10

AI and Consumer Protection

An Introduction

Evelyne Terryn and Sylvia Martos Marquez

10.1 INTRODUCTION

AI brings risks but also opportunities for consumers. For instance, AI can help consumers to optimize their energy use, detect fraud with their credit cards, simplify or select relevant information or translate. Risks do however also exist, for instance, in the form of biased erroneous information and advice or manipulation into choices that do not serve consumers best interests. Also when it comes to consumer *law*, which traditionally focuses on protecting consumers' autonomy and self-determination, the increased use of AI poses major challenges, which will be the focal point of this chapter.

We start by setting out how AI systems can affect consumers in both positive and negative ways (Section 10.2). Next, we explain how the fundamental underpinnings and basic concepts of consumer law are challenged by AI's ubiquity, and we caution against a silo approach to the application of this legal domain in the context of AI (Section 10.3). Subsequently, we provide a brief overview of some of the most relevant consumer protection instruments in the EU and discuss how they apply to AI systems (Section 10.4). Finally, we illustrate the shortcomings of the current consumer protection law framework more concretely by taking dark patterns as a case study (Section 10.5). We conclude that additional regulation is needed to protect consumers against AI's risks (Section 10.6).

10.2 CHALLENGES AND OPPORTUNITIES OF AI FOR CONSUMERS

The combination of AI and data offers traders a vast range of new opportunities in their relationship with consumers. Economic operators may use, among other techniques, *machine learning* algorithms, a specialized subdiscipline of AI, to analyze large datasets. These algorithms process extensive examples of desired and interesting behavior, known as the "training data," to generate computer-readable data-learned

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

knowledge. This knowledge can then be used to optimize various processes.[1] The (personal) data of consumers thus becomes a valuable source of information for companies.[2] Moreover, with the increasing adoption of the Internet of Things and advances in Big Data, the accuracy and amount of information obtained about individual consumers and their behavior is only expected to increase.[3] In an ideal situation consumers know which input (data set) was employed by the market operator to train the algorithm, which learning algorithm was applied and which assignment the machine was trained for.[4] However, market operators using AI often fail to disclose this information to consumers.[5] In addition, consumers also often face the so-called "*black box*" or "inexplicability" problem with data-driven AI, which means that the exact reasoning that led to the *output*, the final decision as presented to humans, remains unknown.[6] Collectively, this contributes to an asymmetry of information between businesses and consumers with market players collecting a huge amount of personal data on consumers.[7] In addition, consumers often remain unaware that pricing, or advertising have been tailored to their supposed preferences, thus creating an enormous potential to exploit the inherent weaknesses in the consumers' ability to understand that they are being persuaded.[8] Another major challenge, next to the consumer's inability to understand business behavior, is that automated decisions of algorithmic decision-making can lead to biased or discriminatory results, as the training data may not be neutral (selected by a human and thus perpetuating human biases) and may contain outdated data, data reflecting consumer's behavioral biases or existing social biases against a minority.[9] This could lead directly to consumers receiving biased and erroneous advice and information.

[1] Agnieszka Jabłonowska, Anna Maria Nowak, Giovanni Sartor, Hans-W Micklitz, Maciej Kuziemski, and Pałka Przemysław (EUI working papers), "Consumer law and artificial intelligence: Challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence – final report of the ARTSY project" (2018), https://ssrn.com/abstract=3228051, accessed December 23, 2022, 7; Martin Ebers "Liability for AI & consumer law" (2021) *JIPITEC*, 12: 206.

[2] Jabłonowska a.o., "Consumer law and AI" 5 and 36.

[3] Jabłonowska a.o., "Consumer law and AI" 49.

[4] Jablonowska a.o., "Consumer law and AI" 5.

[5] CMA, "Online platforms and digital advertising: Market study final report" (July 1, 2020), www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report, accessed December 23, 2022.16; Jablonowska a.o., "Consumer law and AI," 5.

[6] Ebers, "Liability for AI & consumer law" 208; Giovani Sartor, "Artificial intelligence: Challenges for EU citizens and consumers" (January 2019), www.europarl.europa.eu/RegData/etudes/BRIE/2019/631043/IPOL_BRI(2019)631043_EN.pdf, accessed December 23, 2022, 5.

[7] European Commission, DG Justice and Consumers, Francisco Lupiáñez-Villanueva, Alba Boluda, Francesco Bogliacino et al., "Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation: final report" (2022) *Publications Office of the European Union*, https://data.europa.eu/doi/10.2838/859030. 73; Ebers, "Liability AI-consumer law" 208.

[8] EC, "Behavioural study" 103.

[9] Ebers, "Liability for AI & consumer law" 212; CMA, "Digital advertising" 64; Brent Mittelstadt, Johann Laux, and Sandra Wachter, "Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice" (2021) *Common Market Law Review*, 58: 719.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

In addition, AI brings significant risks of influencing consumers into making choices that do not serve their best interests.[10] The ability to predict the reactions of consumers allows businesses to trigger the desired behavior of consumers, potentially making use of consumer biases,[11] for instance through choice architecture. Ranging from the color of the "buy" button on online shopping stores to the position of a default payment method – the choice in design architecture can be based on algorithms that define how choices are presented to consumers in order to influence them.[12]

Economic operators may furthermore influence or manipulate consumers by restricting the information or offers they can access and thus their options and this for purely economic goals.[13] Clustering techniques are used to analyze consumer behavior to classify them into meaningful categories and treat them differently.[14] This personalization can occur in different forms, including the "choice architecture," the offers that are presented to consumers or in the form of different prices for the same product for different categories of consumers.[15] AI systems may also be used to determine and offer consumers the reserve price – the highest price they are able or willing to pay for a good or service.[16]

Although AI entails risks, it also provides opportunities for consumers, in various sectors. Think of AI applications in healthcare (e.g., through mental health chatbots, diagnostics[17]), legal services (e.g., cheaper legal advice), finance and insurance services (e.g., fraud prevention), information services (e.g., machine translation, selection of more relevant content), and energy services (e.g., optimization of energy use through "smart homes"), to name but a few.[18] Personalized offers by traders and vendors could (at least in theory) also assist consumers to overcome undesirable information overload. An example of a consumer empowering technology in the legal sector is CLAUDETTE. This online system detects potentially unfair clauses in online contracts and privacy policies, to empower the weaker contract party.[19]

[10] OECD, "Dark commercial patterns, OECD digital economy papers" (2022) No.336 *OECD Publishing* 9.

[11] Sartor, "AI: challenges for EU citizens and consumers" 14.

[12] OECD, "Dark commercial patterns" 12; CMA, 'Algorithms: how they can reduce competition and harm consumers' (January 19, 2021), www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers, accessed December 23, 2022.

[13] Sartor, "AI: challenges for EU citizens and consumers" 3.

[14] CMA, "Algorithms – how they can harm consumers"; Iqbal H. Sarker, "Machine learning: Algorithms, real-world applications and research directions" (2021) *SN Computer Science*: 160.

[15] CMA, "Algorithms – how they can harm consumers."

[16] Sartor, "AI: Challenges for EU citizens and consumers" 18.

[17] Ahbimanyu S. Ahuja, "The impact of artificial intelligence in medicine on the future role of physician" (2019) *PeerJ* 12; Louise I. T. Lee, Radha S. Ayyalaraju, Rakesh Ganatra, and Senthooran Kanthasamy, "The current state of artificial intelligence in medical imaging and nuclear medicine" (2019) *BJR Open* 5.

[18] For more examples, Jablonowska a.o., "Consumer law and AI" 19 et seq.

[19] Jablonowska a.o., "Consumer law and AI" 33.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

10.3 CHALLENGES OF AI FOR CONSUMER LAW

Section 10.2 illustrated how AI systems can both positively and negatively affect consumers. However, the digital transformation in general and AI specifically also raises challenges to consumer law. The fundamental underpinnings and concepts of consumer law are increasingly put under pressure, and these new technologies also pose enormous challenges in terms of enforcement. Furthermore, because of the different types of concerns that AI systems raise in this context, these challenges make it clear that consumer law cannot be seen or enforced in isolation from data protection or competition law. These aspects are briefly discussed in Sections 10.3.1–10.3.3.

10.3.1 *Challenges to the Fundamental Underpinnings of Consumer Law*

Historically, the emergence of consumer law is linked to the development of a consumer society. In fact, this legal domain has been referred to as a "*reflection of the consumer society in the legal sphere*."[20] The need for legal rules to protect those who consume, was indeed felt more urgently when consumption, above the level of basic needs, became an important aspect of life in society.[21] The trend to attach increasing importance to consumption had been ongoing for several centuries,[22] but the increasing affluence, the changing nature of the way business was conducted, and the massification of consumption, all contributed to a body of consumer protection rules being adopted, mainly from the 1950s.[23] More consumption was thought to equal more consumer welfare and more happiness. Consumer protection law in Europe first emerged at national level.[24] It was only from the 1970s on that European institutions started to develop an interest in consumer protection and that the first consumer protection programs followed.[25] The first binding instruments were adopted in the 1980s, and consisted mostly of minimum harmonization instruments. This means that member states are allowed to maintain or adopt more

[20] Geraint Howells, Ian Ramsay, and Thomas Wilhelmsson, "Consumer law in its international dimension" in G. Howells and T. Wilhelmsson (eds), *Handbook of Research in International Consumer Law*, 2nd ed (Edward Elgar Publishing, 2018), 4.

[21] Howells, Ramsay, and Wilhelmsson, "Consumer law in its international dimension" 4.

[22] Frank Trentmann, *Empire of Things: How We Became a World of Consumers, from the Fifteenth Century to the Twenty-First* (HarperCollins, 2016).

[23] Howells, Ramsay, and Wilhelmsson, "Consumer law in its international dimension," 4–6.

[24] On the emergence of consumer law in the EU, see more elaborately H.-W. Micklitz et al. (eds), *The Fathers and Mothers of Consumer Law and Policy in Europe: The Foundational Years 1950–1980* (2019), EUI, https://cadmus.eui.eu/handle/1814/63766, accessed February 22, 2023.

[25] Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy [1975] OJ C 92/1; Council Resolution of 19 May 1981 on a second programme of the European Economic Community for a consumer protection and information policy [1981] OJ C133/1; See, in more detail, Ludwig Krämer, "European Commission" in Micklitz, *The Fathers and Mothers of Consumer Law*, 26 ff.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

protective provisions, as long as the minimum standards imposed by the harmonization instrument are respected. From 2000 onwards, the shift to maximum harmonization in the European consumer protection instruments reduced the scope for a national consumer (protection) policy.

While originally the protection of a weaker consumer was central in many national regimes, the focus in European consumer law came to be on the rational consumer whose right to self-determination (private autonomy) on a market must be guaranteed.[26] This right to self-determination can be understood as the right to make choices in the (internal) market according to one's own preferences[27] thereby furthering the realization of the internal market.[28] This focus on self-determination presupposes a consumer capable of making choices and enjoying the widest possible options to choose from.[29] EU consumer law could thus be described as the guardian of the economic rights of the nonprofessional player in the (internal) market. Private autonomy and contractual freedom should in principle suffice to protect these economic rights and to guarantee a bargain in accordance with one's own preferences, but consumer law acknowledges that the preconditions for such a bargain might be absent, especially due to information asymmetries between professional and nonprofessional players.[30] Information was and is therefore used as the main corrective mechanism in EU consumer law.[31] Further reaching intervention – for example, by regulating the content of contracts – implies a greater intrusion into private autonomy and is therefore only a subsidiary protection mechanism.[32]

AI and the far-reaching possibilities of personalization and manipulation it entails, especially when used in combination with personal data, now challenges the assumption of the rational consumer with its "own" preferences even more fundamentally. The efficiency of information as a means of protection had already been questioned before the advent of new technologies,[33] but the additional

[26] See also H.-W. Micklitz, "Squaring the circle? Reconciling consumer law and the circular economy" (2019) *EuCML* 229, pointing out that the protective element faded into the background when the EU took over consumer policy in the aftermath of the Single European Act.

[27] On the omnipresent risk of manipulation of such interests and preferences, see Cass Sunstein, "Fifty shades of manipulation" (2016) *Journal of Marketing Behavior*, 213: 32.

[28] Most EU consumer legislation indeed tends to be based on internal market justifications, see Howells, Ramsay, and Wilhelmsson, "Consumer law in its international dimension," 9. See also the legal basis used for most consumer protective directives: Art 114 TFEU rather than Art 169 TFEU.

[29] Howells, Ramsay, and Wilhelmsson, "Consumer law in its international dimension," 35.

[30] Ugo Mattei and Alessandra Quarta, *The Turning Point in Private Law* (Elgar Edward Publishing, 2019) 95.

[31] On the information paradigm that plays a central role in EU consumer policy, see among others: Norbert Reich and H.-W. Micklitz, "Economic law, consumer interests and EU integration" in Norbert Reich et al. (eds), *European Consumer Law* (Intersentia, 2014) 1, 21; Steven Weatherill, *EU Consumer Law and Policy* (Edward Elgar Publishing, 2013) ch 4.

[32] In this sense, see Josef Drexl, *Die wirtschaftliche Selbstbestimmung des Verbrauchers* (Mohr Siebeck, 1998).

[33] See among others for insights from behavioral sciences, Geneviève Helleringer and Anne-Lise Sibony (2017) "European consumer protection through the behavioral lens" *Columbia Journal of European Law*, 23(3): 607–646.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

complexity of AI leaves no doubt that the mere provision of information will not be a solution to the ever increasing information asymmetry and risk of manipulation. The emergence of an "attention economy" whereby companies strive to retain consumers' attention in order to generate revenue based on advertising and data gathering, furthermore also makes clear that "more consumption is more consumer welfare" is an illusion.[34] The traditional underpinnings of consumer law therefore need revisiting.

10.3.2 *Challenges to the Basic Concepts of Consumer Law*

European consumer law uses the abstract concept of the "average" consumer as a benchmark.[35] This is a "reasonably well informed and reasonably observant and circumspect" consumer;[36] a person who is "reasonably critical […], conscious and circumspect in his or her market behaviour."[37] This benchmark, as interpreted by the Court of Justice of the European Union, has been criticized for not taking into account cognitive biases and limitations of the consumers and for allowing companies to engage in exploitative behavior.[38] AI now creates exponential possibilities to exploit these cognitive biases and the need to realign the consumer benchmark with the realities of consumer behavior is therefore even more urgent. There is furthermore some, but only limited, attention to the vulnerable consumer in EU consumer law.[39] Thus, the Unfair Commercial Practices Directive, for example, allows to assess a practice from the perspective of the average member of a group of vulnerable consumers even if the practice was directed to a wider group, if the trader could reasonably foresee that the practice would distort the behavior of vulnerable consumers.[40] The characteristics the UCPD identifies to define vulnerability (such as mental or physical infirmity, age, or credulity) are however not particularly helpful nor exhaustive in a digital context. Interestingly, however, the Commission Guidance does stress that vulnerability is not a static concept, but a dynamic and

[34] The same remark can be made from a sustainability perspective.

[35] Most prominently in the UCPD, see arts. 5–9 and Recital 18 UCPD. See, however, also the case law with regard to the UCTD, where the benchmark of the average consumer is invoked to determine the transparency of contract terms, for example, Case C-348/14 *Bucura*, para. 66; Case C-26/13 *Kásler and Káslerné Rábai*, para. 73–74.

[36] Recital 18 UCPD and see Case C-210/96 *Gut Springenheide and Tusky* [1998] ECR I-4657, para 3.

[37] Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market ("Guidance UCPD"), C/2021/9320, point 2.5.

[38] See, for example, Jason Cohen, "Bringing down the average: The case for a less sophisticated reasonableness standard in US and EU consumer law" (2019) *Loyola Consumer Law Review*, 32:1, p. 2; Rossella Incardona, Cristina Poncibò, "The average consumer, the unfair commercial practices directive, and the cognitive revolution" (2007) *Journal of Consumer Policy*, 30: 36.

[39] See, for criticism on this point, among others. Martijn Hesselink, "EU private law injustices" (2022) *Yearbook of European Law*, 1: 22–23.

[40] Art. 5(3) UCPD. The concrete application of these benchmarks is discussed in more detail below (Section 5 Dark patterns).

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

situational concept[41] and that the characteristics mentioned in the directive are indicative and non-exhaustive.[42] The literature has however rightly argued that a reinterpretation of the concept of vulnerability will not be sufficient to better protect consumers in a digital context. It is submitted that in digital marketplaces, most, if not all consumers are potentially vulnerable; digitally vulnerable and susceptible "*to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer-seller relations and the very architecture of digital marketplaces*."[43] AI and digitalization thus create a structural vulnerability that requires a further reaching intervention than just to reinterpret vulnerability.[44] More attention to tackling the sources of digital vulnerability and to the architecture of digital marketplaces is hence definitely necessary.[45]

10.3.3 *Challenges to the Silo Approach to Consumer Law*

Consumer law has developed in parallel with competition law and data protection law but, certainly in digital markets, it is artificial – also in terms of enforcement – to strictly separate these areas of the law.[46] The use of AI often involves the use of (personal) consumer data and concentration in digital markets creates a risk of abuses of personal data also to the detriment of consumers. Indeed, there are numerous and frequent instances where the same conduct will be covered simultaneously by consumer law, competition law, and data protection law.[47] The German Facebook case of the Bundesgerichtshof[48] is just one example where competition law (abuse of dominant position) was successfully invoked also to guarantee consumer's choice in the data they want to share and in the level of personalization of the services provided.[49] There is certainly a need for more convergence and a

[41] So a consumer can be vulnerable in one situation but not in another, see Guidance UCPD, points 2.6 and 4.2.7.

[42] Guidance UCPD, points 2.6 and 4.2.7.

[43] Natali Helberger, Orla Lynskey, H.-W. Micklitz, Peter Rott, Marijn Sax, and Joanna Strycharz, "EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets," (March 2021), www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf, p. 5.

[44] For recommendations on further reaching interventions, among others in the form of additional prohibited practices; reversal of the burden of proof for the fairness of data exploitation strategies and the concretization of legal benchmarks, see Helberger et al., "Structural asymmetries" 79.

[45] See in the same sense Helberger et al., "Structural asymmetries."

[46] For a plea to move away from a silo approach, see Christof Koolen, "Consumer protection in the age of artificial intelligence: Breaking down the silo mentality between consumer, competition and data," to be published in ERPL 2023; similarly: Wolfgang Kerber, "Digital markets, data, and privacy: Competition law, consumer law and data protection" (2016) *Journal of Intellectual Property Law & Practice*, 865–866.

[47] Opinion of Advocate General AG J. Richard de la Tour, Case C-319/20 *Meta Platforms Ireland*, para. 81.

[48] Decision of BGH of 23 June 2020, KVR 69/19.

[49] The case involved the use of data collected on and off Facebook to provide Facebook consumers with personalized services. It was held that consumers had no choice to refuse such personalized

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

complementary application of these legal domains, rather than artificially dividing them, especially when it comes to enforcement. The case law allowing consumer protection organizations to bring representative actions on the basis of consumer law (namely unfair practices or unfair contract terms), also for infringements of data protection legislation, is therefore certainly to be welcomed.[50]

10.4 OVERVIEW OF RELEVANT CONSUMER PROTECTION INSTRUMENTS

The mentioned challenges of course do not imply that AI currently operates in a legal vacuum and that there is no protection in place. The existing consumer law instruments provide some safeguards, both when AI is used in advertising or in a precontractual stage, and when it is the actual subject matter of a consumer contract (e.g., as part of a smart product). The current instruments are however not well adapted to AI, as will be illustrated by the brief overview of the most relevant instruments below.[51] An exercise is ongoing to potentially adapt several of these instruments[52] and make them fit for the digital age.[53] In addition, several new acts were adopted or proposed in the digital sphere that also have an impact on consumer protection and AI.

10.4.1 *The Unfair Commercial Practices Directive*

The UCPD is a maximum harmonization instrument that regulates unfair commercial practices occurring before, during and after a B2C transaction. It has a broad scope of application and the combination of open norms and a blacklist of practices that are prohibited in all circumstances allows it to tackle a wide range of unfair business practices, also when these practices result from the use of AI.[54] Practices are unfair, according to the general norm, if they are contrary to the requirements

services and the collection of off-Facebook data as this was only possible by completely giving up access to Facebook services. See for a more detailed analysis, Marco Loos and Joasia Luzak, Study of the European Parliament. Update the unfair contract terms directive for digital services (2021), www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf, 31–32.

[50] Case C-319/20 *Meta Platforms Ireland*.

[51] Extra-contractual liability is not covered in this contribution, and we refer to the contribution of Jan De Bruyne and Wannes Ooms in Chapter 8 of this book.

[52] Concretely: The Unfair Commercial Practices Directive 2005/29/EC ("UCPD"); the Consumer Rights Directive 2011/83/EU; the Unfair Contract Terms Directive 93/13/EEC ("UCTD").

[53] European Commission, "Digital fairness – fitness check of EU consumer law," https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en.

[54] Giovanni Sartor, IMCO committee study, "New aspects and challenges in consumer protection: Digital services and artificial intelligence," 2020, pp. 36–37; Guidance UCPD, point 4.2.7.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

of "professional diligence and are likely to materially distort the economic behaviour of the average consumer."[55] The UCPD furthermore prohibits misleading and aggressive practices. Misleading practices are actions or omissions that deceive or are likely to deceive and cause the average consumer to make a transactional decision they would not have taken otherwise.[56] Aggressive practices are practices that entail the use of coercion or undue influence which significantly impairs the average consumer's freedom of choice and causes them to make a transactional decision they would not have taken otherwise.[57]

The open norms definitely offer some potential to combat the use of AI to manipulate consumers, either using the general norm or the prohibition of misleading or aggressive practices.[58] However, the exact application and interpretation of these open norms makes the outcome of such cases uncertain.[59] When exactly does the use of AI amount to "undue influence," how is the concept of the "average consumer" to be used in a digital context; when exactly does personalized advertising become misleading. We make these problems more concrete in our analysis of dark patterns below (Section 10.5). More guidance on the application of these open norms could make the application to AI-based practices easier.[60] Additional blacklisted practices could also provide more legal certainty.

10.4.2 *Consumer Rights Directive*

The CRD – also a maximum harmonization directive[61] – regulates the information traders must provide to consumers when contracting, both for on premises contracts and for distance and doorstep contracts. In addition, it regulates the right of withdrawal from the contract. The precontractual information requirements are extensive and they include an obligation to provide information about the main characteristics and total price of goods or services; about the functionality and interoperability of digital content and digital services, and the duration and conditions for termination of the contract.[62] However, as Ebers mentions, these obligations are

[55] Art. 5 (2) UCPD. See for the (limited) possibilities to take the vulnerable consumer as a benchmark, above point 10.3.3 and below point 10.5.2.

[56] Arts. 6–7 UCPD.

[57] Art. 8 UCPD.

[58] See, for example, the analysis of Johann Laux, Brent Mittelstadt, and Sandra Wachter, "Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice" (2021) *Common Market Law Review*, 58.

[59] See also the conclusion of the European Commission, DG for Justice and Consumers, Francisco Lupiáñez-Villanueva, Alba Boluda, Francesco Bogliacino et al., "Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation: final report," Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2838/859030.

[60] Sartor, "Digital services and artificial intelligence," 2020, 36–37.

[61] With limited exceptions, inter alia, with regard to information obligations for on premises contracts, see art. 5 CRD.

[62] See arts. 5 and 6 CRD, as amended by the Modernization Directive.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

formulated quite generally, making it difficult to concretize their application to AI systems.[63] The Modernization directive[64] – adopted to "modernize" a number of EU consumer protection directives in view of the development of digital tools[65] – introduced a new information obligation for personal pricing.[66] Art. 6 (1) (ea) of the modernized CRD now requires the consumer to be informed that the price was personalized on the basis of automated decision-making. There is however no obligation to reveal the algorithm used nor its methodology; neither is there an obligation to reveal how the price was adjusted for a particular consumer.[67] This additional information obligation has therefore been criticized for being too narrow as it hinders the finding of price discrimination.[68]

10.4.3 *Unfair Contract Terms Directive*

The UCTD in essence requires contract terms to be drafted in plain, intelligible language and the terms must not cause a significant imbalance in the parties' rights and obligations, to the detriment of the consumer[69] Contract terms that do not comply with these requirements can be declared unfair and therefore nonbinding.[70] The directive has a very broad scope of application and applies to (not individually negotiated) clauses in contracts between sellers/suppliers and consumers "in all sectors of economic activity."[71] It does not require that the consumer provides monetary consideration for a good or service. Contracts whereby the consumer "pays" with personal data or whereby the consideration provided consists in consumer generated content and profiling are also covered.[72] It is furthermore a minimum harmonization directive, so stricter national rules can still apply.[73]

The UCTD can help consumers to combat unfair clauses (e.g., exoneration clauses, terms on conflict resolution, terms on personalization of the service,

[63] Ebers, "Liability for AI & consumer law," 210.
[64] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019.
[65] Recital 17 Modernization directive.
[66] The directive had to be implemented by November 28, 2021. The implementing provisions had to be applied from May 28, 2022 (art. 7 Modernization directive).
[67] Loos and Luzak, "Unfair contract terms for digital services," 30.
[68] Ibid., see also critical Agustin Reyna, "The price is (not) right: The perils of personalisation in the digital economy," *InformaConnect*, January 4, 2019, https://informaconnect.com/the-price-is-not-right-the-perils-of-personalisation-in-the-digital-economy/.
[69] Art. 3 (1) UCTD.
[70] Art. 6 UCTD.
[71] Cases C-74/15 *Dumitru Tarcău* and C-534/15 *Dumitraş*.
[72] Commission notice – Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts, *OJ* C 323, 27.9.2019, pp. 4–92, point 1.2.1.2.
[73] Art. 8 UCTD.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

terms contradicting the GDPR)[74] in contracts with businesses that use AI. It could also be used to combat untransparent personalized pricing whereby AI is used. In principle, the UCTD does not allow for judges to control the unfairness of core contract terms (clauses that determine the main subject matter of the contract), nor does it allow to check the adequacy of price and remuneration.[75] This is however only the case if these clauses are transparent.[76] The UCTD could furthermore also be invoked if AI has been used to personalize contract terms without disclosure to the consumer.[77] Unfair terms do not bind the consumer and may even lead to the whole contract being void if the contract cannot continue to exist without the unfair term.[78]

10.4.4 *Consumer Sales Directive and Digital Content and Services Directive*

When AI is the subject matter of the contract, the new Consumer Sales Directive 2019/771 ("CSD") and Digital Content and Services Directive 2019/770 ("DCSD"), provide the consumer with remedies in case the AI application fails. The CSD will apply when the digital element – provided under the sales contract – is thus incorporated or connected with the good that the absence of the digital element would prevent the good from performing its function.[79] If this is not the case, the DCSD will apply. Both directives provide for a similar – but not identical – regime that determines the requirements for conformity and the remedies in case of nonconformity. These remedies include specific performance (repair or replacement in case of a good with digital elements), price reduction and termination. Damages caused by a defect in an AI application continue to be governed by national law. The directives also provide for an update obligation (including security updates) for the seller of goods with digital elements and for the trader providing digital content or services.[80]

[74] For a detailed analysis on the possibilities and shortcomings of the UCTD in a digital context, see: Loos and Luzak, "Unfair contract terms for digital services."

[75] Art. 4 (2) UCTD.

[76] Art. 4(2) UCTD.

[77] See Loos and Luzak, "Unfair contract terms for digital services," 31. The authors propose to introduce a presumption of unfairness, implying that that personalized prices and terms are discriminatory and therefore unfair.

[78] Art. 6(1) UCTD.

[79] Art. 2(5) and art. 3(3) CSD.

[80] For a detailed analysis, see Piia Kalamees, "Goods with digital elements and the seller's updating obligation" (2021) *JIPITEC*, 12: 131; Hugh Beale, "Digital content directive and rules for contracts on continuous supply" (2021) *JIPITEC*, 12: 96.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

10.4.5 *Digital Markets Act and Digital Services Act*

The Digital Markets Act ("DMA"), which applies as of May 2, 2023[81] aims to maintain an open and fair online environment for businesses users and end users by regulating the behavior of large online platforms, known as "gatekeepers," which have significant influence in the digital market and act as intermediaries between businesses and customers.[82] Examples of such gatekeepers are Google, Meta, and Amazon. The regulation has only an indirect impact on the use of AI, as it aims to prevent these gatekeepers from engaging in unfair practices, which give them significant power and control over access to content and services.[83] Such practices may involve the use of biased or discriminatory AI algorithms. The regulation imposes obligations on gatekeepers such as providing the ability for users to uninstall default software applications on the operating system of the gatekeeper,[84] a ban on self-preferencing,[85] and the obligation to provide data on advertising performance and ad pricing.[86] The DMA certainly provides for additional consumer protection, but it does so indirectly, by mainly regulating the relationship between platforms and business users and by creating more transparency. Consumer rights are not central in the DMA and this is also apparent from the lack of involvement of consumers and consumer organizations in the DMA's enforcement.[87]

The Digital Services Act ("DSA"),[88] which applies as of February 17, 2024,[89] establishes a harmonized set of rules on the provision on online intermediary services and aims to ensure a safe, predictable, and trustworthy online environment.[90] The regulation mainly affects online intermediaries (including online platforms), such as online marketplaces, online social networks, online travel and accommodation platforms, content-sharing platforms, and app stores.[91] It introduces additional transparency obligations, including advertising

[81] Art. 54 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. Note that article e 3(6) and (7) and Articles 40, 46, 47, 48, 49, and 50 shall apply from November 1, 2022 and article 42 and Article 43 shall apply from June 25, 2023.

[82] Recitals 2, 4, and 34 DMA.

[83] Recitals 6 and 15 DMA.

[84] Art. 6 (3) DMA.

[85] Art. 6(5) DMA.

[86] Art. 5 (9) and art. 6(8) DMA.

[87] Rupprecht Podszun, 'The Digital Markets Act: What's in It for Consumers?', *EuCML* 2022, 3–5.

[88] 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.

[89] Article 93 DSA. However, Article 24(2), (3), and (6), Article 33(3) to (6), Article 37(7), Article 40(13), Article 43 and Sections 4, 5, and 6 of Chapter IV shall apply from November 16, 2022.

[90] Art. 1 DSA.

[91] European Commission, "The Digital Services Act package" (November 24, 2022), https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package, accessed on December 24, 2022.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

transparency requirements for online platforms[92] and a ban on targeted advertisement of minors based on profiling[93] as well as a ban on targeted advertising based on profiling using special categories of personal data, such as religious belief or sexual orientation.[94] It also introduces recommender system transparency for providers of online platforms.[95] The regulation furthermore obliges very large online platforms to carry out a risk assessment of their services and systems, including their algorithmic systems.[96]

10.4.6 *Artificial Intelligence Act*

The Artificial Intelligence Act ("AI Act") Act, adopted June 13, 2024, provides harmonized rules for "the placing on the market, the putting into service and the use of AI systems in the Union."[97] It uses a risk-based methodology to classify certain uses of AI systems as entailing a low, high, or unacceptable risk.[98] AI practices that pose an unacceptable risk are prohibited, including subliminal techniques that distort behavior and cause significant harm.[99] The regulation foresees penalties for noncompliance[100] and establishes a cooperation mechanism at European level (the so-called European Artificial Intelligence Board), composed of representatives from the Member States and the Commission, to ensure enforcement of the provisions of the AI Act across Europe.[101] Concerns have been expressed whether the AI Act is adequate to also tackle consumer protection concerns. It has been argued that the list of "high-risk" applications and the list of forbidden AI practices does not cover all problematic AI applications or practices for consumers.[102] Furthermore, the sole focus on public enforcement and the lack of appropriate individual rights

[92] Art. 26 DSA; see also art. 39 DSA for additional transparency obligations for very large online platforms.
[93] Art. 28(2) DSA.
[94] Art. 26(3).
[95] Art. 3(s) and art. 27 DSA.
[96] Art. 34 DSA. For a discussion of this risk assessment requirement, see also Chapter 14 of this book on AI and Media by Lidia Dutkiewicz, Noémie Krack, Aleksandra Kuczerawy, and Peggy Valcke.
[97] Art 1(a) "Regulation (EU) 2024/1689 of the European Parliament and the council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations" (Artificial Intelligence Act) ("AI Act").
[98] Explanatory memorandum, AI Act Proposal COM (2021) 206 final, 12; Recital 26 AI Act.
[99] Art. 5(1) (a) AI Act.
[100] Art. 99 AI Act.
[101] Art. 65 AI Act.
[102] See BEUC, Position Paper on the AI Act. Regulating AI to protect the consumer, www.beuc.eu/sites/default/files/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf. See in this regard also Nathalie A. Smuha, Emma Ahmed-Rengers, Adam Harkens, Wenlong Li, James MacLaren, Riccardo Piselli, and Karen Yeung, "How the EU can achieve legally trustworthy AI: A response to the European Commission's proposal for an Artificial Intelligence Act," http://dx.doi.org/10.2139/ssrn.3899991.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

for consumers and collective rights for consumers organization to ensure an effective enforcement has been criticized.[103]

10.5 DARK PATTERNS AS A CASE STUDY

10.5.1 *The Concept of Dark Patterns*

The OECD Committee on Consumer Policy uses the following working definition of dark patterns:

> business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They often deceive, coerce or manipulate consumers and are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances.[104]

A universally accepted definition is lacking, but dark patterns can be described by their common features involving the use of hidden, subtle, and often manipulative designs or marketing tactics that exploit consumer biases, vulnerabilities, and preferences to benefit the business or provider of intermediary services that presents the information that may not align with the consumer's own preferences or best interest.[105] Examples of such marketing practices include (i) *false hierarchy* (the button for the business' desired outcome is more prominent or visually appealing than the others),[106] (ii) *hidden information*,[107] (iii) creating a sense of *false urgency*,[108] (iv) *forced continuity* or *roach motel* (making it significantly more difficult for consumers to cancel their subscription than it was to sign up or automatically renew the service without the user's express consent and repeatedly asking consumers to reconsider their choice).[109] All of these illustrations are practices closely related to the

[103] Natali Helberger, Hans-W. Micklitz, and Peter Rott, *The Regulatory Gap: Consumer Protection in the Digital Economy*, 2021, p. 36, www.beuc.eu/sites/default/files/publications/beuc-x-2021-116_the_regulatory_gap-consumer_protection_in_the_digital_economy.pdf.

[104] OECD, "Dark commercial patterns, OECD digital economy papers" (2022) No. 336, *OECD Publishing*, 8.

[105] Guidance UCPD 101; European Commission, Directorate-General for Justice and Consumers, Francesco Bogliacino, Alba Boluda, Francisco Lupiáñez-Villanueva et al., "Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization: final report" (2022) *Publications Office of the European Union*, https://data.europa.eu/doi/10.2838/859030, 6; Jamie Luguri and Lior Strahilevitz, "Shining a light on dark patterns" (2021) *Journal of Legal Analysis*, 44.

[106] Luguri and Strahilevitz, "Dark patterns" 55 and 58; Lupiáñez-Villanueva et al., "Behavioural study" 64.

[107] Luguri and Strahilevitz, "Dark patterns" 47; Lupiáñez-Villanueva et al., "Behavioural study" 105.

[108] For example, by claiming that a product or service is only available for a limited time, or communicating that the offer will pass to pressure the consumer to make a purchase, Guidance UCPD, 101; Luguri, "Dark patterns" 53 and 100.

[109] Luguri and Strahilevitz, "Dark patterns" 53, 55, and 58.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

concept of choice architecture and hyper personalization discussed in Section 10.2 presenting choices in a non-neutral way.

Dark patterns may involve the use of personal data of consumers and the use of AI.[110] AI is an asset for modifying dark patterns to have a greater impact on consumers behavior in a subtle way. It allows business operators to examine which dark patterns work best, especially when personal data is involved, and dark patterns are adapted accordingly. Examples of the power of the combination of dark patterns and AI can be found in platforms encouraging consumers to become paying members by presenting this option in different ways and over different time periods.[111] Machine learning applications can analyze personal data to optimize dark patterns and find more innovative ways to convince consumers to buy a subscription. They can examine how many hours are spent a day watching videos, how many advertisements are being skipped and whether the app is closed when an ad is shown.[112] The ad play may be increased if the consumer refuses to become a paying member.[113] Such a process can be stretched over quite a long time, making the consumer believe it is its own decision to subscribe, without him feeling tricked.[114] In essence, the combination of AI, personal data and dark patterns, results in an increased ability to manipulate consumers.

10.5.2 *Overview of the Relevant Instruments of Consumer Protection against Dark Patterns*

The UCPD is a first instrument that offers a number of possible avenues to combat dark patterns. As mentioned, it covers a wide range of prohibited practices in a business to consumer context.[115] First, the general prohibition of unfair commercial practices of art. 5 UCPD that functions as a residual control mechanism can be invoked. It prohibits all practices that violate a trader's professional diligence obligation and that cause the average consumer to make a transactional decision that they would not otherwise have made.[116] This includes not only the decision to purchase or not purchase a product but also related decisions, such as visiting a website, or viewing content.[117] As mentioned, the standard of the "average" consumer (of the

[110] OECD, "Dark commercial patterns" 9.

[111] See, for example, referring to YouTube: Zakary Kinnaird, "Dark patterns powered by machine learning: An intelligent combination" (October 13, 2020) https://uxdesign.cc/dark-patterns-powered-by-machine-learning-an-intelligent-combination-f2804ed028ce, accessed February 3, 2023.

[112] Ibid.

[113] Ibid.

[114] Ibid.

[115] Article 2(d) UCPD refers to "any act, omission, course of conduct or representation, commercial communication including marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers."

[116] Art. 5 UCPD, Guidance UCPD 46.

[117] Guidance UCPD 31.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

target group) is a normative standard that has (so far) been applied rather strictly, as rational behavior is the point of departure in the assessment.[118] The fact that the benchmark can be modulated to the target group does however offer some possibilities for a less strict standard in case of personalization, as the practice could then even be assessed from the perspective of a single targeted person.[119]

Article 5(3) UCPD, furthermore creates some possibilities to assess a practice from the perspective of a vulnerable consumer, but the narrow definition of vulnerability as mental or psychical disability, age or credulity is – as mentioned – not suitable for the digital age. Indeed, any consumer can be temporarily vulnerable due to contextual and psychological factors.[120] According to the European Commission, the UCPD provides a non-exhaustive list of characteristics that make a consumer "particularly susceptible" and therefore states that the concept of vulnerability should include these context-dependent vulnerabilities, such as interests, preferences, psychological profile, and even mood.[121] It will indeed be important to adopt such a broader interpretation to take into account the fact that all consumers can be potentially vulnerable in a digital context. The open norms of the UCPD might indeed be sufficiently flexible for such an interpretation,[122] but a clearer text in the directive – and not only (nonbinding) guidance of the Commission guidance – would be useful.

The more specific open norms prohibiting misleading and especially aggressive practices (arts. 6–9 UCPD) can also be invoked. But it is again uncertain how open concepts such as "*undue influence*" (art. 8 UCPD) must be interpreted in an AI context and to what extent the benchmark of the average consumer can be individualized. At what point does an increased exposure to advertising, tailored on past behavior, in order to convince a consumer to "choose" a paid subscription, amount to undue influence? More guidance on the interpretation of these open norms would be welcome.[123]

The blacklist in Annex I of the UCPD avoids the whole discussion on the interpretation of these benchmarks. That list prohibits specific practices that are considered unfair in all circumstances[124] and does not require an analysis of the potential effect on the average (or – exceptionally – vulnerable) consumer. The practices also do not require proof that the trader breached his professional diligence duty.[125] The list prohibits several online practices, including *disguised ads*,[126]

[118] See above, Section 3.3.
[119] See in any event in this sense, Guidance UCPD, point 4.2.7.
[120] Lupiáñez-Villanueva et al., "Behavioural study" 72.
[121] Guidance UCPD, points 2.6, 35.
[122] Lupiáñez-Villanueva et al., "Behavioural study" 72.
[123] Sartor, Digital services and artificial intelligence, 36–37.
[124] Annex 1 UCPD, currently 35 practices are listed.
[125] Case C-435/11 *CHS Tour Services GmbH* v *Team4 Travel GmbH* [2013] ECR I-00057, §45.
[126] Practice 11 Annex I UCPD.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

false urgency (e.g., fake countdown timers),[127] *bait and switch*,[128] and *direct exhortations to children*.[129] However, these practices were not specifically formulated to be applied in an AI context and interpretational problems therefore also occur when applying the current list to dark patterns. Thus, it is for instance mentioned in the Commission guidance that "making repeated intrusions during normal interactions in order to get the consumer to do or accept something (i.e., nagging) *could* amount to a persistent and unwanted solicitation."[130] The same interpretational problem then rises: how much intrusion and pressure is exactly needed to make a practice a "persistent and unwanted solicitation"? Additional blacklisted (AI) practices would increase legal certainty and facilitate enforcement.

Finally, the recently added Article 7(4a) UCPD requires traders to provide consumers with general information about the main parameters that determine the ranking of search results and their relative importance. The effectiveness of this article in protecting consumers by informing them can be questioned, as transparency about the practices generated by an AI system collides with the black box problem. Sharing information about the input-*phase*, such as the data set and learning algorithm that were used, may to some extent mitigate the information asymmetry but it will not suffice as a means of protection.

While the UCPD has broad coverage for most types of unfair commercial practices, the case-by-case approach does not allow to effectively address all forms of deceptive techniques known as "dark patterns." For example, BEUC's report of 2022 highlights the lack of consumer protection for practices that use language and emotion to influence consumers to make choices or take specific actions, often through tactics such as shaming, also referred to as *confirmshaming*.[131] In addition, there is uncertainty about the responsibilities of traders under the professional diligence duty and whether certain practices are explicitly prohibited.[132] Insufficient enforcement by both public and private parties further weakens this instrument.[133]

A second piece of legislation that provides some protection against dark patterns is the DSA. The regulation refers to dark patterns as practices "that materially distort or impair, either purposefully or in effect, the ability of recipients of the service

[127] Practice 7 Annex I UCPD, Commission guidance, point 4.2.7.
[128] Practice 5 (bait) and 6 (bait and switch) Annex I UCPD. The provisions in essence prohibit making offers when the trader knows that he will probably not be able to meet the demand (bait advertising) or making offers at a specified price and then refusing to deliver the product (on time) with the intention of promoting a different product (bait and switch).
[129] Practice 28 Annex I UCPD.
[130] Practice 26 Annex I UCPD. Commission guidance, point 4.2.7.
[131] BEUC, "Dark Patterns and the EU consumer law acquis: Recommendations forbetter enforcement and reform" (February 7, 2022), www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf, accessed December 23, 2022, 9; Lupiáñez-Villanueva et al., "Behavioural study" 66.
[132] Lupiáñez-Villanueva et al., "Behavioural study" 122.
[133] Ibid., 122.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

to make autonomous and informed choices or decisions."[134] The DSA prohibits online platforms from designing, organizing, or operating their interfaces in a way that "deceives, manipulates, or otherwise materially distorts or impacts the ability of recipients of their services to make free and informed decisions"[135] in so far as those practices are not covered under the UCPD and GDPR.[136] Note that the important exception largely erodes consumer protection. Where the UCPD applies, and that includes all B2C practices, the vague standards of the UCPD will apply and not the more specific prohibition of dark patterns in the DSA. A cumulative application would have been preferable. The DSA inter alia targets exploitative design choices and practices as "forced continuity," that make it unreasonably difficult to discontinue purchases or to sign out from services.[137]

The AI Act contains two specific prohibitions on manipulation practices carried out through the use of AI systems that may cover dark patterns.[138] These bans prohibit the use of subliminal techniques to materially distort a person's behavior in a manner that causes or is likely to cause significant harm and the exploitation of vulnerabilities in specific groups of people to materially distort their behavior in a manner that causes or is likely to cause significant harm.[139] These prohibitions are similar to those in the UCPD, except that they are limited to practices carried out through the use of AI systems.[140] They furthermore have some limitations. The ban relating to the abuse of vulnerabilities only applies to certain explicitly listed vulnerabilities, such as age, disability or specific social or economic situation, yet the mentioned problem of digital vulnerability is not tackled. A further major limitation was fortunately omitted in the final text of the AI Act. Whereas in the text of the AI proposal, these provisions only applied in case of physical and mental harm – which will often not be present and may be difficult to prove[141] – the prohibitions of the final AI Act also apply to (significant) economic harm.

The AI Act is complementary to other existing regulations, including data protection, consumer protection, and digital service legislation.[142] Finally, taking into account the fact that this Regulation strongly focuses on high-risk AI and that there are not many private services that qualify as high risk, the additional protection for consumers from this regulation seems limited.

[134] Recital 67 DSA: "Practices that materially distort or impair, either purposefully or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions."
[135] Art. 25(1) DSA.
[136] Recital 67 DSA.
[137] Recital 67 DSA.
[138] Art. 5 AI Act.
[139] Art 5 (a) and (b) AI Act.
[140] Lupiáñez-Villanueva et al., "Behavioural study" 83; Catalina Goanta, "Regulatory Siblings: The Unfair Commercial Practices Directive Roots of the AI ACT," in I. Graef & B. van der Sloot (ed.). *The Legal Consistency of Technology Regulation in Europe* (pp. 71–88). Oxford: Hart Publishing, 2024.
[141] See in this regard Rostam Josef Neuwirth, *The EU Artificial Intelligence Act Regulating Subliminal AI Systems* (Routledge, 2023).
[142] Recital 9 AI Act.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press

The Consumer Rights Directive with its transparency requirement for pre-contractual information[143] and its prohibition to use *pre-ticked boxes* implying additional payments might also provide some help.[144] However, the prohibition on pre-ticked boxes does not apply to certain sectors that are excluded from the directive, such as financial services.[145] The UCPD could however also be invoked to combat charging for additional services through default interface settings and that directive does apply to the financial sector.[146] The CRD does not regulate the conditions for contract termination, except for the right of withdrawal. An obligation for traders to insert a "withdrawal function" or "cancellation button" in contracts concluded by means of an online interface has recently been added to the CRD.[147] This function is meant to make it easier for consumers to terminate distance contracts, particularly subscriptions during the period of withdrawal. This has could be a useful tool to combat subscription traps.

10.6 CONCLUSION

AI poses major challenges to consumers and to consumer law and the traditional consumer law instruments are not well adapted to tackle these challenges. The mere provision of information on how AI operates will definitely not suffice to adequately protect consumers. The current instruments do allow to tackle some of the most blatant detrimental practices, but the application of the open norms in a digital context creates uncertainty and hinders effective enforcement, as our case study of dark patterns has shown. The use of AI in a business context creates a structural vulnerability for all consumers. This requires additional regulation to provide better protection, as well as additional efforts in raising awareness of the risks AI entails.

[143] Information provided to consumers before the conclusion of a contract in distance contracts must be presented in a clear and understandable manner, pursuant to Art. 8 (1) CRD; see also BEUC, "Dark Patterns," 9.

[144] Art. 33 CRD.

[145] Art. 3(3) (d) CRD.

[146] Guidance UCPD, point 4.2.7.

[147] The CRD was amended by Directive (EU) 2023/2673 of 22 November 2023 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC, OJ L, 2023/2673, 28.11.2023. This new article 11a must be transposed by 19 December 2025 and applied from 19 June 2026.

https://doi.org/10.1017/9781009367783.013 Published online by Cambridge University Press