EU consumer law meets digital twins

Diana Mocanu and Anne-Lise Sibony***

Abstract

This article contributes to the unfolding scholarly and policy conversation on regulating AI-powered personalisation practices from the vantage point of consumer protection. We borrow the notion of 'digital twins', originally a technical notion, to refer to AI-powered digital projections of real consumers created for the purposes of personalisation. We explore the mismatch between this very granular, data-rich digital representation of consumers and the very general and abstract legal representation of consumers expressed in the average and vulnerable consumer standards. We do not claim that law should necessarily track market practices it seeks to regulate or adopt representations that mirror trader's practices. Instead, we find value in exposing the clash between market-made and judge-made images of consumers and the consequences that may ensue. The existing and forthcoming EU regulatory response to personalisation is then evaluated and several perspectives for change are presented in the aim of empowering consumer protection against the pitfalls of surveillance capitalism. In this enquiry, we consider the UCPD, GDPR, DSA, DMA, the draft AI Act, and the draft Data Act.

Keywords: Artificial intelligence (AI) – personalisation – consumer law – data harvesting – surveillance capitalism – digital minimalism – unfair commercial practices – UCPD – GDPR – DSA – DMA – AI Act – Data Act.

I. – Introduction

It is ever more common for traders to use Artificial Intelligence (AI) to give marketing a boost. Indeed, AI is uniquely potent to distil big data into consumer profiles that change the sales game. Personalisation may have been known to carpet sellers since the advent of carpets, but AI radically modifies the scale, granularity,

* Diana Mocanu is boursier FRESH of the Fonds National de Recherche Scientifique (FNRS), Belgium and doctoral student at the Centre for Philosophy of Law (CPDR) of the Institute for Interdisciplinary Research in Legal Sciences (JUR-I) of Université catholique de Louvain, Belgium, diana.mocanu@uclouvain.be.

** Anne-Lise Sibony is Professor of European Law at the Université catholique de Louvain, Belgium, anne-lise.sibony@uclouvain.be.

The authors would like to thank Géraldine Amory for her research assistance.

and pervasiveness of personalisation. The challenge this represents for consumer protection has attracted attention from scholars,[1] stakeholders,[2] and policymakers.[3] It has prompted the Commission to revise UCPD Guidelines[4] and undertake a more thorough reassessment of consumer law. Indeed, a second REFIT of consumer law was launched in March 2022,[5] only five years after the previous one was concluded,[6] with personalisation as a specific point of attention, which attests to the current concern.[7]

It is not yet fully clear how this challenge is best conceptualised or addressed. This article seeks to contribute to the unfolding scholarly and policy conversation on regulating personalisation practices. It repurposes the notion of "digital twins",

1 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 – Final Report of the ARTSY Project", *SSRN Scholarly Paper*, Rochester, NY, 2018; U. Kohl, "The Pixelated Person – Humanity in the Grip of Algorithmic Personalisation", in U. Kohl and J. Eisler, *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge, *Cambridge University Press*, July 2021, pp. 1-25; N. de Marcellis-Warin *et al.*, "Artificial Intelligence and Consumer Manipulations: From Consumer's Counter Algorithms to Firm's Self-Regulation Tools", *AI and Ethics*, 2, No. 2, May 2022, pp. 259-268; J. Laux *et al.*, "The Concentration-after-Personalisation Index (CAPI): Governing Effects of Personalisation Using the Example of Targeted Online Advertising", *Big Data & Society*, 9, No. 2, 1 July 2022, 20539517221132536; E. Thelisson and M. Ho-Dac, "Le consommateur européen face à l'intelligence artificielle – Quel cadre règlementaire au sein du Marché unique numérique ? (The European Consumer and Artificial Intelligence – What Regulatory Framework within the Digital Single Market'?)", in M. Combet, *Le droit européen de la consommation au XXIe siècle: état des lieux et perspectives*, 2022, https://hal.science/hal-03639993 (accessed 23 January 2023).

2 BEUC, EU Consumer Protection 2.0 – Structural asymmetries in digital consumer markets, Brussels, March 2021; BEUC, "The Regulatory Gap: Consumer Protection in the Digital Economy Addendum to the report 'Structural asymmetries in digital consumer markets'", Brussels, December 2021.

3 European Parliamentary Research Service and Hendrik Mildebrath, Unpacking "commercial surveillance": The state of tracking, PE 739.266 – December 2022.

4 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, *OJEU*, 29 December 2021, C 526/1; European Commission, produced by European Innovation Council and SMEs Executive Agency (EISMEA) on behalf of the Directorate-General for Justice and Consumers, Directorate E – Consumers, Unit E.2 – Consumer and marketing law, F. Lupiáñez-Villanueva *et al.*, "Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation", April 2022.

5 Digital fairness – fitness check on EU consumer law (examining the continued fitness for purpose of the Unfair commercial practices Directive, the Consumer rights Directive, and the Unfair terms Directive, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en, (accessed 5 January 2023).

6 A regulatory fitness check reviewing the fitness of purpose of 8 consumer law directives was finalised in 2017. The reports are available at https://ec.europa.eu/newsroom/just/items/59332/en (accessed 5 January 2023).

7 The REFIT "will examine the adequacy of the existing EU rules in dealing with consumer protection issues such as, but not limited to, consumer vulnerabilities, dark patterns, *personalisation practices*, influencer marketing, contract cancellations, subscription service contracts, marketing of virtual items and the addictive use of digital products" (emphasis added). Commission's call for evaluation Ref. Ares (2022)3718170 of 17 May 2022, p. 1.

originally a technical notion,[8] to refer to AI-powered digital projections of real consumers created for the purposes of personalisation. This new consumer figure, pieced together by traders, is as far removed as conceivable from the "average consumer" and other images of consumers present in the law.[9] This mismatch raises the question of whether the law as it stands is well suited to protect consumers against the risks and harms of AI-powered personalisation and commercial surveillance practices in use.

To explore this mismatch and its consequences, Part II further explains and situates the notion of "digital twin", Part III confronts it with the representations of consumers embedded in EU consumer law, in particular the average consumer standard. It shows that the two images are in tension on several counts. While law needs not necessarily mimic the market reality it seeks to regulate, the consumer *acquis* does seem insufficient to protect consumers against harmful personalisation. Indeed, new rules adopted for the digital sector (DMA, DSA, Draft Data Act and Draft AI Act) bear on this issue. These rules do not only or primarily aim to protect consumers, but they nonetheless express the EU regulatory response to personalisation. Part IV analyses them from this perspective. Part V briefly discusses the untapped potential of some regulatory options before concluding.

II. – Digital twins

As Kohl *et al.* note, predicting the behaviour of human actors is not only the most fascinating but also the most profitable subject of predictive algorithms.[10] Indeed, profiling has for this reason, become ubiquitous. As a result, the mass production of digital twins or "pixelated persons"[11] has become one of AI's main uses, as well as a market reality that EU consumer law needs to reckon with. This automated production of machine-readable data aggregates is an indispensable intermediary step of automated personalisation, whether personalisation concerns ads, search results, prices, online interfaces, or any other aspect of our digital lives.[12]

---

8 A. STANFORD-CLARK *et al.*, "What Are Digital Twins?" *IBM Developer*, https://developer.ibm.com/articles/what-are-digital-twins (accessed 23 January 2023); "Cheat Sheet: What Is Digital Twin? Internet of Things Blog", *IBM Business Operations Blog*, 4 December 2020, https://www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/ (accessed 23 January 2023).

9 We borrow this apt terminology from Dorota Leczykiewicz and Stephen Weatherill, see D. LECZYKIEWICZ and S. WEATHERILL (eds), *The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law*, Oxford; Portland, Oregon, Hart Publishing, 2016.

10 U. KOHL, "The Pixelated Person – Humanity in the Grip of Algorithmic Personalisation", in U. KOHL, and J. EISLER, *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge, Cambridge University Press, July 2021, pp. 1-25.

11 *Ibid.*

12 H MILDEBRATH, "European Parliamentary Research Service, Unpacking 'commercial surveillance': The state of tracking", December 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739266 (accessed 23 January 2023).

Profiling is often based on "web usage mining" and "driven by the secondary (mis-)use of traces that people leave behind while surfing on the Internet".[13] Personalisation, therefore, can occur without the express consent or even the awareness of the concerned person. It is primarily derived from behavioural data, which consists of information passively recorded through user logins, cookies, and server logs.[14] In addition, biometric data is also sometimes used to detect relevant patterns that allow the identification of a person and their habits or preferences.

With the help of machine learning,[15] this information is aggregated into so-called "persuasion profiles".[16] Virtually all aspects of human life are contained in these profiles, from shopping, food, and entertainment preferences to networks of friends, relationships, other aspects of social life, health, physical movements, driving habbits or sports-related activities. In the case of behavioural biometric profiling, the profiles are inferred from data collected by sophisticated sensor technologies that record, store and aggregate machine-readable data about behaviours like speech, facial expression, key-stroke, gait, gesture, voice and handwritten signatures, blood pressure, heart rate or sleeping patterns.[17] An overwhelming range of the preferences, responses and behaviours of EU consumers themselves are thus aggregated into profiles, the profitability of which resides in their capacity to predict and subsequently influence buying choices.

---

13 *Ibid.*

14 M. Crossley, N.J. Kings and J.R. Scott, "Profiles – Analysis and Behaviour", *BT Technology Journal* 21, No. 1, 1 January 2003, pp. 56-66, as cited by S. van der Hof and C. Prins, "Personalisation and its Influence on Identities, Behaviour and Social Values", in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, New York, Springer, 2008, pp. 111-127.

15 Machine learning (ML) is a specific branch of AI, applied to the resolution of specific and limited problems - such as classification or prediction tasks. Unlike some other types of AI that try to distil human experience (*e.g.* expert systems), the behaviour of machine learning systems is not defined by a predetermined set of instructions. ML models are trained using datasets. During their training, ML systems adapt autonomously to the patterns found among the variables in the given dataset, creating correlations. Once trained, these systems will use the patterns learned to produce their output. Therefore, the performance of ML models depends greatly on the accuracy and representativeness of training data. See *AEDP-EDPS Joint paper*, "10 misunderstandings about machine learning", 20 September 2022, https://edps.europa.eu/data-protection/our-work/publications/papers/2022-09-20-aepd-edps-joint-paper-10-misunderstandings-about-machine-learning_en (accessed 23 January 2023).

16 M. Kaptein *et al.*, "Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles", *International Journal of Human-Computer Studies* 77, 1 May 2015, pp. 38-51,. See p. 41 for the following definition of persuasion profiles: "collections of estimates of the expected effects of different influence principles for a specific individual. Hence, an individual's persuasion profile indicates which influence principles are expected to be most effective".

17 A Yannopoulos, V. Andronikou and T. Varvarigou, "Behavioural Biometric Profiling and Ambient Intelligence", in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen, Cross-Disciplinary Perspectives*, New York, Springer, 2008, pp. 89-103.

These "virtual representations of consumers",[18] are what we refer to in the present article as "digital twins".[19] The notion of digital twin is borrowed from the technical domain,[20] where it is commonly used to designate "a virtual representation of an object or system that spans its lifecycle, is updated from real-time data, and uses simulation, machine learning and reasoning to help decision-making".[21] In its strict sense, a digital twin is a perfect digital replica of an entity (object, place) which exists in the real (offline) world. Therefore, the notion is an aspirational one: in reality, digital replicas (be they replicas of cities or, in our case, of consumers) are not perfectly accurate. They can lack depth, depicting only certain facets or characteristics of the entity in question. They can be outdated, albeit for relatively short amounts of time, despite their claim of being updated from real-time data. Anyone who has recently moved from one Member State to another can attest to this from the ads they will have seen online, and which can lag behind, showing offers tailored for the former place of residence. More generally, the data which make up a digital twin can be incomplete or inaccurate for a variety of reasons. It is also conceivable that not all inferences AI makes from the data translate as correct predictions. What the notion of digital twin seeks to capture is the marketing grail of a wholly accurate digital reflection of a real consumer, known to traders in their most intimate details.

The salience of such a concept i.e., digital twin becomes clear when we consider the bigger picture of the digital society and its operation. Auer argues[22] that "the tools of the digital world amount to no less – but also no more – than the structurally

---

18 N. Helberger, O. Lynskey, H.-W. Micklitz, P. Rott, M. Sax and J. Strycharz, "EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets", BEUC-X-2021-018 (hereafter "Consumer Protection 2.0"), p. 6.

19 The concept of "virtual persons" has also been used in this context, but while it is traditionally used to refer to characters in computer games, the term "digital twins" seemed to us more apt at capturing the true nature of what a profile of an EU consumer actually aims to be like, given the central importance of it being based in reality, on true and accurate information about a consumer in order to serve its predictive function well. While we object to the choice of terms, we subscribe to the underlying understanding of virtual persons or, in our case, digital twins, as "a generalisation into a category of a subset of elements sharing one or more correlations with other elements in a predefined class of data used to make a query in a database and which results in a statistical overview of the attributes of this class". See D.-O. Jaquet-Chiffelle, "Reply: Direct and Indirect Profiling in the Light of Virtual Persons", in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, New York, Springer, 2008), pp. 34-43.

20 A. Stanford-Clark *et al.*, "What Are Digital Twins?", *IBM Developer*, https://developer.ibm.com/articles/what-are-digital-twins/ (accessed 23 January 2023); "Cheat Sheet: What Is Digital Twin? Internet of Things Blog", *IBM Business Operations Blog*, 4 December 2020, https://www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/ (accessed 23 January 2023).

21 "Cheat Sheet: What Is Digital Twin? Internet of Things Blog", *IBM Business Operations Blog*, 4 December 2020, https://www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/ (accessed 23 January 2023).

22 M. Auer, "Autonomy and the Digital Person", *Max Planck Law* (blog), 15 January 2023, https://law.mpg.de/perspectives/autonomy-and-the-digital-person/ (accessed 23 January 2023).

congenial tools of modern society, the fulfilment of the technical promise of modernity, which is essentially countable, in a word: *dividual*". Deleuze aptly coined the concept of the countable "dividual" as the core of modern personhood as early as 1992, opposing it to the old individual associated with indivisible autonomy in the classic sense. Traders using AI can now generate a better, more precise representation of the empirical human being as the "product of digital information". If, in Auer's words, "the indivisible quality of the person disappears behind algorithmically generated type profiles, this means that the individual is no longer conceived as indivisible, equal and free, but rather as divisible, calculable, predictable and in that respect unfree". Nowadays, virtually everyone has a double existence, as human being and as data avatars. Virtually all of us have digital twins (we have more than one because several businesses create them).[23] There is thus a sense in which autonomy is restricted in the digital society and the way in which the law reflects this restriction to protect the legal person as a consumer is in question.

In more technical terms, taking direct inspiration from the above, we define digital twins of EU consumers as virtual representations of their behaviour and preferences spanning their (online) lifetime, updated from real-time data, and using simulation, machine learning and reasoning to help traders' decision-making. Because there is generally a measure of mismatch between the represented consumer and her digital representation, we posit that they are not identical twins (if that were even imaginable in the first place). Rather a digital twin consumer constitutes the reflection of a real consumer in the digital mirror. The quality of this mirror depends on the abundance and quality of the data as well as the degree of sophistication of the algorithms it feeds. Thus defined, digital twins present attributes that differ markedly from those of the average consumer and vulnerable consumer, the legal standards on which EU consumer law operates. These legal standards constitute, to continue with the metaphor, reflections of real consumers in the legal mirror, arguably a distorting mirror at that.

III. – Attributes of digital twins and how they relate to the legal standards

Like the average consumer standard and any other legal standard, digital twins are abstractions. Yet, they are abstractions of a very different kind. This section highlights two key differences that are obvious but deserve to be spelt out. The first is to do with how these abstractions relate to facts (A). The second relates to who creates these abstractions (B). The distinction between average and vulnerable consumer standards is not crucial in relation to either of these aspects. Therefore, we do not refer to it

[23] To the best of our knowledge, governments do not work with digital twins of citizens, at least not yet.

systematically. Similarly, we only refer to the targeted consumer standard[24] where significant for our comparison.

A. – Data creatures v. shield against evidence

As is clear from the foregoing, digital twins are composite pictures made of data, lots of data capturing fine-grained digital observations (to use a more neutral term than "surveillance")[25] of consumer behaviour. In contrast, the average consumer is a standard that allows courts to not get mired in empirical facts. It has been called a normative standard to express its original *raison d'être*: in the European Court of Justice (ECJ) case law on free movement, it provides a yardstick against which to assess which national rules protecting consumers could be justified when they constitute obstacles to free movement.[26] If the only rules that can pass the proportionality test are those which are needed to protect a heroic consumer who is 'normally diligent and circumspect', many obstacles to trade will fall foul of the test. Thus, the Court arguably promoted free movement at the expense of realism regarding consumer behaviour.[27]

---

[24] Article 5 b) refers to this standard and Recital 18 of UCPD explains that "Where a commercial practice is specifically aimed at a particular group of consumers, such as children, it is desirable that the impact of the commercial practice be assessed from the perspective of the average member of that group". What we call the targeted consumer standard is the average member of a targeted group. This is a distinct standard from the vulnerable consumer standard to which Article 5.3 refers without any reference to targeting. Recital 19 explains that "Where certain characteristics such as age, physical or mental infirmity or credulity make consumers particularly susceptible to a commercial practice or to the underlying product and the economic behaviour only of such consumers is likely to be distorted by the practice in a way that the trader can reasonably foresee, it is appropriate to ensure that they are adequately protected by assessing the practice from the perspective of the average member of that group".

[25] In Europe, the Norwegian Consumer Council (NCC) uses the term "surveillance-based advertising" in its communications. See the report NCC, "Time to ban surveillance-based advertising – The case against commercial surveillance online", June 2021, https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf (accessed 23 January 2023); In the US, the Federal Trade Commission has also recently employed the term "commercial surveillance" in an announcement stating its intent to explore rulemaking on the subject. The term was used to refer to "the business of collecting, analysing, and profiting from information about people". See "FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices", Federal Trade Commission, 10 August 2022, https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices (accessed 23 January 2023).

[26] This was the case in the seminal case *Gut Springerheide*, case C-210/96, *Gut Springerheide*, EU:C:1998:369 (in this case trademark rules). See more generally, G. Howells, C. Twigg-Flesner and T. Wilhelmsson Rethinking, *EU Consumer Law*, Routledge, 2018, pp. 48-49.

[27] H.-W. Micklitz, "The Expulsion of the Concept of Protection from the Consumer Law and the Return of Social Elements in the Civil Law: A Bittersweet Polemic", 35 *Journal of Consumer Policy*, 2012, p. 283; Ch. Twigg-Flesner, "The Importance of Law and Harmonisation for the EU's Confident Consumer", in D. Leczykiewicz and S. Weatherill (eds), *The Images of the Consumer in EU Law. Legislation, Free Movement and Competition Law*, Oxford –Portland, Hart Publishing, 2016,

The average consumer standard is an abstract sketch of a super-shopper, and there is no room for empirical evidence about how real consumers behave. As the ECJ ruled in *Gut Springerheide*, where it first introduced the average consumer standard, "the Court took into account the *presumed* expectations of an average consumer who is reasonably well-informed and reasonably observant and circumspect, *without ordering an expert's report or commissioning a consumer research poll*".[28] In the same vein, Recital 18 of the Unfair Commercial Practices Directive (UCPD) indicates that the average consumer test "is not a statistical test". The Commission adds for good measure that "national courts and authorities will have to exercise *their own faculty of judgment*, having regard to the case-law of the Court of Justice, to determine the typical reaction of the average consumer in a given case".[29] Both the digital twin consumer and average consumer embody presumptions about preferences but one set of presumptions is data-based, with the data being aggregated using AI, while the other set is judge-made and does not even seek to incorporate empirical data. One set of presumptions is very granular, and the other is avowedly a rough approximation.[30]

This largely holds also concerning the vulnerable consumer standard. Its origin is different: the EU legislature introduced this standard in the Unfair Commercial Practices Directive as an exception to the average consumer standard. For this reason, and by definition, its content is different. Yet, similarly to the average consumer standard, courts are at liberty to fill the vulnerable consumer standard with their own representations of how young, old, or bereaved consumers behave in certain contexts. Just like the average consumer standard, the vulnerable consumer standard works as a vantage point Courts adopt without any requirement to track consumer behaviour in an empirically informed manner. A similar degree of courts' discretion is compatible with the UCPD when determining who the average consumer of a targeted group is. All of these standards are part of the law that the courts know (*Iura novit curia*); they are not made of facts brought to the court.

Because of the immense granularity gap between them, it is difficult to see how existing legal standards could serve as an effective shield against commercial surveillance, personalisation, and exploitation of consumer data *via* digital twins. An adaptation

p. 183. This internal market heritage is also explicitly stated in the new UCPD guidelines, p. 33: "This concept was indeed developed by the Court of Justice prior to the UCPD. It was codified then by the UCPD to give national authorities and courts common criteria to enhance legal certainty and reduce the possibility of divergent assessments".

28 Case *Gut Springerheide*, paragraph 31, emphasis added.

29 UCPD, Recital 18, emphasis added.

30 In this regard, it is telling that courts in different Member States seem to have very different images of the average consumer, arguably reflecting legal traditions rather than different realities. F. Esposito and M. Grochowski, "The Consumer Benchmark, Vulnerability, and the Contract Terms Transparency: A Plea for Reconsideration", *European Review of Contract Law* 18, No. 1, 26 April 2022), pp. 1-31 (accessed 23 January 2023).

of existing standards is difficult to imagine because the granularity of digital twins is beyond the reach of the law and because, even if it were not, dissolving general standards into individual images would run counter to their harmonisation function. Can the same legal standards shield both courts against facts and consumers against harmful personalisation practices?

B. – TRADER MADE V. LEGAL CREATURES

Digital twins of consumers are the product of traders' efforts to harvest data and their investments in AI to make more profitable use of the ensuing data deluge. They are the intermediary output in the production of personalised advertisements, personalised offers (*e.g.* price or other trading conditions) and personalised choice environments (*e.g.* the appearance of an interface, number of options and order in which they are presented). Legal standards are the product of legal craftsmanship. The average consumer standard is an intermediary product of the Court's reasoning in internal market case law. The vulnerable consumer standard is an addition from the legislature whose content is further specified by national courts. The same is true of the average consumer of a targeted group.

Producing these images of consumers involves very different economics. Traders are incentivised to invest in data harvesting (including dark patterns affecting default privacy settings) and AI to produce granular digital twin consumers. The more data goes into the picture, the more precise targeting will be. The hope is that it will then be more effective and therefore, profitable, whether because traders will sell more goods and services directly due to accurate targeting or because they can charge more for showing ads with a better click-through rate.[31] Courts, on the other hand, do not make a profit from creating more empirically informed presumptions. They have limited resources, and commissioning experts in consumer law disputes will often be considered disproportionate to the monetary stakes. Moreover, courts and claimants may be reluctant to increase litigation costs because of the risk that, if the consumer loses, she will need to pay the costs of expert testimony. In addition, as the above quote shows, the ECJ gave its blessing to doing without market research. In other words, courts face weak incentives to go empirical.

On the other hand, the EU legislature is intent on empirically informed legislation, particularly in consumer protection.[32] This opens new routes. It is too early to say

[31] According to a report cited by the European Parliament research service, the click through rate is 5.3 times higher with targeted ads than standard run-of- network advertising. Unpacking "*commercial surveillance*" (cited n. 1) p. 2.

[32] Since 2010, the European Commission has commissioned no less than 20 behavioural studies to inform or evaluate legislation in the field of consumer protection including one on unfair commercial practices in the digital environment: European Commission, Directorate-General for Justice and

what role standards will play in the emerging regulatory landscape, but it cannot be ruled out that they might serve to incorporate new empirically informed presumptions. For example, preliminary evidence (as well as common sense) would support a presumption that dark patterns are attention-grabbing, distract many subjects from an online task they were undertaking and thus lead consumers to taking decisions they would not otherwise have taken. [33] Such findings could crystallise in presumptions or new rules (bans). To date, the evidence on harmful personalisation practices seems somewhat scant, but research is set to continue.

To summarise, the granularity gap between digital twins and legal standards is considerable and seems to be there to stay, for standards would not be standards if they became granular. This gap seems to create a mismatch between the law and personalisation practices that call for regulatory attention. This said, standards are not set to disappear. It is entirely possible that empirical evidence on harmful personalisation practices could both inform new rules (such as new items on the UCPD blacklist) and the interpretation of what harms average and vulnerable consumers. Indeed, this seems a promising direction for research. [34] In this regard, the Commission and to some extent the European Parliament, rather than the Court, are setting the course on gathering and producing evidence. The next sections review these options, considering existing rules (Part IV) as well as perspectives for reform (Part V).

IV. – Regulating personalisation: the state of play

It is common ground that personalisation is not intrinsically harmful to consumers. [35] Many of us enjoy recommendations (personalised offers, personalised ranking) based on our interests, as inferred from our browsing or buying history. Indeed, some online consumers seek to curate those recommendations to cater to specific needs. No one is therefore suggesting the ban or severe restriction of personalisation in general. Rather, the aim is to prohibit harmful personalisation practices. [36] This is easier said than done. At this juncture, EU law is not well-equipped for the task, nor does it have a clear

Consumers, F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino *et al.*, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation, final report*, Publications Office of the European Union, 2022 (accessed 23 January 2023), hereafter *Behavioural study on unfair commercial practices in the digital environment*.

33 *Behavioural study on unfair commercial practices in the digital environment*, pp. 97-104.

34 *Behavioural study on unfair commercial practices in the digital environment*, p. 239.

35 *Behavioural study on unfair commercial practices in the digital environment* analyses several examples, *e.g.* p. 246.

36 The commissioning of a study on unfair commercial practices in the digital environment attests to this. European Commission, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*, 2022, https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1 (accessed 23 January 2023).

roadmap to that goal. EU law currently regulates, arguably minimally, the flows of data that can be used as input to create digital twins of EU consumers (A), it ensures consumer information about personalisation in such a limited way that it does not deserve more than a cursory mention in this section,[37] especially since the topic will be picked up in the next, and it regulates the use of digital twins for personalisation purposes through the unfair commercial practices directive (B).

A. – Regulating access to inputs to produce digital twins: data harvesting under EU law

The key input to produce digital twins is data. For businesses, it comes for free: they must invest in harvesting but do not pay for the data itself. As Jaron Lanier noted, it is a first in economic history that a key raw material is obtained for free and that there is no ledger for recording the transaction.[38] When it chose to consider data protection as a fundamental right, the EU legislature arguably contributed to validating this arrangement. A few years on, it was not tenable to hold that data is non-tradable, and EU legislation had to introduce some contorted caveats. It recognised – in essence, if not in so many words – that data can constitute the non-monetary consideration for a service.[39] Increasingly, the natural bend of EU law, which is to ensure its free flow of everything, is prevailing and leads to treating data like the input it constitutes.[40] To be sure, EU law is not seeking to reduce the flow of data which businesses generate and from which they create digital twin consumers. Initially, with GDPR, the regulatory

---

[37] The consumer rights directive (CRD) as modified by the Modernisation directive, provides that, when shopping on a platform, consumers must be informed about i) main parameters that influence ranking of offers in response to a query and the relative importance of those parameters as opposed to other parameters (Article 6a, 1 a), ii) personalised pricing (without specifying any saliency or clarity requirement). An additional information requirement flows from the addition of item 11 a to the UCPD blacklist, which bans the practice of "providing search results in response to a consumer's online search query without clearly disclosing any paid advertisement or payment specifically for achieving higher ranking of products within the search results". See generally F. Zuiderveen Borgesius and J. Poort, "Online Price Discrimination and EU Data Privacy Law", *Journal of Consumer Policy* 40, No. 3, 1 September 2017), p. 353; A.-L. Sibony and D. Clifford, "La personnalisation illicite: la perspective du droit européen de la consommation", in F. G'Sell-Macrez (ed.), *Le Big Data et le Droit*, Paris, Dalloz, 2020.

[38] J. Lanier, *Who Owns the Future?*, Reprint ed., New York, Simon & Schuster, 2014.

[39] Directive 2011/83/EU on consumer rights (CRD), *OJ* L 304, 22 November 2011, p. 64 as amended by Directive 2019/2161 (Modernisation directive), *OJ* L 328, 18 December 2019, Article 3 1a. The Court has not yet ruled on whether data could be considered a "remuneration" for a service under Article 56 TFEU but any other decision would be incoherent.

[40] GDPR Recital 9; "Creating a single market for data" is also the aim of the EU Strategy for Data (Communication of the European Commission, COM(2020)66 final). In addition to free flow of data across borders, it aims to foster data-driven innovation and free flow of data across sectors. This is the purpose of the Data Governance Act: Regulation (EU) 2022/868 on European data governance, *OJ* L 152, 3 June 2022, pp. 1-44.

emphasis was on *how* data is collected rather than what data or how much of it.[41] The recent Digital Market Act (DMA)[42] and Digital Services Act (DSA)[43] have modified this perspective by introducing a new focus on *who* can use *what* data. This takes the form of asymmetric obligations that bear on very large platforms and reduce their access to certain sources of data. This said, the EU has not converted to data minimalism. With its Data Act Proposal, the Commission clearly states that the aim is to *increase* the size of the data pie, while inviting more economic actors to have a bite. In the words of the Commission, "the Data Act aims to maximise the value of data in the economy by ensuring that a wider range of stakeholders gain control over their data and that more data is available for innovative use, while preserving incentives to invest in data generation".[44] More precisely, the proposed legislation seeks to clarify *who* can create value from data generated when consumers use a product or related service and under which conditions.[45] In short, far from trying to limit data extraction, EU law seeks to promote fairer harvesting methods and a better yield through more sharing.

What are the implications for the regulation of (manipulative) personalisation? As the law stands, the production and use of digital twins fall at the intersection of consumer protection, data protection, and regulation of the digital single market. It is governed by old, new, as well as forthcoming legislation such as the Digital Services Act, Digital Markets Act, AI Act and the Data Act. The legislative landscape is in flux, in search of adjustments to better respond to harmful personalisation.[46] In this regard, scholars point to the importance of ensuring that new instruments do not preclude further updates to the consumer *acquis* in the digital sphere and recommend using explicit language to that effect.[47]

---

41 At first sight GDPR also seems to regulate *what* data can (or cannot) be collected. Article 9, (1) GDPR prohibits the processing of special categories of personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation), subject to a number of exceptions and conditions detailed in the following paragraphs.

42 Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act) *OJ* L 265, 12 October 2022, pp. 1-66.

43 Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act), *OJ* L 277, 27 October2022, pp. 1-102.

44 Presentation of the Data Act on the Europa website: https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data (accessed 23 January 2023).

45 The Commission tabled the proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, in February 2022.

46 European Commission, Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation, April 2022, p. 7, available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418 (accessed 23 January 2023).

47 M. Veale and F. Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach", *Computer Law Review International* 22, No. 4, 2021, pp. 97-112.

To survey the existing framework, the GDPR is the first port of calling. The recent decision of the Irish data privacy board demonstrates that the GDPR can show its teeth when it comes to personalisation. At stake in this case was how Meta, the parent company of Facebook and Instagram, obtains consent from users to collect their data for personalised advertising. Users were not presented with a self-standing request to consent to personalised ads. Instead, consumers had to give their blanket consent to the company's terms-of-service agreement to access the service. It was in this very lengthy document that one could find a clause about consent to the use of data for personalisation purposes. Not only did the practice lack transparency, but there was also no opt-out. The Irish data protection regulator – after conferring with its European counterparts –[48] held that this was in violation of the GDPR: Meta could not rely on a contractual legal basis under Article 6, GDPR.[49] This decision gives some hope that the GDPR could indeed lead to more transparent data harvesting practices. However, several caveats should be mentioned. First, the decisional process leading up to this outcome demonstrated that there are diverging opinions among EU data regulators.[50] It is thus too early to say whether it indicates the way forward for Europe as a whole.[51] Second, even if the fine was increased during the consultation process among data regulators, its amount remains far below a dissuasive level at roughly 0,3% of Meta's annual turnover.[52] If fines are low, enforcement slow (over four years in this case)[53] and non-compliance difficult to track,[54] the effect of

[48] GDPR mandates this cooperation with the Concerned Supervisory Authorities ("CSAs"). The New York Times writes that there was disagreement between European regulators and that it was only after this meeting that the Irish authority agreed that Meta's behaviour was in violation of GDPR. A. SATARIANO, "Meta's Ad Practices Ruled Illegal Under E.U. Law", *The New York Times*, 4 January 2023, https://www.nytimes.com/2023/01/04/technology/meta-facebook-eu-gdpr.html (accessed 23 January 2023).

[49] Data Protection Commission (Ireland), Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Article 65 GDPR), European Data Protection Board website: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en (accessed 23 January 2023).

[50] The Irish Data Protection Commission (IDPC) is very forthcoming about this aspect, having been overruled by the European Data Protection Board ("the EDPB"). See press release of 4 January 2023, https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland (accessed 23 January 2023). The Irish Authority believed Meta could rely on the "contract" legal basis under GDPR because ad personalisation is of the essence of the services it offers.

[51] The Irish Authority has announced that it will file an action for annulment against the European Data Protection Board for acting ultra vires when directing it to launch new investigations against Meta. *Ibid.*

[52] Our calculation based on the 390 million euros fine and the reported revenue of Meta for 2021 (roughly 117 billion US dollars), https://www.statista.com/statistics/268604/annual-revenue-of-facebook/ (accessed 23 January 2023).

[53] The complaints were filed in 2018 on the day when GDPR came into force. See IDPC press release quoted above.

[54] "Most of the experts consulted during the study considered that data-driven personalisation practices are more problematic than classic dark patterns, especially as they are *more difficult to identify and*

the GDPR is likely to remain modest. Free data will continue to flow *en masse* from consumers to businesses and feed personalisation practices.

This said, the EU also intends to manage the data flows in several ways. First, it wants to rebalance data flow towards European businesses rather than continue to export too much of the precious input generated by European consumers.[55] The concern is more about the competitiveness of European businesses than consumer protection but, if European businesses prove to be more compliant with EU law than their third-country counterparts, this could lead to an improvement for consumers. Second, the EU is making rules to ensure a "fairer allocation of the value from data among actors in the data economy".[56] This means making data flows work not only for web giants but also small businesses and consumers. In this regard, the text of the draft Data Act regulates B2B contracts for the sharing of data. It bans unfair clauses in data-sharing contracts between large platforms and SMEs.[57] Very much in line with Directive 93/13 on unfair terms in consumer contracts, unfair data sharing clauses are defined as those "grossly deviating from good commercial practice in data access and use [significant imbalance], contrary to good faith and fair dealing".[58] In addition to a general ban on unfair clauses, the text contains a blacklist of clauses deemed to be unfair in all circumstances and a grey list of clauses presumed to be unfair.[59] Just like in the unfair terms clauses directive, the sanction of unfair clauses is that they are not binding.[60] The sanction of disallowing both parties to the data-sharing contract to use the data obtained on the basis of an unfair clause seems to have been contemplated.[61] It may have been more dissuasive but must have been abandoned, probably because of lobbying and arguments about the difficulty of implementing this solution in practice.[62]

---

investigate due to the presence of individual personalisation and group segmentation" (emphasis added). The European Commission, Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation, April 2022, p. 40, https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418 (accessed 23 January 2023).

55 Andrea Renda speaks of "repatriatiation": A. Renda, "The Data Act: six impossible things before breakfast?" (blog post), 2 March 2022, https://www.ceps.eu/the-data-act-six-impossible-things-before-breakfast/?mc_cid=797922c3e6/ (accessed 23 January 2023).

56 Draft Data Act, COM(2022) 68 final, p. 2.

57 Article 13 draft Data Act.

58 Article 5.1 draft Data Act.

59 Respectively Articles 13.3 and 13.4 draft DMA.

60 Article 13.1 draft Data Act.

61 Andrea Renda (cited above n. 55), commenting on an earlier draft of the Data Act, mentions this sanction.

62 The debate here is very similar to that which took place before the adoption of Directive 2019/770 on digital contents and digital services. There, the analogy with reimbursement when a sales contract is rescinded had led to envisage demonetization of data when a consumer exercises her right to withdraw from a contract for the provision of digital content or a digital service. Representatives of large platforms explained that not using the data that had already been collected would be very

In order to make data flow also at the initiative of consumers and to their advantage, particularly when they want to switch service providers, the draft Data Act goes some way towards operationalising the right to data portability. This right already exists on paper in the GDPR.[63] The draft Data Act reiterates it and aims to assist in its implementation through more detailed rules.[64] The contemplated rules deal with crucial B2B aspects to deter obstructing strategies but would need to be complemented with rules about B2C interfaces. There are indeed a number of ways to leverage inertia bias in consumers, and unless switching is made truly easy, for example, by mandating a link or QR code leading to an interface requiring minimal effort on the part of the consumer, switching is unlikely to pick up on a massive scale. The general fair design requirement of Article 25 DSA goes in the right direction towards accomplishing this. It remains to be seen whether it is sufficient.

Regarding the aim of ensuring fairness in data exploitation, several disparate provisions from new and forthcoming EU legal instruments bear on this issue. The DSA creates what one might call enhanced transparency requirements about personalisation practices. One such requirement applies to personalised advertising and is *prima facie* similar to that of the consumer rights directive regarding the ranking of offers in response to a consumer query.[65] It obliges platforms to disclose "meaningful information on the main parameters which have led to the automated selection of recipients of advertising".[66] The drafting, however, reflects the legislature's concern that this information shouldn't be buried in the depths of a website: it must be "directly and easily accessible from the advertisement". In addition to this accessibility requirement, a requirement that the information should be easy to understand and salient can be found in one of the recitals.[67] This represents an improvement on similar pre-existing provisions from the consumer rights directive that allowed much room for creative compliance. The DSA also creates a qualified right to actionability. It requires that the interface should allow consumers to change the personalisation settings.[68] However, the reach of this right to control parameters of personalise advertisement is very limited because the choice of whether to offer several personalisation options remains that of the platform.[69] It means,

difficult in practice. This resulted in Article 16.3 c) allowing continued use of personal data when it has been "aggregated with other data by the trader and cannot be disaggregated or only with disproportionate effort".

63 Article 20 GDPR.

64 Article 5 draft Data Act.

65 Article 6 a) 1. a Directive 2011/83/EU on Consumer Rights (as modified by the Modernisation directive).

66 Article 26. (d) DSA

67 Recital 68 DSA.

68 Article 26.1 d) DSA.

69 Under Article 26.1 d) consumers should be guided as to how to change the ad personalisation parameters "where applicable".

therefore that, *if* a platforms decides to give a choice between ad personalisation based on previous purchases or ad personalisation based on previous purchases, search history, and social media activity, it should make this choice clear and salient. In other words, for advertisement, consumer empowerment through information is mediated by law but in the hands of platforms. Given that the whole *raison d'être* of tracking and profiling is advertising, which funds the "free web",[70] the incentives to offer the option to choose less accurate ad personalisation are unclear. They could grow if consumers become more demanding, and low personalisation appears necessary to gain, keep or regain consumers' trust. The DSA provisions on personalisation options do not explicitly refer to the average consumer but the EU legislature does seem to stick to the notion that there is no need for much protection against personalisation unless one is vulnerable (we return to this issue in section IV B).

The DSA also regulates recommender systems, that is, algorithmic determination of what products or services a consumer is likely to want.[71] All providers of online platforms must disclose the main parameters used to make personalised recommendations and, just like for personalised ads, provide consumers with a choice between personalisation options *when such options exist*.[72] Only very large online platforms are under an obligation to provide at least one option which is not based on profiling,[73] similarly to what the DMA mandates.[74] The scope of this opt-out can be interpreted in two different ways. Either the rationale for introducing it is consumer protection but compliance costs were thought to be too high for SMEs or, more likely, the rationale is not consumer protection but creating a level playing field through asymmetric regulation, which is the logic underpinning the DMA. Whichever it is, the new provisions about ad personalisation and recommender systems amount to a limited improvement of consumers' position *vis-à-vis* platforms. This improvement rests on empowerment rather than protection proper, for it hangs on an active right to choose (change settings if platforms offer personalisation

---

70 H. Mildebrath, "Unpacking 'commercial surveillance': The state of tracking", European Parliamentary Research Service, December 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739266.

71 Article 27 DSA.

72 Article 27.3 DSA. Our emphasis. According to this provision, "that [choice] functionality shall be directly and easily accessible from the specific section of the online platform's online interface where the information is being prioritised".

73 Article 38 DSA.

74 The text of Recital 36, DMA reads as follows: "The conduct of combining end user data from different sources or signing in users to different services of gatekeepers gives them potential advantages in terms of accumulation of data, thereby raising barriers to entry. To ensure that gatekeepers do not unfairly undermine the contestability of core platform services, they should enable their end users to freely choose to opt-in to such business practices by offering a less personalised alternative. The possibility should cover all possible sources of personal data, including own services of the gatekeeper as well as third party websites, and should be proactively presented to the end user in an explicit, clear and straightforward manner".

options). In this regard, consumers are more empowered towards very large platforms and search engine than towards other traders, for only the very large players have to offer an opt-out of personalisation.

In this same vein of asymmetric regulation (and consumer empowerment), the DMA obliges "gatekeepers" (very large platforms)[75] to refrain from combining personal data that was acquired during the operation of the "core platform" (*e.g.* Google search) with personal data obtained from other services offered by the same provider (*e.g.* YouTube) or other providers "unless the end-user has been presented with the specific choice and has given consent".[76] In other words, the default becomes personalisation based on a restricted set of data and expanding the sources from which data can be pooled to obtain digital twins becomes subject to consumer opt-in. If enforced, this provision would represent a real change for the prohibited practices that abound at the time of writing. This is one clear instance where the DMA would add to the protection of consumers against profiling practices. A lot will hang upon what strategies gatekeepers adopt to circumvent this far-reaching provision. They could degrade the conditions or quality of their core platform services for users who exercise their right not to be digitally twinned. They could also resort to dark patterns and lead consumers to opt-in for personalisation based on a wealth of data. Again, it is to be hoped that the fair design principles contained in the DSA will prevent this from happening.[77]

To sum up, the existing regulatory framework has been considerably enriched. The focus of the GDPR was on *how* data is collected. With the DMA and DSA, the EU legislature turns its attention to *who* can combine *what* data. In this regard, the limitations imposed to very large online platforms reduce the data pool from which they can generate digital twins. The new provisions create a right to a more pixelated digital portrait. If exercised (against very large platforms), this right could lead to less accurate personalisation, at least until smaller platforms not subject to these limitations catch up and legitimately acquire enough data to produce digital twins made in Europe. Indeed, it is noteworthy that consumer protection is not the sole or main concern of these new legislations.[78] The fairness issues they are concerned

[75] Article 3 DMA defines gatekeepers as undertakings that have (a) a significant impact on the internal market; (b) provide a core platform service which is an important gateway for business users to reach end users; and (c) enjoy an entrenched and durable position, in their operations, or it is foreseeable that they will enjoy such a position in the near future.

[76] Article 5 (1) DMA.

[77] Article 25.1 DSA on provides that "Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions".

[78] Article 1 DSA mentions innovation first, then fundamental rights, including principles of consumer protection. Article 1 DMA mentions internal market as well as "contestable and fair" markets in the digital sector.

with arise between large platforms and small and medium size businesses. When it comes to fairness in business-to-consumer transactions, different rules come into play, to which we now turn.

B. – Prohibiting unfair personalisation

The Unfair Commercial Practices Directive (UCPD) provides a general framework for regulating marketing practices, including AI-powered personalisation practices. As BEUC (the European consumer organisation) writes, the UCPD "appears sufficiently broad and flexible to cover and sanction many of the unfair digital commercial practices that are common today".[79] The Commission's 2021 Guidance Notice on the interpretation and application of the UCPD added a specific chapter on "data-driven practices and dark patterns" which details how principle-based provisions and prohibitions in the UCPD can be used to address unfair data-driven business-to-consumer commercial practices.[80] UCPD, therefore, remains the regulatory cornerstone when it comes to unfair personalisation. This basic framework is being simultaneously expanded and called into question, which raises the issue of the overall consistency of recent changes.

The existing UCPD framework is being expanded in that the DSA clearly builds on the definition of unfair commercial practices and tailors it to interface designs. Article 25 DSA, already cited above, reads as follows: "Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions".

While the UCPD inspiration is clear, two differences are striking.[81] First, the provision makes no reference to professional diligence. This is entirely understandable, as the notion never served its intended purpose in relation to UCPD itself. Indeed, in the original project of UCPD the reference to professional diligence was

[79] BEUC (2022). "Dark patterns" and the EU Consumer Law acquis. Recommendations for better enforcement and reform, https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf (accessed 23 January 2023).

[80] Commission Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, *OJ* C, C/526, 29 December 2021, p. 1 (hereafter "UCPD Guidance", section 4.2.7. p. 99.

[81] Article 5 UCPD defines unfair commercial practices as practices that (a) are contrary to the requirements of professional diligence, and (b) materially distort or are likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.

meant to be operationalised through codes of conduct which were never adopted. Second, Article 25 DSA makes no reference to the average consumer or any other standard. Instead, it refers to "recipient of their services", a broader notion which also includes business users.[82] This leaves the question open as to what type of approach courts will take to appraising deception and manipulation when consumers are concerned. In this regard, it should be noted that the DSA does make a reference to the average consumer standard in both Recital 24 and Article 6. These provisions concern situations where a consumer concludes, *via* the platform, a contract with a trader or service provider other than the platform itself ("intermediated commercial transactions online"). It would apply for example to Amazon marketplace, where consumers can buy from sellers other than Amazon itself, or to Airbnb, where the platform acts as an intermediary and does not itself provide accommodation services. Article 6 DSA provides that such "hosting" platforms are not liable for the faulty good or service offered by another trader unless the information on their interface is unclear and could lead the average consumer to believe that the platform provides the good or service in question or controls the trader or service provider. It would seem coherent to apply the same standard to misleading information under Article 6 and to dark patterns under Article 25. The average consumer standard, therefore, is still present in the new rules.

So is the vulnerable consumer. Moreover, an evolution of the standard can be detected. The recitals of the DSA contain two distinct phrases referring to vulnerable consumers (there are no references in the main provisions). The first, "vulnerable recipients of the service, such as minors"[83] seems to mirror the categorical approach of the UCPD: vulnerability is an attribute of certain groups of consumers that can be identified in relation to characteristics, such as age, that humans (including traders and judges) can observe. The second, namely "persons in vulnerable situations"[84] opens to a broader notion of vulnerability as an attribute that is not intrinsic to certain consumers but linked to a situation that machines can both infer from data and generate. We return to it below.

Meanwhile, the categorical approach to vulnerability is also present in the Proposal for the AI Act.[85] The latest text, of the Council's common position ("general approach") adopted on the 6th of December 2022[86] prohibits any AI system "that

[82] Article 2.1 DSA on Scope reads "This Regulation shall apply to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment".

[83] Recitals 62 and 104 DSA.

[84] Recitals 94 and 95 DSA.

[85] COM(2021)0206.

[86] Available at https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/.

exploits any of the vulnerabilities of a specific group of persons due to their age, disability or a specific social or economic situation, with the objective to or the effect of materially distorting the behaviour of a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm".[87] The reference to social or economic situation marks a slight expansion on Article 5 (3) UCPD, but that does not mean that the overall approach would significantly increase protection against personalisation. Indeed, the AIA praises the opportunities of personalisation,[88] while its dangers are not tackled in any significant detail.

Within the categorical approach to vulnerability, the focus is on protecting children.[89] This is in line with the new European strategy for a better internet for kids (BIK+).[90] In the DSA, it materialises as a standard to appraise transparency. Article 14 provides that, "[w]here an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service *in a way that minors can understand*".[91] The attention to children's wellbeing also translates as specific protection. Minors are the only category of consumers protected against personalised advertising.[92] In both these provisions, minors as considered as one category. While this seems protective in the case of the ban on targeted ads, the benefit of considering children as one homogeneous category is less clear when it comes to transparency obligations. At different ages, children have different understanding capabilities, but there is no requirement that communication be age appropriate, only suitable for "minors". Clearly, the legislature still operates with bright line categories.[93]

---

87 Marking a slight evolution from the proposal, in which Recital 16 and Article 5.1.b) Draft AI Act, which refer only to "age, physical or mental disability".

88 Recital 3, Draft AI Act: "By improving prediction, optimizing operations and resource allocation, and personalising digital solutions available for individuals and organizations, the use of artificial intelligence can provide key competitive advantages to companies and support socially and environmentally beneficial outcomes, for example in healthcare, farming, education and training, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, and climate change mitigation and adaptation".

89 Recitals 71, 83, 89, 95 DSA, Recital 28, Article 9,8 Draft AI Act.

90 Communication of the European Commission, A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), COM(2022)212 final.

91 See also Recital 81 DSA.

92 Article 28 DSA reads "Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor".

93 This is also true of the European Parliament, which has proposed that AI systems used to influence or shape the development of children should be considered high risk. B. Benifei and I.-D. Tudorache, "Draft Report on the proposal for as Artificial Intelligence Act (CJ40_PR(2022)731563)", 2021/0 106(COD), p. 159.

Yet at the same time, the categorical framework of the UCPD is called into question. Of particular interest in this regard is the new interpretation of the average and vulnerable standards in the 2021 UCPD Guidelines.[94] The change is most drastic regarding the average consumer. In the section on data-driven practices, the Commission writes that, for the purposes of assessing such practices, "the benchmark of an average or vulnerable consumer can be modulated to the target group" [no change here] "and, if the practice is highly personalised, even formulated from the perspective of a *single person* who was subject to the specific personalisation".[95] In what looks like a U-turn, enforcers and courts are invited to zero in on a specific consumer subject to a specific personalisation practice. We note, however, that the language used does not refer to *the* targeted consumer herself but to "*a* (single) person", thus – realistically – leaving the possibility that courts will take an abstract view of how one person, in general, would react to extreme personalisation practices. Even so, this could open the courtroom to empirical evidence on the effects of various personalisation practices, and that would be a change from courts' being instructed to rely solely on their "own faculty of judgement" and the Court's case law.[96] Courts could craft new presumptions based on behavioural evidence that will neither need to be case-specific nor in line with the average consumer who is normally observant and circumspect. In other words, there is an opening that would allow courts to modify the content of the average consumer standard and/or multiply standards.

Concerning the vulnerable consumer standard, there is a measure of evolution as well. The Commission invites courts to investigate group (if not individual) characteristics somewhat more in-depth. The guidance notice clarifies that the causes of vulnerability are not exhaustively listed in the text of Article 5 (3) UCPD.[97] Besides "mental or physical infirmity, age or credulity", there can be other circumstances leading to vulnerability. This much was already clear from Recital 19 UCPD.[98] What is new, however, is that the Commission, drawing on a 2016 study on vulnerability it had commissioned,[99] recognises that vulnerability is not necessarily an attribute of certain groups presenting certain characteristics.[100] It can also be "context-dependent".[101] Surveying how social sciences conceptualise vulnerability, the study concluded that

94 Commission Notice, Guidance on the interpretation and application of Directive 2005/29/EC, *OJ* C 526, 29 December 2021, pp. 1-129.

95 UCPD Guidance, p. 100. Our emphasis.

96 Recital 18 UCPD cited above.

97 UCPD Guidance, paragraph 2.6, p. 35.

98 Recital 19 UCPD reads "Where certain characteristics *such as* age, physical or mental infirmity or credulity…" (emphasis added).

99 European Commission, Consumers, Health, Agriculture and Food Executive Agency, Consumer vulnerability across key markets in the European Union: final report, Publications Office, 2016, https://data.europa.eu/doi/10.2818/056024 (accessed 5 January 2023).

100 BEUC 2.0, p. 14

101 UCPD Guidance, paragraph 2.6, p. 35.

vulnerability is best characterised as a spectrum rather than a binary state.[102] The authors identified five dimensions of vulnerability[103] which can result from a variety of causes besides individual characteristics, including market circumstances, situational factors and behavioural phenomena.[104] In this vein, the Commission notes in its guidance that, in the digital environment, vulnerability becomes multi-dimensional and acute because of data collection not limited to socio-demographic characteristics but also includes personal or psychological characteristics, such as interests, preferences, psychological profile and mood.[105] Vulnerability becomes "dynamic and situational", meaning, for instance, that a consumer can be vulnerable in one situation but not in others.[106] As mentioned, this broader notion of vulnerability has already made its way into the DSA.

In a 2022 Report commissioned and published by BEUC, Helberger *et al.* analyse in-depth how to redefine vulnerability in the digital age.[107] Taking inspiration from the work of Marta Fineman,[108] they define digital vulnerability as "a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer-seller relations and the very architecture of digital marketplaces"[109]. Under this approach, vulnerability should no longer be conceptualised as the exception but as the norm. What is more, digital twins serve not only to exploit existing vulnerabilities but to render consumers vulnerable in the first place, in the sense of affecting their ability to rationally deal with a particular marketing practice.[110] The very existence of digital twins creates

[102] European Commission, Consumer vulnerability across key markets in the European Union, London Economics, VVA Consulting and Ipsos Mori Consortium, 2016, hereafter "Vulnerability Study 2016".

[103] 1. Heightened risk of negative outcomes or impacts on well-being; 2. Having characteristics that limit ability to maximise well-being; 3. Having difficulty in obtaining or assimilating information; 4. Inability or failure to buy, choose or access suitable products; 5. Higher susceptibility to marketing practices. Dimensions 4 and 5 are found to have the highest incidence, Vulnerability Study 2016, p. xviii.

[104] More precisely, the authors distinguish five drivers of vulnerability: 1. Personal characteristics; 2. Behavioural drivers; 3. Market-related drivers; 4. Access drivers; 5. Situational drivers, Vulnerability Study 2016, p. 47.

[105] *Ibid*.

[106] UCPD Guidance, p. 100. The Commission further explains that "For example, certain consumers may be particularly susceptible to personalised persuasion practices in the digital environment, while less so in brick-and-mortar shops and other offline environments".

[107] N. Helberger, O. Lynskey, H.-W. Micklitz, P. Rott, M. Sax and J. Strycharz, "EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets", BEUC-X-2021-018 (hereafter "Consumer Protection 2.0").

[108] M. Albertson Fineman, "The Vulnerable Subject: Anchoring Equality in the Human Condition Essay", *Yale Journal of Law and Feminism*, 20 (1), 2008, pp. 1-24.

[109] Consumer Protection 2.0, pp. 5, 10, 13.

[110] Consumer Protection 2.0, pp. 5, 11. N. Herberger *et al.* seem to consider that creating vulnerabilities is more egregious than exploiting vulnerabilities (n. 25, p. 14). We imply that the hierarchy of harm is the other way around but recognise that this point would deserve further discussion.

latent (or "dispositional") vulnerability.[111] The authors of this report conclude that this richer notion of vulnerability calls for a change of approach both in relation to the substantive fairness requirements and to enforcement mechanisms.[112]

Indeed, a change of approach is needed for recognising that vulnerable consumers do not constitute a fixed group disrupts the existing conceptual framework as well as available regulatory options. By way of illustration, consider an OECD report of 2016 on personalised pricing.[113] It outlined two strategies: the first was to ensure transparency (which is minimally implemented in EU consumer law)[114] and the second was to ban targeting vulnerable consumers. But if vulnerable consumers no longer belong to pre-defined categories, the second option becomes normatively impossible. Indeed, the above-mentioned ban on serving targeted ads to children in the DSA can only be formulated because it refers to the well-established category of "minors".

For now, the EU legislature has found a way around this conundrum. It reverts to regulating *what* data can be used for personalisation in general (for all consumers). Article 26 DSA illustrates this approach. It concerns personalised advertising and provides that platforms cannot use sensitive data to personalise ads. The provision refers to Article 9 GDPR for the (categorical) definition of sensitive data. These are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. Under this approach, fairness in personalisation is implicitly defined as relying only on data that reasonably relate to the behaviour of consumers in the market, as opposed to their identity and behaviour in the political or private sphere. This is a strong normative stance for how identity as well as political and private attitudes and behaviour certainly impact on consumption. This is precisely why it is profitable to use sensitive data to personalise ads. In this sense, "reasonably related to consumption" in our provisional formulation does not mean "causally related" and certainly not "correlated". Rather, the legislature articulated a rule that can be read as a reasonableness standard to set limits to marketing rationality. In our reading, EU law appeals to common reason to reduce the granularity and accuracy of digital twins. This sits well with a privacy approach which, in another domain, translates as an obligation to blur faces in pictures taken in public places and published in the press.

This regulatory response to the dilution of the average and vulnerable consumer standards does not exhaust the adaptation of existing rules to better protect consumers against harmful personalisation.

---

111 Consumer Protection 2.0, p. 18.
112 Consumer Protection 2.0, pp. 78-79.
113 OECD, Personalised Pricing in the Digital Era, DAF/COMP (2018)13, pp. 23-26.
114 *Supra*, n. 37.

V. – Regulating personalisation: perspectives

None of the perspectives on the table is radically new, in the sense that they are all constructed with the existing regulatory toolbox. However, there is a distinct potential for innovative use of what EU law holds in store. Consider, to begin with, a right to opt out of personalisation. On paper, the GDPR implies such a right, but it is not effective. It is, therefore, proper to consider whether a genuine opt-out of personalisation could be crafted (A). Second, consider information requirements (B). They are the staple of consumer protection, but the EU legislature has used them with remarkable restraint so far in relation to personalisation when a more robust use is entirely conceivable. Finally, fiduciary duties, known, for example in financial regulation, could be repurposed in relation to data use (C).

A. – Mandatory opt-out of personalisation

'Consent' as the legal basis for using personal data should, according to the GDPR, ensure that consumers give informed consent to personalisation. This amounts to an opt-out. Yet, the *Meta* case illustrates that it leaves room for creative compliance. Would it help to make a personalisation opt-out mandatory? If it were available to Facebook users, for example, to refuse the use of their data for personalisation purposes while still using the service,[115] the European data harvest could become less plentiful for Meta. Indeed, there is some evidence that a sizeable fraction of consumers would probably be inclined to exercise such an opt-out. A 2021 poll conducted in Norway specifically on acceptance of personalised advertising found that only 1 in 5 respondents felt that using personal information to personalise advertising was acceptable.[116] This said, it is far from certain that an opt-out from personalisation would be a game changer.

A first reason for this is that there is an unknown but potentially large number of profiled but resigned consumers.[117] As a partial indication, the Norwegian survey just cited finds that 6 out of 10 respondents felt they had no real choice in the matter. A 2021 OECD study gives even more food for thought in this regard. Despite overall strong negative feelings against personalised pricing (also if financially beneficial), consumers forewarned that prices are personalised continue to shop as before.[118]

---

115 Article 26 DSA does not go that far. See above text at n. 66.

116 Population survey conducted by YouGov on behalf of the Norwegian Consumer Council, translated from Norwegian by the Norwegian Consumer Council, "Consumer attitudes to surveillance-based advertising", June 2021, https://fil.forbrukerradet.no//wp-content/uploads/2021/06/consumer-attitudes-to-surveillance-based-advertising.pdf (accessed 23 January 2023). The same survey found that 2 out of 3 respondents rejected collection of personal information online.

117 U. Pachl, BEUC, "AI and consumer law", the KU Leuven AI Summer School, 14 September, 2022.

118 OECD Digital Economy Papers, "The effects of online disclosure about personalised pricing on consumers – Results from a lab experiment in Ireland and Chile", January 2021, https://www.

A second reason why a personalisation opt-out would not necessarily stem the data stream flowing to traders is that details matter a great deal. A lot would hang on how the option is designed and presented, and in particular on how salient and simple it is, as well as on whether dark patterns and proven psychological effects such as the fear of missing out are circumvented.[119] One open question in this regard is whether the general requirement of fair interface design from Article 25 DSA would suffice or whether there should there be precise requirements for the design of a personalisation opt-out. This calls for a detailed empirical investigation. Should the need arise, specifying the look and feel of an opt-out should not be ruled out. In the past, EU law has produced perfectly detailed rules on how to design energy efficiency labels or cigarette warning messages. It is also intent on producing eco-design rules (which are by nature very detailed) to make more durable goods.[120] If EU law regulates the design of goods for durability, could it not regulate the design of interfaces for autonomy?

B. – Enhanced information requirement

Providing consumers with information is the basic paradigm in EU consumer law. As mentioned, existing legislation contains information requirements about personalisation practices, but they make a mockery of an already discredited regulatory technique.[121] Yet, it is possible to imagine more meaningful information requirements. They would be of the more demanding sort, like those applying in financial matters in relation to unfair clauses. In this area, the Court has ruled that banks giving out a loan should not only explain how monthly repayments are calculated but also what the formula means, in concrete terms, in the consumer's situation.[122] For example, if a consumer takes out a mortgage in Euros with variable interests rates involving indexation on the Swiss Franc, scenarios have to be provided explaining what the monthly repayment in Euros will be when the exchange rate fluctuates. Could such a requirement to explain and illustrate serve as inspiration in relation to personalisation?

---

oecd-ilibrary.org/docserver/1ce1de63en.pdf?expires=1673873861&id=id&accname=guest&checksum=312E0AA7EACA185FA3EA22750962ACFF (accessed 23 January 2023).

119 The fear of missing out is particularly important in the context of social media as this fear is a key ingredient in keeping users checking their feed. For further details see for example D Blackwell *et al.*, "Extraversion, Neuroticism, Attachment Style and Fear of Missing out as Predictors of Social Media Use and Addiction", *Personality and Individual Differences* 116, 1 October 2017, pp. 69-72.

120 The Proposal for a Regulation establishing a framework for setting eco-design requirements for sustainable products and repealing Directive 2009/125/EC is the cornerstone of the Commission's approach to more environmentally sustainable and circular products. For additional details see: https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/sustainable-products/ecodesign-sustainable-products_en (accessed 23 January 2023).

121 *Supra*, n. 37.

122 Case C-26/13, *Kásler*, EU:C:2014:282, paragraph 75.

It is conceivable that Meta or any other data controller would have to explain how the data is used and give examples of personalisation practices. Google already does this to some extent.[123] However, when businesses explain personalisation, they have an obvious incentive to present what consumers stand to *gain* from it. Conversely, it is exceedingly easy to create a compelling narrative of what consumers would *lose* if they opted out. Loss aversion is a well-documented behavioural phenomenon and one businesses can safely rely on when crafting their messages. Like in the case of an opt-out, the question arises whether and how EU law could regulate the framing of messages informing consumers. Again, EU law has some experience with this. The PRIIPs regulation, for example, mandates that when informing a consumer about investment products, financial intermediaries must display (in a standardised format) the risk level of the financial product as well as a narrative explanation about risk.[124]

The analogy may not carry much weight, however, because what is needed in the case of personalisation practices is a narrative about what consumers *gain* from opting out. It seems doubtful that this can be mandated both because of foreseeable pushback against such a regulatory move and because it seems difficult to make a concrete personalised statement concerning the benefits of eschewing tracking. The benefits of digital minimalism are probably best explained in the aggregate rather than for each setting the consumer is made to go through.[125] If this is true, a combination of education to mindful use of social media, which would raise consumer awareness,[126] with fairness by design requirements may be the best option. Article 25 DSA articulates such a fairness by design requirement and is coupled with reporting obligations, which we discuss next, together with fiduciary duties.

C. – Fiduciary and reporting obligation

Enforcement of existing consumer protection rules can become exceptionally onerous in a data-rich environment. It is exceedingly difficult for consumer protection authorities – let alone consumer associations or consumers – to adduce evidence that the data collected has been used to influence consumers to take a decision they

[123] Google Dashboard gives users of Google services an overview of their usage as well as access to their data. From the dashboard, it is also possible to obtain more information on "how data improves your experience" and change privacy settings https://myaccount.google.com/data-and-privacy/how-data-improves-experience (accessed 23 January 2023).

[124] Regulation (EU) No. 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs) (Text with EEA relevance), *OJ* L 352, 9 December 2014, pp. 1-23.

[125] For a convincing plea, see C. *Newport*, *Digital Minimalism: Choosing a Focused Life in a Noisy World*, New York, Portfolio, 2019.

[126] S.S. Chan *et al.*, "Social Media and Mindfulness: From the Fear of Missing out (FOMO) to the Joy of Missing out (JOMO)", *Journal of Consumer Affairs* 56, No. 3, 1 September 2022, pp. 1312-1331.

would not have taken otherwise. For this reason, BEUC recommends a reversal of the burden of proof to render enforcement tractable.[127] It would be for businesses to prove that they are not making an unfair use of data. Such proof could be based on impact assessments by the controller under the GDPR or on a certificate from an independent auditor.[128]

This approach is new, but it sits well with existing elements in the unfair commercial practices framework. As BEUC underscores the notion of "professional diligence" under Articles 5(1) and 5(2), UCPD could be filled with new content, specifically, the duty not to harm through personalisation.[129] One could add that this approach is also in line with Article 5(3), UCPD, which provides that "vulnerable consumer criteria apply if a commercial practice distorts the economic behaviour of a group of consumers who are particularly *vulnerable in a way which the trader could reasonably be expected to foresee*".[130] Even if we do away with the vulnerable consumer standard in its current form, or completely, this passage attests that the notion that vulnerability creates a fiduciary duty is not entirely foreign to the UCPD. Digital twins are exactly what allows traders to foresee – with good accuracy – what commercial practices the consumer is likely to fall for. In this sense, the new fairness standards to be articulated should specify a duty to "personalise for good". The reporting would need to explain, based on audited data, how digital twins are constructed, what sort of predictions can be made on this basis and which subset of predictions are actually used for marketing purposes. Subsequently, empowering willing consumers to have a say in the creation and use of their digital twins could also benefit all sides.

Already this approach begins to enter the legal framework for very large platforms. In the DMA, geared towards securing effective consent before tracking end users outside of the gatekeepers' core platform service for the purpose of targeted advertising, Article 28 introduces an obligation for gatekeepers to organise an independent "compliance function" within their organisation to ensure abiding by the regulation. In addition, Article 15, DMA creates an "obligation of an audit" for platforms designated as gatekeepers. Within six months of its designation, a gatekeeper must submit to the Commission an independently audited description of any techniques for profiling of consumers that the gatekeeper applies. The Commission will then transmit that audited description to the European Data Protection Board.[131] The DSA contains a

[127] BEUC, EU Consumer Protection 2.0, p. 4, pp. 75 et s.
[128] BEUC, EU Consumer Protection 2.0, p. 77.
[129] BEUC EU Consumer Protection 2.0, p. 26 citing G. SPINDLER, A. SEIDEL, "Die Zivilrechtlichen Konsequenzen von Big Data für Wissenszurechnung und Aufklärungspflichten", *Neue Juristische Wochenschrift*, No. 30, pp. 2153-57.
[130] UCPD Guidance, paragraph 2.6.2, emphasis in the original.
[131] Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act), *OJ* L 265, 12 October 2022, pp. 1-66, Article 15.

similar obligation: Article 37 provides for a mandatory annual compliance audit for very large platforms and search engines. It remains to be seen how this system will take shape, in particular, what measures will ensure that auditing is exempt of conflicts of interest. [132] It is too early to tell whether human compliance officers and regulators can manage the system, but its entry into operation in 2023 will certainly produce data and experience to refine our notion of fairness and the practice of compliance.

VI. – Concluding remarks

Digital Twins are a marketing grail and a threat to consumer privacy, health and economic interests. Initially, EU consumer law seems at odds with this new reality because it operates on the basis of standards that are highly abstract rather than empirically informed. Both normative reasons (the functioning of the internal market) and courts' incentives enshrine this approach in consumer law. Yet, EU law is reacting to harmful personalisation. It does so in several different ways. First, within consumer law, the interpretation of both the average and the vulnerable standards are being questioned to a point where the very notion of standards and their harmonisation function could dissolve. Second, an array of existing and new rules for the digital sector (GDPR, DMA, DSA, Draft AI Act, and Draft Data Act) have a bearing on personalisation practices. These rules follow a different approach from that of consumer law. Instead of *ex post* prohibition of unfair practices, the emphasis is on *ex ante* design requirements. In this regard, Article 25 DSA on fair interface design is a central provision and a lot will hang upon its enforcement. The new regulatory framework also changes enforcement strategy, relying on compliance departments, reporting obligations and independent audits.

Substantively, the focus has shifted from *how* data is collected (GDPR) to *who* can access and use *what* data (DMA, DSA, AI Act). Consumer protection is only one of the aims of the new framework and, without spelling it out explicitly, the new rules create a right to less granular digital twins and, therefore, less accurate personalisation. In other words, they sand somewhat the digital mirror which very large platforms hold to consumers. This is done by limiting the use of sensitive personal data for personalising advertisements, offering a (limited) right to personalisation options as well as, more forcefully, banning ad personalisation for children. If granularity in digital twins of EU consumers breeds vulnerability in human consumers, as the BEUC

[132] According to Article 28 (7), DMA, "the management body of the gatekeeper shall define, oversee *and be accountable for* the implementation of the governance arrangements of the gatekeeper that ensure the independence of the compliance function, including the division of responsibilities in the organisation of the gatekeeper and the prevention of conflicts of interest". Article 37(3) is more detailed about conflicts Auditors may find themselves in.

report on Consumer Protection 2.0 convincingly argues, this strategy may not be ill conceived, and the questions are mainly whether the approach should be pursued more vigorously and whether the enforcement mechanisms are robust.

Regarding substantive rules, one regulatory option will need more attention, namely whether the law could weaponise rather than hinder personalisation. After all, if platforms have granular information about age, why should they not be submitted to an obligation to communicate to children in an age-appropriate manner rather than allowed to have one single communication for children of all ages. More generally, could platforms be asked to personalise for good in exchange for being generously let to harvest data for free? Regarding enforcement, a question for the next phase of legal reform will be whether AI assisted enforcement could help control all the new reporting DMA and DSA mandate.