Challenges of digitalisation for consumer contracts

Mak, V.

ANNUARIO DI DIRITTO COMPARATO E DI STUDI LEGISLATIVI

2020

Edizioni Scientifiche Italiane

Anno 2020, vol. XI

Edito con la collaborazione scientifica del Dipartimento di Diritto, Economia, Management e Metodi quantitativi (DEMM) dell'Università degli Studi del Sannio e con gli auspici del Dipartimento di Diritto comune patrimoniale dell'Università degli Studi di Napoli «Federico II», del Dipartimento di Scienze Giuridiche «C. Mortati» dell'Università della Calabria e del Dipartimento di diritto comparato e penale dell'Università degli Studi di Firenze.

Registrato presso il Tribunale di Napoli al n. 62 del 28 settembre 2009 Responsabile: Angela Del Grosso

Accettazione dei contributi inviati all'*Annuario di diritto comparato* - Procedura di *peer review*

L'*Annuario di diritto comparato* pubblica contributi scientifici che sono soggetti a una procedura di *peer review* a doppio cieco. Gli articoli e gli altri contributi inviati all'Annuario sono preliminarmente valutati dalla Direzione. Se sono ritenuti potenzialmente adatti alla pubblicazione, la Direzione nomina due revisori. I revisori sono selezionati in base alle conoscenze richieste per valutare il contributo. I revisori valutano il contributo senza conoscere l'identità dell'autore e l'autore non conosce l'identità dei revisori. Al termine della procedura di valutazione, la Direzione può domandare all'autore di apportare modifiche al proprio contributo. I contributi valutati positivamente dai revisori sono accettati per la pubblicazione. I contributi pubblicati dall'Annuario sono di regola selezionati su invito.

Publishing with the *Annuario di diritto comparato* - Peer review policy

The Annuario di diritto comparato publishes scholarly contributions that are subject to a double blind peer review process. The articles and other contributions submitted to the *Annuario* undergo a preliminary assessment by the Editorial Board. If they are potentially suitable for publication, the Editorial Board will appoint two referees. The referees are selected on the basis of their expertise. The referees do not know the authors' identity nor does the author know the identity of the referees. At the end of the peer review process, the Editorial Board may ask the author to revise her or his contribution, on the basis of the referees' comments. The contributions which receive a positive assessment by the referees will be accepted for publication. Contributions to the *Annuario* are generally solicited by invitation.

Periodico esonerato da B.A.M., art. 4, 1° comma, n. 6, d.P.R. 627 del 6-10-78

INDICE

Parte I
Itinerari di diritto digitale

Parte II
L'intervista

Parte III
Studi

Parte IV

Itinerari bibliografici, recensioni ed eventi

Parte I

ITINERARI DI DIRITTO DIGITALE

Vanessa Mak*

CHALLENGES OF DIGITALISATION FOR CONSUMER CONTRACTS

1. Digitalisation, meaning the increased use of digital technologies in all realms of society, has rapidly changed consumer markets. The last decade has seen the emergence of new products and services based on digital technologies, a pivotal point being the introduction of the iPhone in 2010. The smartphone has become ubiquitous and it provides a gateway for businesses to offer all kinds of applications ('apps') that enable users to purchase goods or to enjoy online services such as listening to music or watching videos. Other digital services for consumers include cloud services, games, social media, platform services, and the Internet of Things (IoT) that connects physical appliances (such as smart TVs, fridges, cars) to the internet.

The digitalisation of consumer markets has given rise to new legislation in Europe as well as in the US, albeit with a relatively small scope. Until now, EU legislation has introduced some specific rules for non-conformity and remedies, parallel to similar rules in sale of goods law[1]. Also, rules have been introduced to enhance the transparency of contract terms for consumers as well as for small traders in the platform economy[2]. In

* I would like to acknowledge my gratitude to Femke Schemkes, LL.M., a junior lecturer at Tilburg Law School, who provided excellent research assistance and who partly co-wrote the Dutch-language report on which this article is based. I am particularly indebted for her research on 'free' digital services (section 5 of this article).

[1] 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 L136/1 (Digital Content Directive).

[2] Directive (EU) 2019/2161 of the European Parliament and of the Council of

 ISSN 2039-9871

the US, the adoption of the EU's General Data Protection Regulation (GDPR) in 2016 has inspired the development of new data protection rules in the state of California, including transparency requirements with regard to the use and processing of personal data, and a right to retrieve personal information[3].

Many aspects of digitalisation in consumer markets, however, are unregulated or are covered by existing rules of contract or tort law of which it is unclear how well they are tailored to the challenges of digitalisation. This article will consider some of these challenges and asks as a more general question: how can consumers in digital markets be empowered by law and/or policy?

The structure of the article is as follows. Section 2 takes stock of the challenges posed by digitalisation in consumer markets, focusing specifically on contractual relationships[4]. The following sections analyse which rules apply to some specific issues, and whether new rules should be introduced for the protection of consumers. Issues discussed include power relations in the platform economy (section 3); transparency concerning the professional status of the seller or provider, the price and other terms of the contract, and the ranking of listings (section 4); and 'free' digital services where the consumer provides personal data in exchange for a service (section 5). Noting that there are difficulties in addressing the complexities of digitalisation in consumer markets, section 6 examines which alternative policies could be adopted to empower consumers in these markets. The article concludes that a mix of regulation and policies can best address the challenges of digitalisation for consumer contracts.

2. Which challenges can be identified with regard to the digitalization of consumer contracts? The scholarly literature on this topic has

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 [2019] OJ L328/7 (Modernisation Directive); 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 [2019] OJ L186/57.

[3] The California Consumer Privacy Act 2018 became effective on 1 January 2020. For a brief overview see www.digitalguardian.com/blog/what-california-data-privacy-protection-act, last accessed 23 March 2020.

[4] Challenges also exist in tort law but, for reasons of space, these will not be discussed in this article.

ISSN 2039-9871

revealed at least four main issues. I will discuss them here briefly, with reference to relevant literature[5].

First, the use of data by traders has increased the power asymmetry that characterizes consumer law. Businesses tend to have more information on product characteristics and product quality than consumers, as they are on the production and distribution side of the market. One of the aims of consumer law is to empower consumers through information rights so that they have a more equal position to businesses and can make informed decisions about the goods and services that they purchase[6]. The increased use of data by traders, however, upsets the balance that consumer law seeks to pursue. By gathering personal data from consumers and running analyses on aggregated sets of data, businesses are in a position to pinpoint the preferences of groups of consumers and to target advertising on the basis of these preferences. In that way, they can influence the purchasing decisions that consumers make[7]. Also, data analysis may be used for price personalisation[8]. This creates new inequalities in the relationships between businesses and consumers, and therefore new challenges for consumer contract law.

Power relations also arise in other respects in the data economy. Online platforms, such as Uber, Airbnb, Amazon and AliExpress, have become very powerful by connecting (professional and non-professional) traders and consumers across different markets. They benefit from being at the connecting point between two markets, namely the supply side at which traders operate and compete, and the demand side where consumers search for products and services. In such two-sided markets, online platforms can quickly gain large market shares by becoming *the* portal that users turn to if they wish to obtain certain products or services. Such network effects can make it hard for competitors to enter the market. Also, consumers can become dependent on

[5] This part picks up several issues that I discussed in an earlier paper, which have evolved in the meantime but which remain challenges. See V. Mak, *Contract and Consumer Law* in V. Mak, T.F.E. Tjong Tjin Tai, A. Berlee (eds.), *Research Handbook on Law and Data Science*, Cheltenham, 2018, pp. 17-38.

[6] See I. Ramsay, *Consumer Law and Policy*, 3rd ed., Oxford, 2012, chs. 2 and 3.

[7] Compare S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, NYC, 2019.

[8] S. Dengler, J. Prüfer, *Consumers' Privacy Choices in the Era of Big Data*, TILEC Discussion Paper No. 2018-0014, www.ssrn.com/abstract=3159028, last accessed 23 March 2020.

 ISSN 2039-9871

certain platforms through lock-in effects (e.g. if apps are offered on a specific platform only)[9]. The gathering of consumer data is an essential aspect of these dynamics, as data analysis can provide platforms with information on their users' preferences, which enables them to target consumers with advertising or to personalize offers or prices. Seeing however that the use of data in this way is not restricted to platforms, this article will focus on the power relations arising from the use of data in business-to-consumer relationships in a general sense[10].

Second, transparency can be problematic for consumers who wish to purchase goods or services through online platforms[11]. It can be unclear whether the seller or provider is acting in a professional capacity which, if that were the case, would mean that rules of European consumer law (applicable to B2C relations) would apply. It can also be unclear how a price is being calculated, in particular if algorithms are used by a platform or trader to determine a personalised price. Furthermore, if listings are ranked in a certain order on a website, it can be unclear to users how that ranking was determined and whether the highest listed rankings are based on quality or on other factors, such as sponsorship or other ties between a platform and external traders. While some of these issues have been addressed by the EU's recent Directive on the modernisation of consumer protection[12], the lack of transparency continues to be problematic in relation to many online platforms. That can lead to unsatisfactory outcomes for consumers, who may be disappointed by what they buy, and on another level it could diminish the trust that users have in online platforms.

Third, contract law has not successfully devised a regime that suits so-called 'free' services, where a consumer provides data in exchange for a digital service rather than a payment in money. Specific problems

[9] C.A.N.M.Y. Cauffman, *The Commission's European Agenda for the Collaborative Economy – (Too) Platform and Service Provider Friendly?*, in *Journal of European Consumer and Market Law,* V, 6, 2016, pp. 235-243.

[10] Some platforms, such as Uber, also create new inequalities in the labour market. For further discussion of this topic see J. Prassl, *Humans as a Service*, Oxford, 2018.

[11] See e.g. P. Iamiceli, *Online Platforms and the Digital Turn in EU Contract Law: Unfair Practices, Transparency and the (Pierced) Veil of Digital Immunity*, in *European Review of Contract Law*, XV, 4, 2019, p. 407 ff.; M.B.M. Loos, J.A. Luzak, *Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers*, in *Journal of Consumer Policy*, XXXIX, p. 86 ff.

[12] Modernisation Directive, cit. See further section 3.

concern the ways in which data protection is integrated into contractual rules concerning 'free' services, and the adaptation of contract rules to such services, when contract law is normally concerned with economic transactions in which something of quantifiable value is provided[13]. Although many pages have been filled with discussions on these matters, a number of important questions remains unresolved.

3. What measures can be taken to address power relations in the platform economy arising from the aggregation of data by platforms, with detrimental effects on the users of platforms? The answer to this question is only to some extent a question of consumer law. The problem is really one of market ordering, in which regulation can be one aspect of a broader policy mix. Moreover, regulation in this context includes not only consumer law but also, and perhaps primarily, competition law and data protection law.

Competition law is often seen as the primary instrument for market regulation. Its goal is to guard fair competition between traders in markets for goods and services, resulting in a high level of welfare (reflected in a diverse supply of goods and service of high quality), low production costs, and innovation[14]. In markets 'disrupted' by online platforms both of these goals can come under pressure as competitors find it hard to enter markets in which one platform has become the most popular one[15]. Competition law has some tools to address these problems. The three main instruments are the prohibition of agreements that restrict competition, sanctions for the abuse of market power, and merger control. Agreements that restrict competition, or cartels, are prohibited under Art. 101 of the Treaty on the Functioning of the European Union (TFEU). Another route would be for competition authorities to fine businesses whose platform has become dominant in a particular market (Art 102 TFEU). However, dominance in itself is

[13] N. Helberger, F. Zuiderveen Borgesius, A. Reyna, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, in *Common Market Law Review*, LIV, 2017, pp. 1427-1466.

[14] I. Ramsay, *Consumer Law and Policy*, cit., ch. 3.

[15] The term 'disruption' is often used in relation to online platforms but it is not completely correct, as platforms do not push existing providers out of markets but instead provide alternative services and often create new demand. For example, Airbnb has not taken away business from hotels but offers alternative services for tourists, namely apartment rentals.

 ISSN 2039-9871

not prohibited. Businesses can only be fined if their actions amount to abuse of a dominant position. Until now, the cases in which online platforms have been sanctioned on the basis of this provision are limited. As a third alternative, fair competition can be pursued through merger control[16]. The European Commission has exercised its powers under that heading quite actively in relation to large tech companies. Examples are the proposed mergers of *Microsoft/Skype*, *Facebook/Whatsapp*, and *Microsoft/LinkedIn*[17].

Still, legal scholars have questioned whether these actions are sufficient and whether other instruments should be introduced to curb the power of online platforms. One might think of measures that ensure 'multi-homing, low switching costs, data portability, open non-proprietary standards and technological features, the availability of interface information, access to intellectual property and consumer awareness of path dependencies, lock-in-effects and the costs of not having competition', captured by Podszun and Kreifels under the heading 'smart regulation'[18]. Another alternative, suggested by Sauter, is to recognize a duty of care of online platforms towards their users, comparable to duties of care in tort law or to public law duties of care in financial services regulation[19]. Such a duty of care should oblige platforms to combat unfair market practices or illegitimate transfers of welfare, and it should entail that action is taken against discriminatory behaviour of dominant businesses. The duty of care could also entail that platforms prevent data breaches or other infringements of data protection rules[20].

At the same time, it is important to realise that the increased use of data can also have beneficial effects on competition. As scholars and competition authorities have pointed out 'the more information is available and the better such information can be processed, the better

[16] Council Regulation (EC) No. 139/2004 of 20 January 2004 on the control of concentrations between undertakings [2004] OJ L24/1 (the EC Merger Regulation).

[17] For a discussion of these cases see R. Podszun, S. Kreifels, *Data and Competition Law* in V. Mak, T.F.E. Tjong Tjin Tai, A. Berlee (eds.), *Research Handbook on Law and Data Science*, Cheltenham, 2018, p. 197 ff.

[18] R. Podszun, S. Kreifels, *Digital Platforms and Competition Law*, in *Journal of European Consumer and Market Law* 2016, V, 1, p. 39.

[19] W. Sauter, *Online uitbuiting van consumenten voorkomen: een zorgplicht voor dominante ondernemingen?*, in *Markt & Mededinging* 2019, 3, pp. 105-111.

[20] *Ivi*, p. 109.

ISSN 2039-9871

the matching in markets'[21]. Data could therefore be an effective instrument in the reduction of information asymmetries, intransparencies and misallocations due to wrong or misleading information.

4. Another challenge for consumers in the digital economy is transparency. In an environment where transactions are concluded at a distance and with counter-parties who are strangers, it can be hard to establish who the other party is and whether they are trustworthy. Also, information, and the presentation of information, becomes vital for determining the characteristics and quality of goods and services. These issues are the classic topics at which legal rules on transparency are aimed. In the digital economy, however, new rules are needed to address some specific information asymmetries. One will be discussed here: transparency concerning the professional status of the seller or provider (section 4.1).

Further complexity is added by the use of technology, for example in determining the price or the ranking of listings on a website. Many online traders use algorithms to personalize prices for specific groups of consumers (section 4.2), or to determine which adverts are the most appealing and should therefore have a prominent place on their website (section 4.3). While such practices are not prohibited, they should be monitored and perhaps even regulated to ensure that consumers are treated fairly.

4.1. Online platforms enable small traders to offer their goods or services on national, or even global, market places that would otherwise have been out of their reach. In many cases, such suppliers will be individual sellers who do not qualify as professional traders. They are the mirror image of the consumer: a natural person not acting in the course of a business or profession, but instead of buying this person is selling goods and services[22]. The contracts that are concluded between

[21] Podszun, Kreifels (n. 17), p. 187, with reference to Autorité de la Concurrence/Bundeskartellamt *Competition Law and Data*, www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2, last accessed 23 March 2020; A. MacAfee, E. Brynjolfsson, *Big Data: The Management Revolution*, in 90 *Harvard Business Review*, 2012 www.hbr.org/2012/10/big-data-the-management-revolution, last accessed 23 March 2020.

[22] Compare I. Brown, C.T. Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age*, Cambridge, MA, 2013, p. 183 ff.

 ISSN 2039-9871

such suppliers and consumers are C2C contracts. They are not subject to consumer protection laws, which apply only to B2C relations, but are governed by the default rules of contract law.

One question that becomes important in these circumstances is whether it is clear to the consumer that he or she is dealing with a non-professional supplier. Often, it is not, in particular on platforms where goods are offered by various parties, including individual suppliers, small traders, and the platform operator itself. In such cases, a consumer might be unaware when they enter into a contract that they are dealing with a non-professional party and that there for the rules of consumer law do not apply.

The EU's new Modernisation Directive seeks to address this problem through a provision added to the Consumer Rights Directive[23]. The new Art. 6a obliges platform operators to indicate to consumers, before they are bound to a distant contract or any corresponding offer, whether «a third party offering the goods, services or digital content is a trader or not, on the basis of the declaration of that third party to the provider of the online marketplace» [Art 6a *sub* 1(b)]. Somewhat superfluously, the platform operator is also obliged in such cases to inform the consumer that «the consumer rights stemming from Union consumer protection law do not apply to the contract» [Art 6a *sub* 1(c)].

While this provision improves transparency towards consumers, it can easily be criticized. Relying on the declaration from the trader means that the platform provider does not take responsibility for verifying that the information is correct. The possibilities for a consumer to invoke sanctions against the platform are therefore limited. If the required information is missing altogether, the platform operator (as well as the trader) could be held liable on the basis of a misleading omission [see the new Art. 7 *sub* a(ii)(f) in the Unfair Commercial Practices Directive (UCPD)][24]. Presumably, both the platform operator and the supplier failing to disclose that they are a trader will also be in breach of Art. 6(1)(g) UCPD, which sanctions a misleading action regarding the consumer's rights[25]. The consumer could, in accordance with the

[23] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [2011] OJ L304/64 (Consumer Rights Directive).

[24] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22.

[25] See C. Twigg-Flesner, *Bad Hand? The 'New Deal' for EU Consumers*, in *GPR* 2018, 4, p. 172.

ISSN 2039-9871

rules of the Modernisation Directive, instigate an individual action in contract or tort, depending on how the rules are implemented in the legal system of the consumer's residence. Further, consumer authorities could impose sanctions, such as fines, the rules for which have been extended by the Modernisation Directive to ensure a more consistent approach to sanctions in current EU directives[26].

Another problematic aspect of the new transparency rule concerning the supplier's professional status is that it does not provide objective criteria for determining when a supplier is a professional trader. That is a problem as many suppliers on online platforms start out small, e.g. selling goods from their living room, and that it is hard even for them to determine when they change from being a private supplier to being a (small) trader[27]. The Court of Justice of the EU (CJEU) has provided some guidelines in its judgment in *Kamenova*, but these leave room for interpretation. The Court states that the following circumstances are indicative of the trader acting as a trader in the meaning of the UCPD[28]:

whether the sale on the online platform was carried out in an organised manner, whether that sale was intended to generate profit, whether the seller had technical information and expertise relating to the products which she offered for sale which the consumer did not necessarily have, with the result that she was placed in a more advantageous position than the consumer, whether the seller had a legal status which enabled her to engage in commercial activities and to what extent the online sale was connected to the seller's commercial or professional activity, whether the seller was subject to VAT, whether the seller, acting on behalf of a particular trader or on her own behalf or through another person acting in her name and on her behalf, received remuneration or an incentive; whether the seller purchased new or second-hand goods in order to resell them, thus making that a regular, frequent and/or simultaneous activity in comparison with her usual commercial or business activity, whether the goods for sale were all of the same type or of the same value, and, in particular, whether the offer was concentrated on a small number of goods.

These criteria are not cumulative, nor is the list intended to be exhaustive. It therefore remains for the national judge in specific cases,

[26] C. Twigg-Flesner, *op. cit.*, p. 173.
[27] See also C. Twigg-Flesner, *op. cit.*, p. 172.
[28] C-105/17 *Kamenova*, ECLI:EU:C:2018:808, para 38.

 ISSN 2039-9871

taking account of the circumstances of the case, to determine whether a supplier qualifies as a professional trader or not. If a supplier has legal personality, that is seen as a strong indication that he must qualify as a professional trader[29].

4.2. The Modernisation Directive picks up also on personalised pricing, which is not a new issue but which has become more prominent with the increased use of algorithms by online traders. In Art. 6 of the Consumer Rights Directive a provision will be added that obliges traders to inform consumers «where applicable, that the price was personalised on the basis of automated decision-making»[30]. By way of background, recital 45 explains that «[c]onsumers should… be clearly informed when the price presented to them is personalised on the basis of automated decision-making, so that they can take into account the potential risks in their purchasing decision».

These rules introduce some degree of transparency in relation to personalised pricing, improving upon a practice that has been debated for longer. The issue is that, while dynamic pricing or price discrimination are not prohibited, many consumers perceive the practice as unfair. Price discrimination, in economic terms, means that different prices are calculated for the same services, taking account of characteristics that pertain to different groups of consumers or users. Examples are discounts for certain age groups (the elderly, or the under-25-year-olds) in museums, and price differences for similar seats on a plane, calculated based on the presumption that business travellers are willing to pay higher prices than holiday goers. For that reason, flights departing on Mondays or Fridays are often more expensive, and prices tend to be higher for flights booked at short notice[31]. In the latter case, the calculation of the price is not only an example of price discrimination but also of dynamic pricing, as the price can change depending on the time of booking. Another example of dynamic pricing is the calculation of

[29] Compare (in Dutch) M.Y. Schaub, *Wie is handelaar?*, in *TvC*, 2019, 1, p. 9 and p. 13.

[30] Consumer Rights Directive, cit., Art. 6 *sub* 1(ea).

[31] Other factors may include address, marital status, birthday and travel history. See *How much…? The rise of dynamic and personalised pricing*, in *The Guardian* 20 November 2017, www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.html, last accessed 23 March 2020.

ISSN 2039-9871

fares by Uber, where the algorithm leads to higher prices at peak moments with few available drivers (famously: New Year's Eve)[32]. These practices are, according to economists, not unfair but they can actually lead to optimal results. Buyers pay the price that they are willing to pay, and suppliers sell their stock at the highest price feasible[33].

In consumer law, for this reason, personalised pricing has until now been unregulated. The increased use of algorithms, however, has led consumer protection advocates to plead for new rules, starting with transparency. Algorithms have upset the existing balance of consumer law as they enhance the power asymmetry between consumers and traders. Although algorithms can be designed in many different forms, for pricing they all make use of consumer data. Consumers, by providing data in exchange for a service or as part of a transaction, give traders additional instruments to determine precisely what price they can ask in order to achieve the highest profit. This new dynamic in data-driven economies, it has been argued, should be adjusted through consumer protection law. A starting point is the adjustment of transparency rules, so that consumers at least know that algorithms are used to personalise pricing.

The new Art. 6 *sub* 1(ea) of the Consumer Rights Directive should provide a minimum of transparency. One may wonder, however, whether the provision goes far enough. Indicating that personalised pricing has been used is a first step, but that does not tell the consumer *how* personalised pricing is used. What factors were taken into account? What does the trader know about this particular consumer to place him or her in a certain personalised pricing category?[34]. The European legislator may not have been in a position to impose stron-

[32] *Yes, Uber expects New Year's Eve surge pricing. Here's what to expect*, in *Fortune*, 29 December 2017, www.fortune.com/2017/12/29/uber-surge-pricing-new-years-eve, last accessed 23 March 2020.

[33] M. Bourreau, A. De Streel, *The Regulation of Personalised Pricing in the Digital Era*, OECD 21 November 2018, available at www.ssrn.com/abstract=3312158, last accessed 23 March 2020.

[34] The GDPR contains stronger obligations for data controller's in this respect. Art. 13 *sub* 2(f) provides that the controller shall provide the data subject with information concerning «the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject».

 ISSN 2039-9871

ger information duties on traders. For one thing, algorithms are often protected as trade secrets, so that traders can only be obliged to disclose the minimum of how an algorithm was designed and which factors it takes into account[35]. Interestingly, however, the new provisions on transparency concerning the ranking of listings on websites included in the Modernisation Directive, as well as similar provisions in the EU regulation on platform-to-business relationships (P2B)[36], address that limitation directly and work around it[37]. One might see it as a missed opportunity that the same obligation was not included for personalised pricing, but perhaps in future case law the application of the UCPD with regard to misleading omissions can provide some guidance[38].

Should consumers be dissatisfied with prices calculated on the basis of personalised pricing, they may still have one ground for recourse in European consumer law. The failure of a trader to disclose information on personalised pricing could, depending on the circumstances, be qualified as a misleading omission under the UCPD (Art 7). In that case, the consumer can invoke the individual remedies available to him in contract or tort, or a consumer authority could impose sanctions if the infringement affects the collective interests of consumers.

4.3. Third, and last, transparency is a concern in relation to the ranking of listings on websites. Consumers can be misled if they are unaware that a prominent advert on a website appearing as one of the first results for a search is a sponsored ad, or if it is placed first because of other factors that have little to do with the quality of the good or service.

The Modernisation Directive tackles this problem, therein following the French *Loi de la République numérique* of 2016 and the 2019 P2B Regulation applicable to small traders in Europe. The ELI Model

[35] Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1.

[36] 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 [2019] OJ L186/57 (P2B Regulation).

[37] See below section 4.3.

[38] Compare A. De Streel, F. Jacques, *Personalised Pricing and EU Law*, conference paper, available at www.econstor.eu/bitstream/10419/205221/1/de-Streel-Jacques.pdf, last accessed 23 March 2020, p. 9.

Rules on Online Platforms, which were adopted in February 2020, also contain a provision on rankings (Art 4)[39]. Each of these rules stipulates more or less the same, namely that an online platform provider is obliged to disclose which parameters are used in determining the ranking of listings on its website. In the words of the Modernisation Directive, which adds a new paragraph to Art. 7 UCPD, «general information, made available in a specific section of the online interface that is directly and easily accessible from the page where the query results are presented, on the main parameters determining the ranking of products presented to the consumer as a result of the search query and the relative importance of those parameters, as opposed to other parameters, shall be regarded as material». And, being regarded as material, the omission of such information will be actionable as a misleading omission under the UCPD.

These provisions seem to provide adequate solutions for guaranteeing the transparency of rankings on commercial websites. As a more general challenge, it is worth pointing out that other information – e.g. political adverts on social media platforms – is not covered by this provision, as it does not appear in response to a consumer's search query. In this respect, one challenge for the digital community is to prevent the influencing of public opinion through social media platforms' algorithms. Another challenge, related to this, is to balance free speech with other fundamental rights, such as non-discrimination. Germany is one of the first countries in the world to consider regulating the selection algorithms used by social media platforms[40]. It is beyond the scope of this article to discuss this issue in more detail.

5. If one asks which development in the digital economy has challenged consumer protection the most, it may well be the increasing emergence of 'free' digital services. The word 'free' is in parentheses as the services are not actually rendered without compensation, but rather a consumer receives them in exchange for data. Examples are the use of free wifi at an airport, often in exchange for a phone number or an email

[39] European Law Institute (ELI), *Model Rules on Online Platforms*, available at www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf, last accessed 23 March 2020.

[40] See www.blogs.lse.ac.uk/medialse/2019/05/29/germany-proposes-europes-first-diversity-rules-for-social-media-platforms.

 ISSN 2039-9871

address; downloading a health or exercise app for free, but allowing it to gather data on the consumer's health or on their exercise regime; or social media apps such as TikTok, Instagram and Facebook, which can be downloaded for free but at the same time gather great amounts of data from their users, also by analysing their posts, photos and videos.

Much has been written about the ways in which contract law qualifies contracts when 'payment' occurs with data instead of with money. Most legal systems are based on the idea that contracting involves the exchange of goods for money and reflect that in their sales law, if not necessarily in the rules concerning services[41]. English law refers to consideration, meaning 'something of value', as an essential element in the formation of contractual relationships. Only if consideration has been given can a promise be enforceable[42]. The problem with data is that, although it may be of value in aggregated form, the individual data of one specific user is either not worth as much or is not of quantifiable value[43]. While the solution could be to conceptualise the provision of data by consumers as a form of consideration[44], some legal systems have opted simply to interpret the 'money' requirement in contract law broadly so that it also includes data[45]. Another solution, adopted in the EU Digital Content Directive, is to conceptualise the provision of data as the consumer's side of a contractual agreement, while the trader supplies digital content or digital services. That approach makes it possible also to distinguish between situations in which data is provided because it is necessary for the performance of the contract or compliant with other legitimate processing grounds listed in the GDPR – and therefore not regarded as 'payment' – and situations in which data is

[41] See § 433(2) of the German Civil Code that says that «[t]he buyer is bound pay the seller the agreed price», and Art. 7:1 of the Dutch Civil Code, which states that «sale is the agreement under which one of the parties engages himself to deliver a thing and the other party to pay a price in money in return».

[42] H. Beale (gen. ed.), *Chitty on Contracts*, 33rd ed., London, 2019, ch. 4.

[43] See T. Hören, *Big Data and the Legal Framework for Data Quality*, in *International Journal of Law and Information Technology*, 2017, XXV, p. 26.

[44] C. Langhanke, M. Schmidt-Kessel, *Consumer Data as Consideration*, in *Journal of European Consumer and Market Law*, 2015, IV, 6, pp. 218-223.

[45] The European Commission has also confirmed this interpretation in relation to the UCPD. See European Commission, *Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices*, Commission Staff Working Document, SWD/2016/0163 final.

ISSN 2039-9871

actually provided in exchange for a service[46]. As a general conclusion, one could say that the use of personal data in exchange for a service has been integrated into contract law, with consideration for the fact that data protection is a fundamental rights and should be protected as such. This means that contract law applies without prejudice to the regime for data protection laid down in the GDPR.

Seeing that a shift has occurred in accepting the provision of data by consumers into contract law, the main question is no longer *whether* consumers can provide personal data as part of a contractual exchange, but rather *how* contract law applies to such types of contracts. In that respect, some issues have not been fully fleshed out. Important aspects are: 1) the relationship between consent in the GDPR and consent in contract law, in particular when traders make use of general terms and conditions; 2) the consequences of a (partial) termination of the contract for the return of personal data; 3) consumer remedies for breach of the GDPR. Other issues, such as under what conditions non-conformity of digital content can be established, in particular in the light of future updates, are also important but seem to have been settled for now in the Digital Content Directive[47]. It should be noted, also, that the issues discussed here are also relevant for contracts for the supply of digital content or digital services where the consumer does pay a price, but besides that provides personal data to the supplier.

5.1. The GDPR stipulates that the processing of personal data is allowed if it is necessary for one of the legitimate purposes listed in Art. 6 GDPR, or as an alternative, if the data subject has given consent for the processing of data. For consumers, the second ground is in practice the primary one, as commercial purposes in general do not qualify as a legitimate purpose.

Consent under the GDPR should be given «by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her» (recital 32, and see Art. 4 *sub* 11 and Art. 7 GDPR). These conditions for freely and expressly given consent are

[46] Compare Art. 3 *sub* 1 Digital Content Directive and recitals 24 and 25. This provision was designed to comply with Art. 6 of the GDPR.

[47] Conditions for non-conformity were debated in that context. See on this point Mak, *Contract and Consumer Law*, cit., pp. 34-35.

 ISSN 2039-9871

significantly stricter than the requirements for consent in contract law. In contract law, consent signifies the agreement of the parties to enter into a contract, expressed through the concurrence of an offer and its acceptance by the other party[48]. In consumer contracts, furthermore, it is common practice for traders to use standard terms and conditions which consumers can only accept in a 'take it or leave it' manner[49].

Unsurprisingly, these two approaches to consent in many cases do not match. Suppliers often put privacy clauses in their general terms and conditions, where consumers fail to notice them. By accepting the terms and conditions, the requirements of the GDPR will not have been fulfilled[50], yet in contract law a consumer will have become bound to the terms of the contract. The clause, from that perspective, has become enforceable. Further work is needed to bring the two notions of consent closer together[51].

5.2. Art. 16 of the Digital Content Directive (DCD) stipulates which obligations a trader has towards a consumer in case of termination of the contract. Although the provision has tried to comply with requirements from contract law and from the GDPR, in particular the right to withdraw consent (Art 7 *sub* 3 GDPR), some aspects remain unclear.

First, termination of a contract would normally entail that both parties are obliged to undo their performances. In a sale of goods contract, this would mean that the buyer returns the goods to the seller, while the seller refunds the price that the consumer paid for them. If the contract is for a 'free' digital service, where the consumer has provided personal data, it becomes much harder to return or refund what has been given. In this respect the DCD has aimed to find a solution by following

[48] These requirements apply to synallagmatic contracts involving two parties, which are generally taken to be the paradigmatic example of a contractual relationship. See H. Beale c.s. (eds.), *Cases, Materials and Text on Contract Law. Ius Commune Casebooks for the Common Law of Europe*, 2nd ed., Oxford, 2010, ch. 8.

[49] Albeit that the trader is obliged to provide (access to) the terms and conditions before the conclusion of the contract, and that for electronic contracts the terms must be provided on a durable medium. See Art. 7 *sub* 1 and recital 10 Consumer Rights Directive.

[50] Note also Art. 7 *sub* 2 GDPR which states that 'the request for consent shall be presented in a manner which is clearly distinguishable from the other matters'.

[51] See also the conflicts and contradictions identified by N. Helberger, F. Zuiderveen Borgesius, A. Reyna, *The Perfect Match?*, cit., pp. 1461-1462. See also E. Kosta, *Consent in European Data Protection Law*, Leiden, 2013.

the consequences of withdrawal of consent under the GDPR (Art 16 *sub* 2 DCD). Therefore, the trader must after termination without undue delay erase all personal data concerning the consumer (see Art. 17 GDPR, or 'the right to be forgotten'). The trader must also enable the consumer to retrieve their personal data (Art 20 GDPR, concerning data portability). If the personal data have been sold on to third parties, the trader must take reasonable steps to inform controllers which are processing the personal data that the data subject (i.e. the consumer) has requested the erasure of the data and any links to, or copy or replication of it (Art 17 *sub* 2 GDPR). The application of this provision can be problematic in cases where the trader has already processed the consumer's data through, for example, an aggregated analysis.

Second, other contractual problems can arise. In case of termination of a contract, it can be practically impossible for a consumer to return the supplied content or services. Digital content can often easily be reproduced (e.g. music, videos, or other files), and the trader can therefore not be sure that the consumer retains a copy on their own computer or other device. Art. 17 DCD aims to solve this problem by stipulating that, after termination, «the consumer shall refrain from using the digital content or digital service and from making it available to third parties.» That goes some way towards solving the problem, although the trader may in practice not be able to confirm whether or not the consumer has stopped using the content on his own computer. Where it is technically possible, the trader may prevent further use of the digital content by the consumer by making it inaccessible (Art 16 *sub* 5 DCD).

Third, the consequences of the partial termination of a contract are unclear. An example could be the case in which a consumer removes his or her photo albums from Facebook but otherwise continues to use their account. Would this constitute a withdrawal of consent, meaning that the trader has to erase the data and enable the consumer to retrieve them?[52].

5.3. Finally, in relation to 'free' digital services an area that is in many respects uncharted is that of remedies for breach of the GDPR. If a trader fails to comply with the GDPR and, for example, a data

[52] Compare N. Helberger, F. Zuiderveen Borgesius, A. Reyna, *The Perfect Match?*, cit., p. 1463.

 ISSN 2039-9871

breach occurs[53], are remedies available to consumers on the basis of their contract with the trader?

The unauthorised use of data could be actionable in contract law. However, the legal possibilities for consumers are restricted to specific situations. For instance, if data are used for purposes other than the ones for which consent has been given, the consumer might seek to rescind the contract on the basis of misrepresentation. For such a claim to succeed, the trader must have misinformed the consumer with regard to the use of data[54]. Also, the consequence would be avoidance of the contract. Should the consumer not wish to uphold the contract, an alternative route would be to seek amendment of the terms of the agreement. That, however, would require the consumer to ask the trader to renegotiate the contract.

The unauthorised use of data could also be a ground for a claim in damages. One could think of cases in which loss occurs due to the use of data for other purposes than for which consent was given, or of cases in which inaccurate use of data leads to financial loss (e.g. loss of government benefits). Whether damages can be claimed depends on the rules of national laws.

In cases where a consumer suffers harm as a result of a data breach, tort law could provide a basis for liability. However, as things stand, national legal systems have not yet found adequate ways to determine when damages for data breach should be awarded, and to what amount. The legal grounds for damages could potentially be breach of privacy or loss of reputation. In practice, however, it is often hard to prove causality[55].

6. Legal regulation is only one way to address the challenges of digitalisation for consumer contracts. At least four alternative policies could be considered. I discuss them briefly, putting in perspective the legal analysis that was presented in the previous sections.

The first alternative is privacy by design, meaning that a digital environment is designed in such a way that consumers can make informed

[53] Data breach concerns the situation where personal data get into the hands of third parties or in the public domain without authorisation.

[54] H. Beale (gen. ed.), *Chitty on Contracts*, cit., ch. 7.

[55] B. van Alsenoy, *Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation*, in *JIPITEC*, 2016, 3, pp. 274-275.

choices about how much data they wish to share with businesses. The GDPR puts a broadly phrased obligation on data controllers to explore technological options for privacy by design or by default (Art 25 GDPR). One practical way of designing such an environment would be to offer two options: one 'regular' offer of free digital services in which the consumer provides data, and another similar offer but now against payment and with greater privacy protection, i.e. anonymous. Economic research suggests that consumers, even if they do not have a specific taste for privacy nor make strategic choices, are likely to choose the anonymous option[56]. Legislators, at the EU level but also at the national level, however do not seem to favour this option[57]. One reason can be that it could exclude consumers who are not in a position to provide payment in exchange for greater privacy protection. Another example of privacy by design, which is already available to consumers, is the use of technologies that enable anonymised browsing (e.g. VPN connections).

Second, an alternative to regulation would be to increase the possibilities for data portability. Art. 20 GDPR states that the data subject «shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller» in certain circumstances. The way in which this right can be exercised in practice is subject to further technological developments. The Guidelines to Art. 20 suggest that 'application programming interfaces' (API) could be used to transfer data from one platform to another. Currently, however, few platforms offer such options, or adequate alternatives[58].

[56] S. Dengler, J. Prüfer, *Consumers' Privacy Choices in the Era of Big Data*, cit.

[57] See (in Dutch) C. Spierings, *Het nieuwe goud: betalen met data*, in *Maandblad voor Vermogensrecht*, 2019, 6, p. 214. The market for privacy by design is also relevant for trader who, as data controllers, are trying to purchase privacy-oriented technologies or seek to stimulate their production. See L.A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in *Oslo Law Review*, 2017, IV, 2, p. 119.

[58] Facebook has announced that it is working on a tool that would allow easy transfer of photos or videos to another platform, such as Google. See *Facebook addresses antitrust concerns with new tool that lets you transfer photos to Google*, *CNBC*, 2 December 2019, www.cnbc.com/2019/12/02/facebook-releases-new-data-portability-tool-for-photos.html, last accessed 23 March 2020.

 ISSN 2039-9871

Third, the monetisation of data could be pursued. It has been noted that it is difficult to quantify the value of data[59]. Nonetheless, consumers could have a stronger position vis-à-vis businesses if a value could be attached to data. For example, if a specific monetary value was attached to the number of 'likes' that someone receives for a social media post, that could be a bargaining tool between the user and the platform. It could make visible how much a certain user account is worth, both to the platform and to the user itself, and thereby enable negotiation for better terms and conditions, or payment upon leaving the platform. Still, while this solution seems promising, it has to be borne in mind that data protection is a fundamental right and that the monetisation of data could be the first step on a slippery slope[60].

Fourth, certificates and other signals (e.g. labels) could provide an alternative to regulation. They could be used to inform consumers of the way in which their data is used by a business and of the data protection rights that they enjoy under EU law. Specific certificates or labels concerning data protection currently do not exist, apart from a certificate for 'electronic trust services' that indicates that an online trader complies with the authentication standards of the eIDAS Regulation[61]. One could envisage the development of EU standards for responsible data use, or the development of certificates or signals through private regulation[62].

These alternative policy options confirm that regulation is not the only instrument that can empower consumers in the digital market. Adopting a bird's eye perspective, it would seem that a mix of regulation and alternative policy options would be the preferred approach

[59] T. Hören, *Big Data*, cit.

[60] European Data Protection Service (EDPS), *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017, available at www.edps.europa.eu/sites/edp/files/publication/17-03- 14_opinion_digital_content_en.pdf, last accessed 23 March 2020.

[61] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market [2014] OJ L257/73.

[62] Bundesministerium für Wirtschaft und Energie, *Weissbuch Digitale Plattformen. Digitale Ornungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe* 2017, available at www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.html, accessed on 23 March 2020, p. 71, 107.

at this time. Digital goods and services are being developed at such a rapid pace that regulation can hardly keep up. Flanking policies could be developed faster, and with the input from businesses and consumers, therefore tailoring more directly to their needs. The regulatory framework, however, would determine within which boundaries choices and trade-offs can be made between economic interests and data protection. In this respect, competition and consumer law will remain leading, and it will be a challenge for lawyers working in these fields to come up with new ideas and solutions to empower consumers in the digital market.

Abstract

Many aspects of digitalisation in consumer markets are unregulated or are covered by existing rules of contract or tort law of which it is unclear how well they are tailored to the challenges of digitalisation. This article will consider some of these challenges and asks as a more general question: how can consumers in digital markets be empowered by law and/or policy? Issues discussed include power relations in the platform economy; transparency concerning the professional status of the seller or provider, the price and other terms of the contract, and the ranking of listings; and 'free' digital services where the consumer provides personal data in exchange for a service. Noting that there are difficulties in addressing the complexities of digitalisation in consumer markets, the article examines which alternative policies could be adopted to empower consumers in these markets

Molti aspetti della digitalizzazione nei mercati cui partecipano i consumatori non sono regolamentati, né sono coperti dalle norme esistenti in materia di diritto contrattuale o di illecito, le quali non sono necessariamente all'altezza delle sfide poste dalla digitalizzazione. L'articolo prende in considerazione alcune di queste sfide e pone una domanda più generale: come possono i consumatori che prendono parte ai mercati digitali essere sostenuti dal diritto e/o dalla politica, per essere riconosciuti come attori pienamente abilitati? Le questioni discusse includono le relazioni di potere nell'economia della piattaforme digitali, la trasparenza in merito alla condizione professionale del venditore o del fornitore, al prezzo e ad altre condizioni del contratto, come pure il grado di priorità che gli annunci hanno *online* e servizi digitali "gratuiti", in cui il consumatore fornisce dati personali in cambio di un servizio. Preso atto delle difficoltà collegate alla complessità della digitalizzazione nei mercati di consumo, l'articolo esamina quali politiche alternative potrebbero essere adottate per responsabilizzare i consumatori che operano questi mercati.

 ISSN 2039-9871

Keywords

Consumer law, contract law, digital content, data protection, transparency.

Diritto dei consumatori, diritto contrattuale, contenuti digitali, protezione dei dati, condotta trasparente.

ISSN 2039-9871