1. **Regulating the Wild World of Digital Services in the EU**

Joasia Luzak

I. INTRODUCTION

When the scope of application of the Consumer Rights Directive[1] was discussed in the first decade of the twenty-first century, the attention of scholars and policymakers focused on contracts for the supply of digital content.[2] Ensuing discussions considered whether these could be a type of contract for the sale of consumer goods, for the provision of services or *sui generis* contracts. This uncertainty, which stemmed from the lack of a clear definition of digital content, continued to plague national laws until the adoption of the Digital Content and Digital Services Directive.[3]

For the first time, this more recent measure also singled out the provision of digital services. Previously these were perceived as either just a type of digital content or a subcategory of services, and therefore the need for their separate regulation was overlooked.[4] However, this separate recognition of digital services contracts did not guarantee their comprehensive regulation in the European consumer protection framework. Aware of this gap, the European legislator has recently turned towards the complex landscape of digital services and the new risks that they may bring to consumer protection. However, the scattered and piecemeal character of the ensuing regulation of this European market sector does not bode well for the prospect of effective enforcement in the coming years. This chapter critically analyses the scope of application of various current European consumer protection measures concerning digital services, identifying substantial gaps therein and emphasises the need for a legislative review on the EU level.

In section II we will look at the notion of digital services as introduced by the Digital Content and Digital Services Directive; its broad scope of application also encompassing digital services for the provision of which consumers did not provide a monetary payment. Thereafter the various specificities of addressing non-conformity of digital services will be discussed. Sections III and IV illustrate common practices of digital service providers and examine to what extent the current

---

[1] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [2011] OJ L-304/64 (Consumer Rights Directive, CRD).

[2] See e.g. Natali Helberger et al, 'Digital Content Contracts for Consumers' (2013) 36 Journal of Consumer Policy 37-57; Hervé Jacquemin, 'Digital Content and Sales or Service contracts under EU law and Belgian/French law' (2017) 8(1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 32-35.

[3] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L-136/1 (Digital Content and Digital Services Directive, DCDSD).

[4] See e.g. European Commission, 'Proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content' COM(2015) 634 final, Recital 11.

framework of consumer protection could regulate these, with a particular focus on unfair contract terms and unfair commercial practices. Paragraph V is future-oriented, introducing recent EU legislative developments and analysing their potential impact on users of digital services. The conclusion lists the identified consumer protection issues that arise when consumers engage with the providers of digital services and provides recommendations for the revision of the current European consumer protection framework.

II. DIGITAL CONTENT AND DIGITAL SERVICES DIRECTIVE

1. The notion of a 'digital service'

Article 2(2) of the Digital Content and Digital Services Directive (DCDSD) defines a 'digital service' as:

> "*(a) a service that allows the consumer to create, process, store or access data in digital form; or*
>
> *(b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service*".

Recital 19 DCDSD mentions as examples of digital services: software-as-a-service, e.g. video and audio sharing or other file hosting, word processing, games accessed in the cloud and social media. Currently, we could list such popular and diverse digital service providers as YouTube, Netflix, Steam, Dropbox or Facebook. The breadth of the definition of digital services, and the fact that it does not refer to the method in which traders may supply digital services, should make this definition future-proof. Despite the EU legislator having now defined the notions of 'digital services' and 'digital content' separately, in practice it may not always be easy to determine whether in the performance of a particular contract data is shared with consumers as digital content, products or as a service. Some authors suggest differentiating between transactions based on the availability of data, with temporary availability characterising services more often than digital content or products.[5]

The reasoning behind the adoption of the DCDSD encompasses the usual concerns about the costs that cross-border traders incur due to the lack of harmonised legal framework and the EU policymakers' wish to increase consumer confidence in e-commerce. Yet, additional reasons focus on the need to tackle specific, common issues related to the provision of digital content and digital services. These pertain to the often-encountered poor quality of digital content or digital services, the failure to supply them or the unilateral, unexpected modification of digital content or digital services.[6]

---

[5] Lena Mischau, 'The Concept of Digital Content and Digital Services in European Contract Law' (2022) 1 EuCML 6-13.

[6] Recital 5 and Article 1 Directive 2019/770.

Consequently, it is not surprising that the DCDSD both defines non-conformity of digital content and digital services, as well as providing consumer remedies that account for the above-mentioned issues.[7]

Nevertheless, it is not clear why it was necessary to specifically differentiate between digital content and digital services in the DCDSD, since its main purpose was to introduce a new framework for establishing non-conformity and awarding remedies. Whether consumers acquire digital content or digital services, the same subjective and objective conformity requirements, rules on traders' liability, remedies for lack of conformity, and rules on failure to supply, apply to their contracts. Whilst other legal instruments may award consumers with different rights, depending on whether consumers acquire digital services or digital content, this is not the case for the current DCDSD framework. Therefore, we could interpret the separation of digital services from the notion of digital content as EU policymakers drafting a future-proof instrument, anticipating a possibility that these two types of consumer acquisitions could start further deviating from one another.

Shortly following the adoption of the DCDSD, the notion of 'digital services' has indeed been introduced to other EU consumer protection measures.[8] And thus, we may find the same notion of 'digital services' used in the Consumer Rights Directive, with service contracts now also explicitly encompassing digital services.[9] Further, the notion of a 'product' in the Unfair Commercial Practices Directive[10] now explicitly refers to digital services and digital content.[11]

2. Non-monetary payment for the provision of digital services

When we analyse the scope of application of the DCDSD, we find that it only applies to such digital services that have been paid for, or where consumers undertook to pay a price for this service. However, the second sentence of Article 2(1) DCDSD also recognises the provision of personal data by consumers as payment, provided that the service provider does not exclusively process the personal data for the purposes of supplying the service, or due to compliance with legal requirements. This controversial provision allowed for the recognition of the monetary character of the collection and

[7] This regulatory focus also follows from the adoption of the DCDSD alongside Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods [2019] OJ L-136/28. EU policymakers deliberated for a while whether it would be best to include remedies for non-conforming digital content in the Directive 2019/771. The decision to separate these two measures allowed the scope of the DCDSD to be expanded to include digital services, whilst also addressing specific issues of this sector, such as the lack of delivery or access.

[8] Directive (EU) 2019/2161 of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L-328/7 (Modernisation Directive).

[9] Modernisation Directive introduced this notion to the new Article 2(1)(6) and (16) CRD.

[10] Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L-149/22 (Unfair Commercial Practices Directive, UCPD).

[11] Modernisation Directive introduced this notion to the new Article 2(1)(c) UCPD.

processing of consumers' personal data by digital service providers for the first time in EU consumer law.[12]

The controversial character of this solution stems from the possibility of this provision circumventing the current data protection regime.[13] In short, by using data as an element of contractual consideration, legitimacy might be given to traders utilising data as a commodity, weakening the status of data protection as a fundamental right.[14] However, without the DCDSD recognising that the provision of data could amount to a payment, consumers would likely be put at a contractual disadvantage, due to the applicability of national rules on gratuitous contracts. EU policymakers could not ignore the reality that providers of social media and other digital services often claim to supply consumers with 'free' digital services, whilst they base their business models on profiting from consumers' data.[15] Hence, this novel legislative solution could be cautiously applauded.[16]

The DCDSD's provisions do not, however, account for other types of non-monetary payments that consumers commonly provide in exchange for access to digital services. For example, the DCDSD does not apply to digital service contracts which have been concluded as a result of consumers providing their time and attention as consideration for the service, e.g. watching advertisements to access digital services.[17] This is one of the areas that still requires further legislative attention.

3. Modification of digital services

Whilst consumers often turn to digital services due to the ease and flexibility with which they can be adapted to their needs,[18] this does not mean that they always trust digital service providers to match the service to these needs. Consequently, Article 19 DCDSD limits the possibility of digital service providers modifying a digital service if it is supplied over a period of time to consumers; beyond a

[12] See more on this development e.g. M Narciso, ''Gratuitous' Digital Content Contracts in EU Consumer Law' (2017) 5 Journal of European Consumer and Market Law 198-206.

[13] See e.g. Laura Drechsler, 'Data as Counter-Performance: A New Way Forward Or A Step Back For The Fundamental Right of Data Protection?' (2018) at https://cris.vub.be/ws/portalfiles/portal/36462976/IRIS2017_DRAFT_Drechsler_V3.pdf accessed 30 August 2022.

[14] See e.g. Jorge Morais Carvalho, 'Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771' (2019) 5 Journal of European Consumer and Market Law 197.

[15] This will be further discussed in part III. See for examples of such statements Marco Loos and Joasia Luzak, 'Update the Unfair Contract Terms directive for digital services' (February 2021) Study for the European Parliament requested by the JURI committee at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf accessed 30 August 2022, 28.

[16] See e.g. Carvalho (fn 14), 197; Jan Trzaskowski, *YOUR PRIVACY IS IMPORTANT TO U$! Restoring Human Dignity in Data-Driven Marketing* (Ex Tuto 2021) 205-208.

[17] Loos and Luzak (fn 15), 20-21.

[18] Jan Marco Leimeister, Hubert Österle and Steven Alter, 'Digital services for consumers' (2014) 24 Electronic Markets 255-256.

modification that is necessary to maintain the conformity of a digital service, i.e. updates. A contract for the supply of a digital service would need to provide for such modification and indicate a valid reason for it. Further, any modifications should not give rise to additional costs for consumers. Finally, consumers should be entitled to terminate a contract upon receiving notification of a modification, reasonably in advance, before it takes effect, if they preferred to reject this modification. Alternatively, digital service providers should allow consumers to elect to retain the digital service without the modification, at their own risk rejecting the offered support.

The current practice of many digital service providers could be perceived as non-compliant with this last provision, since their online terms and conditions often state that they provide a digital service 'as is'.[19] This may suggest to consumers that they will not have a right to object to any permanent modification of this digital service. Alternatively, digital service providers may limit their notification obligation to situations where the modification is 'material' and has a 'negative impact' on consumers, the assessment of which is left to their discretion.[20] Such practices may mislead consumers about their statutory rights.[21] Article 22 DCDSD provides for a sanction in such circumstances, declaring contractual terms that would derogate from the protection framework set out by Article 19 DCDSD as non-binding on consumers.[22] Provided these provisions are robustly enforced, the above-mentioned types of contractual terms should start disappearing from the standard terms and conditions of digital service providers.

Undoubtedly, digital service providers need to be able to update digital services to maintain both security and conformity with the contract, due to the constant development of the digital environment. A contract may stipulate the digital service providers' obligation to update a service, and the consumers' right to expect such updates.[23] However, this obligation could also simply follow from the necessity to maintain the digital service's conformity with the contract.[24] Furthermore, the digital service providers' compliance with the obligation to provide an update to a digital service, does not equate to ensuring the service's security and conformity, if consumers need to install the update. Consumers may choose to ignore installing updates, yet, as a result of such a decision, they relinquish their rights to a conforming digital service.[25] There could be various reasons for consumers declining an update, e.g. their reluctance to get to know the new version of a service or their preference for the

[19] See e.g. Terms and Conditions of iTunes, part 'Additional Apple Music Terms' at https://www.apple.com/uk/legal/internet-services/itunes/uk/terms.html accessed 30 August 2022.
[20] See e.g. Terms and Conditions of YouTube, part 'Develop, Improve and Update the Service' at https://www.youtube.com/static?gl=GB&template=terms accessed 30 August 2022.
[21] Loos and Luzak (fn 15), 22.
[22] Ibid, 24.
[23] Article 7 DCDSD.
[24] Article 8 DCDSD.
[25] Recitals 44 and 47 DCDSD.

previous version thereof. If a contract stipulates, therefore, a right for digital service providers to automatically update provided digital services, this could infringe consumers' statutory rights to refuse a specific update.[26]

Considering the binding nature of the provisions of the DCDSD, pursuant to its Article 22, a contractual term undermining consumers' statutory right to refuse an update would be non-binding on consumers. A similar non-binding effect should apply to any limitations or exclusions of the digital service providers' liability in case of intentional or grossly negligent conduct in modifying digital services. For example, if a digital service provider does not provide updates within a reasonable time after a lack of conformity or a security risk should have been identified. It should be noted that whilst digital service providers have an obligation to offer updates, consumers should retain a choice to reject such updates. Nevertheless, pursuant to Recital 47 DCDSD, the rejection should not lead to the digital service providers' liability if non-conformity could have been prevented by the update. Other contractual terms that exclude or limit liability in such circumstances should be assessed as unfair, and consequently non-binding.[27]

Interestingly, amongst harmonised remedies for the non-conformity of a digital service we do not find an option for consumers to withhold performance of their obligations, e.g. a payment or a provision of data, if a digital service provider interrupts or suspends the supply of a digital service. Recital 18 DCDSD leaves this matter to the Member States to regulate. Therefore, consumers' legal position in such cases will vary in different Member States.[28] This is a weakness of the DCDSD.

4. Data rights

Lastly, some of the DCDSD provisions address issues beyond the consequences of consumers receiving non-conforming digital services or the failure to supply digital services. Importantly, the Directive recognises that the use of a digital service is often irrevocably linked to sharing or creating digital content by consumers. Article 16 DCDSD anticipates the consumers' wish to regain access to such digital content upon termination of a contract with the digital service provider. For example, consumers may upload and share various photographs or videos with their networks when using Facebook or other social media. Following the termination of a contract, digital service providers must make such digital content, other than personal data, available to consumers upon request. This should be provided free of charge, without hindrance, within a reasonable time, and in a commonly used and machine-readable format. This right seems independent of who decides to terminate a contract or

[26] See e.g. Terms and Conditions of iTunes, part 'Third-Party Devices and Equipment' at https://www.apple.com/uk/legal/internet-services/itunes/uk/terms.html accessed 30 August 2022.
[27] See Loos and Luzak (fn 15), 24.
[28] Ibid, 22.

the reason for the termination, thus it could apply when the termination occurs for reasons other than the non-conformity of a digital service.

Whilst the EU policymakers' acknowledgment of the consumers' interest in and the right to access and manage their data is important for ensuring the balance of interests in the digital environment, it is questionable whether consumers will be aware of this right. Its placement in a legislative measure addressing mainly the issues of non-conformity of digital services is troubling, as it may obscure its existence or its relevance for scenarios that do not concern non-conformity.

III. UNFAIR TERMS OF DIGITAL SERVICE PROVIDERS

1. Review of the unfairness framework and its level of harmonisation

In February 2021 the European Parliament published a report[29] that analyses the need to update the Unfair Contract Terms Directive (UCTD)[30] in light of the market practices of digital service providers. As the UCTD was adopted long before digital services dominated the marketplace, its framework may not always be best suited to respond to the risks and challenges generated by digitalisation.[31] Whilst the detailed analysis of this report will not be repeated in this chapter, it will outline some of the report's suggested improvements that could be introduced to the UCTD framework to remedy current regulatory gaps. Such improvements should lead to the revision of many of the standard terms and conditions currently used by digital service providers, which are causing a detrimental imbalance in digital services contracts.

The first recommendation concerns changing the character of Annex I UCTD, from an indicative list of unfair terms, to a list of terms that would always be prohibited/blacklisted, if they are included in contracts between digital service providers and consumers. This could be accompanied by a grey list, being a list of terms presumed to be unfair. Without inclusion of European grey and black lists of unfair terms, the sector lacks certainty. This is the result of the general unfairness test requiring courts to consider all circumstances of each case, as well as the extent to which the term derogates from otherwise applicable provisions of national law.[32] The problem of uncertainty is not limited to the sector of digital services, however, such services often tend to be provided cross-border, amongst others due to the use of online platforms and portability of devices, on which they are received.[33]

---

[29] Ibid.

[30] Council Directive 93/13/EEC on unfair terms in consumer contracts [1993] OJ L 95/29 (Unfair Contract Terms Directive, UCTD).

[31] See Loos and Luzak (fn 15), 6.

[32] CJEU case C-415/11 *Aziz* ECLI:EU:C:2013:614, para 69; CJEU case C-226/12 *Constructora Principado* ECLI:EU:C:2014:10, para 21. See Loos and Luzak (fn 15), 47.

[33] See e.g. European Commission, 'The Digital Services Act package' (version from 5 July 2022) at https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package accessed 30 August 2022; Council of the EU,

Consequently, there is a greater risk for both digital service providers and consumers stemming from the lack of further action on the European level to promote more harmonisation.

2. Unfair terms in the digital environment

The second recommendation is that the terms currently listed in Annex I UCTD be updated to include (potentially) unfair terms which are commonly used by digital service providers. Some examples of such terms are discussed below.

2.1. Binding consumers to unseen terms

For example, Article 1(i) Annex I UCTD states that it may be unfair to irrevocably bind consumers to terms with which they had '*no real opportunity of becoming acquainted before the conclusion of the contract*'. This provision does not require digital service providers to ensure that consumers read their terms, but rather to draw their attention to the terms' existence and provide consumers with an opportunity to read them, e.g. by removing any time pressure to do so. It is a common practice of digital service providers to provide a hyperlink on their websites to standard terms and conditions and subsequently ensure that a provision in these terms declares them binding. Together with Marco Loos, the author of this chapter argued that such a market practice provides insufficient genuine opportunity for consumers to notice contractual terms, let alone feel enticed to read them.[34] Consequently, the binding force of standard terms could be challenged. The provision in the Annex could clarify that a disclosure of terms and conditions through a hyperlink does not automatically create a genuine opportunity to become acquainted with them. It would be for the digital service providers to prove that they tried to draw consumers' attention to the hyperlink, and consequently to their terms and conditions. They could achieve this by using a tick box or otherwise asking for an express confirmation of the consumers' awareness of applicable terms and conditions.[35]

2.2. Browse-wrap contracts

Another term that should be blacklisted, which is just one of many examples provided in the report,[36] is a term declaring users bound to a contract with digital providers, just based on users having

'Portability of digital services across the EU: Council adopts new rules' (press release of 8 June 2017) at https://www.consilium.europa.eu/en/press/press-releases/2017/06/08/portability-of-digital-services/ accessed 30 August 2022.

[34] See Loos and Luzak (fn 15), 8.

[35] Ibid. Similar suggestions for ensuring links stand out were made by American lawyers in response to the district court's finding that hyperlinked terms were not always validly incorporated into concluded contracts, see e.g. Meighan E O'Reardon and Rachel G Newell, 'Think Before You Link: The Legal Risk with Nested Hyperlinks in Online Terms' (Pillsbury Law, 17 September 2020) at https://www.pillsburylaw.com/en/news-and-insights/legal-risk-nested-hyperlinks.html accessed 30 August 2022.

[36] See Loos and Luzak (fn 15), 49-52.

accessed services of such providers.[37] This practice results in browse-wrap contracts being concluded. The report further suggests that the enforcement of browse-wrap contracts could be prevented through the use of the unfairness test. Indeed, such terms create an imbalance in parties' rights and obligations to the detriment of consumers, contrary to good faith.[38] The imbalance arises when consumers can access the digital service without digital service providers having first drawn their attention to their terms and conditions, and thereafter giving consumers a real opportunity to read these terms. Digital service providers should not be able to claim that users of their services provided actual consent to the conclusion of a contract, as they may have never seen the contractual terms and conditions. To protect consumers from concluding browse-wrap contracts, digital service providers should always inform them that they are about to conclude a contract simply by accessing their services, provide them with the terms and conditions of this contract, and ask for confirmation of the consumer's intention to enter into a contract. [39]

2.3. Prohibiting negative reviews

Furthermore, consumers searching for digital services of a particular type are likely to look up online reviews for digital service providers in that sector, replacing the conventional word-of-mouth with its electronic version. Consequently, the veracity of online comparison and review sites is key to consumer decision-making.[40] For this reason, it is important to blacklist any terms that seek to prohibit or discourage consumers from publishing negative reviews.[41] Such prohibitions could result in consumers only receiving a partial picture of the quality of a given digital service (provider).

2.4. Digital inheritance

For an example of a term that should be greylisted, we could look at terms prohibiting digital inheritance. Digital service providers may have a legitimate interest in limiting the possibility of their users transferring their rights under the contract to third parties. For example, such practices could lower the number of potential users for their services. However, this justification is less relevant when we consider whether national inheritance rules should apply to digital services. Due to the diverse landscape of digital services, survivors of deceased consumers could try to claim access to the data stored in a digital service, e.g. Dropbox. Alternatively, they could try claiming any virtually owned

[37] This would only apply if browse-wrap contracts could actually meet the requirements of the formation of a valid contract, which could be contested. See e.g. Elizabeth MacDonald, 'When is a contract formed by the browse-wrap process' (2011) 4 International Journal of Law and Information Technology 285-305.
[38] See Loos and Luzak (fn 15), 17.
[39] Ibid.
[40] See also Madalena Narciso, 'The Unreliability of Online Review Mechanisms' (2022) 45 Journal of Consumer Policy 349-368.
[41] See Loos and Luzak (fn 15), 33.

assets linked to the provision of digital services, e.g. in a multiplayer online game. An argument could be made that, as long as digital inheritance does not impact the position of other consumers, which could, for example, happen when a successor of a deceased consumer took ownership of their character in a multiplayer online game, heirs should also be entitled to inherit digital rights.[42] However, as there could be legitimate reasons for excluding such a transfer of rights, no-survivor clauses should only be presumed unfair. Digital service providers could then argue to the contrary.[43]

3. Sanctions for unfairness

Third, the report recommends strengthening the sanctions that digital service providers would face if they use unfair terms. Currently, any unfair term used by digital service providers is non-binding on consumers, pursuant to Article 6 UCTD. If an unfair contract term can be removed from a contract without endangering its core, the contract itself remains in place, even if the annulment of the contract was more beneficial to consumers. This follows from the need to restore the contractual balance between the parties by removing unfair terms from contracts, rather than the wish to promote consumers' interests.[44]

However, if the Annex contained a blacklist, then the use of such terms could be sanctioned more harshly. Consequently, where a blacklisted term was used, courts could be given leave to declare the whole contract non-binding, if this was advantageous to consumers, rather than just the unfair term.[45] After all, digital service providers should be required to adhere to professional diligence standards, which include the obligation to ensure their terms and conditions are compliant with Annex I UCTD. Moreover, infringement of such standards could lead to the finding of an unfair commercial practice, pursuant to Article 5 UCPD, if it also impacted consumer decision-making. The sanctions for finding an unfair commercial practice include an option to terminate a contract which has been concluded on the basis of such a practice. The topic of unfair commercial practices of digital service providers is further discussed in the following section.

4. Unfairness of infringing data protection rules

[42] Ibid, 27.
[43] The topic of digital inheritance and national rules regulating this issue have been discussed in two issues of the Journal of European Consumer and Market Law, see for more details: Kristin Nemeth and Jorge Morais Carvalho, 'Digital Inheritance in the European Union' (2017) 6 Journal of European Consumer and Market Law 253.
[44] CJEU case C-453/10 *Pereničová and Perenič* ECLI:EU:C:2012:144, paras 31, 33.
[45] See Loos and Luzak (fn 15), 8, 48.

The fourth recommendation follows from the link that the report draws between the EU consumer protection framework and the General Data Protection Regulation.[46] Lack of compliance with the principles and obligations of the GDPR, leads to digital service providers facing the sanctions envisaged in this Regulation. However, the deterring effect could be stronger if, in addition to having to pay administrative fines, a non-compliant digital service provider could be exposed to negative contractual consequences, e.g. pursuant to the UCTD. This could arise from any standard term being determined as unfair if it contradicts the GDPR.[47]

As a result of these additional sanctions applying, users of digital services could withhold performance or demand the termination of a contract, whilst digital service providers would not be able to rely on a limitation or exclusion of liability for the breach of data protection principles. For example, if digital service providers draft a term excluding their liability for any lack of accuracy in the personal data they process, this term could be considered unfair.[48] After all, Articles 16 and 17 GDPR give data subjects respectively a right to demand rectification or erasure of inaccurate data without delay.

A general exclusion of liability by digital service providers would need to be interpreted narrowly, as it would only apply to situations where they had no knowledge of the inaccuracy or where the rectification of the data would not be feasible without excessive costs. Most consumers would not be aware of such limitations, which means that a broadly formulated term could convince them that they have no rights in such situations. Such a term has, therefore, the potential of causing significant imbalance in parties' rights and obligations, contrary to good faith and to the detriment of consumers.

IV. UNFAIR PRACTICES OF DIGITAL SERVICE PROVIDERS

1. Applicability of the UCPD

The recent revision of the UCPD confirmed the broad scope of its application by extending the notion of a 'product' to also include digital services and digital content explicitly.[49] The concept of commercial practices defined in Article 2(d) UCPD is also broad, such that it encompasses activities and conduct of digital service providers both prior to and post-supply of the digital service. Interestingly, whilst the Modernisation Directive clearly aims to align the CRD to the DCDSD, regarding its applicability to

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to processing of personal data and on the free movement of such data [2016] OJ L-119/1 (General Data Protection Regulation, GDPR).

[47] See Loos and Luzak (fn 15), 34; Natali Helberger, Frederik Zuiderveen Borgesius and Augustin Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1451.

[48] See Loos and Luzak (fn 15), 35-36.

[49] New Article 2(c) UCPD following amendment introduced by the Modernisation Directive.

consumer contracts concluded in exchange for consumers supplying their personal data, this has not been reflected in the revision of the UCPD framework. We could therefore question whether a digital service provider's commercial practice could be deemed unfair where they did not receive monetary payment for it.

The CJEU has previously stated that even if a consumer does not purchase a particular product, but is at a stage of considering such a purchase, the framework of the UCPD remains applicable.[50] Therefore, the monetary exchange between parties is not a pre-condition to apply the UCPD. Consequently, we could extrapolate this reasoning to claim that the UCPD also applies to the provision of such digital services for which consumers do not pay money. This would require a wide range of digital service providers to comply with the UCPD. This interpretation should be confirmed by the EU legislator to both ensure consistent application of the UCPD framework in Member States and provide more legal certainty.

2. Misleading information

In the pre-contractual stage, digital service providers need to be especially careful not to provide consumers with any misleading information. This could follow from a wrong classification of the provided digital content as a digital service, or vice versa. Consumers should know what type of product they are acquiring, as the wrong classification may impact their rights. For example, consumers enjoy the right of withdrawal when acquiring digital services, but it could be excluded when they are supplied with digital content.[51] Another example is where digital service providers present themselves as non-professional parties, which could evoke an impression that the consumer protection framework does not apply to the concluded contract; a commercial practice which is blacklisted by Item 22 Annex I UCPD. A further example can be found in the infamous statement of digital service providers that their services are provided 'free' to consumers, whilst they are profiting from the collection and processing of consumer data.[52] If the recognition of non-monetary forms of payment for the provision of digital services is recognised, as suggested above, claims referring to the 'free' character of digital services should be considered misleading, and therefore unfair.[53]

3. Unfair data collection and processing

[50] CJEU case C-281/12 *Trento Sviluppo and Centrale Adriatica* ECLI:EU:C:2013:859, para 36.
[51] Article 16(m) CRD and Recital 30 Modernisation Directive.
[52] See e.g. Marcin Kulesza, 'Italian court says Facebook isn't free' (in principle blog, 13 February 2020) at https://codozasady.pl/en/p/italian-court-says-facebook-isnt-free accessed 30 August 2022.
[53] See Loos and Luzak (fn 15), 21, 28-29; Cemre Bedir, 'Contract Law in the Age of Big Data' (2020) 16(3) European Review of Contract Law 355.

Both before and during the performance of the contract, digital service providers may require consumers to share their personal data. The question then arises whether they should collect and process data beyond what is necessary for the provision of a service.[54] In a pre-contractual stage, the data that consumers share could help digital service providers steer them to specific offers, by ranking them to match consumer preferences, or adjust the content of these offers, e.g. pricing.[55] Such practices introduce a certain level of personalisation to digital services. Whilst, in a contractual stage, digital service providers may reserve for themselves a unilateral right to revise their terms and conditions to improve the provision of digital services, with further data collection necessary to facilitate this improvement. This may be problematic, if consumers are not given an option to refuse such an improved service, but rather are tied into newly created, additional services, which in practice could have been offered separately.[56]

In both the above-mentioned scenarios, digital service providers use collected data to conduct their business more effectively. Yet, if consumers remain unaware of such practices taking place, they may be misled as to the extent of data protection awarded to them, and more importantly about the limitations in their choice architecture that may impact their decision-making.[57] In recognition of this problem, the European legislator have specified further information obligations regarding the use of data collected prior to the conclusion of a contract. The Modernisation Directive introduced an obligation for digital service providers to disclose that certain offers have been positioned higher or better in search results, if changes in ranking were paid for by these providers.[58] Further, they also need to disclose occurrences of personalised pricing based on automated decision-making.[59]

We are awaiting the CJEU's decision regarding the classification of the practice of tying increased data collection to the provision of a new version of digital services.[60] Hopefully, the CJEU will recognise that more could be done to improve consumer protection in the area of digital services in light of high volumes of collected and processed consumer data. For example, since Article 5 GDPR

[54] On difficulties of establishing what data is 'necessary' for the performance of a contract see e.g. Bedir (fn 53), 354. See also Trzaskowski (fn 16), 56-59.

[55] See e.g. Maurits Kaptein et al, 'Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles' (2015) 77 International Journal of Human-Computer Studies 38-51; Marc Bourreau & Alexandre de Streel, 'The regulation of personalised pricing in the digital era' (OECD publication, 25 September 2020) DAF/COMP/WD(2018)150 at https://one.oecd.org/document/DAF/COMP/WD(2018)150/en/pdf accessed 30 August 2022.

[56] Decision of BGH of 23 June 2020, KVR 69/19; Rupprecht Podszun, 'Facebook Case: The Reasoning' (28 August 2020) at https://www.d-kart.de/en/blog/2020/08/28/facebook-case-the-reasoning/ accessed 30 August 2022.

[57] The term 'choice architecture' was first introduced by Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving decisions about health, wealth, and happiness* (Yale University Press 2008).

[58] See Recitals 18 and 20 Modernisation Directive and a newly introduced Item 11a in Annex I UCPD.

[59] See Recital 45 Modernisation Directive and a newly introduced Article 6(1)(ea) CRD.

[60] Request for a preliminary ruling in case C-252/21 *Meta Platforms and Others (Conditions générales d'utilisation d'un reseau social)* [2021] OJ C-320/16.

stresses that collection and processing of personal data should correspond to such important principles as purpose limitation and data minimisation, enforcement authorities could take a narrow view as to what counts as 'necessary' data for the provision of digital services.[61] This does not mean that collection and processing of data could not be at the core of the business of digital service providers, especially if it replaced monetary payment by consumers. However, we could expect that in the latter cases, digital service providers clearly inform consumers about their business model and are transparent about their data collection and processing practices.[62] Otherwise, we could find them not only in breach of the GDPR requirements but also accountable for omitting to disclose essential information to consumers, since this could qualify as a misleading omission pursuant to Article 7 UCPD.

A further inquiry should be made into the potential aggressive character of certain data collection practices of digital service providers, pursuant to Articles 8 and 9 UCPD. For example, if the notion of 'coercion' was interpreted broadly, it could encompass situations where digital service providers use consumer data to personalise offers presented to consumers, if this significantly impaired consumers' decision-making. The question remains as to when digital service providers' practices cross the line of social tolerance, particularly in respect of the pre-contractual phase, in which they often take the form of coercive advertising.[63] We would likely need to find evidence of such practices restricting both the freedom of choice and the freedom of conduct of consumers.[64] Previously, scholars suggested that digital exploitative practices would more easily be evidenced as amounting to undue influence rather than coercion. Nevertheless, the current unfair commercial practices framework would make even that claim challenging for consumers to substantiate.[65]

Regarding practices of digital service providers, intuitively we would likely perceive the revision of contractual terms to increase data collection as an example of undue influence, if it occurs after consumers have already invested in a particular digital service, given that they may consequently be reluctant to discontinue use of the service. However, it is yet unclear whether the existence of a

---

[61] See e.g. Rafqa Touma, 'TikTok has been accused of 'aggressive' data harvesting. Is your information at risk' (The Guardian, 19 July 2022) at https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk accessed 30 August 2022. See comments on the interpretation of the 'necessity' of processing personal data for the purposes of the legitimate interests pursued: Case C-252/21 *Meta Platforms and Others (Conditions générales d'utilisation d'un reseau social)* EU:C:2022:704, Opinion of AG Rantos, paras 61, 64-66. AG Rantos highlights indeed the exceptional character of such processing by referring to it as having to be 'strictly necessary'.

[62] See further, on various issues related to the use of data for persuasion profiling purposes: Loos and Luzak (fn 15), 31-32.

[63] See e.g. Natali Helberger et al, 'EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets' (BEUC March 2021) at https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection.2.0.pdf accessed 30 August 2022 67.

[64] The CJEU so far required evidence of such restrictions to recognise the aggressive character of commercial practices, see e.g. CJEU C-628/17 *Orange Polska* ECLI:EU:C:2019:480. See also ibid, 68.

[65] See e.g. Helberger et al (fn 63), 66-71.

relationship between a digital service provider and a consumer, developed because of the consumer's investment of time and resources in a particular digital service, could lead to a finding that the digital service provider holds a position of power in that relationship.[66]

4. Unfair reviews and professional diligence standard

The practice of consumers giving service reviews, provides an example of a possible unfair commercial practice by digital service providers arising post-contractually. In relation to posting online reviews, we could identify a variety of possible unfair commercial practices, e.g. reviews purportedly submitted by consumers, which have been drafted by professional parties, posting false reviews, and not-disclosing that reviews have been paid for.[67] Further, digital service providers may try to inhibit, or even prohibit, posting of negative reviews online; a practice which clearly impacts both the freedom of choice and the freedom of conduct of consumers.[68]

The newly revised blacklist aims to address concerns about the impact that online word-of-mouth has on consumers, whilst also guaranteeing the reliability thereof. It is therefore surprising that the European legislator did not take the opportunity to include a greater number of digital service providers' practices in the Annex. This is especially jarring when we consider that the general unfairness test of Article 5 UCPD requires commercial practices to be contrary to traders' professional diligence to qualify as unfair. This test is purposefully vague, allowing it to be future proof. However, its practical application to current commercial practices is weakened, due to national enforcement organisations' lack of resourcing to pursue findings of unfairness, particularly on such an uncertain basis.[69] A further problem relates to the lack of common standards of skill, care and honest market practices in the digital environment. Whilst there is increased self-regulation of the digital services market in certain areas, such as regarding illegal hate speech online or online advertising,[70] this is not yet omnipresent and its transnational character is piecemeal.

V. NEW LEGISLATIVE DEVELOPMENTS

[66] See also Joanna Strycharz and Bram Duivenvoorde, 'The exploitation of vulnerability through personalised marketing communication: are consumers protected?' (2021) 10(4) Internet Policy Review 14-16.
[67] These occurrences have now been blacklisted in new items 23b and 23c of Annex I UCPD. See also Narciso (fn 40, 349-368.
[68] See Loos and Luzak (fn 15), 34.
[69] See e.g. Helberger et al (fn 63), 71-73.
[70] See e.g. European Commission, 'Code of conduct on countering illegal hate speech online' (May 2016) at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en or Stichting Reclame Code, 'Reclamecode Social Media & Influencer Marketing (RSM) 2019' https://www.reclamecode.nl/nrc/reclamecode-social-media-rsm/ accessed 30 August 2022.

1. Modernisation Directive

As previously mentioned, the most recently adopted EU legislative act within the consumer protection framework, the Modernisation Directive, explicitly specified digital services as products that may be the object of commercial practices. Consequently, they are regulated by the UCPD framework. This clarification is a welcome addition. Nevertheless, there are some issues with respect to the other obligations introduced to the UCPD by the Modernisation Directive.

1.1. Transparent ranking of online search results

Firstly, questions arise as to the scope of application of the new prohibition of ranking online search results according to payments received from traders and service providers, unless the paid character of such results is transparently published.[71] Recital 20 of the Modernisation Directive also mentions that 'indirect payment' will lead to this new disclosure obligation, which should make it broadly applicable. However, the prohibition only applies when a payment aims to 'achieve higher ranking'.[72] This may prove difficult to prove, especially if such a result is implied in the payment of a general listing fee.

Further critique pertains to the limitation of the applicability of this information obligation, since it only binds digital service providers when consumers entered a search query online.[73] This means that the order of any other information provided to consumers, e.g. of online advertisements on websites of digital service providers, will not need to be justified. Similar concerns can also be raised regarding the disclosure obligation introduced by the new Article 7 paragraph 4a UCPD. Pursuant to which, providers of digital services facilitating a search of products offered by different traders or consumers, commonly referred to as comparison websites, must disclose the main parameters determining the ranking of products following a consumers' search query.

1.2. Ensuring authenticity of consumer reviews

Another new blacklisted practice is the posting of consumer reviews without having first taken reasonable and proportionate steps to check whether they have been submitted by genuine consumers of the specific product or service. Additionally, commissioning or submitting false reviews is also prohibited.[74] One of the weaknesses of this prohibition lies in its vague wording: When would digital service providers' authenticity checks be considered reasonable and proportionate?[75] It is

[71] Recital 20 and Article 3 Modernisation Directive introduced new Point 11a to Annex I UCPD.
[72] See e.g. Trzaskowski (fn 16), 94-95.
[73] Ibid, 95.
[74] Article 3 Modernisation Directive introduced new Points 23b and 23c to Annex I UCPD.
[75] See also Mateja Durović and Tim Kniepkamp, 'Good advice is expensive – bad advice even more: the regulation of online reviews' (2022) 14(1) Law, Innovation and Technology 146-147.

unclear whether they would need to employ any technological measures to comply with this provision, such as a multi-factor authentication or identification verification, or whether they could rely on self-declaration by the person posting the review as to their non-professional character.

Moreover, the scope of the pre-contractual material information digital service providers must disclose now encompasses information on how they ensure the authenticity of online reviews.[76] Failure to provide this information could amount to misleading consumers by omission. One of the weaknesses of this disclosure obligation already identified concerns the risk of overloading consumers with technical data on the processing of online reviews.[77]

1.3. Data management following withdrawal from a contract

Amongst the changes introduced to the CRD, digital services have been explicitly included as service contracts, clarifying the applicability of the CRD to digital service contracts.[78] The definition of digital services follows the concept introduced in the DCDSD.[79] As previously mentioned, the scope of the CRD was extended to also apply to contracts where consumers provide data in exchange for the supply of digital content or digital services. Consequently, new provisions were added to Article 13 CRD regulating the data management obligations of traders when consumers use their right of withdrawal.

The issue of data management following the consumers' termination of a contract is complex, regardless of whether the termination occurs because of the use of the right of withdrawal, a non-conformity, or for other reasons.[80] It becomes more contentious when the data was a part of or the sole consideration for the conclusion of a contract, and the digital service provider used Article 6(1)(b) GDPR as the legal basis for the collection and processing of the personal data. Here, the European legislator falls back on the GDPR, obliging digital service providers to comply with its provisions if consumers withdraw from a contract, as far as their processing of the personal data of consumers is concerned.[81] Of particular relevance may be the principle of storage limitation from Article 5 GDPR, restricting the digital service provider's processing and storage of the personal data following a consumers' withdrawal from a contract, as well as the data subject's right to erasure from Article 17 GDPR.[82] The CRD further addresses the consequences of a withdrawal for data other than the personal data, by obliging traders to limit their use of any content created or provided by consumers during

[76] Article 3 Modernisation Directive introduced new Article 7(6) UCPD.
[77] Durović and Kniepkamp (fn 75), 147.
[78] Article 4 Modernisation Directive revised Article 2(1)(6) CRD accordingly.
[79] Article 4 Modernisation Directive introduced Article 2(1)(16) CRD.
[80] See e.g. Bedir (fn 53), 363-364.
[81] Article 4 Modernisation Directive introduced Article 13(4) CRD.
[82] See European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (version 2.0, 8 October 2019) at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf accessed 30 August 2022, 12.

their use of digital services.[83] Exceptionally, pursuant to the same provision, digital service providers may continue to use such content if it:

(a) has no utility outside the context of the digital content or digital service supplied by the trader;

(b) only relates to the consumer's activity when using the digital content or digital service supplied by the trader;

(c) has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts; or

(d) has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content.

As an example, we could think here about consumers playing online video games and creating content within them, either themselves or with other consumers, that could not easily be disaggregated from the game if it becomes part of its virtual world. Otherwise, as the new Article 13(7) CRD stipulates, consumers may retrieve their data and shared digital content for free, in a commonly used format and without inconvenience from the digital service provider. Correspondingly, the new Article 14(2a) CRD introduces an obligation upon consumers to refrain from the continued use of the digital service, following their withdrawal from the contract.

1.4. Transparency as to automated decision-making

An interesting addition is digital service providers' new obligation to clarify when the price of supplying their services was personalised on the basis of automated decision-making.[84] The obligation does not expect digital service providers to provide details of how the personalisation affects a given consumer, e.g. whether the price offered to them is beneficial or detrimental when compared to prices offered to other consumers. Digital service providers also have no duty to reveal which data has influenced the process of personalisation. Providing consumers with only an indication that personalisation has occurred, without mentioning either its justification or consequences, seems dissatisfactory and unlikely to guarantee transparency.[85] Recital 45 of the Modernisation Directive mentions that the objective of this obligation is to allow consumers to "(…) *take into account the*

[83] Article 4 Modernisation Directive introduced Article 13(5) CRD.

[84] Article 4 Modernisation Directive introduced Article 6(1)(ea) CRD.

[85] We could also hypothesise whether automated decision-making could ever be transparent, as even revealing all the technical details, on which basis the automation occurs, is unlikely to account for machine learning. We should also not expect average consumers to be able to understand this technology. This would mean that terms on automated decision-making could not be excluded from the scope of the unfairness test, even if they defined main obligations of parties in a contract.

potential risks in their purchasing decision. (…)".[86] Yet, considering the limitations of this new disclosure obligation, it is unclear how this objective could be met.

1.5. Information obligations for online marketplaces

Another anticipated change to the CRD, was the introduction of the notion of an 'online marketplace' as a digital service "…*operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers"*.[87] Digital service providers who offer such services will need to comply with an additional set of information obligations. Although the original scope of information obligations was quite extensive in the CRD, the operation of online marketplaces raised further concerns regarding online information asymmetry. In particular, whether the involvement of third parties could confuse consumers as to who they were concluding a contract with and what terms bound them.[88]

Consequently, the new Article 6a CRD obliges digital service providers, whose services qualify as online marketplaces, to clearly identify parties offering goods, services, or digital content through their services. This identification needs to refer to the professional or consumer character of third parties, which is determined based on their self-declaration. If a third party is a consumer, the new Article 6a(1)(c) CRD provides that digital service providers need to notify users of their online marketplace that the consumer protection framework will not apply to the concluded contract. Further, the new Article 6a(1)(d) CRD provides that digital service providers will need to explain any responsibilities shared between them, as operators of an online marketplace, and third parties.

Finally, if the operation of an online marketplace involves ranking the search results and offers presented to consumers, digital service providers operating such a marketplace need to clarify the main parameters determining the results of such ranking. This last obligation seems to go beyond disclosing the paid placement in the ranking of a particular search result or an offer. However, it seems to remain at the discretion of digital service providers to determine what the main parameters are, and the level of detail in the explanation provided to consumers. This element of discretion weakens the overall protective intent of this new provision. Moreover, these new disclosure obligations apply only to online marketplaces, rather than to a broader category of online platforms. Recital 20 of the Modernisation Directive suggests that providers of services such as search engines and comparison websites are excluded from the scope of this notion. There is also uncertainty about the applicability

[86] This was previously identified as an example of 'shallow transparency', see Trzaskowski (fn 16), 245.
[87] Article 4 Modernisation Directive introduced Article 2(1)(17) CRD.
[88] Recital 27 Modernisation Directive.

of these obligations to social media, when they act as an online intermediary, which is further aggravated by the recent Digital Service Act.

2. Digital Services Act

As the proposal for the Digital Services Act (DSA)[89] has only just been adopted[90] and its final version is not going to be applicable until February 2024,[91] this paragraph will only briefly mention a few concerns about the newly adopted rules in relation to the governance of the digital services market.

First, the DSA aims to regulate the activities of online intermediary services, which automatically means that it will become a key piece of legislation for digital service providers. The draft focuses heavily on the duties of online platforms, as a type of provider of hosting services, distinguishing these from very large online platforms. Recital 13 of the DSA mentions two types of possible online platforms: social networks and online marketplaces. This distinction is unfortunate if it will have the effect of limiting the scope for the interpretation of the notion of an 'online marketplace' in the CRD.[92] Nevertheless, a proposed regulatory improvement lies in the distinguishing of very large online platforms, based on the size of their audience, assigning more obligations to them, due to their potential to cause greater harm.[93] These very large platforms will need to conduct annual risk self-assessments and subject themselves to independent audits, pursuant to Articles 34 and 37 DSA. It should be noted that contrary to the draft provisions, mechanisms have been introduced to ensure the independence of such audits (Article 37(3) and (7) DSA).[94]

The focus of a substantial part of the DSA is on replacing the currently binding provisions of the e-Commerce Directive,[95] addressing issues of content moderation. This give rise to questions regarding monitoring obligations, due diligence and transparency in reporting. The continued lack of an obligation for online platforms to actively search their platform for illegal content is not surprising, as its introduction could not only limit their freedom to conduct business but also infringe users'

[89] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (COM/2020/825 final) (draft Digital Services Act, draft DSA).
[90] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services [2022] OJ L-277/1 (Digital Services Act, DSA).
[91] With a few exceptions related to transparent reporting obligations of online platforms and the monitoring of their activity, which will start applying as of 16 November 2022, see Article 93 DSA.
[92] On other misalignment issues between the DSA and the CRD see e.g. Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12(4) European Journal of Risk Regulation 761-763.
[93] Article 33 and Recital 57 of the DSA.
[94] This is a response to the critique expressed previously by e.g. Cauffman and Goanta (fn 92), 770-771.
[95] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L-178/1 (e-Commerce Directive).

freedom of expression.[96] This should, however, not stand in the way of placing an obligation on online platforms to conduct spot checks for illegal content, as recommended by the European Consumer Organisation.[97] The expectation that online platforms will engage in greater monitoring, simply because the risks related to voluntary monitoring activities have been removed, is questionable.[98]

One of the innovative elements of the DSA is to oblige online platforms to employ trusted flaggers to notify them of any illegal content, which is supposed to strengthen the already existing act-upon-notice rule (Article 22 DSA). Curiously, the DSA does not place any obligations as to the frequency or intensity of monitoring required from trusted flaggers, which could lead to platforms fully outsourcing such monitoring to them.[99] Whilst specifying that notices from trusted flaggers should have priority, it also does not require any particular notices to be addressed by online platforms on the basis of any identified type of activity or content.[100]

Interestingly, Article 26(1)(d) DSA attempts to fill one of the gaps identified above in the revised UCPD, i.e. the lack of an obligation on digital service providers to disclose "*the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters*". It is unclear why the obligation does not encompass the need to mention all parameters used by digital service providers in this process. Further, this provision may be perceived as legitimising personalisation of online content or persuasion profiling, which could bring about consumer harm and expose consumers to various vulnerabilities.[101] Such practices, if not prohibited, could require issuing additional, explicit warnings to consumers raise awareness of the potential harm flowing from engaging with such digital service providers.

VI. CONCLUSION

The gaps identified in this chapter may lead readers to question the soundness of the EU consumer protection framework, its coherence, and its future. It is not reassuring to note that the most recent legislative developments show an improved but not yet comprehensive approach by European policymakers to tackle digital services market related issues. Whilst the need to assure high levels of

---

[96] See Explanatory Memorandum to draft DSA (SWD(2020) 348 final), point 3.

[97] BEUC, 'The Digital Services Act Proposal' (BEUC position paper, 9 April 2021) at https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf accessed 30 August 2022, 14.

[98] Article 7 DSA. See also Cauffman and Goanta (fn 92), 768-770.

[99] BEUC (fn 97), 23.

[100] Recital 62 of the DSA mentions the possibility for online platforms to use trusted flaggers to quickly and reliably act against content "*incompatible with their terms and conditions, in particular against content that is harmful for vulnerable recipients of the service, such as minors*".

[101] BEUC (fn 97), 27-28.

consumer protection, as mandated by Article 38 of the EU Charter of Fundamental Rights,[102] should not invalidate the fundamental right of digital service providers to conduct their business, more balance could be sought between these two rights.

Throughout this chapter various solutions and recommendations have been proposed that should improve the status quo, without distorting the balance between the mentioned fundamental rights. The most needed improvements in the area of digital services require policymakers to start recognising various types of non-monetary payments, which consumers commonly provide in exchange for access to digital services. Further, there is an urgent need to update the UCTD framework, explicitly prohibiting various unfair terms that are frequently used by digital service providers, such as terms infringing GDPR principles, no-survivor clauses, and terms claiming formation of browse-wrap contracts. This revision could re-think the harmonisation character and the system of sanctions of the UCTD, as well. Whilst the framework of the UCPD has recently been updated, this revision adjusted its provision to the digital environment in a piecemeal way. This chapter argues for more certainty in some of its main concepts, e.g. professional diligence in the digital environment.

Finally, due to the so-far fragmented landscape of EU consumer protection measures, it is undoubtedly a taxing endeavour to try to design a new, comprehensive regulation to fit in it. It is unhelpful that digital services significantly vary, continuously evolve, and often are difficult to monitor, with the latter easily visualised as the new Wild West. The newest regulatory approach, the DSA, proposes some innovative solutions in its attempt to effectively regulate a core of this market: online intermediary services. Also here, the suggested further tweaks to its provisions, would help better achieve this aim, e.g. by requiring online platforms to conduct spot checks for illegal content or by addressing the harmful character of persuasion profiling.

To conclude, the old Wild West, and the lawlessness associated with it, disappeared following the introduction of a combination of governmental regulations promoting new forms of land ownership and significant improvements in infrastructure. Likewise, whilst digital technology grows exponentially, it is the regulatory element that so far struggles to keep pace and innovate further to improve the consumer protection framework online.

[102] Charter of Fundamental Rights of the European Union [2012] OJ C-326/391.