Consumer contract law and data-driven technologies

Mak, V.; Tjong Tjin Tai, T.F.E.; Berlee, A.

2. Consumer contract law and data-driven technologies

Vanessa Mak

1. INTRODUCTION

Data has been called the new oil of society, in a metaphor that draws a parallel with that other commodity that in the days of the industrial revolution spawned a lucrative and fast-growing industry.[1] One legal institution that could also be compared to oil, though in a different way, is contract. Contract can be regarded as the oil or grease that makes the wheels of society run smoothly. It lays down an ordering mechanism that determines which agreements—sales transactions, loans, commitments to provide a service—can be enforced and under what conditions.[2]

However, rather than improving the function of contract as an oil of societal interaction, data appears to be upsetting the established order. To give an example: data-driven technologies are being used to learn about consumer preferences and to tailor production and advertising to these preferences.[3] Very little of what happens in this 'black box' of data is transparent to consumers. Whilst contract laws around the world in the last decades have been infused with transparency obligations for traders, aiming to give consumers a stronger legal position in relation to (economically stronger) businesses,[4] the use of data in the consumer market threatens to diminish that protection. Another question for contract law is whether, now that data research enables traders to learn about the individual preferences of consumers, the general 'consumer' category in contract laws still works for defining areas in which weaker contracting parties require legal protection.[5] As a third example, a more specific

[1] 'The World's Most Valuable Resource Is No Longer Oil, But Data' *The Economist* (6 May 2017).

[2] JM Smits, *Contract Law. A Comparative Introduction* (2nd edn, Edward Elgar Publishing 2017) 3–5; and see H Collins, *The Law of Contract* (4th edn, CUP 2008) x, who regards contract law as intertwined with morality, social and economic policy, and therefore as having a regulating function.

[3] V Mayer-Schönberger and K Cukier, *Big Data* (Eamon Dolan/Houghton Mifflin Harcourt 2013) 104–5.

[4] For the development of this idea in European private law, see E Hondius, 'The Protection of the Weak Party in a Harmonised European Contract Law: A Synthesis' (2004) 27 *Journal of Consumer Policy* 245.

[5] See for an explorative study, C Busch, 'The Future of Pre-Contractual Information Duties: From Behavioural Insights to Big Data' in C Twigg-Flesner (ed), *Research Handbook on EU Consumer and Contract Law* (Edward Elgar Publishing 2016) 221.

problem for contract law is whether transactions in which a consumer 'pays' by providing personal data in exchange for receiving a service—e.g., access to a WiFi network at the airport—should be treated similarly to contracts in which a price is paid in money. Should consumers have similar rights and remedies in contract law if the service does not function properly?[6]

This chapter aims to give an overview of the contractual issues that have arisen in relation to the use of data. Since the use of data has far-reaching consequences for consumer markets, the chapter focuses on issues that have come to the fore in those markets and the regulatory responses that have emerged, or are emerging, in consumer law.[7] The opening part (section 2), however, presents a general introduction to the ways in which the existing elements of contract law such as the rules on formation, content, defects of consent and remedies are touched by the rise of the data economy.[8] It considers in particular what effects the use of data has on the autonomy of contracting parties, and on the balance of contractual fairness. Continuing with these themes, the next parts (sections 3– 5) examine three more specific issues for consumer contract law, namely transparency, fairness, and the question whether the 'consumer' concept needs adjusting. Those issues will be considered in the light of

---

6 This question became prominent in Europe due to the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content (DCD) COM(2015) 634 final, which proposed that when a consumer actively supplies personal data or other data this can constitute a counter-performance in contract. See art 3(1) of the proposed Digital Content Directive. The final version of the Directive does not qualify the provision of data as a counter-performance, leaving it to national laws to determine whether the provision of digital content or services by a trader and the related provision of personal data by a consumer constitutes a contract or should be treated as quasi-contract. See 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 (Digital Content Directive) [2019] OJ L136/1, art 3(1) and compare A Metzger, 'A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services' in S Lohsse, R Schulze and D Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0?* (Nomos/Hart 2020) 25, 30ff.

7 In business-to-business relationships some contractual issues have arisen that might also warrant further research or possibly regulatory action. For cloud storage, for example, the EU is planning to compile a set of rules in the form of an EU Cloud Rulebook and a Guidance on public procurement of data processing services. See <https://digital-strategy.ec.europa.eu/en/policies/cloud-computing> accessed 18 August 2023.

8 For an analysis of the rise of the 'data economy' and the economic, societal and legal challenges that it poses, see 'Data is Giving Rise to a New Economy' *The Economist* (6 May 2017). The European Union has made 'building a European data economy' one of the goals of its Digital Single Market strategy; see Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building a European Data Economy COM(2017) 9 final.

existing regulation, primarily in Europe, as laid down in the form of information duties for traders, unfair terms control, and unfair commercial practices regulation.[9] The focus of this chapter will be mainly on the EU, with occasional references to the US, seeing that Europe has developed a fairly coherent regime of harmonised consumer contract law that in many aspects already applies to data-related contracts. An analysis of this framework can provide a useful basis for further debate and comparison with other jurisdictions in the world. Issues that are for now unregulated will also be highlighted, where relevant with reference to proposed rules that may or may not become law in the near future.[10] Section 6 concludes, drawing together some of the lines set out in the previous sections, and providing an outlook for future research on data and contract law.

2. DATA AND CONTRACT LAW

Even if examples of data processing in private law relationships abound, as the issues highlighted in the introduction make clear, it is not immediately obvious that contract law should apply to these cases. At a fundamental level, there may be a problem of fit, i.e., the suitability of contract law to deal with cases in which data protection laws have already sought to balance the economic and fundamental rights of individuals. There may also be a problem of fit on a more specific level, namely where the existing rules of contract law are unable to accommodate transactions involving data. I will elaborate on both points, considering first the fundamental question why contract law should be concerned with data, and then the more specific question how—or, in which respects—it should be concerned with data.

2.1 Why Should Contract Law be Concerned with Data…

Contract law, as part of private law, is concerned with the economic ordering of society.[11] All rules of contract law therefore deal with transactions that represent economic value, either in the form of a performance being exchanged for a counter-performance (a synallagmatic contract), or in the form of a one-sided per-

---

[9] In Europe, relevant legislation includes Directive 2011/83/EU on consumer rights (Consumer Rights Directive (CRD)) [2011] OJ L304/64; Directive 93/13/EEC on unfair terms in consumer contracts (Unfair Terms Directive (UCTD)) [1993] OJ L95/29; and Directive 2005/29/EC on unfair business-to-consumer commercial practices in the internal market (Unfair Commercial Practices Directive (UCPD)) [2005] OJ L149/22.

[10] Such as the Digital Content Directive (n 6).

[11] Cf Micklitz, who calls it economic law. See K Purnhagen and P Rott (eds), *Varieties of European Economic Law and Regulation. Liber Amicorum for Hans Micklitz* (Springer 2014).

formance (e.g., a donation).[12] Data is of value too, yet the application of contract law to transactions involving data is not automatic. Two points are problematic.

First, even though it is clear that data has economic value for the companies that use it to calibrate their production and marketing towards consumer preferences,[13] it is hard to attach specific value to the data of *individual* consumers. Their data is in itself not of significant value to a company. It only becomes valuable once it is combined with the data of hundreds or thousands of other customers. Big data analysis enables companies to deduct preferences from this large pool of consumer data. Nevertheless, even if it is impossible to attach specific value to the data provided by an individual consumer, one might say that it is at least clear *that* the consumer's data is of value to the company. Therefore, contract law might be extended to contracts in which a counter-performance to obtain a good or service exists of 'payment' with data.[14] After all, why should Google be allowed to make money from my data, while I receive nothing?[15] Some social media platforms have, in recognition of this point, started offering payment to content creators such as Australian "sleepfluencer" Jakey Boehm who earned 34,000 dollars simply by allowing other users to disrupt his sleep in exchange for money.[16] However, such schemes only benefit the most popular creators.

Second, the application of contract law to a particular category of data, namely: personal data, is problematic. Personal data, i.e., data that is related to an identified or identifiable natural person,[17] is subject to data protection regulation in many jurisdictions. That means that strict rules apply concerning the processing of such data,

---

12 Donations, or gifts, are considered contracts in some, but not in all legal systems. In English law, for example, promises for donation are void for lack of consideration, unless they are laid down in a deed; whereas in German law gifts are treated as a form of contract, albeit with certain formalities. See for a comparative perspective H Beale and others (eds), *Cases, Materials and Text on Contract Law. Ius Commune Casebooks for the Common Law of Europe* (2nd edn, Hart Publishing 2010) 60, 89; Smits (n 2) 72, 104.

13 See e.g. 'How Companies Learn Your Secrets' *New York Times* (16 February 2012).

14 On which topic, see further Op Heij in Chapter 4.

15 The YouTube video 'Data to Money: How Much does Google Owe You?' makes some suggestions as to how payments to individual users of Google (or other companies) could be organised. See <www.youtube.com/watch?v=W8kA-EZReA0> accessed 18 August 2023.

16 G Weiss, S Bradley and N McAlone, 'How Creators Make Money Livestreaming on TikTok, YouTube, Amazon, and more' (5 June 2023) <https://www.yahoo.com/tech/money-livestreaming-platforms-twitch-tiktok-181642434.html?> accessed 18 August 2023.

17 This is the definition laid down in art 4(1) of the General Data Protection Regulation (GDPR) which will become applicable from 25 May 2018. See Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.

with the aim of safeguarding privacy. Rather than being concerned with economic ordering, as contract law is, data protection regulation is considered part of fundamental rights protection.[18]

Yet, in practice personal data can be part of contracts for goods or services in several ways. It might be that data are necessary for the proper functioning of a good or service. For example, for 'location services' on a mobile phone app to work it is necessary for the supplier of the app to have access to the customer's GPS location.[19] It may also be that personal data are requested by a supplier in exchange for a service, such as the example that was earlier given of WiFi services at an airport. In that case, the data are not necessary for the proper functioning of the service, but may constitute a counter-performance or 'payment' by the customer. Thirdly, data may be produced or generated by the user of a digital service. Examples of this category can be posts on social media, including texts, photos and videos, that can be traced to an identified or identifiable user.[20] When data is part of a contractual transaction, the question arises whether contractual rights and remedies can be applied to that transaction. Only the first category is unproblematic here, as data protection laws generally allow processing when personal data is necessary for the performance of a contract.[21] For the other two categories—personal data as counter-performance and personal data produced or generated by the user of a digital service—no easy answer exists. Some lawyers are vehemently opposed to the application of contractual regimes to personal data, on the basis that it would be unethical for data subjects to be able to trade their data in an economic transaction.[22] At the same time, the alternative view holds that personal data should be integrated into the framework of contract law, as it is an economic reality that it is used as a counter-performance in exchange for obtaining (mostly) a service. Contract law, which is concerned with economic transactions, would be the appropriate place to deal with 'payment' with data.[23] The same argument that was put forward in relation to the difficulty of establishing the value of individual data applies here: if Google earns money through advertising deals based

---

[18] In Europe, see e.g., arts 7 and 8 of the EU Charter of Fundamental Rights, art 16 of the Treaty on the Functioning of the European Union (TFEU), and art 8 of the European Convention on Human Rights (ECHR).

[19] See for this example recital 14 of the proposed Digital Content Directive (n 6).

[20] These types of data are also subject to intellectual property rights, on which see Chapter 9.

[21] For Europe see GDPR (n 17), art 6(1)(b).

[22] See G Buttarelli, the European Data Protection Supervisor (EDPS), 'Address to Socialists and Democrats Group workshop on the Proposed Digital Content Directive at the European Parliament' (12 January 2017) 3, who compares the market for data to the market for live human organs. The speech is available at: <www.edps.europa.eu/sites/default/files/publication/17-01-12_digital_content_directive_sd_en.pdf> accessed 18 August 2023.

[23] To this effect, C Langhanke and M Schmidt-Kessel, 'Consumer Data as Consideration' (2015) 4 *Journal of European Consumer and Market Law* 218, 219.

on the analysis of personal data,[24] why should the user of its search engine not have contractual rights and remedies if the service does not function properly?[25]

2.2 …and How?

If it is established that contract law should concern itself with data, the implications of that choice will need to be run through. How can issues concerning data be dealt with within the doctrinal systems of existing contract laws? Generally speaking, all contract law systems in the world will have to consider issues arising in relation to the following, archetypical aspects of contract law.

General principles of contract law

Contract laws around the world recognise autonomy and fairness as general principles underlying the specific rules of contract law.[26] Autonomy is generally defined as the fundamental right of individuals to shape their own future through voluntary actions, and in private law translates into the freedom to decide with whom and on which terms to contract.[27] In the data economy, new questions arise as to how autonomy should be perceived, for example to what extent individuals should be free to transfer their personal data in exchange for goods or services.[28] In that context, the

---

[24] The assumption here is that the data that a user enters into Google's search field can be traced back to them, and is hence data relating to an identifiable natural person.

[25] An additional question is whether a user of Google's search engine has a contract with Google, and when it would be concluded. This question is not settled by case law. Presumably, an argument could be made that there is a contract between Google and the user, which is concluded when the user starts a search on the website, and thereby accepts Google's offer for providing a web-searching service. See E Mik, 'Contracts Governing the Use of Websites' (2016) *Singapore Journal of Legal Studies* 70, 71. Even if no contractual relationship can be established, in the EU certain information duties may rest on a provider on the basis of the E-Commerce Directive. See Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market [2000] OJ L178/1, art 5.

[26] Other principles of contract law, such as a trust principle (Vertrauen in German, vertrouwen in Dutch law), the principle that agreements are binding (*pacta sunt servanda*), legal certainty, or a principle of consensualism, are recognised by various legal systems. This chapter focuses on autonomy and fairness as the primary principles that are impacted by the data economy, which are moreover the principles shared by virtually all contract laws in the world.

[27] WH van Boom and A Ogus, 'Introducing, Defining and Balancing "Autonomy v Paternalism"' (2010) 3 *Erasmus Law Review* 1.

[28] See e.g., E Kosta, *Consent in European Data Protection Law* (Brill 2013) 138, who advocates a rights-based approach to the use of personal data, in which the consent of the data subject is examined in the light of autonomy. This can mean that data protection law should restrict the possibilities for data subjects to dispose of or trade their personal data on the market for information.

fundamental right to privacy is also a relevant benchmark,[29] though it is not a principle of contract law.

Formation: from oral, to written to digital

The 'datafication' of the consumer market goes hand in hand with digitalisation. One area in which this is apparent, in particular when taking a historical perspective, is the formation of contract. The recognition of a contract as a legal figure that represents a binding agreement between two or more parties goes back to Roman times. Initially an oral agreement between two parties, established through the proclamation of a *stipulatio* in the presence of witnesses,[30] it became practice for contracts to be laid down in writing.[31] Until this day, although contracts may validly be concluded orally,[32] they are often laid down in writing. Since the rise of e-commerce, 'in writing' also can mean that the contract is recorded in digital form and confirmed by an electronic signature.[33] In consumer contracts, EU law furthermore requires that general terms and conditions are made available to the consumer in a way that allows one to store and reproduce them.[34]

Content and transparency

With regard to contracting in the data economy, however, more important than requirements about form are transparency requirements. Is it clear to the other party on which terms one wishes to enter into a contract, and if so, are those terms clear and intelligible? Moreover, are they valid, and if they diverge from default rules of contract law, do they do so within the boundaries of what the law allows? For

---

[29] Compare N Helberger and others, 'Big data en het consumentenrecht' in PH Blok (ed), *Big data en het recht* (Sdu 2017) 151, who uses autonomy, fairness and privacy as benchmarks for her evaluation.

[30] Albeit that the concept of a reciprocal or synallagmatic contract was established later than the earliest form of a binding promise, the stipulatio. See R Zimmermann, *The Law of Obligations: Roman Foundations of the Civilian Tradition* (OUP 1996) 68–9; B Nicholas, *An Introduction to Roman Law* (OUP 1962) 161–3.

[31] Zimmermann (n 30) 71; Nicholas (n 30) 194ff. See for a comparative overview of current European contract laws J Gordley, *The Enforceability of Promises in European Contract Law* (CUP 2001) 2.

[32] This rule is not codified in German or French law, but it is in Dutch law. Article 3:37 of the Dutch Civil Code stipulates that 'unless provided otherwise, declarations, including communications, can be made in any form and can be inferred from conduct.' See Smits (n 2) 101.

[33] For an overview of formal requirements per country, see G Spindler and F Börner (eds), *E-Commerce Law in Europe and the USA* (Springer 2002). See also I Walden and J Hörner, *E-Commerce Law and Practice in Europe* (Woodhead Publishing 2001), in particular Section 2. In Europe, rules concerning electronic signatures are laid down in Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market [2014] OJ L257/73.

[34] Directive 2000/31 (n 25), art 10(3).

business transactions, it is generally presumed that parties are by themselves able to investigate the terms of the contract and to negotiate the bargain that the other party is willing to make. The transparency required from the offeror ranges from systems that only require honesty in relation to statements, such as English law, to systems that require the disclosure of essential information about the terms and subject-matter of the contract, such as German and French law.[35] The transparency required in business-to-consumer contracts, by contrast, across the board is of a higher standard. Consumer protection rules in Europe require that the trader discloses detailed information about, inter alia, the price of the goods or services offered, the product characteristics, and the conditions under which terms may be changed.[36]

Conformity and remedies

The rules on the performance of contracts, and the remedies that are available when a party does not live up to a contractual promise, will have to be reassessed in the data economy. Debates on contracts for the supply of 'digital content' have been held at several stages in the development of rules of consumer contract law in Europe, but have only in 2019 led to legislation at the EU level. Early proposals for legislation, in the Consumer Rights Directive and the proposed Common European Sales Law (CESL), were either more modest or (in the case of the CESL) rejected during the legislative process between the European Parliament, the Council and the Commission.[37] A new attempt was made with the 2015 proposal for a Digital Content Directive, which was presented in tandem with a directive on online and distance sales contracts that later became a revised Consumer Sales Directive. Both were adopted as legislation in 2019.[38] The Digital Content Directive introduces rules on conformity and available remedies for non-conformity of digital content. The term 'digital content' includes data which is produced and supplied in digital form, i.e., in bytes, such as audio, video, apps, games and software, as well as services that allow the creation, processing or storage of data in digital form (cloud services) or the sharing of data (social media).[39] For this type of content, the Directive proposes con-

[35] J Cartwright, 'Defects of Consent in Contract Law' in AS Hartkamp and others, *Towards a European Civil Code* (4th edn, Kluwer Law International 2010) 537, 542.

[36] See further part 3 below.

[37] Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law COM(2011) 635 final, recital 17; Consumer Rights Directive (n 9) recital 19 and i.a. arts 2(11) and 9(2)(c). The only national jurisdiction in the EU that, at that time, had introduced specific rules on digital content was the United Kingdom in the UK Consumer Rights Act 2015.

[38] Digital Content Directive (n 6); 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, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28.

[39] See Digital Content Directive (n 6), art 2(1) and (2). Amendments proposed by the Presidency after the first reading of the proposed Directive by the Parliament and

formity rules and remedies that are tailored to the nature of digital content, in particular its non-physical character.[40] One difficulty is to demarcate the boundary between digital and physical goods, in particular in relation to the Internet of Things,[41] and further research will need to focus on the question of how the two can be distinguished. Another question is which conformity requirements should apply, which can be problematic as legal standards for the quality of data are lacking in existing laws.[42] The Digital Content Directive has introduced subjective requirements concerning description, fitness for purpose, instructions and updates that should be further specified in the contract (art 7). It also stipulates objective requirements with which all digital content and digital services should comply, elaborating which reasonable expectations consumers may have with regard to fitness for purpose, quality (including functionality, compatibility, accessibility, continuity and security), and updates (including security updates) (art 8). Due to the swiftness with which digital technologies are developed and the reasonable expectations with regard to the 'state of the art' of these technologies, it nevertheless remains difficult to successfully sue traders for non-conformity.[43]

---

the Council introduced a distinction between 'digital content' and 'digital services'. See Council of the European Union, Contracts for the Supply of Digital Content Interinstitutional File 2015/0287 (COD), art 1.

[40] This chapter focuses on aspects of contracting in the data economy that are thought to influence contract law in more fundamental ways. For an in-depth analysis of the suitability of various remedies, including repair, replacement, termination and damages, see e.g., M Loos and others, *Digital content contracts for consumers. Analysis of the applicable legal frameworks and suggestions for the contours of a model system of consumer protection in relation to digital content contracts, final report: Comparative analysis, law & economics analysis, assessment and development of recommendations for possible future rules on digital content contracts* (University of Amsterdam 2011). With an executive summary of the main points, a study performed for the European Commission is available at: <https://research.tilburguniversity.edu/en/publications/analysis-of-the-applicable-legal-frameworks-and-suggestions-for-t> accessed 18 August 2023.

[41] The 'Thing' in Internet of Things can be defined as 'any physical entity capable of connectivity that directly interfaces the physical world, such as embedded devices, sensors and actuators'; see G Noto La Diega and I Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (2016) 7 *European Journal of Law and Technology*, available at: <https://ejlt.org/index.php/ejlt/article/view/450> accessed 18 August 2023.

[42] For an analysis based on German law, but of wider impact, see T Hoeren, 'Big Data and the Legal Framework for Data Quality' (2017) 25 *International Journal of Law and Information Technology* 26.

[43] By way of illustration: the Dutch consumer organisation Consumentenbond's claim against Samsung with regard to the unavailability of security updates for older models of smartphones failed on the ground that there was no convincing evidence proving that Samsung's security update policy automatically resulted in critical security risks for consumers. See District Court The Hague 30 May 2018, ECLI:NL:RBDHA:2018:6310, para 4.12–4.16.

Liability of third parties

One characteristic of the data economy is that many contractual relationships are of a tripartite nature. Contracts are not just concluded between traders and consumers, e.g. when consumers purchase digital content in the form of apps or movies, but also very often through intermediary platforms with whom traders and consumers have contractual relationships. For example, traders and consumers can connect through platforms like Amazon or Vinted for the sale of consumer goods. On these platforms, moreover, traders include professional as well as non-professional actors. The latter category consists of natural persons, i.e. consumers, who have moved to the supply side of the market. They are often referred to as 'prosumers', a term conflating the terms 'consumer' and 'producer'.[44] In all of these constellations, liability for defective performance under existing laws will primarily be attributed to the trader. That seems justifiable in the light of doctrines of privity, which hold that third parties have no rights or duties in relation to a contract concluded between other parties. However, in the data economy it can lead to inequalities, as intermediary platforms escape liability while they are also the most powerful actor in the transaction, making profits based on commissions and on data aggregation used for targeted advertising.[45]

In sum, the rise of the data economy does not seem to upset the doctrinal structures of contract laws at a fundamental level. However, it does raise questions as to how existing doctrines can respond to the emergence of data-driven technologies, in particular when it comes to rebalancing autonomy and fairness. This brings us to a number of specific issues that have come up in relation to consumer contracts in the data economy: how to safeguard transparency, how to (re-)define fairness, and whether there is a need for adjustment of the 'average consumer' benchmark that has been a cornerstone of EU consumer law in the last decades. To some extent, existing regulation may be able to provide adequate answers to the question which rights consumers can enforce against traders or suppliers. Overall, however, a re-evaluation of consumer contract law is needed to determine whether new or revised regulation is required for contracting in the data economy. I will examine this question first in relation to transparency in consumer contract law.

3. TRANSPARENCY IN DATA-DRIVEN CONTRACTS[46]

Consumer contract law, globally, embraces the idea that the consumer should be provided with information that puts them on a (more) equal footing with traders.

---

44 A Toffler, *The Third Wave* (Bantam Books 1980) 280.

45 Compare, V Mak, 'How Can Consumer Interests Be Protected When Consumer Identities Are Increasingly Diffuse?' in H-W Micklitz and C Twigg-Flesner (eds), *The Transformation of Consumer Law and Policy in Europe* (Hart Publishing 2023) 43–63.

46 The term 'data-driven' is used as a broad indication of contracts in which consumers provide personal data in exchange for products or services. Compare C Busch and

Information can serve to diminish the asymmetry between consumers and businesses in terms of knowing the quality of products and services, whether the price is fair, and whether the terms and conditions of purchase are otherwise fair and reasonable towards the consumer.[47] The balance between autonomy and fairness in contract law is so restored. Especially in European law, this idea of transparency is reflected in numerous information requirements for traders in consumer contracts. The most generally applicable rules on this are laid down in the Consumer Rights Directive,[48] whilst rules for specific contracts can be found in the Consumer Credit Directive, the Mortgage Credit Directive and the Package Travel Directive.[49] These Directives require the trader to disclose information about the characteristics of a good or service, the price, the address details of the trader, as well as other terms of the contract.[50]

In the data economy, the question how transparency towards consumers can be guaranteed demands renewed scrutiny. The complexity of data-driven technologies means that it is not always clear to consumers how the services provided by the trader operate (e.g., with algorithm-based services, such as Google, or listings on Airbnb). This could be seen as intransparency with regard to the characteristics and quality of a service.[51] Further, the way in which a price is calculated, or whether the consumer pays a 'price' if they pay with data, is not always clear. Third, thorny questions arise when the 'data' at the heart of a transaction are personal data.

Existing regulation to some extent addresses the question how transparency of data use can be safeguarded in consumer contracts. However, one complication is that the GDPR and contract laws function as separate regimes with distinct consequences. Issues of transparency will be addressed in this section, saving some more general questions on contractual fairness for section 4 below.

---

others, 'Should Data Drive Private Law?' (2022) *Technology and Regulation* 81–87, <https://techreg.org/article/view/12285> accessed 18 August 2023.

47 I Ramsay, *Consumer Law and Policy* (3rd edn, Hart Publishing 2012) 49ff.

48 Directive 2011/83/EU (n 9).

49 Directive 2008/48/EC on credit agreements for consumers (Consumer Credit Directive) [2008] OJ L133/66; Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property (Mortgage Credit Directive) [2014] OJ L60/34; Directive (EU) 2015/2302 on package travel and linked travel arrangements (Package Travel Directive) [2015] OJ L326/1.

50 For distance and off-premises contracts, which will likely include the majority of (online) contracts involving data, see the requirements laid down in Directive 2011/83/EU (n 9), art 6. See also for e-commerce contracts Directive 2000/31/EC (n 25), art 5 and art 10.

51 The question whether to attach transparency requirements to algorithmic listings is under consideration in the European Law Institute's project, ELI, 'Model Rules on Online Platforms'. For more information, see the project website at: <www.europeanlawinstitute.eu/projects-publications/completed-projects/online-platforms/>.

3.1 The GDPR Regime

Can, and should, contract law interfere with data protection regimes?[52] The simple answer is that contractual agreements on the use of personal data cannot go beyond the boundaries laid down in data protection rules. In Europe,[53] the relevant framework for data protection follows from the GDPR. The Regulation determines that personal data may only lawfully be processed if consent has been given by the data subject (or in this case: the consumer) to the processing of their personal data for one or more specific purposes, or if processing is necessary inter alia for performance of the contract, compliance with a legal obligation, or for the purposes of the legitimate interests pursued by the controller of the data.[54] While it may be debated what amounts to 'consent' or what falls within the scope of 'legitimate interests', the provision establishes that situations in which these conditions are not complied with will constitute unlawful processing of personal data. In contract law, that could mean that significant limitations are placed on the use of data as payment. The processing of data for commercial purposes is unlikely in itself to constitute a 'legitimate' interest, and whether the consumer has given consent for the processing of personal data can be doubtful. In consumer contracts, such consent would mostly be obtained through the consumer's agreement with a set of general terms and conditions, in which a term is included on data processing. Although the agreement with standard terms binds the consumer in contract law, it is no longer considered as valid 'consent' under the GDPR.[55] That fits with the critical stance taken in the literature as to whether agreement with standard terms amounts to consent in data protection law. Studies have shown that most consumers do not actually read terms and conditions before agreeing

---

52 This question was already highlighted above, part 2.1.

53 The US regimes, by comparison, are less stringent in their prohibitions on the use and processing of personal data. See e.g. S Bilgic, 'Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act' (2018) 32 *Harvard Journal of Law & Technology* 321–355.

54 Article 6(1) GDPR, which specifies also that the last condition 'shall not apply to processing carried out by public authorities in the performance of their tasks'.

55 European Data Protection Board (EDPB), 'Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1' (adopted 4 May 2020) available at: <www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf> accessed 18 August 2023, para 81. According to recital 32 of the GDPR consent:

> 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, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. More specific rules to this effect are laid down in art 4(11), 7 and (for children) 8.

to them, in particular in online contracts where the consumer is required to click an agree-button before downloading a product.[56] In all cases where an online opt-in is required, therefore, high acceptance rates are found, which is problematic as the acceptance of terms (even if unread) may give suppliers the affirmation that they are entitled to disclose and process data more widely.[57] Even if it has been established that consent cannot be obtained through the use of standard terms, enforcement remains a problem. Workable alternatives to the current informed consent construction in data protection law will need further research.[58] Enforcement problems also occur with regard to the alternative ground for processing, i.e. the existence of a ‘legitimate ground’. This ground is also often used by business, although concerns have been raised with regard to the rightful use of this legal basis.[59]

3.2 Specific Rules in Consumer Contract Law

Existing legislation in contract law, and on occasion extending to tort law, may nonetheless go some way towards protecting consumers. In Europe, a safety net against the unlicensed use of consumers’ personal data is provided by the transparency requirements found in Directive 2005/29/EC on unfair commercial practices and Directive 93/13/EEC on unfair contract terms. These Directives can provide some relief to consumers when the contract terms were not transparent in relation to the trader’s use of (personal) data. In those circumstances, perhaps contrary to the intuition of a data protection lawyer, the consumer will be considered to be contractually bound. The lack of valid consent under the GDPR triggers the legal consequences available under that regime, such as the right to retrieve data. In contract law, however, a term concerning data use is not by definition void. It is nonetheless likely to be voidable by

---

[56] See e.g., B Custers and others, ‘Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law’ (2013) 10 *Journal of Law and Technology* 435; R Böhme and S Köpsell, ‘Trained to Accept? A Field Experiment on Consent Dialogs’ in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010) 2403; A Acquisti, ‘Nudging Privacy: The Behavioral Economics of Personal Information’ (2009) 7 *Security & Privacy Economics* 82.

[57] DJ Solove, ‘Introduction: Privacy Self-Management and the Consent Dilemma’ (2013) 126 *Harvard Law Review* 1880, 1899.

[58] It has been suggested that a system based on fair transactions, combined with a consent requirement in cases where the risks for the data subject of allowing processing are high, could perform better than the current model; see B Schermer, B Custers and S van der Hof, ‘The Crisis of Consent’ (2014) 16 *Ethics and Information Technology* 171.

[59] This concern became apparent already before the entry into force of the GDPR. See e.g. the results of a GDPR readiness study discussed by W Nauwelaerts, ‘GDPR – The Perfect Privacy Storm: You Can Run from the Regulator but You Cannot Hide from the Consumer’ (2017) 3 *European Data Protection Law Review* 251, 253. See also CJEU, Case C-252/21 *Meta Platforms Inc v Bundeskartellamt*, ECLI:EU:C:2023:537.

the consumer as an unfair term, although the precise conditions under which a term can be avoided depend on national law.[60] The rules on unfair commercial practices may also provide relief.

It should be noted, however, that the conditions for application of these Directives are such that the effect on consumer protection in relation to transparent use of data is limited. Such conditions relate to specific aspects of liability, e.g. causation requirements, but also a limitation of the remit of the Directives to transactions of an economic nature.

Looking first at the Unfair Commercial Practices Directive (UCPD), the most useful ground for contesting consent to data processing arguably is a misleading omission. If a trader fails to disclose, or fails to disclose in a clear, intelligible and timely manner, that personal data provided by the consumer will be processed and used for commercial activities of the trader, this could amount to an unfair omission. The Directive's stipulation that such an omission is actionable if it fails to identify 'the commercial intent of the commercial practice' could arguably be extended to data, since data have commercial value for the trader.[61] Still, for a successful action on the basis of the Directive the consumer will also have to prove that the misleading omission caused them to make a transactional decision—i.e., that they concluded a contract—that they would otherwise not have made.[62] Further, the available remedies are not harmonised by the Directive. It will therefore depend on the rules applicable in the consumer's country of residence what remedies are available and whether these exist in contract or tort law, or whether enforcement is regulated beyond private law, e.g. in administrative law or criminal law. In some EU Member States the consumer may be able to rescind or avoid the contract and to reclaim the price, whilst sometimes damages may be claimed.[63] Damages can be a problematic

---

[60] In Dutch law, art 3:40 sub 2 DCC stipulates that a term infringing a legal duty will be considered void. However, the provision adds that a term will be considered voidable if it serves to protect only one of the parties in a contractual relationship. For consumer contracts, that rule applies.

[61] In support of this argument, European Commission, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2021] OJ C526/19, with reference to art 7(2) and No 22 of Annex I to the UCPD.

[62] Directive 2005/29/EC (n 9), art 7(2). An alternative ground for action would be where the trader claims to deliver a 'free' service, yet requires the consumer to provide personal data in exchange. See M Loos and J Luzak, 'Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers' (2016) 39 *Journal of Consumer Policy* 63, 67.

[63] Rescission or avoidance are possible in Belgium and the Netherlands. For an overview of available remedies, see the country reports on unfair commercial practices published in the *Journal of European Consumer and Market Law*, issues 5 and 6 of 2015, and issue 2 of 2016.

remedy, however, since it will often be difficult to establish what loss the consumer has suffered as a result of the misleading practice.[64]

In addition, Directive 93/13/EEC on unfair terms in consumer contracts (UCTD) might be of use in relation to general terms and conditions that infringe data protection regulation. Terms that allow the trader to process data beyond what the GDPR regime stipulates as 'legitimate use' could potentially be set aside,[65] whereas contracts in which the consumer 'pays' for a good or service by providing personal data to the trader could be subject to the Directive too.[66] Some caution is however required when drawing this conclusion, as Directive 93/13/EEC appears to have been drafted only with the economic interests of consumers in mind, and to have been applied only in that vein. Cases like *Kásler*, *RWE Vertrieb* and *Invitel* emphasise that the consumer has the right to know on what terms they agree to enter into a contract. The consumer's knowledge extends to being aware of the *economic* consequences that signing up to the terms of the contract will have.[67]

Besides specific conditions for the availability of remedies, it is important to realise that the application of these Directives to contracts involving the processing of data is limited by their focus on the economic nature of transactions. This area of law has not been subject to a process of 'constitutionalisation' of contract law, which has won some ground in European contract law in the protection of consumers against unfair terms in mortgage agreements.[68] Still, cautious steps towards integrating the fundamental right of data protection into private law are being taken. An example can be seen on the case law on the UCPD. The Directive fully harmonises rules relating to unfair commercial practices harming consumers' economic interests,[69] and the transactions covered go beyond monetary performances. As determined by the CJEU in *Peek & Cloppenburg*, the concept of 'payment' must be interpreted as anything that brings an economic advantage to a consumer. This leaves open the possibility

---

[64] The comparison in tort will be with the transaction that the consumer would otherwise have made. Presuming that consumers often have made up their minds about wishing to buy a certain product or service, they would likely have chosen an alternative to the trader's offer, and not have gotten a cheaper deal. Damages are then nil.

[65] Such terms would infringe a legal duty—the protection of personal data—and would be considered unfair on that ground in most legal systems in Europe. The same might be the case if terms and conditions diverge to the detriment of the consumer from default rules of law that are not mandatory; compare the substantive unfairness test of CJEU, Case C-415/11 *Mohamed Aziz v Catalunyacaixa* ECLI:EU:C:2013:164, para 68.

[66] Cf Loos and Luzak (n 62) 67.

[67] CJEU, Case C-26/13 *Kásler v OTP Jelzalogbank Zrt* ECLI:EU:C:2014:282, para 74; CJEU, Case 92/11 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV* ECLI:EU:C:2013:180; and CJEU, Case 472/10 *Nemzeti Fogyasztovedelmi Hatosag v Invitel Tavkozlesi Zrt* ECLI:EU:C:2012:242.

[68] H-W Micklitz and N Reich, 'The Court and Sleeping Beauty: The Revival of the Unfair Contract Terms Directive' (2014) 51 CML Rev 771.

[69] See European Commission Guidance [2021] OJ C526/6 (n 61).

that the provision of data counts as a transactional performance.[70] For further discussion of digital content contracts and payment with data, see Chapter 3 in this volume.

Further developments concerning transparency in digital markets may arise from the Digital Fairness Fitness Check launched by the European Commission in 2022. The Fitness Check targets three EU Directives relating to transparency and information duties in the pre-contractual stage: the UCPD, the UCTD and the CRD.[71] Although this scope directs the focus of the Fitness Check to questions of transparency, its stated objective is 'to analyse whether additional legislation or other action is needed in the medium-term in order to ensure equal fairness online and offline'.[72] Whether the Commission's analysis will indeed impact fairness remains to be seen, with outcomes of the project expected in the course of 2024. In the meantime, the adoption of the Digital Content Directive in 2019 has given rise to some reflection on the definition of fairness in consumer contract law. The following section examines the state of play.

4. REASSESSING FAIRNESS IN DATA-DRIVEN CONTRACTS

As was illustrated by the analysis of transparency in the previous section, existing regulation provides some protection for consumers against a lack of information when concluding a contract involving the processing of data. Yet, most national legal systems, as well as EU law, recognise that information alone is not sufficient to protect consumers, for example because people's ability to process information is limited.[73] Another challenge, particular to data-driven contracts, is the 'digital asymmetry' that consumers experience in digital markets: the structural imbalance between tech-providers and consumers, due to consumers' structural and universal

70 Compare M Narciso, 'The Unfair Commercial Practices Directive – Fit for Digital Challenges?' (2022) 11 *Journal of European Consumer and Market Law* 147.

71 See the European Commission, 'Call for Evidence for an Evaluation/Fitness Check' Ares(2022)3718170. For updates on this Fitness Check, see <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 18 August 2023.

72 European Commission Call for Evidence (n 71) 1.

73 This insight has been informed in recent decades by the growing body of empirical studies on consumer behaviour. For an analysis of the impact of behavioural economics on European consumer law, see the collection of essays in A Alemanno and A-L Sibony, *Nudge and the Law. A European Perspective* (Hart Publishing 2015). For EU law's stance, see CJEU C-195/14 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Teekanne GmbH & Co KG* (*Teekanne*) ECLI:EU:C:2015:361.

inability to fully understand the digital architecture.[74] Even if information is provided, the complexity of digital architectures makes it impossible to fully convey to consumers what will happen with the data that they provided. In practice, therefore, the information paradigm falls short and consumers often conclude contracts without being fully aware of what they are signing up to.[75]

By way of solution, in particular in national contract laws, rules are found that restrict party autonomy with an eye to the protection of weaker contracting parties, such as consumers, and ensure that contracts are fair or reasonable. These rules vary from general rules of fairness or equity to specific, mandatory rules of consumer protection. EU law also contains a number of instruments that at least touch upon substantial fairness.[76]

One difficulty in this respect is that it is not established what contractual fairness entails and how far contract laws can go to protect it. This question has yet to be answered, but regulators have been grappling with it. By way of illustration, it is helpful to consider the implementation of the Digital Content Directive (DCD) (on which see also Chapter 4).

At the national level, the introduction of the DCD has led to discussions on the need for additional protection in contract law for consumers. I highlight the Netherlands as an example. The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* (AP)) advised the Dutch legislator in the course of the implementation procedure of the DCD to insert additional provision into the Dutch Civil Code (DCC) with an eye to preventing too rapid consent by consumers to the processing of personal data.[77] The AP's proposal suggested that a list of specific additions to the 'consent' requirement of the GDPR should be introduced for digital content contracts concluded between traders and consumers. Such additions included, inter alia, specific requirement for consent for the processing of special categories of (sensitive) personal data, processing that is not (or hardly) limited in time, and processing without delimiting

---

74 N Helberger and others, *EU Consumer Protection 2.0. Structural Asymmetries in Digital Consumer Markets* (BEUC Report, March 2021) <www.beuc.eu/brochure/eu-consumer-protection-20-structural-asymmetries-digital-consumer-markets-0> accessed 26 October 2022; A Jablonowska and others, 'Consumer Law and Artificial Intelligence. Challenges to the EU Consumer Law and Policy Stemming from the Business' Use of Artificial Intelligence' (2018) EUI Working Paper Law 2018/11, <https://cadmus.eui.eu/handle/1814/57484> accessed 26 October 2022; S Zuboff, *The Age of Surveillance Capitalism* (Public Affairs 2019).

75 S Zuboff, *The Age of Surveillance Capitalism* (Public Affairs 2019).

76 E.g. the fairness test of the UCTD, which the CJEU elaborated in C-415/11 *Aziz* (n 65).

77 Autoriteit Persoonsgegevens, 'Advies wetsvoorstel Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud' (16 April 2020) <https://autoriteitpersoonsgegevens.nl/uploads/imported/advies_implementatiewet_richtlijnen_verkoop_goederen_en_levering_digitale_inhoud.pdf> accessed 18 August 2023.

with which or how many third parties the data may be shared.[78] Non-compliance with the suggested additions should, according to the AP, give the consumer the right to rescind the contract in its entirety.

This proposal was not followed by the Dutch legislator in the implementation of the DCD, in part because national legislators lack competence for introducing rules in areas of law subject to full harmonisation through EU law. The Dutch legislator has however indicated a willingness to put forward proposals for additional regulation at the EU level.[79] Also, even without immediate follow-up in legislation, the debate ensuing upon the AP's proposal illustrates which questions arise in defining a new balance of fairness in relation to contracts involving the provision of personal data. In essence it asks the question whether consumers' autonomy should be curtailed with an eye to safeguarding that they would in substance get 'a fair deal'.[80]

The general view amongst authors in the Netherlands for now appears to be that the addition of consent requirements in consumer contract law should be kept to a minimum, as the GDPR regime differs too much from contract law to integrate the two in a meaningful way.[81] In particular, even if consent in practice often overlaps with the acceptance of an offer in the contractual sense, the legal consequences of the two are distinct.[82] On a more general level, the AP's suggestion to allow consumers to rescind the contract in its entirety is hard to fit into the Dutch law of obligations from a doctrinal perspective. The AP suggests that the legal basis for rescission could be found in the general principle of good faith (art 6:248 DCC). That provision can in Dutch law indeed be a legal basis for setting aside an entire contract. However, it is ill-suited for the use envisaged by the AP. It is an open norm that gains practical substance through its application in individual cases in which judges, wheighing all circumstances, can reach individualised outcomes. The rules proposed by the AP would do something else, namely introduce rules determining specific instances of consent that would be considered unfair in all circumstances. That type of rule is

---

[78] Autoriteit Persoonsgegevens Advies (n 77) 6–7.

[79] Kamerbrief Minister van Economische Zaken en Klimaat, 'Resultaten van het onderzoek over betalen met persoonsgegevens en consumentenbescherming' (18 November 2022) available at: <www.rijksoverheid.nl/documenten/kamerstukken/2022/11/18/resultaten-van-het-onderzoek-over-betalen-met-persoonsgegevens-en-consumentenbescherming> accessed 18 August 2023.

[80] Autoriteit Persoonsgegevens Advies (n 77) 2.

[81] Compare V Mak and G-J Zwenne, 'Onderzoek over betalen met persoonsgegevens en consumentenbescherming', Onderzoekstudie in opdracht van het Ministerie van Economische Zaken en Klimaat (EZK) (November 2021) available at: <www.rijksoverheid.nl/documenten/kamerstukken/2022/11/18/resultaten-van-het-onderzoek-over-betalen-met-persoonsgegevens-en-consumentenbescherming> accessed 18 August 2023; A Berlee and D Op Heij, 'Het consumentenrecht en het gegevensbeschermingsrecht. Waar het complementeert en waar het schuurt' in W van Boom and others (eds), *Vooruitgedenkboek Burgerlijk Wetboek 1992–2022* (Boom juridisch 2023) 93.

[82] Berlee and Op Heij (n 81) 107.

not so much a reflection of the general principle of good faith, but rather of a policy choice made by the legislator with the intention of protection of the weaker party in a transaction.[83]

One alternative route that could nevertheless be considered, provided that contracts involving data processing are considered to fall within the scope of unfair terms control,[84] is to stipulate that such terms are presumed to be unfair or are always considered unfair. In Dutch law, the legislator could to that end add certain clauses concerning consent for the processing of data to the grey and/or blacklists of unfair terms (art 6:236 and 6:237 DCC). These lists contain terms that are presumed to be unfair (grey list) or that are in all circumstances considered unfair (blacklist).[85] The unfair terms regime is concerned with individual terms and does not as a rule affect the validity of the entire contract. Consumers could benefit from the addition of this type of protection in contract law, which would apply alongside the GDPR regime for consent. It would give them the possibility to rescind unfair terms and on that basis claim remedies in contract law, such as compensation or a discount.[86] Adding provisions to the unfair terms regime could therefore enhance consumer protection. The grey list would in that case seem most suitable, as none of the types of consent demarcated by the AP as potentially unfair will be unfair in all circumstances.[87]

The discussion on contractual fairness is likely to continue beyond consent and unfair terms. At the EU level, initiatives have been taken to obtain more control over the use of so-called 'dark patterns' by operators of online marketplaces. Dark patterns are manipulative practices used by websites or online platforms with the aim of manipulating consumers or tricking them into purchases. The EU proposal for a Data Act defines them as 'design techniques that push or deceive consumers into decisions that have negative consequences for them'.[88] The current legal framework does not contain specific rules or regimes for regulating dark patterns, but covers them through a combination of instruments: the UCPD, the GDPR, the proposed Data and

---

83 Mak and Zwenne (n 81) 14–15.

84 See above, section 3.2.

85 They implement and form an addition to the terms listed in the Annex to the UCTD.

86 The legal basis for compensation could be art 3:53 sub 2 DCC, which allows a court to award monetary compensation if after rescission a performance cannot be undone, as is likely to be the case when data has been provided and has been processed.

87 Mak and Zwenne (n 81) 12. For an alternative approach, compare M Loos and J Luzak, 'Update the Unfair Contract Terms Directive for Digital Services' Study requested by the JURI Committee of the European Parliament (February 2021) available at: <www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf> accessed 18 August 2023.

88 European Commission Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) COM(2022) 68 final, recital 34.

AI Acts, and the Digital Services Act (DSA)[89] and Digital Markets Act (DMA).[90] The use of dark patterns may in the future lead to further reflections on the meaning of fairness for contracting in the digital market place.[91]

5. FROM AVERAGE CONSUMER TO PERSONALISED CONTRACTING?

Finally, a fundamental challenge to consumer contract law is posed by the use of data as a means to personalise transactions. With traders learning the personal preferences of each consumer through their purchases, online searches, likes on social media, and other activities that are registered as data and available for analysis by the trader, it has become possible to target advertising or even specific offers to individual consumers. Online stores like Amazon, but also brick-and-mortar stores like supermarkets,[92] provide consumers with personalised recommendations and discount offers. This practice may be the harbinger of a shift from standardisation to personalisation in consumer law.[93] The question is whether regulation should be responsive to this change, and if so, how. The discussion will focus next on the potential implications for contract law.

The primary consequences in contract law of the personalisation of consumer contracts would relate to the assessment of transparency and fairness, as discussed above. The benchmark used for assessing whether information given to consumers through advertising or terms of the contract was fair, or whether standard terms of the contract were fair, are the 'presumed expectations of the average consumer who

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

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

91 For an evaluation the current regulation see I Graef, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' in R Woodcock (ed), *Toward an Inframarginal Revolution: Markets as Wealth Distributors* (CUP 2023) (forthcoming), also available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4411537> accessed 18 August 2023.

92 As an aside: the distinction between online and physical stores is becoming less pronounced as they venture into each other's territory. Amazon has opened its first physical stores, whilst many supermarkets operate websites through which customers can order goods for home delivery.

93 On this topic see in this volume also Busch and De Franceschi, Chapter 16. See Busch (n 5) 221.

is reasonably well-informed and reasonably observant and circumspect'.[94] This 'average consumer' is perceived as a consumer who is able to process information concerning the product or service that is purchased. In general, it is considered to be efficient to work with a broadly defined category of 'consumers'. While there can be a large variety of consumers, the defining characteristic of all of them is that they generally have a weaker bargaining position than traders or suppliers.[95] Tailoring rules of consumer protection to a consumer who is broadly defined as a natural person not acting in the course of a business or profession, and combined with the also general notion of an 'average consumer', means that the majority of consumers will be included, and therefore protected, through consumer law.

Exceptions exist in some cases. Besides the general category of 'average consumers', a category of 'vulnerable' consumers is recognised in the UCPD who are vulnerable because of their mental or physical infirmity, age or credulity.[96] The idea of working with a specific target group, such as vulnerable consumers, has been deemed to improve legal certainty. Since the targeted group is more clearly defined, it is easier for the legislator and the courts to determine what level of protection fits with these types of consumers—and to ensure that it is neither too high nor too low.

It has been suggested that a similar approach can be applied to cases in which the trader has personalised information about a consumer. According to Rott: 'spricht auch nichts dagegen, dann, wenn der Unternehmer mit kommerzieller Kommunikation auf den einzelnen Verbraucher zielt, die "Zielgruppe" auf eben diesen einzelnen Verbraucher zu beschränken'.[97] In other words, the target group may be limited to one person, whose preferences are known to the trader. That idea could well be operationalised in the online market, in which many traders will have data stored on the previous purchases or searches of a consumer on their website.

Whether that approach is desirable is another question. Counter-arguments can be that such an approach would infringe upon the privacy of the consumer, or that it is still inefficient to work with individual approaches for each consumer.[98] Furthermore, the relation between the personalised assessment of unfair commercial practices and unfair terms would have to be calibrated with existing individual approaches in contract law, i.e. the application of rules on defects of consent such as mistake, misrepresentation, duress. It would therefore also raise new, doctrinal challenges for contract law.

---

[94] CJEU, Case C-210/96 *Gut Springenheide GmbH v Oberkreisdirektor des Kreises Steinfurt - Amt fur Lebensmitteluberwachung* EU:C:1998:369, para 31; *Kásler* (n 67) para 74.

[95] See Hondius (n 4).

[96] Unfair Commercial Practices Directive (n 9), art 5(3).

[97] P Rott, 'Der "Durchschnittsverbraucher" – ein Auslaufmodell angesichts personalisierten Marketings?' (201) *Verbraucher und Recht* 163.

[98] V Mak, 'De "gemiddelde consument": van fictie naar feit?' (2017) *Ars Aequi* 592, 598–599.

Other challenges relate to the emergence of new categories of market actors, such as the 'prosumer' on online platforms, as was highlighted in section 2.[99] How contract law should respond to such developments requires further analysis. It might be that adaptation of existing rules suffices, but one could also consider the introduction of a third category of prosumers, alongside consumers and traders.

6. CONCLUDING REMARKS

Although the main outlines of doctrines in contract law have been long-settled, it can be seen that the emergence of data-driven technologies in consumer markets has led to new challenges. Legislators at the national level as well as at the EU level are grappling with the question of how to protect consumers in markets in which the complexity of digital architectures hinders the application of rules aimed at transparency and fairness. Digital architectures based on marketing techniques using profiling, algorithms, and dark patterns are becoming so opaque that the provision of information can hardly enable consumers to make sound decisions concerning the conclusion of contracts.

This chapter has explored in which way the application of existing regulation can provide some solutions and in what respect progress can still be made to integrate contract law and data protection. EU Directives, in particular the UCTD and the UCPD, can provide some relief for consumers who have consented to the use of (personal) data by agreeing to contract terms to that effect. Therefore, some protection is available against regularly occurring practices of including terms concerning data processing in the standard terms and conditions. However, the conditions under which remedies—in the form of rescission of terms or compensation through damages—are available are restrictive in nature. The focus on the economic consequences of transactions means that existing consumer contract law can only to a limited extent address data protection issues, albeit that cautious steps are being taken towards a broader application of consumer protection rules.

Broader attempts at rebalancing contractual fairness for consumer contracts involving data use have been undertaken. An illustration is the debate in the Netherlands in relation to the implementation of the DCD (section 4 above). For now, however, the suggestion to introduce additional requirements for consent in consumer contract law has not been taken up by the legislator. An opening for consideration of future regulation has nevertheless been created.

Finally, the standard against which transparency and fairness are assessed currently is the 'average consumer', who in EU law is defined as someone who is reasonably well-informed and reasonably observant and circumspect. Advances in technology create opportunities for personalisation of contractual offers. Besides objections for using such technologies from a privacy perspective, the integration of personalised

---

99 See section 2.2 above.

approached into existing consumer contract law would require more study. Can they be connected to broader doctrines in general contract law, or would too much be lost in terms of consumer protection? That question in itself sets the tone for future discussions on consumer contract law and data-driven technologies.

ACKNOWLEDGMENT

This publication is part of the project 'These Shoes Don't Fit! How can consumer interests be protected when consumer identities are increasingly diffuse?' (with project number VI.C.211.012) of the research programme Vici SGW which is financed by the Dutch Research Council (NWO). For details on the project see <consumerid.eu>.