer of the website, in contrast, are neither traders in the terms of the UCPD nor online platforms. Thus, they could only be targeted if they were added by the legislator to the list of potential addressees of action under the UCPD. One model for this would be product liability law, with liability being imposed on the producer, and also on the producers of components of the product. As in product liability law, one could foresee a system whereby each player who is not ultimately responsible will have to name its contracting partner (or be liable themselves) so that finally the truly responsible person could be found and targeted.

Again, this should not absolve the final trader from liability though but only the other players that are involved but not themselves responsible.

G. Proposed regulation of the burden of proof in unfair commercial practices law

In the light of the principle of effectiveness, it is a requirement of EU law to improve the position of consumers and of consumer organisations, as otherwise the enforcement of the UCPD in relation of those unfair commercial practices that are hidden in algorithms behind the website design is virtually impossible or excessively difficult. This could be done in different ways, which all find predecessors in EU legislation, draft legislation and/or the case law of the Court of Justice, as analysed above.

It seems clear that there will be no unconditional reversal of the burden of proof or information right. Rather, the consumer organisation will have to show an indication that the trader uses an unfair commercial practice. In the light of the digital asymmetry between the trader and consumers as well as consumer organisations, requirements on that indication should be moderate though, where the suspected unfair commercial practice would be hidden.

Once that indication is established, the trader should be required to give a meaningful explanation of the observed phenomenon. The notion of meaningful explanation is borrowed from Articles 13(2)(f) and 14(2)(g) GDPR. In these provisions relating to automated decision-making, meaningful information (about the logic involved) does not necessarily require a full explanation of the details, or even the disclosure of the algorithm, but it does require the trader to disclose the relevant criteria that are used.

Thus, in the context of the UCPD, 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. If instead consumers or consumer organisations were only granted access to some sort of technical documentation, the consumer organisation would probably need to hire an expert that explains the functionalities; which would be costly and another obstacle to effective enforcement, contrary to the principle of effectiveness.[41]

If the trader fails to provide a meaningful explanation, it would be presumed that the observed phenomenon has been caused by an unfair commercial practice.

Documentation will be crucial. In order to ensure that documentation is available, one would not necessarily have to introduce express documentation obligations, as in the AI Act. Instead, the trader could also produce documentation ad hoc, if needed, as the algorithm should still be available, whereas the unavailability of documentation should be sanctioned with the reversal of the burden of proof.

Traders cannot be excused because they do not have documentation and/or are unable to provide meaningful explanations because they are using infrastructure that was provided by third parties. However, the (EU) legislator could consider helping such traders with a right to

41 On costs as a relevant factor of effectiveness, see, for example, ECJ, 1 December 1998, Case C-326/96 B. S. Levez v T. H. Jennings (Harlow Pools) Ltd, ECLI:EU:C:1998:577, para. 51; ECJ, 16 May 2000, Case C-78/98 Shirley Preston and others v Wolverhampton Healthcare NHS Trust and others and Dorothy Fletcher and others v Midland Bank plc, ECLI:EU:C:2000:247, para. 60.

redress. Moreover, in order address structural problems, the legislator could introduce separate liability of third parties that supply elements to the infrastructure that make commercial practices of the trader unfair.

Finally, the protection of trade secrets will need to be taken 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. Article 8(4) of the proposed Product Liability Directive points the way forward.

VIII. Concluding reflections

While the digital fitness check of consumer law is underway, a "new digital order" is forming that will affect and potentially reconfigure digital markets, the underlying power relationships and the reach and role of consumer law and consumer organisations. Ambitious legal frameworks such as the Digital Services Act (DSA), the Digital Markets Act (DMA), and the emerging AI Act add their own solutions to harms that consumers experience due to unfair digital commercial practices. So far, consumer law, in the form of the Unfair Commercial Practice Directive, the Unfair Terms Directive and the GDPR, has served as the first line of defence against data-driven forms of misleading or aggressive targeting, dark patterns and exploitative data practices. In an earlier report, we discussed the potential and limits of consumer law to tackle the underlying digital asymmetries and the strategic exploitation of vulnerabilities that enable unfairness in the first place. In this follow-up report, we critically scrutinised the emerging regulatory framework and the extent to which it will alleviate concerns raised earlier, provide new innovative solutions but also create new challenges to digital consumer protection.

One core problem of the protection of consumers in the digital sphere is the existence of enormous digital asymmetries in the form of control over data, knowledge, infrastructures, and powerful algorithmic models that are optimised to maximise profits, clicks, engagement, addiction, and dependency. Consumers certainly benefit from a plethora of new applications and services, the ease of seamless integration, cross-border platforms and effortless customisation. This new level of customer convenience does, however, come at a price, in the form of loss of control, loss of privacy, new forms of addiction, susceptibility to manipulation, and structural dependencies. But in the commercial relationship between Very Large Online Platforms and Very Large Search Engines, one of the core premises of European consumer protection law – the idea of the average, reasonably circumspect consumer who is in the best position to protect their interests, negotiate the best conditions and vote with their feet – is fundamentally broken because of the degree of digital asymmetry.

The DSA, in combination with the DMA, is the European attempt to tackle some of the underlying asymmetries and power dynamics, for example in the form of systemic risk provisions, new procedural safeguards, more transparency towards consumers, regulators, and society, and the allocation of new powers and responsibilities for the European Commission as the "Überregulator" of digital markets. The DSA, the upcoming AI Act, and the DMA, are also adding new instruments of consumer protection. Examples are the bans on certain 'dark patterns' in the DSA, certain forms of manipulative AI systems in the AI Act, and new rights, such as new transparency rights, the prohibition to target based on childrens' data, the right to recommendations not based on profiling or a right to know whether the consumer interacts with a human or an AI.

It is early days, and we will yet have to see how this new digital order will work out in practice, if and what difference it will make. This is all the more true as the new instruments seem

rather underdeveloped, broadly worded, not co-ordinated with the existing consumer law acquis and leaving considerable discretion to private companies and standardisation bodies. The recommender provisions in the DSA, for example, seem promising at first sight but upon closer look probably do not reach deep enough into the technology stack to make any significant changes to the position and protection of the interests of consumers. Other provisions will need to be tested in practice to allow any meaningful conclusions, such as the provisions on dark patterns, the transparency requirements or the right to know the interlocutor. And yet, the present report was able to identify some important points of attention for consumer law, consumer law scholars, and consumer protection agencies alike. In the following, we will list some, without the ambition to be complete or do full justice to the richness of the findings in this report.

The new digital order introduces new rights and opportunities for consumers. One challenge moving ahead is to identify how exactly they relate to or add to existing consumer protection law. Both the DSA and the AI Act, for example, while targeting certain forms of deceptive or manipulative uses of digital technology and AI systems, also explicitly make reference to the provisions of the Unfair Commercial Practice Directive and the GDPR, but what they add in practice, how to distinguish which practice falls under which legal framework (and therefore also: which enforcement mechanism) and how enforcement between the different regulatory instances shall be organised is still very unclear. Then, there are emerging questions of consistency between consumer law and the new digital order. This report has demonstrated how both the DSA and the AI Act leaned heavily on the Unfair Commercial Practice Directive's concept of consumer vulnerability but also developed the concept further, broadened it and attached different legal consequences.

By transporting established notions from consumer law into a new context and regulatory framework that serves similar but also very different and new regulatory goals, the new digital order is also meshing together previously distinct concepts and spheres. The very understanding of the consumer is a first example. While the consumer under consumer law is essentially defined as and situated in the sphere of commercial interactions and agreements, the 'consumer' under the DSA is also a user, a citizen or even a content provider. As a consequence, the provisions that must protect the consumer against interference with their rights against unfair distortions of their economic decision-making power suddenly also protect their political decision making power or fundamental rights. On the one hand, the fusion of consumer and citizen rights, of individual and societal interests, reflects the reality of individuals in digital environments. On the other hand, it challenges clear-cut distinctions and conceptualisation of vulnerability, harm or misleading practices that underlie traditional consumer law. One challenge going ahead is again consistency, and how consumer law will accommodate or not accommodate such 'sphere transgressions", and how the two legal orders – consumer protection law and the new digital order – will relate to, and complement each other.

The expansion and extension of the new digital order into matters that so far were mostly subject to more classic consumer protection law also raises important questions for the role and substance of consumer law itself and consumer protection organisations. The need to update consumer law to the demands of the digital environment remains unchanged, and this report has made some important suggestions to that end, such as concrete suggestions on the need to reconsider the burden of proof, or how to make the Unfair Commercial Practices Directive more 'digital proof'. The question is how consumer law will or must position itself vis-à-vis the new digital order: more modestly as a safety net or as a complementary and authoritative

order that adds more conceptual clarity, interpretation and concrete rights for consumers in addition to those that the DSA and the AI Act offer. Seeing the vagueness or even lack of clear conceptualisations of notions such as manipulation or harm, and the relative distance that the European Commission as a digital regulator has to the daily reality of consumers on the ground, it is clear that consumer law and consumer organisations must continue to have an important complementary role, or even new roles, such as representing the interests of consumers in standardisation bodies or auditing and risk impact procedures.

Then, there are also more structural challenges ahead. The new digital order relies on concepts such as harm, vulnerability, manipulation, systemic risk to consumer protection and fundamental rights. The use of those concepts and broadening of their scope is not accompanied by precise definitions, leaving definitional voids and a certain level of conceptual messiness. Maybe the most pressing question is: whose task is it then to define, operationalise and fill these concepts with meaning? Traditionally, under consumer law that task would be reserved for judges and, to some extent, to consumer protection authorities, experts or academics. Under the new digital order, the power and burden to define when an algorithmic application is manipulative, or forming a systemic risk to consumer rights is shifting to new entities: to platforms, the providers of AI systems, and the European Commission as "Überregulator". This shift of the power and responsibility to define and operationalise key concepts of consumer protection and the leading role that private parties, such as platforms, developers and private standardisation bodies play triggers very practical challenges, like the lack of expertise, guidance but also the limited scope for regulatory or judicial oversight of the privatisation of consumer protection. The EU law as it stands, the DSA, the AIA and the UCPD taken together, leaves many questions open, to be concretised either by the private regulators, by the EU regulator through delegating or implementing decisions, by harmonised European standards and codes of practices. What remains from the praised ex-ante risk regulation, which stands behind the EU Digital Policy Legislation in practice? Or are we de facto moving to an ex-post control mechanism where the years to come will show the true impact of the DSA, DMA and the AIA on the level of protection, through national and European supervisory authorities and perhaps a pro-active European judiciary like in the GDPR? As the human rights chapter in this report concluded: "For now, the case law on the Charter is insufficient to provide a clear indication on the substantive level of protection offered by Charter rights to consumers in the digital economy." But if not the Charter, what or who else must provide the necessary guidance? And necessary such guidance will be, because private companies are no regulators or experts in human rights law and consumer protection, and also have no economic incentives to become those in the future.

Consumer law and the role of consumer protection organisations will change. Not only because of the new challenges from digitalisation and algorithmisation of markets but also because of the tectonic shifts in the governance of those markets – from national regulators to the Commission, new forms of co-governance between regulators and big tech companies, re-interpretations of traditional concepts and values in consumer law in the broader context of the digital society, new forms of cooperation. Therefore, not only individual rules must be subject to the fitness check, but consumer law itself.

IX. Annex: Proposals for a future Digital Fairness Act

I. A Right to Constructive Optimisation

Laurens Naudts, Natali Helberger, Marijn Sax, Michael Veale

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.

(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.[1]

(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) 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

1 Recital 4 is modelled to reflect (and protect) the values of self-development and self-determination as introduced and defined by Young in: Iris Marion Young, Justice and the Politics of Difference (Princeton, New Jersey: Princeton University Press, 1990), https://doi.org/10.2307/j.ctvcm4g4q; Iris Marion Young, Inclusion and Democracy (Oxford University Press, 2002), https://doi.org/10.1093/0198297556.001.0001.

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. The right to constructive optimisation should not be interpreted to create joint controllership on the side of consumers under the GDPR.

(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.

Article 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 XXX AIA. The scope and reach of the burden of proof follows Art. 12 UCPD (see below under 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 EMFA, 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 Art. 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 Practice Directive.

Concrete recommendations

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

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.

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.

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 Article 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 and 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 accountability groups, 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).

In a similar way, the failure to offer users a choice in the sense of Art. 27 (3) DSA creates a presumption of a systemic risk/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) Art. 5(2)(a) is meant to explain how such a right to constructive optimisation can inform also the interpretation of Art. 5 (2)(a) UCPD

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."

II. Regress of the Trader under the UCPD

Hans-W. Micklitz

December 2023

1) UCPD, GDPR and the Regress of the Trader

The first issue concerns the relationship between the UCPD and the GDPR. The anthology starts from the premise that the use of unlawfully obtained data – whatever their origin might be, has to be regarded as unfair commercial practice.[2] This consequence needs to be reiterated as there is still the (mis)perception that infringements of data protection law can only be prosecuted through the GDPR and the competent public authorities. In *Metaverse v. Verbraucherzentrale Bundesverband,* the CJEU confirmed that Art. 80 GDPR does not preclude the Member States from granting consumer organisations standing to initiate an action for injunction against infringements of the GDPR which are covered by the UCPD.[3]

The second issue concerns the responsibility of the 'trader', Art. 2 UCPD, who in commercial practices 'is acting for purposes relating to his trade, business, craft or profession and anyone acting in the name of or on behalf of a trader'. It seems that Art. 2 UCPD is designed in a way to cover new intermediaries, not least due to the comprehensive definition of commercial practices. There is one issue, though, which deserves to be regulated – the possible redress of a trader who has become subject to an injunction, but where the data on which the advertisement is built derives from a third party, typically one of the big tech companies. Art. 20 of the Digital Content and Digital Services Directive 770/2019 might serve as a source of inspiration.

2) Redress of the Trader under the UCPD

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 SME providers, who can afford the collection and processing of the data needed to build an advertising campaign. The provision in Directive 770/2019 runs as follows.

> ***Article 20 Right of redress***
>
> Where the trader is liable to the consumer because of any failure to supply the digital content or digital service, or because of a lack of conformity resulting from an act or omission by a person in previous links of the chain of transactions, the trader shall be entitled to pursue remedies against the person or persons liable in the chain of commercial transactions. The person against whom the trader may pursue remedies, and the relevant actions and conditions of exercise, shall be determined by national law.

2 M. Namyslowska, Future Proofing the Unfairness Test.

3 CJEU Case C-319/20 *Meta Platforms Ireland Limited v Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2022:322 (79) *Therefore, as the Advocate General observed in point 72 of his Opinion, that provision does not preclude the Member States from exercising the option it offers them in that consumer protection associations are entitled to take action against infringements of the rights provided for by the GDPR through, as the case may be, rules intended to protect consumers or combat unfair commercial practices, such as those provided for by Directive 2005/29 and Directive 2009/22.*

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 the 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.

Art XXX to amend 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.

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

Recital

Traders may use data for the building of advertising which they have bought on the market and over which they are unable to 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 who do not have the resources to collect and process the data themselves. These traders who are liable under the UCPD should be granted a right to redress against the company from which they bought the data. The right to redress presupposes that he acted in good faith and does not know or should 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.

III. Future-Proofing the Unfairness Test[4]

Monika Namysłowska

1. Proposal for new provisions in the UCPD

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 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.

(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 business-to-consumer 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

4 The research leading to this Chapter was partly supported by the National Science Centre (*Narodowe Centrum Nauki*) in Poland based on decision No. 2018/31/B/HS5/01169.

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.

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 (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).

Article 5(6) UCPD

The Commission is empowered to adopt delegated acts to amend this Directive by updating Annex I.

2. General remarks

As indicated in Chapter 6, Section V, the changes proposed in this Chapter can be incorporated into the UCPD. Detailed proposals will be presented below based on the systematic proposals drafted by Natali Helberger, Hans-W. Micklitz, Peter Rott, and Marijn Sax in the document **'Article 5a'**. However, as mentioned above, these proposals could also be part of a new chapter in the UCPD or a new legal act.

3. Amendments to the UCPD

3.1. New Article 5a

Proposals for operationalising the new general clause are **based on Article 5a UCPD**, as drafted by Natali Helberger, Hans-W. Micklitz, Peter Rott, and Marijn Sax:

'1. A digital commercial practice shall be unfair if it

2. is contrary to the requirements of professional diligence, and/or

a) establishes structural, informational or relational digital asymmetries/vulnerabilities, and

b) it materially distorts or is likely to materially distort autonomous decision making.'

The research undertaken in this project underscores the need to revise Article 5a to address the concept of digital professional diligence,[5] accommodate the multifaceted nature of consumer harm,[6] and ensure it functions as a horizontal safety net.[7] The proposed **new wording of Article 5a UCPD** reads as follows:

'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 the autonomous decision-making.'

Article 5a corresponds to Article 5 UCPD, specifically addressing digital commercial practices and the distinctive nature of infringements within the digital environment. To be fully effective, an additional provision in Article 5a is necessary, namely a **new paragraph 1 to Article 5a** - a general prohibition of unfair digital commercial practices. Its wording mirrors Article 5(1) UCPD, shifting the focus to digital commercial practices: 'Unfair digital commercial practices shall be prohibited.' This general prohibition will be clarified by Article 5a(2) in the same way that Article 5(2) elaborates on the general prohibition of unfair commercial practices set out in Article 5(1) UCPD.

The most evident and undisputed change is adding the phrase 'digital' to 'professional diligence' in point a) so that it reads:

'A digital commercial practice shall be unfair if it is contrary to the requirements of **digital professional diligence** (...).'

This change is a fine-tuning of the UCPD due to introducing the definition of digital professional diligence into Article 2.

I would like to propose **additional changes** to the previously suggested Article 5a, stemming from my research on enabling the UCPD to serve as a safety net for consumer issues and the consumer harm caused in the digital environment.

The next changes require **repealing point b)** of the previous proposal: 'establishing structural, informational or relational digital asymmetries/vulnerabilities.' This pivotal condition for combating unfairness is now embedded in the definition of digital professional diligence, including a reference to digital asymmetry and digital vulnerability. Superfluous repetition might cause interpretative challenges, especially when it concerns foundational concepts.

The general prohibition will be clarified by Article 5a(2) in the same way Article 5(2) elaborates on the general ban on unfair commercial practices set out in Article 5(1) UCPD. An additional

5 See Chapter 6, Section III.
6 See Chapter 6, Section IV.
7 See Chapter 6, Section V.

amendment to transform the UCPD into a horizontal safety net in the digital environment pertains to modifications in point a) by adding the phrase **'and/or the law'** so that it would read as:

> 'A digital commercial practice shall be unfair if it is contrary to the requirements of digital professional diligence and/or the law (...)'.

The term 'law' will not be defined in the UCPD.

Fulfilling the criteria of being contrary to the requirements of digital professional diligence and/or the law does not mean the digital commercial practice is automatically unfair. Also, the **second requirement** has to be fulfilled. In Section V of Chapter 6, I presented four options for this requirement:

> A digital commercial practice is unfair if (...) it materially distorts or is likely to materially distort:
>
> 1) consumer's behaviour;
>
> 2) consumer's behaviour in a manner that it causes or is likely to cause harm;
>
> 3) consumer's autonomous decision-making;
>
> 4) consumer's autonomous decision-making in a manner that it causes or is likely to cause harm.

As the most convenient, I consider the requirement proposed in the document 'Article 5a' by Natali Helberger, Hans-W. Micklitz, Peter Rott, and Marijn Sax. It states:

> 'A digital commercial practice is unfair if (...) it materially distorts or is likely to materially **distort consumer's autonomous decision-making**.'

Given the final text of the AIA, I also find **option No. 4** acceptable. This option reads:

> 'A digital commercial practice is unfair if (...) 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.'

The reasons for this are outlined in Chapter 6, Section V.

3.2. Amendments to Article 2

Below, I will present **new definitions** that need to be introduced to Article 2 UCPD, and I will suggest corrections to the changes proposed in the document 'Article 5a.'

A) 'Business-to-consumer digital commercial practices'

Previous research studies defined **digital commercial practices** as:

> '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 connected with the promotion, sale or supply of a product to consumers, whether or not that product is provided for remuneration'.

To broaden the applicability of the UCPD, an extension of this concept to encompass indirect connection with promotion, sale or supply is plausible as pointing to the characteristics of the digital environment. This effect will be achieved either through a broader formulation ('relating to a digital environment directly or indirectly connected with the promotion, sale or supply') or by omitting the word 'directly' ('relating to a digital environment connected with the promotion, sale or supply'). Even so, there is a possibility that not every consumer infringement will fall under the horizontal safety net. However, the comprehensive definition of digital commercial practices ensures that most will be encompassed.

B) 'Digital professional diligence'

The proposed definition of 'digital professional diligence' reads as follows:

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

As I pointed out in Chapter 6, Section V, this definition refers to key concepts introduced and elaborated upon in the 'EU Consumer Protection 2.0' report.

The definition of digital professional diligence is operational only when the UCPD includes **definitions of its key concepts**, namely digital vulnerability and digital asymmetry. Natali Helberger, Hans-W. Micklitz, Peter Rott, and Marijn Sax formulated the respective definitions in the 'Article 5a' analysis. Fully accepting their findings, I suggest minor corrections.

C) 'Digital asymmetry' and 'Digital vulnerability'

Before I provide detailed comments on both definitions, I would like to address a common concern regarding the 'Article 5a' document. Throughout the text, in both the Recitals and Articles, the phrases 'digital environment,' 'digital consumer environment,' 'digital choice environment,' and 'digital consumer/choice environment' are used. Using different but similar terms requires **clarification** regarding whether these represent separate concepts or one unified concept.

While capturing the nuances and specifics of the digital world is important, ensuring that the terminology used in a Directive remains consistent and unambiguous is equally crucial. Each term introduced in a legal context can be seen as a distinct legal concept, demanding its unique interpretation. Multiple terms with subtle differences increase the risk of misinterpretation, especially when these terms can be construed as addressing overlapping or interrelated areas. Employing a single term throughout any legal act establishes a consistent reference point. This consistency eliminates potential misunderstandings arising from using various but similar terminologies. A single, comprehensive term offers a balance of specificity and broad applicability, making it a suitable choice for a clear and effective UCPD. I opt for '**digital environment**' as an overarching concept, encompassing various digital environments and thus providing a broad and direct understanding.

Moving on to detailed comments, the **original definition of digital vulnerability** reads as follows:

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

> capacities to deal with the external factors. They may be situational, information or source bound and can include the lack of digital literacy, personal biases, etc. External factor covers the digitally mediated relationship, the digital consumer environments/digital choice environments, the knowledge gap and can include control over (personal) data into the preferences and behaviour of consumers, the design of digital consumer environments, the lack of interoperability, the way default settings are configured, etc.'

I suggest splitting the above definition into two parts. The **first sentence** would remain in the definition placed in the normative part of the UCPD, e.g. in Article 2 containing definitions. The **second part** of the definition could be moved to the Recitals as part of a new Recital. Directives follow a hierarchical structure where the main text provides the core principles or rules, while the Recitals serve as critical interpretative tools and give context, rationale, and illustrations. Thanks to this, the main body of the UCPD remains uncluttered. Moreover, keeping the illustrative examples separate ensures that the UCPD is not overly prescriptive and remains adaptable.

The remaining changes adapt the text to the language of the UCPD:

New paragraph of Article 2: '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.'

New recital of the UCPD: 'Internal factors refer to variations in digital capacities to deal with external factors. They may be situational, information or source-bound, including, for example, the lack of digital literacy or personal biases. External factors cover the digitally mediated relationship, the digital consumer environments/digital choice environments and the knowledge gap, and include, for example, control over personal data into the preferences and behaviour of consumers, the design of digital consumer environments, the lack of interoperability or the way of default settings configurations.'

In turn, the original definition of **digital asymmetry** reads as follows:

> 'Digital asymmetry refers to a situation of imbalance in relation to the knowledge and understanding of the functioning and impact of a digital commercial practice (informational asymmetry), imbalances in the (ongoing) commercial relationship that a digital consumer environment creates and maintains (relational), respectively 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 a digital choice environment (structural asymmetry).'

The definition of digital asymmetry should not be divided like the definition of digital vulnerability, as the examples provided therein form subsequent definitions (of informational, relational, and structural asymmetry). In this definition, it is, however, crucial to emphasise that the imbalance concerns the **trader-consumer relationship**. I propose to strike out '(ongoing)' in the phrase '(ongoing) commercial relationship' and 'and impact' in 'functioning and impact of a digital commercial practice', as functioning encompasses the impact. The modifications conform the text of the new paragraph of Article 2 to the linguistic style of the UCPD:

> '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).'

3.3. Amendments to Annex I

While I support the expansion of Annex I in Section V and, potentially, the creation of a **separate black list** under the heading 'Digital commercial practices which are in all circumstances considered unfair,' I do not propose adding additional blacklisted practices beyond those suggested in the 'EU Consumer Protection 2.0' report and those currently proposed in ongoing legislative procedures for time constraints in preparing this report.

3.4. Commitology procedure

As I indicated in Chapter 6, Section V, the UCPD should be expanded to allow the Commission to issue **delegated acts** for quicker changes to Annex I. The corresponding provision could read as Article 5(6):

> 'The Commission is empowered to adopt delegated acts to amend this Directive by updating Annex I.'

IV. Article 12 UCPD: Burden of Proof

Peter Rott

(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.

Related 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.

Explanation

Article 12 is largely borrowed from the forthcoming Product Liability Directive but has been adapted to the situation of digital asymmetry.

As the related recital indicates, the threshold of plausibility in the terms of Article 12(1) should not be high. The notion of meaningful explanation is borrowed from Articles 13(2)(f) and 14(2)(g) of the General Data Protection Regulation (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, in order to highlight what is meant by meaningful (Article 11 Artificial Intelligence Act in combination with Annex IV). 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.

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 is able to explain its function and provide related evidence, or that the third party does so on his behalf.

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

Article 12(3) 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.

Article 12(4) 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 Article 64 (2) of the forthcoming Artificial Intelligence Act that foresees disclosure of the source code not to the public at large but only to public enforcement authorities.

BEUC The European Consumer Organisation

Co-funded by the European Union

The content of this publication represents the views of the authors only and it is their sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.

BEUC – The Consumer Voice in Europe

Rue d'Arlon 80 – B – 1040 Brussels