European Review of Private Law 2 & 3-2023 [427–468]

Consumer Protection in the Age of Artificial Intelligence: Breaking Down the Silo Mentality Between Consumer, Competition, and Data*

Christof KOOLEN**

Abstract: Consumer protection calls for a broader conceptualization. Narrow views, where consumers are reduced to their economic interests, are no longer sustainable. Instead, they should be seen as consumer-citizens whose consumption choices have profound implications on society as a whole. In the face of artificial intelligence (AI)-driven practices, the pursuit of a more holistic level of consumer protection therefore requires a combined approach; a defence in depth that hinges on reciprocal interactions between consumer law, competition law, and data protection law. The complementarity between each branch ensures that different aspects of consumer welfare – consumer autonomy, consumer choice, and the right to data protection – are adequately safeguarded. Doing so ensures that consumer protection is not only about empowering consumers, but also about building safer digital spaces and creating a level playing field for entrepreneurs where innovation can thrive.

Résumé: La protection des consommateurs nécessite une conceptualisation plus large. Une vue étroite, où la protection des consommateurs est réduite à la sauvegarde de leurs intérêts économiques, n'est plus viable. Ils devraient plutôt être considérés comme des consommateurs-citoyens dont les choix de consommation ont des implications profondes pour la société dans son ensemble. Face à l'intelligence artificielle également, la protection des consommateurs exige donc une approche holistique et combinée; une défense cohérente et efficace qui repose sur des interactions étroites et profondes entre le droit de la consommation, le droit de la concurrence, et le droit de la protection des données. La complémentarité entre ces derniers garantit que les différents aspects du bien-être des consommateurs – l'autonomie du consommateur, le choix du consommateur, et le droit à la protection des données – sont adéquatement protégés. Ainsi, la protection des consommateurs ne consiste pas seulement à donner du pouvoir aux consommateurs, mais aussi à construire des espaces numériques plus sûrs et à créer des conditions de concurrence équitables pour les entreprises, où l'innovation peut prospérer.

* Acknowledgements: This work was supported by a grant of the Research Foundation Flanders (FWO) [grant number 11G0920N]. The author is grateful to Prof. Dr. Evelyne Terryn for providing valuable input on the draft version of this paper. Special thanks also go to Prof. Dr. Mathias Verbeke for offering suggestions for improvement regarding the technical aspects of AI systems.

** Author information: Christof Koolen works as a Ph.D. Researcher at the Institute for Consumer, Competition & Market (KU Leuven, Belgium). He holds a Master of Laws from the KU Leuven and a Magister Juris degree from the University of Oxford. He conducts research on the legal implications of smart devices within the EU internal market. Email: christof.koolen@kuleuven.be.

Zusammenfassung: Der Verbraucherschutz erfordert eine breitere Konzeptualisierung. Enge Sichtweisen, bei denen die Verbraucher auf ihre wirtschaftlichen Interessen reduziert werden, sind nicht mehr haltbar. Stattdessen sollten sie als Verbraucher-Bürger betrachtet werden, deren Konsumentscheidungen tiefgreifende Auswirkungen auf die Gesellschaft als Ganzes haben. Angesichts der KI-gesteuerten Praktiken erfordert das Streben nach einem ganzheitlicheren Verbraucherschutz daher einen kombinierten Ansatz, einen umfassenden Schutz, der auf den Wechselwirkungen zwischen Verbraucherrecht, Wettbewerbsrecht, und Datenschutzrecht beruht. Die Komplementarität zwischen den einzelnen Rechtsgebieten stellt sicher, dass die verschiedenen Aspekte des Verbraucherwohls – Autonomie des Verbrauchers, Auswahl des Verbrauchers, und das Recht auf Datenschutz – angemessen geschützt werden. Auf diese Weise wird sichergestellt, dass es beim Verbraucherschutz nicht nur um die Stärkung der Verbraucher geht, sondern auch um den Aufbau sicherer digitaler Umgebungen und die Schaffung gleicher Wettbewerbsbedingungen für Unternehmer, in denen Innovationen gedeihen können.

1. Introduction

1. The use of artificial intelligence (AI) in a commercial setting is no longer a matter of science fiction. Continued technological advances in this area of information technology have drastically altered how interactions between consumers and businesses take place.[1] While difficult to ascribe a fixed definition to AI, it is typically perceived as machinery that is capable of mimicking human intelligence by demonstrating skills such as reasoning, learning, and creativity.[2] A considerable body of scholarship addresses how AI influences consumers' decision-making processes. In this respect, several noteworthy topics such as product recommender systems,[3] personalized shopping experiences,[4] and digital market manipulation[5] have seen coverage in literature. If anything, these contributions highlight that the market presence of AI has fundamentally altered how consumers' decision-making processes unfold in digitized environments. From that

1 L. Bjørlo, Ø. Moen & M. Pasquine, 'The Role of Consumer Autonomy in Developing Sustainable AI: A Conceptual Framework', *Sustainability* 2021, vol. 13, p 2332, doi: 10.3390/su13042332.

2 R. Devillé, N. Sergeyssels & C. Middag, 'Basic Concepts of AI for Legal Scholars', in J. De Bruyne & C. Vanleenhove (eds), *Artificial Intelligence and the Law* (Antwerpen: Intersentia 2021), p 2.

3 See for instance, C. Busch, 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law', *The University of Chicago Law Review* 2019, vol. 86, p 324.

4 See for instance, D. Clifford, *The legal limits to the monetisation of online emotions* (Leuven: KU Leuven 2019), pp 46–48, https://lirias.kuleuven.be/retrieve/540729.

5 See for instance, A. Mathur et al., 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites', *Proceedings of the ACM on Human-Computer Interaction* 2019, pp 5–6, doi: 10.1145/3359183; K. Manwaring, 'Emerging information technologies: challenges for consumers', *Oxford University Commonwealth Law Journal* 2017, vol. 17, pp 277–279, doi: 10.1080/14729342.2017.1357357.

perspective, the question arises where to strike the balance between consumer protection and technology-enabled innovation.

2. The emergence of AI raises questions which are not only technical, but also legal in nature.[6] One area of research concerns the implications of AI for consumers and consumer law. The rationale underpinning consumer law is clear: consumers generally find themselves in a disadvantaged position when interacting with businesses and should thus benefit from enhanced protection when committing to business-to-consumer (b2c) contracts. Accordingly, rules on consumer protection are put in place to remedy imbalances, which are the result of power asymmetries between businesses and consumers. Logically, these rules should also find application to situations where b2c interactions are influenced by AI.

3. The interplay between AI and consumer protection is a timely topic, with many discussions playing out within the framework of a digital transformation in Europe. Driven by a shift from analogue to digital, the functionality and performance of AI hinges to a large extent on interconnectivity and data aggregation.[7] Trends in the consumer goods and services industry – such as the growing platform economy and the steady uptake of smart devices – cater exactly to these needs and provide the bedrock for new, AI-driven business models. Accordingly, there is a conversion taking place from a digitized society to an increasingly algorithmic society; a society where AI is able to strongly influence the dynamics of consumer markets.

4. In our capacity as EU consumers,[8] we are all likely to be confronted with AI systems at some point in our lives, be it via price setting algorithms, product recommendation engines, or personalized advertising. In these cases, AI has the potential to offer tangible benefits to consumers (for instance, in the form of reduced search costs), but also to reinforce existing power asymmetries between contracting parties. While AI interactions oftentimes cannot be circumvented, it must be assured that AI's promise of convenience and efficiency does not come with a loss of consumer autonomy, insufficient levels of transparency and, more generally, an unsatisfactory level of consumer protection.[9] However, connecting

6 K. Niziол, 'The challenges of consumer protection law connected with the development of artificial intelligence on the example of financial services (chosen legal aspects)', *Procedia Computer Science* 2021, p 4103, doi: 10.1016/j.procs.2021.09.185.

7 BEUC, 'Automated decision making and Artificial Intelligence – A consumer perspective', BEUC Position Paper, 2018, p 3, https://www.beuc.eu/publications/beuc-x-2018-058_automated_deci sion_making_and_artificial_intelligence.pdf.

8 The notion of 'consumer' is defined in Art. 2 of the Consumer Rights Directive as '*any natural person who [...] is acting for purposes which are outside his trade, business, craft or profession*'.

9 BEUC, 'AI Rights for Consumers', BEUC Position Paper, 2019, p 1, https://www.beuc.eu/publica tions/beuc-x-2019-063_ai_rights_for_consumers.pdf.

the consumer protection rationale to AI uncovers complex dynamics between data protection law, consumer law and competition law, which typically do not lend themselves well to be framed in a unified way. The result is a 'silo approach' towards consumer protection, where a clear demarcation remains between the different branches of law due to the diverging objectives of each branch.

5. In this contribution, it is argued that developments in the realm of AI put strain on the current consumer protection framework and that a move away from the current silo approach between data protection law, consumer law, and competition law is needed in order to ensure an adequate level of consumer protection. While the goal is to better protect consumers, consumer law alone is not up to the task to offer appropriate relief, given that problems triggered by AI transect multiple branches of law. Therefore, a strong intradisciplinary response is desirable where the EU consumer protection acquis is complemented with the insights from other legal domains.

6. To substantiate this argument, this article adheres to the following structure. Firstly, ideas surrounding AI, consumerism and consumer law are contextualized (s. 2). Secondly, attention is given to some of the implications of b2c AI interactions and how this ties into a silo-based approach to consumer protection (s. 3). Thirdly, an analysis takes place which illustrates that protecting consumers from harmful AI practices ensues from not only consumer law, but also data protection law and competition law (s. 4). Specific attention goes to revisiting the core consumer protection principles (s. 4.1) and studying the intersection between consumer, competition, and data (s. 4.2). The contribution concludes by recapitulating the main arguments of this paper (s. 5).

7. The topic of AI and consumer protection is vast, and it is therefore necessary to observe several limitations within this article. Firstly, the focus of this contribution lies on b2c interactions that involve AI systems. Hence, situations where consumers acquire AI-based goods or services – consequently triggering conformity assessment questions pursuant to Directive 2019/770 and Directive 2019/771 – are not considered.[10] Secondly, the interplay between AI and product liability rules is not assessed either, given that this topic has already been extensively discussed elsewhere in literature.[11] Thirdly, questions pertaining to situations where AI

---

10 M. Ebers, 'Liability For Artificial Intelligence And EU Consumer Law', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2021, vol. 12, pp 215-219.

11 See for instance, T. Cabral, 'Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive', *Maastricht Journal of European and Comparative Law* 2020, vol. 27, pp 615 et seq., doi: 10.1177/1023263X20948689; P. Čerka, J. Grigienė & G. Sirbikytė, 'Liability for damages caused by artificial intelligence', *Computer Law & Security Review* 2015, vol. 31, pp 376 et seq., doi: 10.1016/j.clsr.2015.03.008.

automatically concludes contracts for consumers (i.e., the AI agency hypothesis) are left to general contract law.[12]

2. Intertwining AI With Consumerism and Consumer Law

2.1. AI, Its Meaning, and Implications

8. Our brains offer individuals the capacity to display intelligence. In this context, intelligence is understood as an ability to acquire or demonstrate skills such as abstract reasoning, critical thinking, logic, and self-awareness. These skills can be learned and improved in the course of our life span, thus contributing to greater intelligence. As an aggregate of billions of neurons, our brains are capable of tackling the enormous range of tasks and challenges that we throw at it on a daily basis. For instance, when faced with a broken light bulb, we can interpret why it is pitch dark in a given room, analyse the underlying cause of darkness, and subsequently act upon that information by replacing the light bulb. The flexibility of our brains to be applied to and cope with new situations forms the crux of *human intelligence.*

9. Human intelligence is not the only source of intelligence, however. It is also possible to rely on meticulously designed machines to reproduce something akin to human intelligence. Instead of appealing to human cognitive features, machines rely on mathematics, binary logic and predictability.[13] Contrary to humans, machines can more easily leverage the advantages of raw computing power and memory storage to perform quintillions of calculations per second.[14] This type of intelligence can best be described as *artificial intelligence.*[15]

---

12 See for instance, M. Herbosch, 'The Diligent Use of AI Systems: A Risk Worth Taking?', *Journal of European Consumer and Market Law* 2022, vol. 11, p 14; S. Bennis, 'AI and the Consumer', in J. De Bruyne & C. Vanleenhove (eds), *Artificial Intelligence and the Law*, pp 481–484.

13 Consider C. Adriaansz, 'Betekenisvolle transparantie voor algoritmische besluitvorming', *Computerrecht* 2020, vol. 43, p 83, who writes that early conceptions of artificial intelligence revolve around conditional statements and adhere to a flowchart-like '*if … then … else*'-logic. The objective of these simple AI models is to provide solutions to problems by applying a fixed sequence of operations. Such sequences of operations are known as algorithms.

14 P. Louridas, *Algorithms* (Massachusetts: MIT Press 2020), pp 21–23 notes that algorithms themselves are not particularly revolutionary in that they consist of basic calculations such as additions, subtractions, divisions, and multiplications and that they can easily be performed by pen and paper. The next logical step, however, is to code algorithms in computer programming languages, thereby leveraging the advantages of modern-day computing.

15 Nowadays, the flowchart-logic has gradually been left behind and is currently being replaced with an ability to learn from experience – similar but not identical to humans. Algorithm becomes machine learning, and machine learning eventually becomes deep learning. Sequences of operations are no longer specified in advance, but are established on the go and, moreover, can be altered by the AI system itself when the need to do so arises.

10. While sharing similarities, human intelligence and artificial intelligence are not the same. On a slightly comical note: while a computer can effortlessly defeat a human in a game of chess, it will face serious hurdles when attempting to replace a broken light bulb. By way of comparison, it shows that humans are predominantly contingent on their critical thinking skills, whereas the functionality of machines hinges for the most part on having access to input data to brute force its way towards an appropriate solution for a given problem.[16] Critical thinking and reasoning essentially ensure that human intelligence can easily be applied to new circumstances, whilst artificial intelligence will struggle to deal with changes in its operating environment when no appropriate points of reference are available in the input data on how to cope with these changes.

11. The rapid uptake of AI is linked to several evolutions such as an exponential increase in computing power, upgrades to memory capacity, and improved access to vast quantities of data. The result of these evolutions is that AI introduces profound changes in our society. For instance, while simple algorithms provided a straightforward method for calculating the surface area of a rectangle, deep learning models have paved a path for complex use cases, which include facial recognition, virtual assistants, and even self-driving cars.[17] These novel applications all have in common that contemporary AI models are capable of parsing large datasets in exceedingly smaller time frames and identify patterns therein with increasing levels of precision. These use cases eventually tie into the creation of new opportunities for conducting business and for automating monotonous and highly repetitive tasks.

2.2. AI and Its Role in Mapping Consumption Patterns

12. The computerization of retail markets is more ubiquitous than one might expect.[18] From an entrepreneur's perspective, although consumers remain the driving force behind commerce and although day-to-day business operations continue to involve intricate decisions regarding product offerings, price setting and advertising, the market presence of AI changes how such decisions are being

16 In a similar fashion, see A. Jabłonowska et al., 'Consumer law and artificial intelligence. Challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence', EUI Working Paper LAW 2018/11, 2018, pp 69-70, https://cadmus.eui.eu/handle/1814/57484.

17 C. Thorun & J. Diels, 'Consumer Protection Technologies: An Investigation Into the Potentials of New Digital Technologies for Consumer Policy', *Journal of Consumer Policy* 2020, vol. 43, pp 177-178.

18 C. Ruers & L. Hovhanisian, 'Is het gebruik van prijsalgoritmes eerlijk? Over de toepassing van dynamic pricing en personalized pricing en de toegenomen aandacht van autoriteiten voor fairness', *Tijdschrift voor Consumentenrecht en handelspraktijken* 2022, vol. 1, p 6; T. Espeel, 'Affaire

made.[19] Similarly, from a consumer's point of view, digital technology is increasingly infiltrating our everyday lives while we spend time on social media platforms, buy products through e-commerce websites, and pay for groceries in local retail markets. At every step along this process, data is being generated.[20]

13. Data aggregation as such serves little purpose; its value specifically lies with the finding of new and improved ways to make use of those data.[21] AI is at the centre stage when pursuing this goal.[22] By way of illustration, the contents of a database, which contains the details of millions of grocery store purchases, may seem random and completely arbitrary at first.[23] Nevertheless, there is often more than meets the eye. For instance, a positive correlation may reveal itself between consumers buying cake mixes and cake frosting and consumers buying birthday candles. In the same vein, purchasing a subset of roughly 25 different products can apparently give an accurate indication whether someone is pregnant or not.[24] It appears that consumers' shopping behaviour is not so random after all.

14. AI can easily be tailored to uncover hidden patterns that lie hidden within large datasets.[25] By studying the interactions between various parameters, it becomes possible to capture these findings and to generate analytical models, which can accurately forecast future consumer purchase decisions. Hence, an important take-away is that contemporary AI models not only produce descriptive output (e.g., what items are most popular), but also generate predictive analytics about future consumption behaviour by drawing inferences and make extrapolations on the basis of aggregated data.[26] Businesses can subsequently rely on these findings to alter their commercial behaviour on the market and to influence

---

Amazon EU: Commerce en ligne: libre choix des moyens de communication avec les consommateurs ?', *Revue Européenne de Droit de la Consommation* 2020, vol. 2, p 334.

19 E. Alpaydin, *Machine Learning* (Cambridge: MIT Press 2021), pp xiii–xv.

20 E. Alpaydin, *Machine Learning*, pp xiii–xv.

21 M. Ebers, 'Regulating AI and Robotics – Ethical and Legal Challenges', in M. Ebers & S. Navas (eds), *Algorithms and Law* (Cambridge: Cambridge University Press 2020), pp 62–63.

22 This is also purported in European Commission, 'On Artificial Intelligence – A European approach to excellence and trust', EC White Paper, 2020, p 8, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

23 E. Alpaydin, *Machine Learning*, p xiv.

24 C. Duhigg, 'How Companies Learn Your Secrets' (*The New York Times Magazine* 16 Feb. 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

25 R. Devillé, N. Sergeyssels & C. Middag, in *Artificial Intelligence and the Law*, p 4.

26 C. Koolen, 'Transparency and Consent in Data-Driven Smart Environments', *European Data Protection Law Review* 2021, vol. 7, p 185, doi: 10.21552/edpl/2021/2/7; S.-A. Elvy, 'Commodifying consumer data in the era of the Internet of Things', *Boston College Law Review* 2018, vol. 59, p 444.

consumers in their doings. As a result, AI effectively influences how we, consumers, consume.

2.3. Evolution of Consumerism and Consumer Law

15. Given both its complexity and potential, the extensive usage of AI challenges the current understanding of consumer protection. Over the past decades, the predominant idea underpinning consumer law has been that it aims to ensure the free choice[27] of the average consumer on the market.[28] Consumer law therefore safeguards the private autonomy of the consumer and the right to self-determination on the market through active and well-informed decisions. In essence, consumer law protects the economic rights of consumers.[29] This economic approach towards consumer law, which is clearly present in the EU consumer protection instruments, has been subject to criticism in the past.[30] Some writings have questioned the focus on protecting economic rights due to the diffuse nature of consumers' economic interests.[31] Other scholarly works have put question marks over consumers' ability to make rational purchase decisions in the face of increasingly complex, multidimensional products.[32] Recent literature, drawing heavily from behavioural economics and the *nudge theory*,[33] also underscores that consumers' autonomy is curtailed by external influences, cognitive biases and heuristics (e.g., the way how information is presented or time constraints experienced during decision-making processes).[34]

---

27 Article 8, UCPD; ECJ 13 Sep. 2018, C-54/17 *Wind Tre*, para. 45.

28 N. Averitt & R. Lande, 'Consumer choice: the practical reason for both antitrust and consumer protection law', in P. Nihoul, N. Charbit & E. Ramundo (eds), *Choice – A New Standard for Competition Law Analysis?* (New York: Concurrences Review 2016), p 250.

29 In this sense, see Council Resolution of 14 Apr. 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy [1975] OJ C 92/1: '*Whereas the improvement of the quality of life is one of the tasks of the Community and as such implies protecting the health, safety and economic interests of the consumer*'.

30 B. Duivenvoorde, 'Datagedreven marketing en de toekomst van het consumentenrecht: tijd voor een nieuwe beschermingsgedachte?', *Tijdschrift voor Consumentenrecht en handelspraktijken* 2021, vol. 4, p 200.

31 For example N. Reich, 'Protection of Consumers' Economic Interests by the EC', *Sydney Law Review* 1992, vol. 14, p 23 who highlights that the economic interests of consumers are diffuse.

32 J. Kapeller, B. Schütz & S. Steinerberger, 'The impossibility of rational consumer choice: A problem and its solution', *Journal of Evolutionary Economics* 2013, vol. 23, pp 42 et seq.

33 R. Thaler & C. Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness* (London: Penguin Books 2009), pp 19 et seq.

34 A. Keirse & T. Bouwman, 'Nudging Financial Decisions: Protecting Weaker Parties while Promoting Autonomy', *Texas International Law Journal* 2019, vol. 54, pp 205–206.

16. Nowadays, it is submitted that digitization – including the use of AI – is yet again challenging the fundamentals of consumer law.[35] Among others, the uptick in AI-driven business models further undermines the basic assumption that the average consumer is capable of making autonomous decisions.[36] The ability of AI to, for instance, encourage more consumer spending, funnel consumers to certain products, or target them with promotional notifications at optimal times puts strain on the very right to self-determination that is – in current consumer law – still seen as a right to decide in accordance with one's own preferences.[37]

17. Considering the implications of AI, it is necessary to challenge the narrow view that consumer law is synonymous to a set of rules that merely protects the economic rights of consumers as well as the related view that consumer law only has a role to play if the payment of a 'price' is at stake. A novel understanding of consumer law requires that other considerations should come to the forefront as well – notably the protection of consumers' privacy and the protection of fair competition. Whereas privacy-related concerns[38] are often at the forefront during scholarly discussions on AI, fair competition is equally at risk when consumer-facing AI systems implement anticompetitive strategies, such as leveraging market power for self-preferencing purposes.[39] Factoring in these other interests will therefore produce solutions to digitization-based consumer protection problems that do not exclusively emanate from the traditional EU consumer law acquis (i.e., consumer law *sensu stricto*), but also from other branches of law. Stated otherwise, consumer protection is not only a matter for consumer law; it also involves looking at data protection law and competition law.

35 BEUC, 'AI Rights for Consumers', p 2; BEUC, 'Automated decision making and Artificial Intelligence, p 7.

36 M. Gal & N. Elkin-Koren, 'Algorithmic Consumers', *Harvard Journal of Law & Technology* 2017, vol. 30, p 322.

37 D. Gkikas & P. Theodoridis, 'AI in Consumer Behavior', in M. Virvou et al. (eds), *Advances in Artificial Intelligence-based Technologies* (Cham: Springer 2022), p 165: '*Marketing is an art of influence and it aims to find touch points where customers are open to influence. These touch points refer to a primary potential set of choices that customers have, which are known as the "funnel". The marketing goal is to reduce the primary funnel and lead the customers towards a narrowed set of choices of potential purchases as the consumers weigh the facts, consider the choices and finally purchase the product*'.

38 Most authors take issue with traders acquiring increasing amounts of personal data about consumers, which encompasses an associated risk of algorithmic discrimination or unfair algorithmic conduct.

39 J. Crémer, Y-A de Montjoye & H. Schweitzer, 'Competition policy for the digital era', European Commission Study 2019, pp 65-66, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

18. This contribution is another attempt to argue that a future-proof understanding of consumer law cannot be limited to merely protecting economic interests. By bringing other values within the scope of consumer protection, it becomes possible to update existing views in order to ensure that consumer law operates as a proper autonomy-enhancing toolbox.[40] This broader perspective requires that consumers are no longer reduced to their economic interests, but that they should be seen as *consumer-citizens*,[41] whose consumption choices have profound implications on society as a whole.[42] In this context, it should be recalled that the extensive reliance of AI systems on personal data not only affects consumers' economic welfare, but also other aspects of consumer-citizens' lives.[43] Convergence between different complementary branches of law is needed to ensure effective protection, as traditional interpretations of consumer law do no longer suffice and deprive consumers of much-needed protection in increasingly digitized environments.

3. Usage of AI in b2c Markets

3.1. A Closer Look at Recommender Systems

19. Prior to commencing the legal analysis, it is a worthwhile endeavour to briefly consider the potential and limits of AI. A proper discussion on AI's functionality allows us to pinpoint common problems, which will serve as anchoring points for the subsequent parts of this paper. To that end, a closer look at the subclass of AI-based recommender systems is particularly illustrative. At present, recommender systems are abundantly deployed on e-commerce websites[44] where they provide consumers with personalized product recommendations, and on social media platforms[45] where they determine the content shown to users.

---

40 In support of this argument, see also I. Graef, D. Clifford & P. Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law', *International Data Privacy Law* 2018, vol. 8, pp 202–203, doi: 10.1093/idpl/ipy013.

41 N. Helberger et al., *EU Consumer Protection 2.0 – Structural asymmetries in digital consumer markets* (Brussels: BEUC 2021), p 53; M. Lammi & M. Pantzar, 'The data economy: How technological change has altered the role of the citizen-consumer', *Technology in Society* 2019, vol. 59, p 1, doi: 10.1016/j.techsoc.2019.101157.

42 ECJ 2 Dec. 2021, C-319/20 *Meta Platforms Ireland*, Opinion of Advocate General J. Richard de la Tour, para. 1.

43 As elaborately expanded upon in N. Helberger et al., *EU Consumer Protection 2.0*, pp 26 et seq.

44 For Amazon: B. Rabowksy & L. Morrison, 'What's new in recommender systems' (*Amazon Web Services* 17 Nov. 2020), https://aws.amazon.com/blogs/media/whats-new-in-recommender-sys tems/; L. Hardesty, 'The history of Amazon's recommendation algorithm: Collaborative filtering and beyond' (*Amazon* 22 Nov. 2019); for Zalando: M. Braun, 'Recommendations Galore: How Zalando Tech Makes It Happen' (*Zalando Engineering Blog* 2 Dec. 2016), https://engineering. zalando.com/posts/2016/12/recommendations-galore-how-zalando-tech-makes-it-happen.html.

45 For Instagram: I. Medvedev, H. Wu & T. Gordon, 'Powered by AI: Instagram's Explore recommender system' (*Meta AI* 25 Nov. 2019), https://ai.facebook.com/blog/powered-by-ai-instagrams-

20. The starting point for any recommender system is the so-called *recommendation problem.* In essence, the recommendation problem is a computational estimation exercise when a model is tasked to predict the response of a user to a particular item.[46] By relying on prior training data, the objective is to suggest *novel* items for which the user's predicted response is high.[47] Recommender systems rest on the underlying assumption that hidden dependencies exist between users and items, which can eventually be cast in a mathematical model.[48] This model can subsequently be leveraged for the purpose of filtering information and offering a *personalized* customer experience. Typical use cases either revolve around predicting a response for individual user-item combinations ('items you may also like') or require returning a sorted ranking of recommendations for a given user ('best search results').[49] In both instances, the model yields tailored recommendations on the basis of users' past purchases, search activity, and indicated preferences.[50]

21. For recommendation problems, the interactions between users and items are typically represented by means of a matrix. Once all known interactions between users and items are entered into the matrix, the model is tasked to calculate levels of similarity between different user-item interactions. In more technical terms, this similarity assessment involves building a multidimensional vector space by means of a feature extraction process, where variables pertaining to the user[51] and the item[52] are mapped and represented in the form of a vector.[53] At this point, several methods[54] are available to compute distances between vectors, which provide a measure of how similar two user-item interactions are. This information can then be used to recommend items that are similar to a user's preferences, based on historical data, as shown below in Table 1.

---

explore-recommender-system/; for YouTube: C. Goodrow, 'On YouTube's recommendation system' (*YouTube* 15 Sep. 2021), https://blog.youtube/inside-youtube/on-youtubes-recommendation-system/.

46 X. Ning, C. Desrosiers & G. Karypis, 'A Comprehensive Survey of Neighborhood-based Recommendation Methods', in F. Ricci et al. (eds), *Recommender Systems Handbook* (New York: Springer, 2nd edn 2015), p 37; G. Adomavicius & A. Tuzhilin, 'Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions', *IEEE Transactions on Knowledge and Data Engineering* 2005, vol. 17, p 734, doi: 10.1109/TKDE.2005.99.

47 *Ibid.*

48 L. Lü et al., 'Recommender Systems', *Physics Reports* 2012, vol. 519, pp 2–3.

49 F. Ricci, L. Rokach & B. Shapira, 'Recommender Systems: Introduction and Challenges', in F. Ricci et al. (eds), *Recommender Systems Handbook*, pp 6–7.

50 L. Lü et al., *Physics Reports* 2012, pp 2–3.

51 For example country of residence, age, gender, or income.

52 For example price, color, purpose, size, weight, or battery life.

53 M. Grbovic et al., 'E-commerce in Your Inbox: Product Recommendations at Scale', *Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* 2015, p 1810, doi: 10.1145/2783258.2788627.

54 For example cosine similarity.

Table 1. Simplified illustration of how recommender systems rely on matrices.[55] *User-item interactions indicated in grey are 'most similar' to one another and thus can be used to determine the rating* $User_5$ *would give to* $Product_3$*. In this case, the* $User_5$*-*$Product_3$ *combination would yield a negative rating*

	Product1	**Product2**	**Product3**	**Product4**
User1	👍	👎	👍	👍
User2		👍	👎	👎
User3	👍	👍	👎	
User4	👎		👍	
User5	👍	👍	?	👎

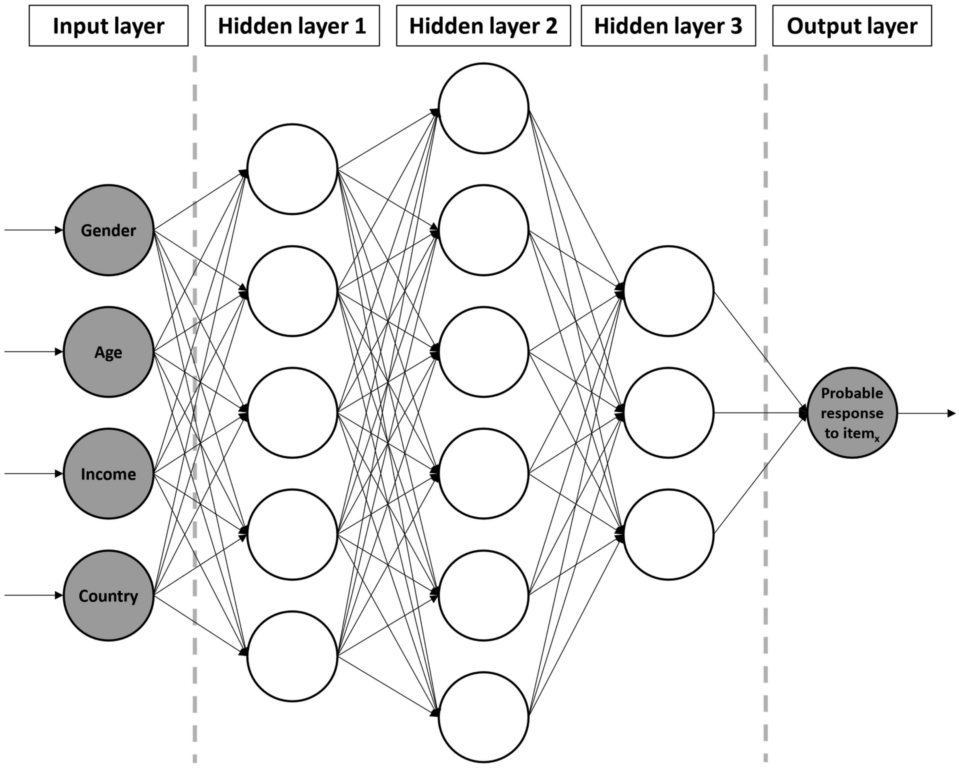
22. Traditional machine learning approaches usually involve laborious manual steps such as the aforementioned feature extraction process. However, the state of the art on recommender systems has drastically changed following evolutions in the realm of *deep learning.*[56] Data are no longer parsed in a straightforward (linear) fashion but, instead, flow from an input layer to an output layer, with several transformative steps (i.e., a neural network) in between (see Figure 1).[57] Information is continuously taken from one layer and passed on to the next over several iterations until eventually an accurate output is produced. Contemporary deep learning models are not only more accurate in terms of their predictions, they also do away with the need for human intervention to construct feature sets. Accordingly, it has slowly altered the way how contemporary recommendation problems are modelled.

55 Adopted from C. Pinela, 'Recommender Systems – User-Based and Item-Based Collaborative Filtering' (*Medium* 6 Nov. 2017), https://medium.com/@cfpinela/recommender-systems-user-based-and-item-based-collaborative-filtering-5d5f375a127f.

56 I. Goodfellow, Y. Bengio & A. Courville, *Deep Learning* (Cambridge: MIT Press 2016), pp 5-8.

57 *Ibid.*

Figure 1. Topology of a neural network with three hidden layers[58]



3.2. *The Case for and Against AI*

23. The extensive usage of AI in b2c transactions is generating a lot of discussion nowadays. Several authors underscore that considerable risks surround AI-driven business models[59] In this respect, it is particularly important to keep track of how complex algorithms are used and to consider the implications for consumer protection. What is especially perilous is the finding that AI can significantly impede the level of autonomy

58 Adopted from A. Wulf & O. Seizov, 'Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU', *European Business Law Review* 2020, vol. 31, p 618, doi: 10.54648/EULR2020024.

59 J. Laux, S. Wachter & B. Mittelstadt, 'Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice', *Common Market Law Review* 2021, vol. 58, pp 726–729, doi: 10.54648/COLA2021048; S. Bennis, in *Artificial Intelligence and the Law*, pp 464–465; A. Jabłonowska et al., Consumer law and artificial intelligence, pp 19 et seq.; M. Gal & N. Elkin-Koren, *Harvard Journal of Law & Technology* 2017, p 322.

experienced by consumer-citizens on online marketplaces.[60] Within the context of this paper, three specific aspects are worth shedding light on.

24. For one, it must be kept in mind that AI contributes to an ever-increasing knowledge gap between businesses and consumers.[61] It is useful to keep in mind that, from a commercial point of view, AI models' goal is either to boost product sales or to increase the diversity among sold products.[62] From that perspective, it is not far-fetched to state that AI-driven data analytics can show an inclination to blur the lines between personalized offers and manipulative suggestions.[63] In other words, they may feature code snippets that inadvertently stimulates the AI system to show consumers things that they do not necessarily need in the first place or to slightly distort the choices available to the consumer (e.g., by only showing premium products). As such, AI models can exert *undue influence*[64] on consumers and steer them towards purchase decisions they would not have taken otherwise.[65]

25. A second aspect to consider for consumer-citizens is *transparency* vis-à-vis data collection and processing practices.[66] Growing information asymmetries suggest that, while undertakings are increasingly getting better insights into their customer base by virtue of having access to data, customers themselves are not necessarily in a position to assess the quality of the advice provided to them based on these insights.[67] As argued elsewhere, the current notice-and-consent framework is particularly ill-suited to cope with AI-driven data analytics: it will prove difficult for the average consumer to deduce what information is collected and how that information is used to generate personalized recommendations.[68] In the face of this limited level of transparency, the risk of AI systems issuing erroneous recommendations should not be overlooked.

---

60 As argued by, among others, L. Bjørlo, Ø. Moen & M. Pasquine, *Sustainability* 2021, p 2332; M. Lippi et al., 'The Force Awakens: Artificial Intelligence for Consumer Law', *Journal of Artificial Intelligence Research* 2020, vol. 67, p 176, doi: 10.1613/jair.1.11519; P. Picht & G. Loderer, 'Framing Algorithms: Competition Law and (Other) Regulatory Tools', *World Competition* 2019, vol. 42, p 416, doi: 10.54648/woco2019022.

61 BEUC, 'EU Consumer Protection 2.0 – Protecting fairness and consumer choice in a digital economy', BEUC Position Paper, 2022, p 8, https://www.beuc.eu/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf.

62 F. Ricci, L. Rokach & B. Shapira, in *Recommender Systems Handbook*, pp 5-6.

63 S. Bennis, in *Artificial Intelligence and the Law*, p 465.

64 Article 2(j), UCPD: '*"undue influence" means exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer's ability to make an informed decision*'.

65 J. Laux, S. Wachter & B. Mittelstadt, *Common Market Law Review* 2021, p 746; N. Helberger, F. Borgesius & A. Reyna, 'The perfect match? A closer look at the relationship between EU consumer law and data protection law', *Common Market Law Review* 2017, vol. 54, pp 1455-1456.

66 C. Adriaansz, *Computerrecht* 2020, pp 88-90; A. Wulf & O. Seizov, *European Business Law Review* 2020, p 622.

67 A. Jabłonowska et al., Consumer law and artificial intelligence, pp 11-12.

68 C. Koolen, *European Data Protection Law Review* 2021, pp 185-186.

26. A third dimension under purview are the implications of personalized advertising and, notably, personalized pricing.[69] Regardless of whether such strategies are truly welfare-enhancing or whether they entail consumer harm, it is accepted knowledge that the pursuit of consumer autonomy calls for *price transparency.*[70] In reality, however, it is often not obvious whether consumers are presented with a standard offer or a personalized offer. The UK's Competition and Markets Authority confirms that such personalized pricing strategies can be relied upon to lower customer churn rates by considering, for instance, the typical characteristics demonstrated by consumers looking to switch to a competitor.[71] By leveraging this information, the firm can alter its pricing strategies and seek recourse to behaviour akin to predatory pricing.[72] In line with paragraphs 24 and 25, informational asymmetries in terms of prices charged for products removes consumer-citizens' ability to compare prices, which is core to the principle of effective competition.

27. Be that as it may, these points of critique are not to say that AI only brings about negative consequences. For instance, it is known that recommender systems are able to efficaciously filter out counterfeit products and aid in preventing fraudulent e-commerce transactions. Moreover, it is equally true that these systems can positively enhance the shopping experience of consumers, either through helping them discover items they might not have found otherwise or by shortening the path towards a purchase. Furthermore, it should be recalled that each consumer has different preferences and, when AI has a good understanding of what a particular consumer wants, tailor-made recommendations can genuinely aid users in navigating information-heavy shopping environments.

3.3. Fairness Deficit

3.3.1. The Silo-Based Approach to Consumer Protection

28. It follows from the above that the implications of using AI in a commercial setting are not limited to one legal domain. Instead, in the face of AI-driven data analytics, at least three different branches of law are relevant to consider when

---

69 M. Grochowski et al., 'Algorithmic Price Discrimination and Consumer Protection: A Digital Arms Race?', *Technology and Regulation* 2022, vol. 2022, pp 41–42; N. Helberger et al., *EU Consumer Protection 2.0*, p 112; C. Veljanovski, 'Algorithmic Antitrust: A Critical Overview', in A. Portuese (ed.), *Algorithmic Antitrust* (Cham: Springer 2022), p 53.

70 S. Scheuerer, 'Artificial Intelligence and Unfair Competition – Unveiling an Underestimated Building Block of the AI Regulation Landscape', *GRUR International* 2021, vol. 70, pp 836–837, doi: 10.1093/grurint/ikab021.

71 CMA, 'Algorithms: How they can reduce competition and harm consumers' (*Gov.uk* 19 Jan. 2021), https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers/algorithms-how-they-can-reduce-competition-and-harm-consumers.

72 *Ibid.*

pursuing a high level of consumer protection. Those three branches are consumer law,[73] competition law,[74] and data protection law[75].[76] On the one hand, it is true that European legislative instruments pertaining to consumers, competition, and data belong to different regulatory frameworks[77] and have distinct objectives,[78] which subsequently ties into a silo-based approach towards consumer protection.[79] On the other hand, it is equally accurate that all three domains share a direct or indirect goal of protecting consumers by virtue of contributing to a fair market order, thus hinting at a possibility to shift from the current silo-based approach to consumer protection to a more coherent protective regime. In other words, it is important to not overlook instances where these different rulesets interact with one another.[80] For this reason, and especially with the effective protection of consumers at stake, it is useful to engage in an exercise of interpretative thinking that would allow for such interactions to occur in a harmonious manner.

29. Prior to suggesting any interpretative changes, however, it is necessary to search for common ground between these three legal branches. Against this background, it is argued by several scholars that the principle of *fairness*[81] acts as a linchpin within all three domains.[82] Pursuant to this line of reasoning, the

---

73 See above at para. 24.

74 See above at para. 26.

75 See above at para. 25.

76 Also supporting this view: W. Kerber, 'Digital markets, data, and privacy: competition law, consumer law and data protection', *Journal of Intellectual Property Law & Practice* 2016, vol. 11, pp 865–866, doi: 10.1093/jiplp/jpw150: '*This article claims that it is necessary to develop a sophisticated integrated approach of the proper legal provisions in competition, consumer, and data protection law (and also intellectual property) in order to develop a well-functioning legal order for the protection of privacy in the digital economy*'.

77 ECJ 2 Dec. 2021, C-319/20 *Meta Platforms Limited*, Opinion of Advocate General R. De La Tour, para. 79.

78 M. Botta & K. Wiedemann, 'The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey', *The Antitrust Bulletin* 2019, vol. 64, p 434, doi: 10.1177/0003603X19863590.

79 In the context of Art. 102 TFEU, see A. Scharf, 'Exploitative business terms in the era of big data – the Bundeskartellamt's Facebook decision', *European Competition Law Review* 2019, vol. 7, p 332: '*the legality of abusive conduct is unrelated to compliance or non-compliance with other legal rules*'.

80 ECJ 2 Dec. 2021, C-319/20 *Meta Platforms Limited*, paras 80–81.

81 This text has no ambition to minutely scrutinize the many facets of fairness, neither substantively nor procedurally. Within the scope of this contribution, it suffices to state that 'fairness' encompasses an element of not showing favouritism or bias. See also the dictionary definition of 'fairness' at Merriam Webster: '*the quality or state of being fair; lack of favoritism toward one side or another*'.

82 I. Graef & S. Van Berlo, 'Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility', *European Journal of Risk Regulation* 2020, vol. 12, p 697, doi: 10.1017/err.2020.92; I. Graef, D. Clifford & P. Valcke, *International Data Privacy Law* 2018, pp 202–203; N. Zingales, 'Between a

principle of fairness suggests that a certain degree of balance[83] should exist between opposing interests. For consumer law, fairness implies that b2c contracts do not, contrary to the requirement of good faith, bring about significant imbalances in the parties' rights and obligations to the detriment of the consumer.[84] In the context of competition law, the fairness principle revolves around securing the economic freedom of market participants.[85] To that end, reference is made to the notion of 'competition on the merits' (i.e., competition relating to price, choice, quantity, quality, or innovation). For data protection law, the principle of fairness contained in Article 5(1) GDPR calls for a balance between the asymmetric relation that exists between data subjects and data controllers.[86]

30. The application of fairness across these three legal branches should not be studied in isolation of one another, due to the notable overlaps that exist between the different regimes. Effective consumer protection is not a matter of or-or, but rather and-and. This sentiment is further corroborated based on the finding that AI has extensive potential to tilt the scales in favour of predominantly commercial interests, to the detriment of consumers. This may subsequently hint at the existence of a *fairness deficit* during AI-based transactions and give rise to instances of one-sidedness.

3.3.2. Breaking Down the Silo Mentality

31. In view of maintaining a healthy balance in AI-driven markets, it is necessary to break down the silo mentality that currently exists between consumer law, competition law, and data protection law. Substantively speaking, the main principles originating from one legal branch should at least be considered in the context of the two other branches.[87] This strategy would strengthen the positioning of consumers on the market and turn them into consumer-citizens by virtue of safeguarding their right to self-determination. The suggested approach to consumer protection is therefore a *combined approach*, a defence in depth so to speak, that hinges on reciprocal interactions between consumer law, competition law, and data protection law. This ensures that consumer protection is not only about

---

rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law', *Computer Law & Security Review* 2017, vol. 33, p 557, doi: 10.1016/j.clsr.2017.05.018.

83 H. Kalimo & K. Majcher, 'The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace', *European Law Review* 2017, vol. 42, p 216.

84 Unfair Contract Terms Directive, Art. 3; C. Willett, *Fairness in Consumer Contracts: The Case of Unfair Terms* (Hampshire: Ashgate Publishing 2007), p 85.

85 B. Keirsbilck, *The New European Law of Unfair Commercial Practices and Competition Law* (Oxford: Hart Publishing 2011) p 521.

86 D. Clifford & J. Ausloos, 'Data Protection and the Role of Fairness', *Yearbook of European Law* 2017, vol. 37 p 131, doi: 10.1093/yel/yey004.

87 I. Graef, D. Clifford & P. Valcke, *International Data Privacy Law* 2018, p 210.

empowering consumers, but also about building safer digital spaces and creating a level playing field for entrepreneurs where innovation can thrive.[88]

32. Although convincing arguments can be found favouring a combined protective approach, it could equally be argued that this would unnecessarily blur the lines between these legal domains.[89] After all, each branch has its own distinct objectives and scope of application. However, in the author's view, consumer law, competition law as well as data protection law can be applied in a more coherent manner without compromising the integrity of each respective branch. In fact, a *rapprochement* is necessary exactly because the boundaries of these legal regimes are becoming increasingly blurry. Nowadays, it is rarely the case that legal issues relating to digital technology exclusively trigger the application of one single branch of law.[90] Moreover, striving towards a more coherent approach does not imply subsuming one legal branch under the other. Instead, the goal is to aim for complementarity and to ensure that all three legal branches are at least mindful of one another.

3.3.3. Building Coherence

33. Clarifying the complementarity between the different branches of law quickly shifts the discussion towards a *how-to* question: how to build coherence between consumer, competition, and data?[91] A useful starting point for answering this question is by considering which elements bring market conduct within the ambit of each legal branch. A close reading of the relevant legal instruments and guidance documents reveals the following. Firstly, consumer law comes into effect once a consumer is confronted with the deployment of 'commercial practices' by a trader within the internal market.[92] Secondly, competition law is relevant to consider when commercial conduct impairs genuine undistorted competition on the

---

88 European Parliament, 'Consumer policy: Principles and instruments' (*European Parliament* 1 Dec. 2021), https://www.europarl.europa.eu/factsheets/en/sheet/46/consumer-policy-principles-and-instruments.

89 F. Bostoen, 'When competition law met data protection: the Bundeskartellamt's Facebook decision' (*CoRe Blog* 18 Feb. 2019), https://www.lexxion.eu/en/coreblogpost/bundeskartellamt-facebook-decision/.

90 ECJ 2 Dec. 2021, C-319/20 *Meta Platforms Limited*, para. 81: '*Instances of the interaction between the law relating to the protection of personal data, consumer law and competition law are frequent and numerous, since the same conduct may be covered simultaneously by legal rules belonging to those different areas. Such actions contribute to making the protection of personal data more effective*'; N. Helberger, F. Borgesius & A. Reyna, *Common Market Law Review* 2017, p 1429; N. van Eijk, C. Hoofnagle & E. Kannekens, 'Unfair Commercial Practices: A Complementary Approach to Privacy Protection', *European Data Protection Law Review* 2017, vol. 3, p 336, doi: 10.21552/edpl/2017/3/7.

91 I. Graef, D. Clifford & P. Valcke, *International Data Privacy Law* 2018, p 201.

92 Unfair Commercial Practices Directive, Recital 2 and Art. 2.

common market.[93] Thirdly, data protection law has a bearing on any processing activities involving personal data from natural persons located in the EU.[94]

34. It quickly becomes apparent that more than one legal branch can apply at the same time. For instance, the collection of personal data for the purpose of issuing personalized recommendations may fall within the ambit of the GDPR, but such conduct could also trigger the application of Article 102 TFEU (e.g., when a dominant undertaking engages in self-preferencing practices[95] via a product recommender system). Similarly, b2c contract terms and commercial practices that relate to privacy policies can prompt questions under the Unfair Contract Terms Directive (UCTD) and the Unfair Commercial Practices Directive (UCPD) in conjunction with the GDPR.[96] Furthermore, it is also possible that all three branches apply simultaneously. This is the case when, for instance, a dominant firm relies on its market power to force data subjects to agree to unfettered data processing practices.[97]

35. Complementary effects are likely to occur when the application of consumer law, competition law, or data protection law intersects, the reason being that each branch protects a different aspect of consumer welfare.[98]

- Consumer law protects *consumer autonomy* by empowering consumers to make well-informed transactional decisions.
- Competition law enables *consumer choice* by keeping markets competitive and free from distortion.
- Data protection law upholds individuals' fundamental *right to data protection* by ensuring that personal data are processed in a fair and transparent manner.

In that way, each legal branch adds its own layer of protection. A combined approach ensures that consumer law enables the autonomous exercise of a choice, which presupposes that competition law guarantees the availability of a range of different choices, which presupposes that data protection law prevents any choice offered from going against the fundamental right to data protection. Accordingly,

93 Guidance on the Commission's enforcement priorities in applying Art. 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings [2009] OJ C 45/7, para. 1.

94 General Data Protection Regulation, Recital 2 and Arts 2–3.

95 For example ECJ 10 Nov. 2021, T-612/17 *Google and Alphabet/Commission (Google Shopping).*

96 For example ECJ 28 Apr. 2022, C-319/20 *Meta Platforms Ireland.*

97 For example Request for a preliminary ruling in C-252/21 *Meta Platforms and Others*; *Bundeskartellamt* in Case B6-22/16, *Facebook* [2019], https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

98 S. Scheuerer, *GRUG International* 2021, p 834; I. Graef, 'Blurring Boundaries of Consumer Welfare', in M. Bakhoum et al. (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?* (Berlin: Springer 2018), p 131.

the protection provided by one branch complements the protection enjoyed by a different branch, which eventually leads to consumer protection in a broad sense, as illustrated in Table 2.

Table 2. Consumer protection should not be limited to consumer law as such. A holistic approach to consumer protection requires that the functioning of one branch is complemented with the substantive principles of any of the other two branches whenever relevant.

	Consumer Protection Sensu Lato		
Legal branch	Consumer law	Competition law	Data protection law
Legal instruments	CRD; UCTD; UCPD	Articles 101–102 TFEU; Merger control	GDPR; ePrivacy Directive
Benchmark	Average consumer	Consumer welfare	Data subject
Protected value	Consumer autonomy	Consumer choice	Right to data protection
Enforcement authority	Consumer authorities and consumer associations	National Competition Authorities (NCAs) and the European Commission	Data Protection Authorities (DPAs)

36. Whether a legal issue relates to a data subject, an average consumer or a consumer's welfare, at the end of the day, it concerns the same individual.[99] This indicates that all three legal branches must work together to cope with the consequences of AI being opaque and having the potential to negatively impact different facets of consumers' lives.[100] Even though each legal domain has its own objectives and mode of application, to avoid instances of *unfairness*, the pursuit of adequate consumer protection dictates that the insights from different branches are combined whenever relevant. This approach will contribute to a much-needed holistic approach towards consumer protection in the face of AI-driven market practices.[101]

99 See I. Graef, in *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach?*, p 123, who states that competition law sees consumers in a more generalist sense compared to consumer law and data protection law.

100 M. Ebers, *Journal of Intellectual Property, Information Technology and E-Commerce Law* 2021, p 208.

101 European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy', EDPS Opinion 2014, pp 36–37, https://edps.europa.eu/sites/default/files/publication/14-03-26_competitition_law_big_data_en.pdf: '*it may be sensible for the Commission and*

4. A Multipronged Approach to Consumer Protection

4.1. Revisiting the Core Consumer Protection Principles

37. Remedying the fairness deficit calls for a revisit of the core values and ideas that underpin the EU consumer protection acquis. In this respect, two fundamental principles should be recalled: the proper functioning of the internal market and the protection of consumers as such.[102] The first principle is inspired by a desire to create a trustworthy European market without internal frontiers where cross-border commerce can thrive, whereas the second principle builds on the fact that consumers qualify as the weaker contracting party within the context of b2c transactions.[103] It is especially this disadvantaged or unequal position of consumers vis-à-vis their professional counterparties that requires further attention.[104] Traditionally, this inequality is addressed in three ways.

38. A first strategy entails enabling rational decision-making behaviour on behalf of consumers by providing pre-contractual information.[105] It is assumed that by making information pertaining to the transaction and the underlying product available to consumers, those consumers are sufficiently capable of catering to their own interests. Hence, from the perspective of the average consumer, who is believed to be reasonably observant and circumspect,[106] the expectation is that this individual can make informed transactional decisions when presented with clear and comprehensive precontractual information.

39. A second strategy revolves around the need to address the unequal position in terms of contractual bargaining power between the trader and the consumer.[107] B2c contracts are mostly offered on a *take-it-or-leave-it* basis to the consumer, which suggests that the ability of the consumer to influence the content of the

---

the EDPS at EU level together with national competition, consumer protection and data protection authorities to agree upon a more holistic approach to enforcement'; A. Scharf, *European Competition Law Review* 2019, p 333.

102 B. Duivenvoorde, *Tijdschrift voor Consumentenrecht en handelspraktijken* 2021, p 198; S. De Pourcq, *Oneerlijke handelspraktijken en bedingen in contracten tussen ondernemingen* (Antwerp: Intersentia 2018), p 339.

103 B. Duivenvoorde, *Tijdschrift voor Consumentenrecht en handelspraktijken* 2021, p 198.

104 ECJ 4 Oct. 2018, C-105/17 *Kamenova*, para. 34.

105 Directive 2011/83/EU of the European Parliament and of the Council of 25 Oct. 2011 on consumer rights [2011] OJ L 304/64; Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 Nov. 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328/7.

106 ECJ 30 Apr. 2014, C-26/13 *Kásler*, para. 74.

107 Directive 93/ 13/EEC of 5 Apr. 1993 on unfair terms in consumer contracts [1993] OJ L 95/29.

agreement is either severely limited or completely non-existent. This subsequently ties into situations where the professional contracting party can abuse its contractual freedom by unilaterally inserting unfair contact terms into the b2c agreement.[108] To alleviate some of the detrimental implications associated with such practices, legislators have adopted rules that prohibit the use of contract terms that create significant imbalances between the respective rights and obligations of the business and consumer. In essence, the goal of this intervention is to prevent and correct unbalanced contractual situations from coming into being by limiting the contractual freedom in b2c situations.

40. A third and final strategy concerns the protection against unfair commercial practices.[109] Even when consumers are provided with clear and comprehensible precontractual information and even when no unfair terms are present in the b2c agreement, these two sets of rules do not prevent businesses from seeking recourse to commercial practices that could be labelled as 'unfair'. Certain types of commercial conduct can easily distort consumers' free and well-informed decision-making processes, for instance when presented with false impressions[110] or deceptive interface designs[111] (i.e., dark patterns). When faced with such instances of unfair conduct, additional correction mechanisms are available to consumers in view of prohibiting traders from deploying such commercial practices.[112]

41. The combination of these three facets of consumers protection – pre-contractual information, unfair contract terms, and unfair commercial practices – makes it clear that the focal point of consumer law lies, for the most part, on enabling consumers to make *informed choices.* As such, it refrains from corrective interventions in respect of the range of (competitive) options available to the consumer and

108 Unfair Contract Terms Directive, Art. 6: unfair contract terms are not binding on the consumer; ECJ 4 Jun. 2009, C-243/08 *Pannon.*

109 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L 149/22.

110 ECJ 18 Oct. 2012, C-428/11 *Purely Creative and Others.*

111 For example displaying a countdown timer to claim a special offer, mentioning that an item in your online shopping basket is the last one available, stating that several other potential purchasers are looking at the same item; M. Ebers, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2021, p 209; J. Luguri & L. Strahilevitz, 'Shining a Light on Dark Patterns', *Journal of Legal Analysis* 2021, vol. 13, p 43, doi: 10.1093/jla/laaa006; A. Mathur et al., *Proceedings of the ACM on Human-Computer Interaction* 2019, p 1; BEUC, '"Dark Patterns" and the EU consumer law acquis', BEUC Position Paper 2022, p 4, https://www.beuc.eu/publications/beuc-x-2022-013_dark_patters_paper.pdf.

112 Unfair Commercial Practices Directive, Art. 5: unfair commercial practices are prohibited; ECJ 29 Nov. 2011, C-453/10 *Pereničová.*

gives no consideration either to the wider implications of certain choices apropos the fundamental right to data protection.

42. In the author's view, the protection principles that underpin consumer law are insufficient to efficaciously preserve consumer-citizens' interests in the age of AI. Even though novel legislative changes are underway in the form of a proposal for an AI Act[113] and the Digital Services Act,[114] consumer law alone is not up to the challenge to cope with the ongoing digital transformation. Instead, the pursuit of adequate consumer protection requires a much broader view where other values are considered as well. A high level of consumer protection can only be achieved through means of interactions between different branches of law: data protection law when personal data are at stake, competition law when consumer choice comes under attack, and consumer law when commercial conduct puts strain on consumer autonomy (see Figure 2). Several scholars subscribe to the same view, which arguably serves as an indication that discussions on whether consumer law, competition law, and data protection law *should* be applied concurrently are ending,[115] and that the question should shift towards *how* coherent concurrent application can be achieved.[116] The next section provides further guidance on how these interactions could be shaped.

---

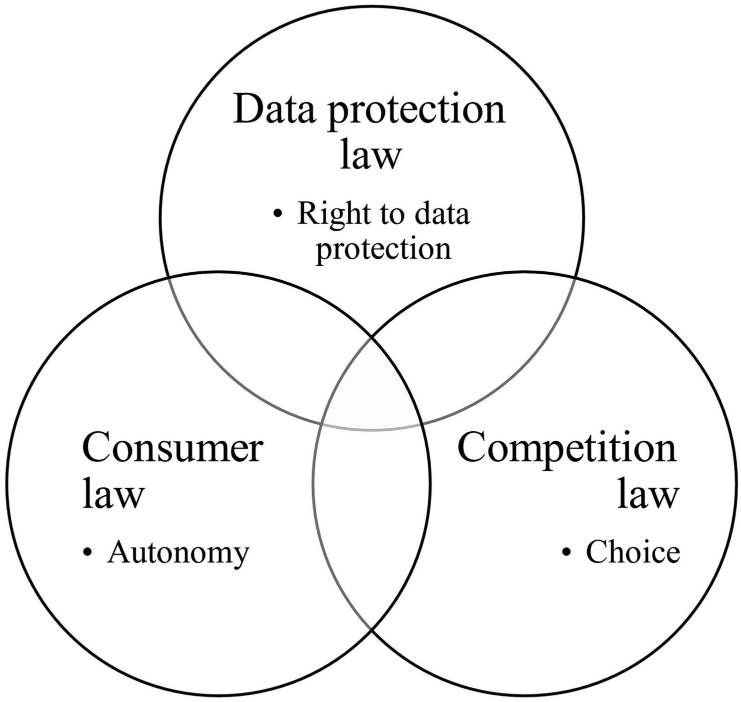
113 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2021] COM(2021) 206 final; the proposed Artificial Intelligence Act acknowledges that AI can manipulate consumers and, thus, puts forward a number of initiatives to improve consumer protection in situations where AI systems are deployed (e.g., prohibiting certain forms of AI systems, imposing conformity assessments, enforcement checks and transparency obligations). In doing so, the draft text demonstrates a clear desire to move away from the regulatory status quo.

114 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1; the Digital Services Act predominantly aims to modernize the current liability regime for online intermediaries and, to that end, subjects intermediary service providers to extensive transparency obligations. Art. 27 is of note, as it mandates online platforms to set out in their Terms & Conditions the main parameters used in their recommender systems.

115 *Contra* A. Kotsios, 'Paying with Data: A Study on EU Consumer Law and the Protection of Personal Data' (*Uppsala University* 2022), pp 406–410, https://www.diva-portal.org/smash/record.jsf?pid=diva2:1620480, who questions the added value of a combined approach: '*the question is not whether potentially personal data have an economic value, but whether this value is also relevant for consumer law or if there are any reasons for consumer law to regard this value as relevant*'.

116 I. Graef, D. Clifford & P. Valcke, *International Data Privacy Law* 2018, p 200; W. Kerber, *Journal of Intellectual Property Law & Practice* 2016, p 856; N. Zingales, *Computer Law & Security Review* 2017, p 558; M. Botta & K. Wiedemann, *The Antitrust Bulletin* 2019, pp 444–445.

Figure 2. Overview of the possible interactions between consumer law, competition law, and data protection law.[117] *For AI-driven business models, the consumer-data, the competition-data, and the consumer-competition-data intersections are relevant to consider.*



4.2. Intersection Between Consumer, Competition, and Data

4.2.1. Enhancing Consumer Law Through Data Protection Law

43. Consumer law is relevant to consider when contracts are concluded in a b2c setting. With many b2c transactions taking place online nowadays, there is extensive room for entrepreneurs to deploy AI models – such as recommender systems – on e-commerce websites and assorted online platforms.[118] The functionality and accuracy of those models are heavily dependent on the availability of input data. Personal recommendations will be more accurate when more data points about the consumer are available. To quench firms' thirst for data for AI

117 Adopted from EUROPEAN DATA PROTECTION SUPERVISOR, Privacy and competitiveness in the age of big data, p 2.

118 As recalled, AI systems can be used for prospection purposes, for instance by composing a profile of each user.

training purposes, businesses face strong incentives to use broadly worded privacy policies. In addition, analyses of privacy policies also reveal that traders severely underreport the usage of online tracking technologies.[119] Although questionable from a legal perspective, such practices aid in the creation of extensive datasets pertaining to consumers and their shopping behaviour and, moreover, corroborate the shift towards data-driven business models. In these circumstances, it is also apparent that consumer law intersects with data protection law.[120]

44. According to Michiel Rhoen, if a data subject is also a consumer, there is a role to be played by both consumer law and data protection law during the pursuit of a high level of consumer protection.[121] This interaction between 'consumer' and 'data' is necessary to counterbalance, on the one hand, a reduction of the level of data protection enjoyed by individuals and, on the other hand, a shift in terms of informational power from data subjects to data controllers.[122] The starting premise for this counterbalancing exercise is that consumers *contractually* agree to extensive data collection practices, often by accepting the Terms of Service during a website visit. The implication thereof is that consumer law should ensure fair contracting, whilst data protection law ensures fair data processing.[123,124]

45. On balance, the adoption of the GDPR has significantly improved the position of data subjects in digital markets. Nevertheless, it should be borne in mind that data subjects often lack the ability to set limits to data processing activities, given that b2c (data processing) agreements are drafted unilaterally and in non-negotiable terms by data controllers.[125] This aptly explains why scholars are vocal about consent – as it is presently conceptualized – being an inherently flawed mechanism.[126] With the

119 R. Amos et al., 'Privacy Policies over Time: Curation and Analysis of a Million-Document Dataset', *Proceedings of the Web Conference* 2021, p 2, doi: 10.1145/3442381.3450048.

120 M. Nisevic, 'A study on the personal data processing and the UCPD focused on Italy, Germany and the UK', *Maastricht Journal of European and Comparative Law* 2021, vol. 28, p 9.

121 M. Rhoen, 'Beyond consent: improving data protection through consumer protection law', *Internet Policy Review* 2016, vol. 5, p 6, doi: 10.14763/2016.1.404.

122 *Ibid.*, pp 3–4.

123 It is worth emphasizing that data protection law aims to empower data subjects in the context of data processing practices. This sense of empowerment is built on three pillars. Firstly, the lawfulness of processing activities, for instance by asking the data subject's consent. Secondly, the adherence to several core data processing principles, such as fairness and transparency. Thirdly, the stipulation of several data subject rights under the GDPR, including the right of access and the right of erasure.

124 N. Helberger, F. Borgesius & A. Reyna, *Common Market Law Review* 2017, p 1427.

125 ECJ 27 Jun. 2000, C-240/98 to C-244/98 *Océano Grupo Editorial and Salvat Editores*, para. 25: '*the consumer is in a weak position vis-à-vis the seller or supplier, as regards both his bargaining power and his level of knowledge. This leads to the consumer agreeing to terms drawn up in advance by the seller or supplier without being able to influence the content of the terms*'; M. Rhoen, *Internet Policy Review* 2016, p 3.

126 M. Durovic & F. Lech, 'A Consumer Law Perspective on the Commercialization of Data', *European Review of Private Law* 2021, vol. 29, p 712, doi: 10.54648/erpl2021038.

majority of data subjects agreeing to privacy statements without reading them, it is relatively easy to expose consumers to phenomena such as algorithmic profiling and personalized recommender systems, even though the GDPR aims to curb automated processing[127] to some extent via Article 22(1) GDPR.[128]

46. From that perspective, it can be questioned whether consumers genuinely enjoy a sufficient level of autonomy to make well-informed autonomous decisions pertaining to their data protection rights.[129] The risk remains that individuals make choices that are, technically speaking, compliant with rules on data protection, but questionable at best from a consumer law point of view. In other words, there is a non-zero risk that data subjects (unknowingly) make choices that effect their data protection rights beyond what would be desirable, for instance due to a consent gap[130] or a lack of transparency.[131] Can the combined application of consumer law and data protection law assist in alleviating some of these concerns? Legal scholarship indicates that this is indeed the case; consumer law can and should play a role in the context of data processing activities.[132] To that end, three elements must be considered: (1) the provision of information in accordance with the CRD and the GDPR, (2) the scrutiny of unfair contract terms relating to data processing under the UCTD, and (3) the evaluation of commercial data-driven practices in light of the UCPD.

---

127 Consider, for instance, L. Tosoni, 'The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation', *International Data Privacy Law* 2021, vol. 11, pp 161-162, doi: 10.1093/idpl/ipaa024, who argues that Art. 22 GDPR does not contain a general ban on automated individual decision-making, but merely confers a right on data subjects to resist such processing activities; M. Fierens, E. Van Gool & J. De Bruyne, 'De regulering van artificiële intelligentie (deel 1) – Een algemene stand van zaken en een analyse van enkele vraagstukken inzake consumentenbescherming', *Rechtskundig Weekblad* 2021, vol. 25, p 977.

128 Although not the focus of this paper, the availability of other data processing grounds, such as 'necessary for the performance of the contract' and 'legitimate interests', further exacerbates these effects by rendering consent unnecessary altogether in some situations.

129 J. Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy', in A. De Franceschi & R. Schulze (eds), *Digital Revolution – New Challenges for Law* (Munich: Verlag C.H. Beck 2019), pp 25-28.

130 That is a discrepancy between what the consumer intended to consent to and what he or she actually consented to.

131 C. Koolen, *European Data Protection Law Review* 2021, p 186.

132 D. Svantesson, 'Enter the quagmire – the complicated relationship between data protection law and consumer protection law', *Computer Law & Security Review* 2018, vol. 34, pp 30-32, doi: 10.1016/j.clsr.2017.08.003; P. Rott, 'Data protection law as consumer law – How consumer organisations can contribute to the enforcement of data protection law', *Journal of European Consumer and Market Law* 2017, vol. 6, p 113; M. Rhoen, *Internet Policy Review* 2016, p 2.

4.2.1.1. Information obligations

47. Providing information to consumers is a first step in overcoming information asymmetries and closing the knowledge gap that typically exists between consumers and businesses.[133] In this respect, when a b2c agreement involves the processing of personal data, compliance with both the CRD (in the capacity of trader[134]) and the GDPR (in the capacity of data controller[135]) is mandatory.[136] Consequently, consumer law and data protection law stand united as they both underscore the importance of transparency and, to that end, impose a range of information obligations on trader-data controllers.[137]

48. As concerns the GDPR, specific attention goes to providing information[138] about the purposes of the processing activities as well as the legal basis for processing.[139] Following the adoption of the Omnibus Directive,[140] the CRD is now also more attentive to the implications of data-driven market practices.[141] This includes, for instance, a novel obligation to inform consumers about personalized pricing practices[142] and the main parameters used for determining a product's ranking[143] during a search query.[144] It is also worth noting that some of the logic from the CRD extends to the GDPR, including the requirement to supply information in a clear and comprehensible way by virtue of plain and intelligible language.[145]

---

133 Martin Ebers notes that use of AI as such can easily be a source of misunderstanding for consumers due to the opaqueness of those systems: M. Ebers, *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2021, p 210.

134 CRD, Art. 2(2).

135 GDPR, Art. 4(7).

136 Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights [2021] OJ C 525, p 13.

137 For the CRD, see Art. 6; for the GDPR, see Arts 12–14.

138 Note that the GDPR does not preclude the usage of seals and certifications to enable data subjects to quickly assess the level of data protection offered by products or services: GDPR, Recital 100.

139 GDPR, Arts 13(c) and 14(c).

140 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 Nov. 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328/7.

141 CRD, Art. 3: '*This Directive shall also apply where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content*'; Omnibus Directive, Arts. 4(5)-(6).

142 CRD, Art. 6(1)(ea).

143 UCPD, Art. 2(1)(m).

144 CRD, Art. 6a.

145 CRD, Art. 8; GDPR, Art. 12.

49. Yet, the added value of the interaction between both branches of law especially lies with the ability to scrutinize precontractual information obligations involving AI-driven practices pursuant to consumer law, as the provided information forms an integral part of the underlying data processing agreement.[146] As stated in the 2021 *Guidance on the interpretation and application of the CRD*, when a trader-data controller relies on a consumer's consent or any other processing ground – apart from 'necessary for compliance with a legal obligation'[147] – for data processing purposes, the contract at hand will be subject to the requirements of the CRD.[148] Elsewhere, it is also argued that interactions between the CRD and the GDPR create room for considering consumers' individual context when making transactional decisions: since product offerings are personalized, information on how such offers came about in the first place could perhaps also be personalized.[149] Another aspect to consider are the consequences of exercising the right of withdrawal pursuant to Article 9 CRD. Arguably, a termination of a b2c agreement through means of the withdrawal right also implies a withdrawal of the legal basis for data processing.[150] This puts trader-data controllers in a position whether they either need to re-evaluate their processing grounds or discontinue data processing of the consumer-data subject altogether.

4.2.1.2. Unfair contract terms

50. Attaining transparency in itself is not enough, though. Scenarios where data collection practices are inherently unfair should not be overlooked, even when they are contractually agreed upon by the consumer. When contract terms[151] pertain to data processing activities, these provisions are not only caught under the GDPR, but also under the UCTD.[152] As a result, pursuant to the UCTD, any contractual provision '*which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the*

146 Guidance on the interpretation and application of Directive 2011/83/EU, pp 13–14.

147 GDPR, Art. 6(c).

148 Guidance on the interpretation and application of Directive 2011/83/EU, p 14.

149 N. Helberger, F. Borgesius & A. Reyna, *Common Market Law Review* 2017, p 1439.

150 Guidance on the interpretation and application of Directive 2011/83/EU, p 53.

151 Note that Art. 4(2) UCTD contains a carve-out for contract terms that form the main subject matter of the agreement, insofar as these terms are drafted in plain and intelligible language.

152 Some discussion exists whether data can be seen as a counterperformance or payment and whether it is opportune to consider situations involving data processing within the scope of the UCTD. In this respect, see A. Kotsios, Paying with Data, p 310. However, the reader should keep in mind that the UCTD can also find application to contracts where no consideration is specified (such as personal guarantees and security agreements), as confirmed in Case C-74/15, *Tarcău* [2015] ECLI: EU:C:2015:772. Consider also: CMA, 'Unfair contract terms guidance', CMA Guidance document 2015, p 22, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450440/Unfair_Terms_Main_Guidance.pdf.

parties' rights and obligations arising under the contract, to the detriment of the consumer'.[153]

51. Two examples of the interplay between unfair contract terms and data protection can provide more clarity. A first situation involves contract terms that afford trader-data controllers more leeway to deal with a data subject's personal information than permitted by law (e.g., by stating that data transfers are permissible without restrictions).[154] Such provisions will not only give cause for concern under the GDPR, but they are also likely to qualify as 'unfair' in the sense of the UCTD. A second instance concerns consent clauses where data subjects' attention is drawn away from the data processing activities.[155] This may happen, for instance, when small print is ambiguously worded and easy to overlook. In the same vein, requiring data subjects to 'opt-out' of giving their consent cannot be accepted either.[156]

52. On a more general note, Natali Helberger et al. put forward some interesting ideas, such as the ability to interpret the principles of data minimization[157] and purpose limitation[158] of the GDPR in conjunction with the UCTD.[159] Furthermore, the UCTD could also serve as a counterbalancing mechanism in instances where consent is given without much consideration.[160] To corroborate this line of reasoning, these scholars refer to two German injunction proceedings against Facebook[161] and Apple,[162] where it was held that privacy policies and contract terms relating to personal data processing activities must also comply with rules on unfair contract terms.[163]

53. If anything, the resulting interactions demonstrate that the rights and obligations derived from privacy agreements are relevant to consider within the context of the UCTD. In doing so, the UCTD acts as a useful fairness assessment tool for analysing the conditions under which consumers agree to their data being processed. As a result, it offers more flexibility compared to a purely GDPR-based approach, balances situations where data subjects have no genuine ability to set limits to the processing of their personal data, and ensures that data subjects find

---

153 UCTD, Art. 3(1).
154 CMA, 'Unfair contract terms guidance', p 123.
155 *Ibid.*
156 ECJ 1 Oct. 2019, C-673/17 *Planet49.*
157 GDPR, Recital 156 and Art. 5(c).
158 GDPR, Art. 5(b).
159 N. Helberger, F. Borgesius & A. Reyna, *Common Market Law Review* 2017, p 1451.
160 *Ibid.*
161 *Kammergericht*, Urteil vom 22 Sep. 2017-5 U 155/14, *Facebook*; this case was eventually referred to the CJEU for a preliminary ruling (Case C-319/20). See below at para. 57.
162 *Landgericht Berlin*, Urteil vom 30 Apr. 2013-15 O 92/12, *Apple.*
163 N. Helberger, F. Borgesius & A. Reyna, *Common Market Law Review* 2017, p 1452.

themselves in a position where they can understand the practical significance[164] of privacy policies.

4.2.1.3. Unfair Commercial Practices

54. A final aspect to consider is whether data processing activities can also fall under the ambit of the notion 'commercial practice' contained in the UCPD.[165] Commercial practices are understood as all types of conduct that are directly connected with the promotion, sale or supply of a product to consumers.[166] By relying on this definition, it is not far-fetched to argue that the deployment of AI and, more specifically, the processing of personal data for personalized advertising and product recommendation purposes qualify as commercial practices in the sense of the UCPD.[167] As a result, this would open the door to assess the fairness of the commercial conduct at hand. This view is also put forward in the 2021 *Guidance on the interpretation and application of the UCPD*: '*A trader's violation of the GDPR or of the ePrivacy Directive will not, in itself, always mean that the practice is also in breach of the UCPD. However, such privacy and data protection violations should be considered when assessing the overall unfairness of commercial practices under the UCPD, particularly in the situation where the trader processes consumer data in violation of privacy and data protection requirements,* i.e., *for direct marketing purposes or any other commercial purposes like profiling, personal pricing or big data applications*'.[168]

55. A ruling by the Italian Competition Authority (ICA) against Facebook also supports this view. In particular, the ICA held that conduct qualifies as misleading when Facebook allows users to register an account on its platform without timely

164 Case C-61/19, *Orange Romania* [2020] ECLI:EU:C:2020:901, para. 52: '*it is for the data controller to demonstrate that the data subject has, by active behaviour, given his or her consent to the processing of his or her personal data and that he or she has obtained, beforehand, information relating to all the circumstances surrounding that processing, in an intelligible and easily accessible form, using clear and plain language, allowing that person easily to understand the consequences of that consent, so that it is given with full knowledge of the facts*'; ECJ 30 Apr. 2014, C-26/13 *Kásler and Káslerné Rábai*, para. 75.

165 UCPD, Art. 2(d).

166 *Ibid.*

167 In support of this view: J. Trzaskowski, *Your Privacy Is Important To Us* (Copenhagen: Ex Tuto Publishing 2021), p 105: '*[the average consumer] must be aware of how personal data are recorded and used for behaviour modification. He must understand his preferences with regard to not only economic decisions, but also decisions relating to how he administers his attention and time in general*'; N. Helberger, F. Borgesius & A. Reyna, *Common Market Law Review* 2017, pp 1454-1456; M. Rhoen, *Internet Policy Review* 2016, pp 7-8.

168 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 C 526, p 19.

and adequately notifying them that their personal data would be used for advertising purposes and, moreover, emphasizing the 'free of charge' nature of the platform via a '*It's free and always will be!*' tagline.[169] The Berlin Court of Appeals arrived at a similar conclusion in its judgment against Facebook. The judgment corroborates that making the availability of a service conditional to consumers' consent to data processing constitutes a transactional decision (*geschäftliche Entscheidung*) under the UCPD.[170] On a more substantive level, the Court objects to the steps used to send friend requests to third parties via the 'Find My Friends'-function and, in addition, takes issue with the inadequate notification on personal data processing during the account registration process.[171]

56. All in all, granting consent for the purposes of personalized product recommendations or advertisements forms an integral part of consumers' ability to make free and autonomous choices. For entrepreneurs, this implies that rules on professional diligence must be considered and that an infringement of data protection law may also trigger a breach of EU consumer law. Admittedly, while the boundary between legitimate persuasion based on personalized advertising and illegitimate coercion by exerting undue influence is sometimes difficult to draw, combining insights from the UCPD and the GDPR would improve the overall positioning of consumers in the context of data-driven market practices.

4.2.1.4. C-319/20 – Meta Platforms Ireland

57. The discussion on whether interactions between consumer law and data protection law are possible, has now largely been settled following the CJEU judgment in *Meta Platforms Ireland.*[172] As highlighted in the Opinion of Advocate General Jean R. De la Tour: '*personal data processing is liable to affect individuals not only in their capacity as natural persons enjoying the rights conferred by [the GDPR] but also in their capacity as consumers*'.[173] As a result, links can be established between infringements of rules on unfair commercial practices or unfair contract terms and infringements of rules on data protection.[174] The

---

169 *Autorita' Garante della Concorrenza e del Mercato*, 24 Jan. 2020 – IP330, *Facebook*; for the press release in English, see *Autorita' Garante della Concorrenza e del Mercato*, 'ICA starts non-compliance proceedings against FB' (*ACGM* 24 Jan. 2020), https://en.agcm.it/en/media/press-releases/2020/1/IP330.

170 *Kammergericht*, Urteil vom 24 Jan. 2014–5 U 42/12, *Facebook*, p 33.

171 *Ibid.*

172 ECJ 28 Apr. 2022, C-319/20 *Meta Platforms Ireland.*

173 ECJ 2 Dec. 2021, C-319/20 *Meta Platforms Ireland*, para. 1.

174 ECJ 28 Apr. 2022, C-319/20 *Meta Platforms Ireland*, para. 66: '*The infringement of the rules intended to protect consumers or to combat unfair commercial practices [...] may be related, as in the present case, to the infringement of the rules on the protection of personal data of those consumers*'.

judgment also underscores that consumer protection associations are entitled to bring legal proceedings for infringements of data protection law on the grounds that some unfair commercial practices and some unfair terms and conditions concerning the processing of personal data, are also liable to affect the rights of consumers.[175] Since the capacity of data subject may coincide with that of a consumer, it indeed seems plausible that rules intended to protect consumers can be relied upon to ensure effective consumer protection against data processing practices. As such, there are clear signs of convergence and complementarity between the protection of consumer rights and the protection of personal data.

4.2.2. *Enhancing Competition Law Through Data Protection Law*

58. It is important to not overlook the effects AI has on the structure of the market and how this subsequently affects consumer welfare. Although data plays a pivotal role in outperforming competitors in AI-driven markets, the welfare effects associated with personalization are not always apparent.[176] By contrast, they entail a risk of exclusion when only select few players have access to personal data.[177] By extension, when a firm maintains a dominant position on a data-driven market, questions may arise as to whether that firm can exert its influence to extend data processing activities beyond what is necessary for the purpose of making a certain product available to end users. Thus, given that data may constitute a competitive advantage for firms, it is relevant to study the interaction between competition law and data protection law.

59. Of particular note are situations where consumers are faced with a limited range of substitutable choices for a given product. In such instances, dominant undertakings essentially maintain a position where they can de facto force users to consent to data processing when no substitutable, less privacy-intrusive products are available to choose from.[178] As a result, questions on the validity of consent arise. When firms make the use of a product conditional on granting permission to process personal data and when consumers have no genuine ability to rely on a competitor-data controller for the delivery of that product, the question arises whether consent is truly freely given and whether it forms an accurate representation of that consumer's right to self-determination.[179] The consumer is essentially

175 ECJ 28 Apr. 2022, C-319/20 *Meta Platforms Ireland*, para. 83; see also ECJ 29 Jul. 2019, C-40/17 *Fashion ID*, para. 63.

176 C. Ruers & L. Hovhanisian, *Tijdschrift voor Consumentenrecht en handelspraktijken* 2022, p 10.

177 M. Bourreau, A. de Streel & I. Graef, 'Big Data and Competition Policy: Market Power, Personalised Pricing and Advertising', CERRE Project Report 2017, p 8, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920301.

178 I. Graef, D. Clifford & P. Valcke, *International Data Privacy Law* 2018, pp 210-211.

179 *Ibid.*

presented with a false dilemma: either consent to data processing and have the ability to enjoy services rendered, or withhold consent and be left empty-handed altogether. Therefore, in applying competition law, attention should also be given to how market power is used for the purposes of data processing.

60. However, the question on integrating data protection values within competitive assessments is not without controversy.[180] The predominant argument is, again, that both branches pursue different objectives.[181] However, many scholars are vocal about an approximation between these two branches.[182] As purported elsewhere, overlaps exist in that they both aim to improve consumer welfare and remedy power asymmetries.[183] This turns the discussion to the *how to*-question. The answer to this question relies on the understanding that an infringement of rules on data protection can also be indicative of exploitative or exclusionary conduct, which is harmful to consumer welfare. From that point onwards, it is not a matter of attempting to extend consumer welfare to non-economic values but, instead, to evaluate how data protection principles could be reconciled with the internal logic of competition law.[184] To that end, at least two different theories of consumer harm are available: (1) seeing data as a price parameter for competition, and (2) seeing data as a quality parameter for competition.

4.2.2.1. Data as a price parameter for competition

61. Pursuant to traditional competition law rationale, when markets offer no real choice to consumers, dominant firms can exploit their customers by means of charging above-competitive prices.[185] In digital markets, however, many products are offered 'free of charge', which, at first sight, renders discussions on excessive

---

180 A. Gorecka, 'A Confusing Relationship between Privacy and Competition Law – A Way Forward for EU Competition Law and Algorithms Pricing', *Indian Journal of Artificial Intelligence and Law* 2020, vol. 1, p 23; M. Botta & K. Wiedemann, *The Antitrust Bulletin* 2019, p 434; O. Lynskey & F. Costa-Cabral, 'Family ties: The intersection between data protection and competition in EU law', *Common Market Law Review* 2017, vol. 54, pp 12–14, doi: 10.54648/COLA2017002.

181 See above at para. 28.

182 See among others, A. Witt, 'Facebook v. Bundeskartellamt – May European Competition Agencies apply the GDPR?', *TechREG Chronicle* 2022, p 2: '*In the age of data-based business models, it is unhelpful to look at competition and privacy issues in isolation*'; K. Wiedemann, 'Data Protection and Competition Law Enforcement in the Digital Economy: Why a Coherent and Consistent Approach is Necessary', *IIC – International Review of Intellectual Property and Competition Law* 2021, vol. 52, p 915, doi: 10.1007/s40319-021-01090-6; I. Graef, D. Clifford & P. Valcke, *International Data Privacy Law* 2018, p 200; O. Lynskey & F. Costa-Cabral, *Common Market Law Review* 2017, p 49: '*data protection concerns should matter for the application of competition law*'; H. Kalimo & K. Majcher, *European Law Review* 2017, p 231.

183 O. Lynskey & F. Costa-Cabral, *Common Market Law Review* 2017, p 14.

184 *Ibid.*

185 R. Whish & D. Bailey, *Competition law* (Oxford: Oxford University Press 2021), pp 756 et seq.

pricing moot. Yet, the reality is that undertakings are not necessarily charging prices in monetary terms, but rather in terms of personal data.[186] Hence, intuitively speaking, consumers are paying with their personal details. This opens the discussion on whether the price calculus used for anticompetitive conduct involving excessive pricing can also be applied to data.[187]

62. Offering a product for free on the market in return for being allowed to collect personal data from users is not problematic in itself. If consumers are happy with the services rendered in return for sharing their personal information, paying a price in 'data' is not particularly revolutionary. If anything, it confirms the view that data is increasingly becoming a tradable commodity.[188] However, if the range of products to choose from is limited, this also ties into the possibility to apply competitive theories on excessive pricing to data-driven conduct. When a price expressed in data is not 'fair' in comparison to the product received, it may be possible to capture such conduct under EU competition law. Especially when a dominant firm leverages its position to extract more personal information than necessary to deliver a certain product, this may become problematic for competition law and, moreover, trigger questions considering the principles of data minimization and purpose limitation.

63. From a practical point of view, the finding of an excessive price requires, as a prerequisite, a suitable methodology to valuate data.[189] In this respect, the OECD has put forward some noteworthy calculation methods.[190] Prominent strategies either revolve around a market-based or individual valuation of data. As to the former, one may consider, for instance, the net income a firm is able to acquire per data record. Meta's quarterly earnings report affords us a good example: on average, Meta is able to extract USD 40.96 per user on Facebook in 2021.[191] As concerns the latter, one may also consider the willingness-to-pay for individuals

---

186 M. Gal & D.L. Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement', *Antitrust Law Journal* 2016, vol. 80, p 7.

187 E. Deutscher, 'How to measure privacy-related consumer harm in merger analysis? A critical reassessment of the EU Commission's merger control in data-driven markets', EUI Working Paper LAW 2018/13, 2018, p 13, https://cadmus.eui.eu/bitstream/handle/1814/58064/WP_2018_13.pdf.

188 A. De Franceschi & M. Lehmann, 'Data as Tradeable Commodity and New Measures for Their Protection', *Italian Law Journal* 2015, vol. 1, p 51.

189 A. Gorecka, 'Defining Privacy in the Competition Law Sphere', SSRN Scholarly Papers 2021, p 10, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3937387.

190 OECD, 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value', OECD Digital Economy Papers 2013 No 220, pp 18 et seq., http://dx.doi.org/10.1787/5k486qtxldmq-en.

191 Meta, 'Meta Earnings Presentation Q4 2021' (*Meta – Investor Relations* 2 Feb. 2022), p 15, https://s21.q4cdn.com/399680738/files/doc_financials/2021/q4/Q4-2021_Earnings-Presentation-Final.pdf.

to *not* share their data as a benchmark. At present, however, there is no agreement on what the most suitable valuation method for personal data would be and, thus, how to measure consumer harm when a monopoly price is set in data. As a result, it is a worthwhile endeavour to explore other avenues to match competition law with data protection.

4.2.2.2. Data as a quality parameter for competition

64. Following the difficulties faced when attempting to assess the economic value data adds to an undertaking, other strategies have surfaced as well. Another leading approach is that data protection could also be perceived as a quality parameter for competition.[192] According to this view, data protection is something valuable in itself. This suggests that poor levels of data protection can or should be perceived as a degradation of quality of the product under consideration.[193]

65. Many consumers are likely 'privacy pragmatists' i.e., they have a pragmatic attitude towards data protection.[194] Hence, when a particular product offers useful functionality to users, it may be worthwhile to sacrifice some degree of personal data in order to benefit from the product's advantages. Consumers would thus have to weigh the benefits originating from data-driven practices against the associated reduction in terms of data protection.

66. Recent developments in the realm of communication apps afford us a good example of these intricacies. In 2021, popular messaging app WhatsApp announced that it would introduce novel changes to their privacy policy, which would allow the app to share personal data with its parent company Meta (previously known as Facebook).[195] From then onwards, information such as personal

---

192 E. Deutscher, How to measure privacy-related consumer harm in merger analysis?, p 11; O. Lynskey & F. Costa-Cabral, *Common Market Law Review* 2017, p 27; European Data Protection Supervisor, 'Opinion on coherent enforcement of fundamental rights in the age of big data', EDPS Opinion 8/2016, 2016, p 13, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.

193 O. Lynskey & F. Costa-Cabral, *Common Market Law Review* 2017, p 27.

194 N. Draper, 'From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates', *Policy & Internet* 2017, vol. 9, p 232, doi: 10.1002/poi3.142.

195 X, 'Messaging services: Global grapevines', *The Economist* 2021, vol. 438, iss. 9229, pp 50-51: '*Facebook announced a revision to WhatsApp's terms of service which many took to mean that their personal data would be used for a wider range of purposes. The result was a rush to download Telegram and Signal, two apps with much smaller user bases – around 500m for Telegram, far fewer for Signal – which market themselves on promises of enhanced privacy. Between January 6th and 19th Signal was downloaded 45m times and Telegram 36m, according to Sensor Tower, a provider of data. Pavel Durov, Telegram's boss, called it the "largest digital migration in human history"*'; X, 'Answering your questions about WhatsApp's January 2021 Privacy Policy update' (*WhatsApp* 4 Jan. 2021), https://faq.whatsapp.com/general/security-and-privacy/answering-your-questions-about-whatsapps-privacy-policy/?lang=en.

contact details, metadata pertaining to conversations, microphone recordings, location data, ... would be forwarded to Meta. WhatsApp's privacy policy indicates that data sharing would help you '*complete purchases and transactions*' and enable the company to show you '*relevant offers and ads across the Meta Company Products*'.[196] Users unwilling to accept these novel Terms of Service, were prevented from using WhatsApp. The result of these privacy changes was a massive exodus among WhatsApp users to several other communication apps, notably Signal[197] and Telegram.[198] These two apps were able to capture the attention of the public due to their privacy-friendly nature compared to WhatsApp.[199]

67. In applying this reasoning, the level of data protection offered via a product thus forms part of the product's overall value proposition.[200] Under competitive market circumstances, when companies introduce drastic privacy changes, this may trigger some consumers to switch to a competitor-product. This also seems logical from a supply and demand point of view: when demand for privacy-oriented products exists, such products would logically come into being, barriers to market entry permitting. Vice versa, in the face of limited product substitutes, reduction in terms of data protection may, as a quality dimension under competition law, equate to consumer harm.[201]

4.2.2.3. Data as a competitive advantage

68. Although not directly consumer-oriented, it must also be considered that data can serve as an input that is necessary for competition.[202] Firms in possession of vast datasets will evidently be inclined to use the acquired information to gain an edge over their competitors. Once firms find themselves in a position where they can collect large quantities of data, strong feedback loops are formed: more data implies more accurate predictions, which attracts more customers. More customers yield more data, and thus contribute to even better predictions. In other words, firms benefitting from market power are likely to maintain their foothold in the

196 X, 'WhatsApp Privacy Policy' (*WhatsApp* 4 Jan. 2021), https://www.whatsapp.com/legal/privacy-policy/?lang=en (note that users located in the EEA may automatically be directed to a different version of this privacy policy due to the applicability of the GDPR).

197 See https://signal.org/en/: '*Say "hello" to a different messaging experience. An unexpected focus on privacy, combined with all of the features you expect*'.

198 See https://telegram.org/.

199 Note, however, that some of the disadvantages of truly private apps soon became apparent. For instance, users were missing out on functions that heavily relied on personal data (e.g., location sharing). As a result, some users have switched back to WhatsApp over time.

200 Case M.7217, *Facebook/Whatsapp* [2014] C(2014) 7239 final, p 15.

201 Case M.8124, *Microsoft/LinkedIn* [2016] C(2016) 8404 final, pp76–77.

202 I. Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Alphen aan den Rijn: Kluwer Law International 2016), pp 152–153.

market via continuous data aggregation. From the perspective of a novel potential competitor, however, not having access to data corresponds to a barrier to market entry. Under the right circumstances, when a dominant firm refuses to grant a competitor-firm access to data, such conduct may generate market foreclosure effects and, pursuant to the essential facilities doctrine, amount to an abuse of dominance.[203] This illustrates that competition law and data protection law also interact with one another when firms are fully dependent on other undertakings' data assets in view of competing on the market and expanding the range of product choices to consumers.

69. While the topic of *data as essential facility* has been extensively covered by Inge Graef, this situation also ties into a peculiar subset of problems: is a dominant undertaking entitled to justify a refusal to grant access to data by asserting that this would entail an infringement of data protection obligations?[204] At present, these discussions have surfaced in a number of cases before NCAs. For instance, in *GDF Suez* the French competition authority held that data could be shared to increase the competitive structure on the market for gas suppliers, but that data subjects can opt-out of their data being shared with other gas suppliers.[205] Another illustrative judgment, also rendered by the French competition authority, concerns Apple's newly imposed App Tracking Transparency (ATT) policy.[206] In essence, the ATT policy is a standardized framework through which owners of Apple devices must explicitly indicate how third-party apps can make use of their personal data, thereby essentially raising the barrier to collect personal data. App developers brought a case against Apple on the grounds that the ATT policy raised suspicions of self-preferencing whilst also impairing third-party apps in the course of their data processing activities. However, the French competition authority held that the ATT standardized consent framework was not likely to impose excessive or disproportionate restrictions on the activities or third-party app developers.[207] The newly introduced transparency policy was not found to be inherently unfair but, instead, fell squarely in line with Apple's overarching objective to protect iOS users' privacy.[208] Interestingly, as of June 2022, a new case on Apple's tracking rules for

---

203 *Ibid.*

204 I. Graef, D. Clifford & P. Valcke, *International Data Privacy Law* 2018, p 221; nowadays, some further guidance on this topic can be found in the Proposal for a Data Act. A close reading of the proposed Art. 1(3) Data Act suggests that data sharing practices for the purpose of competition should not frustrate data subjects' fundamental rights, even if this would imply creating a barrier to market entry.

205 *Autorité de la concurrence*, Décision n° 14-MC-02, *GDF Suez* [2014] p 52; while understandable from one point of view, it has been argued that consent would arguably have been a more appropriate processing ground.

206 *Autorité de la concurrence*, Décision n° 21-D-07, *Apple* [2021] p 37.

207 *Ibid.*, p 4.

208 *Ibid.*

third-party apps is pending before the *Bundeskartellamt* (German Federal Cartel Office).[209]

70. All things considered, when assessing the intersection between competition law and data protection law, the main finding is that a combined approach strengthens the positioning of data subjects by putting them in a position to decide for themselves with whom to share their personal data with. At the same time, concepts such as 'data portability' and 'interoperability' prevent scenarios where firms lock in consumers and lock out competitors by means of having access to data. In doing so, the goal remains to offer data subjects an ability to switch to a competitor-firm and transfer their personal data, thus ensuring a genuine range of choices to pick from.

4.2.3. The Consumer-Competition-Data Triad

71. In some situations, firms engage in data processing activities that are both unfair and anticompetitive. Under those circumstances, market conduct is capable of triggering questions under consumer law, competition law, and data protection law, which suggests the need to consider the intersection between all three branches of law.[210] In analysing this intersection, one quickly arrives at the conclusion that it revolves around situations where competition is limited and, thus, consumers face a rather limited range of substitutable data-driven products to choose from. This subsequently creates an opportunity for dominant undertakings to exploit consumers by imposing either unfair terms or by deploying unfair commercial practices pertaining to data processing.[211]

72. The variety among the conditions of application for each legal branch ensures that this category is quite limited in terms of its scope.[212] The 2019 *Facebook* decision by the *Bundeskartellamt* is arguably the most well-known case that meets all the substantive criteria to fall within this intersection.[213] At the core of the dispute were Facebook's Terms & Conditions, which were drafted in such a way that users signing up for the social media platform also had to agree to Facebook collecting their personal data via third-party websites.[214] In its decision, the German Federal Cartel Office held that Facebook abused its market power for the

209 X., 'Bundeskartellamt reviews Apple's tracking rules for third-party apps' (*Bundeskartellamt* 14 Jun. 2022), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html.

210 I. Graef, D. Clifford & P. Valcke, *International Data Privacy Law* 2018, pp 210-211.

211 As explained above, it concerns either significantly imbalanced privacy policy terms, or misleading or aggressive data processing practices.

212 As to the conditions of application of each legal domain, see above at para. 33.

213 *Bundeskartellamt*, B6-22/16, *Facebook* [2019] pp 1-2.

214 *Ibid.*

purpose of extending the collection, usage and merger of data from users on its platform beyond what would be possible under normal, competitive market conditions.

73. The novelty of the *Facebook* decision especially lies in the finding of an infringement of competition and unfair trading law for a violation of rules on data protection; rules which were, prior to the decision, deemed beyond the scope of competition law.[215] For that reason, the decision has attracted a lot of attention in scholarly literature.[216] Given that the *Bundeskartellamt* redefines the connection between consumer, competition, and data, it is a worthwhile endeavour to dive into the decision's substantive ideas. In doing so, it becomes apparent how abusive and unfair conduct can – and arguably should – be rethought of in view of introducing a higher degree of fairness in the relationship between competitor-data controllers and consumer-data subjects.

74. At the outset, it is noted that the issue at stake in *Facebook* revolves around the tech firm impeding data subjects in autonomously deciding what personal data can be processed.[217] Given Facebook's dominant position on the market for social media platforms,[218] such conduct may qualify as an exploitative abuse in the sense of Article 102(a) TFEU as it involves imposing 'unfair trading conditions' on data subjects. This steers the discussion towards the meaning of (un)fairness in this context.[219] Case law suggests that trading conditions are unfair when certain obligations are not necessary for the performance of the main aim of a contract.[220] Equally indicative of unfairness are additional obligations that have no connection with the purpose of the contract.[221] Other cases also make mention of a proportionality dimension, suggesting that situations may qualify as unfair in the absence of a justifiable ratio between the fees charged and the value of a service rendered.[222]

---

215 M. Volmar & K. Helmdach, 'Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation', *European Competition Journal* 2018, vol. 14, p 195, doi: 10.1080/17441056.2018.1538033.

216 Consider, among others, A. Witt, *TechREG Chronicle* 2022, p 1; M. Botta & K. Wiedemann, *The Antitrust Bulletin* 2019, p 428; M. Volmar & K. Helmdach, *European Competition Journal* 2018, p 195; Meta itself has been rather critical of the Bundeskartellamt's decision: X, 'Why We Disagree With the Bundeskartellamt' (*Meta Newsroom* 7 Feb. 2019), https://about.fb.com/news/2019/02/bundeskartellamt-order/.

217 M. Volmar & K. Helmdach, *European Competition Journal* 2018, p 200.

218 *Bundeskartellamt*, B6-22/16, *Facebook* [2019] pp 5–7.

219 M. Volmar & K. Helmdach, *European Competition Journal* 2018, pp 201–202.

220 ECJ 27 Mar. 1974, C-127/73 *BRT/SABAM*, para. 15.

221 Commission Decision IV/31043, *Tetra Pak II* [1991] OJ L 72, para. 107.

222 ECJ 24 May 2007, T-151/01 *Duales System Deutschland* v. *Commission*, para. 121.

75. When considering these elements in relation to one another, there is a convincing argument to be made that conduct involving data processing may qualify as anticompetitive, unfair, or both pursuant to consumer law (i.e., the UCTD and the UCPD) and/or competition law (i.e., Art. 102(a) TFEU). In light of the increasing levels of AI-driven personalization (and the risks that this entails), an expansionist view on consumer protection adds to the objective of safeguarding not only consumers' economic rights, but also their right to self-determination as consumer-citizens within our society.

5. Conclusion

76. Traditional conceptions of consumer law predominantly focused on protecting weaker contract parties against more powerful undertakings. Over time, however, consumer law rules were expanded to pave the way for a right to self-determination: consumers purchase certain goods or services because they have had the opportunity to reflect upon its worth and value in an autonomous manner. A purchase decision is thus an expression of true choice or volition on behalf of the consumer. The introduction of AI signifies shift in legal thinking on this topic. Consumers do no longer act autonomously, but increasingly rely on AI to facilitate purchase decisions. For such algorithmic consumers, the main task for consumer law is now to ensure the protection of the weaker contract party yet again, since commercial AI systems are at liberty to not only promote consumers' interests, but also pursue undertakings' for-profit goals.

77. In light of these evolutions, this contribution assessed the implications of AI on EU consumers. While offering noticeable advantages in some cases, concerns remain about AI inciting consumers to make transactional decisions which they would not have taken otherwise. In some instances, AI puts strain on the notion of consumer autonomy when the AI system presents the consumer with a personalized selection wherein not all alternative purchase options are listed. In other instances, AI is said to deceive consumers when recourse is sought to subliminal manipulation techniques.

78. Although an extensive body of rules exists that finds application to b2c AI interactions, the current legal framework is not sufficiently adapted to protect consumers against the potential harms of AI. In this respect, it was found that AI practices traverse through different legal domains, notably consumer law, competition law, and data protection law. Legal thinking, however, often resorts to a silo-based approach. Such silo-based thinking results in a failure to effectively protect consumers in the face of AI-driven business models.

79. From that perspective, it is argued that a move away from silo-based thinking is needed and, instead, a more holistic approach towards consumer protection is required. The paper therefore suggests a defence in depth: consumer law enables the autonomous exercise of a choice, which presupposes that competition law

guarantees the availability of a range of different choices, which presupposes that data protection law prevents any choice offered from going against the fundamental right to data protection. Accordingly, the protection provided by one branch complements the protection enjoyed by a different branch, which eventually leads to consumer protection in a broad sense; consumer protection that is fit for Europe's transition towards the age of AI.