BEUC The European Consumer Organisation

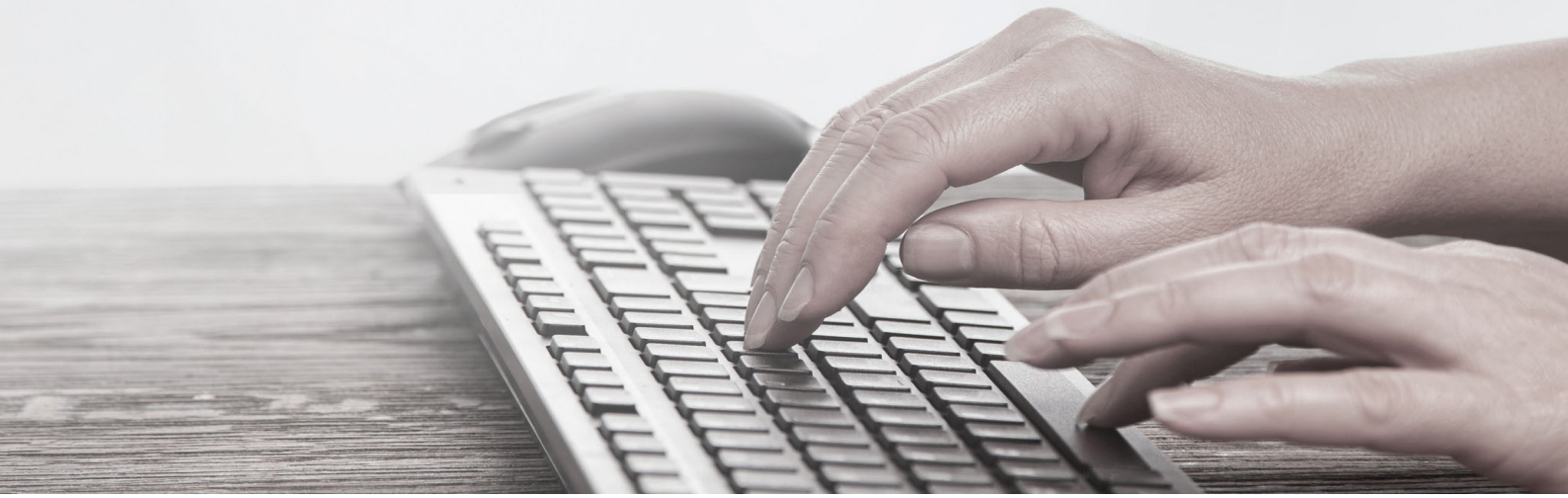
EU CONSUMER PROTECTION 2.0

THE REGULATORY GAP: CONSUMER PROTECTION IN THE DIGITAL ECONOMY

Addendum to the report 'Structural asymmetries in digital consumer markets'

Natali Helberger
Hans-W. Micklitz
Peter Rott

December 2021



ADESSIUM FOUNDATION
European University Institute — Robert Schuman Centre for Advanced Studies
IViR Institute for Information Law
Carl von Ossietzky Universität Oldenburg

The Regulatory Gap: Consumer Protection in the Digital Economy

Addendum to the report 'Structural asymmetries in digital consumer markets'

Hans-W. Micklitz[i], Natali Helberger[ii], Peter Rott[iii]

[i] Professor for Economic Law, Robert Schuman Centre for Advanced Studies at the European University Institute, with a broad track record in European Private and Economic Law, National and European Consumer Law, Legal Theory.

[ii] Distinguished University Professor of Law and Digital Technology, with a special focus on AI at the University of Amsterdam.

[iii] Interim Chair of Civil Law, Commercial Law and Information Law at Carl von Ossietzky University of Oldenburg, Germany.

Table of Contents

I. The Four Regulations and the Consumer Acquis

(1) In 2020, BEUC commissioned a research study entitled *EU Consumer Protection 2.0: Structural asymmetries in digital consumer market*.[1] In that work, we developed the concept of digital vulnerability translated into the legal concept of digital asymmetry. The report concludes with recommendations in a broad perspective with an emphasis on data privacy policies and unfair commercial practices. Within less than half a year, the European Commission published four proposals which will shape the digital market in the EU for the years to come. These are, in chronological order:

- The Digital Governance Act (DGA)[2]
- The Digital Market Act (DMA)[3]
- The Digital Services Act (DSA)[4]
- The Artificial Intelligence Act (AIA).[5]

(2) Two further initiatives have been announced but have not yet led to a proposal for legislative action.

- The proposal for a Data Act including the review of the Directive 96/9/EC on the legal protection of databases[6] is announced for November 2021. It is about fairness in the allocation of economic value among actors of the data economy.
- Still pending and without a concrete time line there might be a proposal for an AI Liability Act. The theoretical and conceptual political debate is quite advanced, though.[7]

(3) We are not aware of any plans of the European Commission to update and adapt the consumer law acquis. So far, the European Commission seems to be in an evaluation process, seemingly relying on revised guidelines on Directive 2005/29/EC which aim at clarifying the potential impact of the UCPD on highly conflictual strategies such as dark patterns or on

---

1 Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax and Joanna Strycharz, EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets, A joint report from research conducted under the EUCP2.0 project, BEUC, March 2021.

2 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final, 25.11.2020 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

3 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final,15.12.2020

4 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final, 15.12.2020, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN

5 Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final, 21.4.2021.

6 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en

7 Zech, H. Liability for AI: public policy considerations. *ERA Forum* **22,** 147–158 (2021) https://doi.org/10.1007/s12027-020-00648-0

whole business models such as personalised advertising.[8] The current guidelines date back to 2016.[9] Implicit to such thinking is the assumption that the current consumer acquis suffices to handle the new challenges.

(4) In the light of the powerful initiative of the European Commission to lay down a framework for the digital economy that attracted political and academic attention worldwide, it is all the more important to investigate whether and to what extent the four proposed acts altogether – in the following simply 'the Four' - include the consumer perspective and the level of protection offered to consumers vis-à-vis digital market practices that create or abuse structural, relational or informational vulnerabilities. In consumer advocacy there is a certain tendency to focus on the AIA. Whilst this is undoubtedly necessary, such a rather limited focus falls short of placing the consumer in the much broader framework that the EU is about to establish and that will in all probability design the digital markets in the EU for many years to come.

(5) Investigating the degree of consumer protection issues in the four new initiatives is important for two reasons: a) to establish to what extent the proposed rules are adequate and sufficient to address concerns about unfair digital commercial practices and b) because the Four aim at full harmonisation by way of a regulation and set new consumer law standards in the digital economy. Therefore, the question arises whether the Four would bar a potential update of the consumer acquis, or of further reaching consumer legislation at a national level. This would be even more problematic, if the Four did not take digital vulnerability/digital asymmetry into account. The consequence would be that the Four set the benchmark for consumer protection in the digital economy and that the existing acquis is reduced to a kind of safety net. The silence of the digital agenda of the European Commission with regard to consumer policy implications seems to contain implicitly a twofold message – firstly, that the existing consumer acquis suffices to deal with consumer issues in the digital economy and, secondly, that the Four regulate what needs to be regulated including potential consumer issues.

(6) If such a reading is correct, two options remain from a consumer policy perspective which could be pursued separately or jointly: to push for amendments of the Four so as to integrate consumer policy, and/or to seek clarification that the Four do not touch upon consumer policy so as to free up room for an update of the existing consumer acquis. That is why the potential scope and reach of the Four needs to be investigated. This study advocates the

---

8 See for an overall attempt to clarify first the meaning of digital commercial practices and outlining the degree to which they are covered by the consumer law acquis, H.-W. Micklitz/ L. A. Reisch/ S. Bietz, Algorithmen und Verbraucher. Eine Studie im Auftrag des Ministeriums für Ländlichen Raum und Verbraucherschutz (MLR) Baden-Württemberg, Stuttgart. Friedrichshafen: Forschungszentrum Verbraucher, Markt und Politik | CCMP (Hrsg.), 2020

9 Commission Staff Working Document Guidance on The Implementation/Application Of Directive 2005/29/EC on Unfair Commercial Practices Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses SWD/2016/0163 final, 25.5.2016.

urgent need to update the existing consumer acquis through the introduction of a revised Art. 5 a) UCPD.

(7) However, even if the Four do not preclude an upgrading of the existing consumer law acquis and even if the European Commission would be read to adapt the UCPD as proposed, they raise an additional concern from a consumer perspective. Roughly speaking, the European Commission proposes only a broad regulatory framework – in the language of the 'new approach', which later became the 'new legislative framework' (NLF).[10] The European Commission lays down 'general requirements' which will have to concretised by the European Standardisation Bodies CEN, CENELEC and ETSI. Compliance with those legally non-binding standards guarantees free access to the digital market. Already the new approach, adopted in 1985 prior to the Single European Act, provoked strong reactions from consumer advocacy, not least because of the unsettled role of consumer organisations in providing input to the technical standardisation. ANEC, the consumer's voice in standardisation, has a right to participate but no right to vote.

(8) The reliance on standardisation in the Four does not really come as a surprise, though. In light of the self-claimed success of the New Approach/NLF, the key role of standardisation bodies in the regulation of the digital economy was foreseeable. It will have to be shown though that the renewed trust in standardisation raises ever stronger concerns from a consumer law, if not a constitutional law perspective. That is why elaborating on the key role of standardisation and the potential deficiencies constitutes a second major concern.

(9) In the following, we will first elaborate on the scope and reach of the Four (under II), before we investigate the relationship between standardisation and consumer protection (under III). The obvious next step then is to dig deeper into the content of the Four. This is done against the background of the main report, with a strong focus on digital vulnerability/digital asymmetry of unfair data privacy policies and unfair commercial practices (under III). The addendum is not meant to fully discuss all the implications for consumers and the potential deficiencies.[11] A second disclaimer is needed: The analysis focuses on the digital economy; it does not discuss the old economy. Therefore it does not discuss to what extent similar rules can cover both strands of the economy.

---

10 The so-called New Approach was approved by the Council on 7 May 1985 in its 'Resolution on a New Approach to technical harmonization and standards', OJ 1985 C 136/1. In 2008, this approach was updated by the so-called New Legislative Framework, which comprises Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products, OJ 2008 L 218/30; Decision 768/2008 on a common framework for the marketing of products, OJ 2008 L 218/82; and Regulation (EU) 2019/1020 on market surveillance and compliance of products, OJ 2019 L 169/1.

11 See, for instance, the reactions of BEUC on the DMA https://www.beuc.eu/publications/beuc-x-2021-030_digital_markets_act_proposal.pdf; DSA https://www.beuc.eu/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf and the DGA https://www.beuc.eu/publications/beuc-x-2021-026_data_governance_act_position_paper.pdf, on the AIA https://www.beuc.eu/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf

II. The Preclusionary Effect of the Four Regulations

(10) The four regulations taken together should be understood as an attempt to set up a regulatory framework in which the digital internal market could blossom while dealing with the risks for consumers, fundamental rights and the digital economy from the proliferation of AI and AI-driven applications, the increasingly central role that data is playing as an economic asset, the winner-takes-it-all dynamics of digital markets, as well as the central position of a small number of (very large) tech companies. All four regulations are based on Article 114 TFEU – the DGA also on Article 16 TFEU – and aim at full harmonisation by way of a regulation. However, it is striking to see that the objective of achieving full harmonisation is more often than not openly addressed, unlike in the recently revised consumer law directives where the 'level of harmonisation' is determined in one specific article.[12] Instead, one has to study the Four carefully to recognise the regulatory 'philosophy'.

(11) The proposals seem to deliberately avoid full harmonisation language. The respective rules on the scope of application, however, all point to full harmonisation: Already the choice of a regulation (and not a directive) signal the intention of the European Commission to lay down a unified framework, with a strong role for the EU in defining the scope and substance of the regulatory framework for the Digital Decade and a conferral of implementing power to the European Commission, including the power to adopt delegatory acts and enforce the rules.[13] The declared goals are to approximate national regulatory measures to avoid or end fragmentation of the internal market and ensure legal certainty for developers.[14] In a first step the competences are transferred to the EU subject to a few clearly defined exceptions, for instance military services. Within the fully harmonised scope, certain residual competences are delegated back to the Member States. The strategy implies that it is for the European Commission to supervise and monitor the residual competences of the Member States and thereby also takes a stronger coordinating role regarding national supervisory authorities and can, like in the case of infringements of the obligations for Very Large Online Platforms in the DSA, take over from, and exclude, the national Digital Services Coordinator.[15] That is why it is necessary to study the Four regulations in detail. For example, the degree of harmonisation within the AIA necessitates a look into the related provisions on 'prohibited practices', 'high risks' and 'certain risks.' Each risk category is, in principle, fully harmonised. Residual competences are granted within the particular category of risk. The overall fall back position for Member States is to rely on regulatory sandboxes so as to

12 See, for instance, Art. 4 Directive 771/2019.

13 See e.g. recital 103 and 104 of the DSA or Art. 73 AIA.

14 See e.g Recital 4 DSA.

15 See Recital 96 DSA.

allow innovation for SMEs and startups in particular, most prominently in Article 53 AIA. The purpose of the sandboxes is not to test higher standards of consumer protection, but to lower the standards of control so as to facilitate market access for newcomers.[16] The details will have to be adopted in line with the committee procedure, Article 74 AIA.

(12) In the following we will provide an overview of the Four in order to identify the potential impact on the consumer acquis.

1. DGA and the Consumer Acquis

(13) The DGA defines its scope in Article 1:

> (1) This Regulation lays down: (a) conditions for the re-use, within the Union, of certain categories of data held by public sector bodies; (b) a notification and supervisory framework for the provision of data sharing services; (c) a framework for voluntary registration of entities which collect and process data made available for altruistic purposes.
>
> (2) This Regulation is without prejudice to specific provisions in other Union legal acts regarding access to or re-use of certain categories of data, or requirements related to processing of personal or non-personal data. Where a sector-specific Union legal act requires public sector bodies, providers of data sharing services or registered entities providing data altruism services to comply with specific additional technical administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act shall also apply.

(14) The DGA should be read as an effort to promote the sharing of personal and non-personal data as a means to stimulate AI innovation and the competitiveness and sovereignty of digital markets, also for SMEs and parties other than the large tech platforms.[17] Of particular interest for consumers are the rules on 'data intermediaries' which should play a key role in the overall intention to pave the way for 'data sharing'. Recital 22 sends a clear message:

> Providers of data sharing services (data intermediaries) are expected to play a key role in the data economy, as a tool to facilitate the aggregation and exchange of substantial amounts of relevant data. Data intermediaries offering services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialised data intermediaries that are independent from both data holders and

---

16 See Recital 72 AIA: "The objectives of the regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems with this Regulation and other relevant Union and Member States legislation; to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, and to accelerate access to markets, including by removing barriers for small and medium enterprises (SMEs) and start-ups."

17 On the broader debate on the private law of data, see Ph. Hacker, Datenprivatrecht, Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB, Mohr Siebeck 2020.

> data users can have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power….

(15) Data sharing is seen as a means to promote the digital market and increase innovative potential through creating an enabling and trustworthy environment for the sharing of personal and non-personal data via data intermediaries (DSA). The German debate turns around intermediaries as '*Datentreuhänder*' (data custodian).[18] Such an objective requires a regulatory framework of 'trust', where consumers are ready to share their data with intermediaries. Trust shall set incentives for consumers to voluntarily engage with the data intermediaries. The DGA lays down a number of conditions that data sharing services must comply with, including obligations to protect the security of the data, have procedures in place to prevent fraudulent use of the data and a prohibition of sharing the data for other purposes.[19] The regulatory means are derived from private law – autonomy, contract and consent shall guarantee that the three parties – the owner of the data, the user of the data and the intermediary come together. The DGA does not define intermediaries despite the conceptual uncertainties.[20] The EU Commission differentiates between data marketplaces, industrial data platforms, data trustees, data collaboratives, data cooperatives, and "Personal Information Management Systems" (PIMS).

(16) The latter are of particular importance for consumers. This is not the place to engage with details. What matters is that the DSA relies on 'voluntary industry standards' in an entirely new field of law. One might wonder to what extent the envisaged 'DATA Act' will provide for further specifications on data sharing and the role of data intermediaries. Strikingly, however, the DGA does not convey any actionable rights of the users of data sharing services to demand proper functioning and transparency, with exception to a general right to lodge a complaint that however does not specify what protection worthy expectations users have vis-à-vis data sharing intermediaries.[21] Art. 11 DGA only formulates a due diligence obligation stating that "the provider offering services to data subjects shall act in the data subjects' best interest, when facilitating the exercise of their rights, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses." The innocuous absence of concrete consumer rights and the strong focus on protecting consumers' interest indirectly by laying down the conditions for the safe functioning and use of digital services is a tendency that can be observed through all Four regulations, as we will show throughout this addendum.

---

18 See H. Richter, Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance", Zeitschrift für Europäisches Privatrecht, 2021 forthcoming.

19 See Art. 11 DGA.

20 See BEUC, loc. cit.

21 Arts 24 and 25 of the DGA.

2. *DMA and the Consumer Acquis*

(17) The DMA does not mention the term 'full harmonisation'. The purpose, however, becomes clear in Article 1 (5,) which reads as follows:

> Member States shall not impose on gatekeepers further obligations by way of laws, regulations or administrative action for the purpose of ensuring contestable and fair markets. This is without prejudice to rules pursuing other legitimate public interests, in compliance with Union law. In particular, nothing in this Regulation precludes Member States from imposing obligations, which are compatible with Union law, on undertakings, including providers of core platform services where these obligations are unrelated to the relevant undertakings having a status of gatekeeper within the meaning of this Regulation in order to protect consumers or to fight against acts of unfair competition.

(18) The DMA is meant to complement Article 102 TFEU which deals with the abuse of a dominant position. The digital economy has brought competition law into the limelight as a kind of last resort and safety net so as to deal with possible anticompetitive practices of the GAFAs (Google, Apple, Facebook, Amazon) in the form of data privacy policies, standard contract terms or commercial practices. In the last years, competition authorities have increasingly referred to competition law more generally so as to prohibit practices regarded as being detrimental to consumers. An outstanding example is the so-called Facebook decision by the German *Bundeskartellamt* (German Cartel Office), which has raised much attention, politically as well as academically. Within the scope of the DMA there is neither space for national competition authorities nor for private enforcement of antitrust injuries. This would mean that the Member States' cartel authorities are deprived of the possibility to use national competition law to deal with the market power of the gatekeepers.[22] More generally speaking, there is an unclear overlap between the control of unfair terms in b2b and b2c relationships and the competences of the European Commission.[23]

(19) Last but not least, Article 7 requires that:

> The measures implemented by the gatekeeper to ensure compliance with the obligations laid down in Articles 5 and 6 shall be effective in achieving the objective of the relevant obligation. The gatekeeper shall ensure that these measures are implemented in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC, and with legislation on cyber security, consumer protection and product safety.

---

22 For details see J. Basedow, Basedow, Jürgen, Das Rad neu erfunden: Zum Vorschlag für einen Digital Markets Act (Reinventing the Wheel: The Proposal for a Digital Markets Act). Zeitschrift für Europäisches Privatrecht (ZEuP), Vol. 29, 2021, forthcoming, Max Planck Private Law Research Paper No. 21/2, Available at SSRN: https://ssrn.com/abstract=3773711 and G. Monti, Monti, Giorgio, The Digital Markets Act – Institutional Design and Suggestions for Improvement (February 22, 2021). TILEC Discussion Paper No. 2021-04, Available at SSRN: https://ssrn.com/abstract=3797730 or http://dx.doi.org/10.2139/ssrn.3797730.

23 See Basedow loc. cit, under reference to Art. 6 j) DMA.

(20) This means that the gatekeepers have to respect the consumer acquis. Recital 58 states: 'The gatekeepers should ensure the compliance with this Regulation by design.' However, this clear wording was not integrated into Article 7. What remains is the 'should', which leaves space for the gatekeepers to argue that 'should' does not constitute a binding obligation.

(21) Does this imply that a revision of the consumer acquis is barred from imposing on companies within the scope of the DMA 'compliance by design'? *Lex posterior derogat legi priori*? Or does the DMA provide for a general framework only which may be adapted for specific sectors / issues? A clarification would be helpful.

3. DSA and the Consumer Acquis

(22) The DSA is much more outspoken on harmonisation issues, in the explanatory memorandum, in the recitals as well as in the legal provisions. Article 1 reads:

> (1) This Regulation lays down harmonised rules on the provision of intermediary services in the internal market. In particular, it establishes: (a) a framework for the conditional exemption from liability of providers of intermediary services; (b) rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services; (c) rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and coordination between the competent authorities.
>
> (5) This Regulation is without prejudice to the rules laid down by the following ..(h) Union law on consumer protection and product safety, including Regulation (EU) 2017/2394 [on cooperation between national authorities responsible for the enforcement of consumer protection laws - HM];

(23) Article 1 (5) is the legacy of the interplay between the E-Commerce Directive of 2000 and the Distance Selling Directive 97/7/EC, which was later integrated into the Consumer Rights Directive 2011/83/EU. Article 1 (5) sounds reassuring, although there are questions in two directions. Why does this paragraph explicitly refer to Regulation 2017/2394 but not, for example, to Directive 2020/1818 on representative actions? Does it mean that the latter does not come under the formula 'without prejudice'? This would fit to the pending and not yet solved problem of the relationship between the regulation of enforcement in the fully harmonised GDPR and the discretion of Member States to introduce additional remedies for consumer organisations. This will be discussed below.[24] However, there is a second concern in that the 'without prejudice' formula does not clearly indicate whether and to what extent the consumer law acquis could be upgraded even if the DSA fully harmonised a certain area, although without taking the consumer law perspective sufficiently into account.

[24] See for details under II.5.

(24) One of the major concerns of the DSA is to reform the responsibility and liability regime of providers for intermediary services.[25] This is not the place to do justice to the proposed reform and to contrast it, for instance, with the elaborated proposal of the European Law Institute.[26] What matters is that the proposed regime aims at full harmonisation and does not leave room for an upgrade of the consumer acquis to the extent that consumer law questions are harmonised by the DSA (e.g. the provisions of transparency of online advertising in Art. 24 DSA). Also, it is unclear to which extend the DSA still leaves room to concretise and adopt further-reaching legislation to protect the interests not only of consumers, but also of the society vis-à-vis the use and functioning of e.g. recommender systems on VLOPs (art. 29 DSA). Seeing that the operation of recommender systems touch upon both, consumer interests but also the realisation of public values more generally (pluralism, due prominence of public interest content, etc.) maximum harmonisation would be even more problematic as it impinged on the ability of member states to regulate in matters that have been traditionally left to their authority, including cultural matters as well as matters of national security. How the DSA relates to the announced proposal on AI liability remains to be seen.

(25) And again, it is striking that consumer interests are only marginally protected, at least in relation to Very Large Online Platforms. The list of potential systemic risks of Art. 26 focuses on the dissemination of illegal content, negative effects for fundamental rights and intentional manipulations that can negatively affect the public discourse or electoral processes but not risks for users in their role of consumers. The most clearly consumer-related provision in the DSA is Art. 24 DSA with rules regarding online advertising transparency. But it is unclear what this provision adds to the UCP and GDPR. Finally, Art. 29 and the provisions on recommender systems aim at ensuring more transparency and options for consumers to be able to switch between personalised and non-personalised options. The provision, however, does not provide for an obligation but leaves considerable discretion to Very Large Online Platforms to decide and if applicable, which choices to make available to consumers.[27]

(26) Among others, the DSA contains rules on data access. They reflect the move, also in the academic literature, from data ownership to data '*Treuhänder*' (custodians), to the debate of who should get access to data and under what conditions. There are strong voices which

---

25 For a detailed analysis, see Gerald Spindler: Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU-Digital Services Act (Teil 1) GRUR 2021, 545; Louisa Specht-Riemenschneider and Franz Hofmann, Verantwortung von Onlineplattformen: Ein Plädoyer für funktionszentrierte Vrkehrspflichten, Manuscript 2021 on file with the author.

26 Available at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf. See also Christoph Busch, Europäische Modellregeln für Online-Vermittlungsplattformen, in Peter Rott and Klaus Tonner (eds), Das Recht der Online-Vermittlungsplattformen, 2018, 223.

27 Helberger et. Al. (2021). Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath, Internet Policy Review.

request access for research purposes so as to be able to look into the famous black box or, more generally, to try to understand how machine learning techniques and neuronal nets operate in practice.[28] As long as there is no access, research is limited to so-called 'tinkering'.[29] Meanwhile, the debate has gained momentum, not least through the involvement of competent ministries who are seeking advice on how to regulate data access for research purposes.[30] The DSA is ahead of the curve. Article 31 reads:

> (2) Upon a reasoned request from the Digital Services Coordinator of establishment or the Commission, very large online platforms shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraphs 4 of this Article, for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks as set out in Article 26(1).
>
> (4) In order to be vetted, researchers shall be affiliated with academic institutions, be independent from commercial interests, have proven records of expertise in the fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request.

(27) The data access provisions in Article 31 have been long awaited and are an important step towards gaining a better evidence-based understanding of the potential systematic risks that algorithmic systems in the hands of very large online platforms can create. Seeing the complexity of the issues involved, academic research has an important societal role to play here to support regulators, platforms and consumer advocates alike. Having said so, while Art. 31 DSA is an important step in the right direction, the provision also has its limitations. For instance, data access under draft Art. 31 is strictly limited to the task of identifying a pre-defined list of systemic risks (see Art. 26 DSA) and does not include data access to e.g. study the implications of behavioural commercial targeting strategies for consumer rights, or other fundamental rights than those mentioned in Art. 26 DSA. The personal scope of Art. 31 DSA is also limited, only covering researchers and not data journalists, civic society or consumer organisations. Finally, while demanding access to data for researchers can be an important step towards ensuring transparency and understanding, data access alone will not result in new insights. Instead, policy makers and regulators also need to create the conditions so that researchers can undertake this societal task. On top of this, there are no remedies foreseen

---

28 See the report of the Sachverständigenrat für Verbraucherfragen (Advisory Board for Consumer Affairs), Consumer Friendly Scoring, 2019 https://www.svr-verbraucherfragen.de/en/wp-content/uploads/sites/2/Report-2.pdf

29 M. Perel and N. Elkin-Koren, BLACK BOX TINKERING: Beyond Disclosure in Algorithmic Enforcement 69 Fla. L. Rev. 181 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2741513.

30 Louisa Specht-Riemenschneider Im Auftrag des Bundesministeriums für Bildung und Forschung „Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online- Wirtschaft, Energie und Mobilität" August 2021, who discusses also the respective rules in the DSA.

in case the national authority denies access. How can consumer policy progress without consumer research based on data access?

4. *AIA and the Consumer Acquis*

(28) Throughout the text, the AIA uses the language of 'Union legislation', all in all 21 times, but without explicitly stating that the overall purpose is to fully harmonise AI in the EU. The AIA does not explicitly address consumer concerns, even if it is of outmost importance for the consumer.[31] The AIA refers in Article 3(4) to the 'user' as 'any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity'. This definition excludes individuals using AI systems as 'users' under the AIA unless they are doing so in their professional capacity, as well as those individuals who are subject to the use of an AI system.[32] One might therefore conclude that the AIA only indirectly addresses the consumer.

(29) Nevertheless, the 'consumer' appears five times in the proposal, four times in the Explanatory Memorandum, once in the recitals and not at all in the Articles. The context is always the same. Consumer protection shows up in relation to fundamental rights. Recital 28 is telling:

> Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non-discrimination, consumer protection, workers' rights, rights of persons with disabilities, right to an effective remedy and to a fair trial, right of defence and the presumption of innocence.

(30) This means consumer concerns can only be channelled into the AIA if they enjoy 'constitutional status' under Article 38 of the Charter or be subsumed under one of the more outspoken rights. In short, the consumer acquis matters only as far as it can be 'constitutionalised' and 'individualised'. This is a high benchmark to pass.

a) Scope

(31) The scope is broad especially when read together with the very inclusive definition of AI systems in 3 (1) AIA:

> Article 1 This Regulation lays down: (a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union; (a) prohibitions of certain artificial intelligence practices; (b) specific requirements for high-risk AI systems and obligations for operators of such systems; (c) harmonised transparency rules for AI

---

31 See Ch. Wendehorst, The Proposal for an Artificial Intelligence Act COM(2021) 206 from a Consumer Policy Perspective, Gutachten im Auftrag des Österreichischen Ministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz, October 2021, on file with the author.

32 BEUC Position Paper on AIA, loc cit. Fn. 12

> systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content; (d) rules on market monitoring and surveillance.

(32) Contrary to Article 1(5) DSA there is no 'without prejudice' clarification. The Explanatory Memorandum makes clear where the wind blows[33]:

> Other manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by the *existing* data protection, consumer protection and digital service legislation that guarantee that natural persons are properly informed and have free choice not to be subject to profiling or other practices that might affect their behaviour.

(33) This blunt statement suggests that the European Commission starts from the premise that the existing consumer and digital service legislation suffice to protect the consumer. The question remains whether the AIA is meant to 'freeze' consumer law or whether there is room for an upgrade of consumer protection even within the scope of the AIA. The wording makes one fear the worst. In order to fully catch the importance of the full harmonisation approach of the AIA it is crucial to follow the distinction between prohibited practices, high risks and certain risks, as the AIA specifies with regard to each level of risk the discretion left to the Member States.

b) Prohibited Practices

(34) Article 5 AIA prohibits four particular forms of artificial intelligence which may produce physical or psychological harm: (1) subliminal beyond a person's consciousness, (2) exploitation of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, (3) evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics (social scoring) real-time remote biometric identification systems subject to residual competences left to the Member States in Article 5 (4) AIA.

(35) There are serious doubts whether and to what extent the four prohibitions could turn into an effective tool. Article 5 read in the full harmonisation rhetoric claims to fully cover all potential physical or psychological harms. This does not only seem to be bold but simply wrong.[34] Article 5 AIA is an outstanding example to demonstrate the inappropriateness of the full harmonisation approach. Article 5 AIA bans certain forms of algorithmic manipulation, namely when those exploit the vulnerability of particular groups of persons (the traditional vulnerable groups), in a manipulative fashion and producing physical or psychological harm. This is the extreme case of exploiting group specific digital vulnerabilities.[35] It is therefore also a very unlikely case to happen. The majority of cases of

---

33 P. 14

34 See Michael Veale and Frederik Borgesius, Demystifying the Draft EU Artificial Intelligence Act, Forthcoming in (2021) 22(4) Computer Law Review International.

35 For a critique see also Ch. Wendehorst, loc. cit.

exploitation of digital vulnerabilities will lie below that threshold but still be problematic from a consumer protection point of view. Art. 5 AIA does not address digital vulnerability as a more general phenomenon, contrary to the findings in philosophy, political science, communication theory and law. The big question remains whether Art. 5 AIA will preclude additional consumer regulations that tackle situations in which digital marketing strategies are used to establish structural, relational or informational asymmetries in a way that materially distort autonomous decision making, irrespective of whether or not that user belongs to a particular group.

(36) Again there is more to consider. Does full harmonisation mean that the AIA precludes the possibility to ban practices which create 'only' economic harm to consumers? No and yes. No, because the AIA aims at the protection of fundamental rights. Article 38 of the Charter states that union policies shall guarantee a high level of consumer protection. Two barriers have to be overcome: Article 38 does not grant rights but lays down only a general principle; secondly, economic harm must form an integral part of the principles. Whilst this cannot be excluded, the degree to which consumer law may be constitutionalised through Article 38 has not yet been clarified by the ECJ.[36] It is tempting to argue that the AIA does not touch on the protection against potential economic risks and therefore leaves this issue to other legal instruments such as the Unfair Commercial Practices Directive, or to the Member States. However, does this argument hold in light of the overall philosophy of creating a foreseeable and standardised legal framework for the use of AI systems which aims at establishing legal certainty?[37] One should not forget that the Court of Justice considered the Product Liability Directive to fully harmonise the field,[38] which produced an outcry by the Member States but no legislative action to remedy the highly problematic reasoning of the Court.[39]

c) High Risks

(37) The regulation of 'high risk' AI system covers most of the AIA, it reaches from Article 5 to 51 AIA. The AIA defines high risks and draws a distinction between AI systems as safety components and stand-alone AI systems which affect health, safety and fundamental rights (Article 7 AIA).[40] The former are identified in Annex II through an enumeration of the affected

---

36 Same direction Ch. Wendehorst, loc. cit. distinguishing between safety risks and fundamental rights risks.

37 On the potential preclusionary effects of the AIA, see Martin Ebers, Veronica R.S. .Hoch, Frank Rosenkranz, Hannah Ruschemeier, Björn Steinrötter, The European Commission's Proposal for an "Artificial Intelligence Act" – A Critical Assessment by Members of the Robotics & AI Law Society (RAILS), available on the website of RAILS: www.ai-laws.org

38 ECJ,25/4/2000, Case C-52/00 *Commission v France*, ECLI:EU:C:2002:252, paras 17 ff.; Case C-154/00 *Commission v Greece*, ECLI:EU:C:2002:254, paras 10 ff.; Case C-183/00 *María Victoria González Sánchez v Medicina Asturiana SA*, ECLI:EU:C:2002:255, paras 26 ff.

39 On the reaction of the Member States see Peter Rott, Produkthaftung und Vollharmonisierung – der Rat kartet nach, Recht der Internationalen Wirtschaft 2003, Issue 4.

40 See Martin Ebers, Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, in: Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò (eds.), The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, pending for publication, Cambridge University Press 2022.

EU legislation. The latter cover eight systems listed in Annex III: biometric identification and categorisation (e.g. facial recognition), management and operation of critical infrastructure (e.g. transport), educational and vocational training (e.g. scoring of exams), employment, worker management and access to self-employment (e.g. CV-sorting), access to and enjoyment of essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan), law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence), migration, asylum and border control management (e.g. verification of authenticity of travel documents), and administration of justice and democracy (e.g. applying the law to a concrete set of facts). It is highly debateable whether the list is complete and whether potential economic risks can per se be regarded as not being high-risk.[41] However, the way in which the European Commission is seeking regulatory competences is remarkable. The AIA together with the Annex is meant to set up a complete list of high-risk systems in the field of standalone risks, where the technological progress is particularly fast and where no experience with previous regulatory tools exists. The AIA leaves it for the European Commission, and the European Commission alone, to amend the list, without the participation of the Member States or the European Parliament (see below under II). Member States retain the power to derogate from the conformity assessment procedure 'for exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets'. Consumer protection does not constitute a reason for derogation. Whatever the Member States decide, their derogation is closely monitored and supervised by the European Commission Article 47 AIA.

(38) There is a number of provisions that address users directly, but in most instances the focus is on professional users, Article 3(4) AIA, such as inter alia risk management (Article 9 AIA), transparency requirements (Article 13 AIA), human oversight (Article 14 AIA), automatically generated logs (Article 20 AIA), as provider of high risk systems placed on the market (Article 28 AIA), instructions for use (Article 29 AIA), or as addressees of targeted Member States' actions (Article 55 AIA). It has to be recalled that according to Art. 3(4) AIA, 'users' are understood in the sense of professional users that use and AI system under their authority and not in the course of a personal non-professional activity. Practically this means that these obligations do not apply to consumers.

d) Certain Risks

(39) The so-called 'certain risks' are condensed in one single conclusive rule, Article 52 AIA. Contrary to prohibited practices and high risks, Art. 52 AIA establishes transparency obligations for virtual agents and alike, deepfakes and emotion recognition systems to the

[41] Problematising the risk based approach P. Palka, The Phantom Menace: A Critique of the European Commission's Artificial Intelligence Act Proposal, on file with author, See also Ch. Wendehorst, loc. cit. p. 9 with the proposal to integrate 'AI systems intended to be used by children and similar vulnerable groups as well as AI systems to be used in situations that create specific vulnerabilities, such as virtual assistants used by consumers for taking important decisions'.

benefit of natural persons, which includes consumers. It deserves to be highlighted that the consumer is only directly addressed, when it comes to low level risks.

(40) There are no particular rulings which grant Member States discretion, neither are there rules which empower the European Commission to further specify the notion of certain risks or to develop a particular annex. That is why Art 52 AIA has to define what kind or risks shall be regulated. All those potential risks, which are not covered by Art. 52 AIA, remain unregulated subject to the acquis communautaire. The European Commission proposes three types of risks 1) AI systems intended to interact with natural persons, 2) emotion recognition systems or biometric categorisation, 3) AI systems that generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'). The heading ties together the regulatory message: these three 'risks' are subject to transparency requirements and information obligations. The system can be fully automated, there is no human oversight needed contrary to 'high risks', Article 14 AIA. It is amazing to see how much trust the European Commission has in information processing capacities of consumers, an assumption which runs counter to all theoretical/conceptual and empirical findings on the universal vulnerability of consumers.

(41) Just to repeat for the sake of clarity, AI systems which are not prohibited and which do not come under the high risks Annex II and III are NOT automatically covered by Article 52 AIA. The provision is not a catch-all safety net, if it covers only three types of risks and again – these risks are fully harmonised. There is no leeway for Member States to deviate from Article 52 AIA.

e) Minimal Risks

(42) All other AI systems are submitted to the general rules of the acquis communautaire, in our case the consumer protection and data privacy regulation.[42] Providers of those AI systems are free to choose to voluntarily apply the requirements for trustworthy AI and adhere to voluntary codes of conduct (Article 69 AIA). There is not even an obligation to inform the consumer that they might be used as guinea pigs, let alone a kind of a fall back for Member States who have discovered that there are risks that deserve to be regulated. The full harmonisation approach leaves it to the European Commission to eventually take measures so as to initiate a formal amendment of the regulation. The European Commission is empowered to change the Annexes II and III unilaterally.

f) CE-Mark

(43) Prior to the adoption of the General Product Safety Directive 92/59/EC, consumer circles were unsuccessfully advocating the introduction of a particular 'safety mark'. The European Commission resisted and paved the way for a CE mark which can have many meanings,

42 See Ebers, loc. cit.

reaching from compliance with pure technical specifications up to product safety requirements. The AIA embarks on new territory. The CE mark shall now indicate compliance with protection against physical or psychological harm and with respect for fundamental rights. Recital 67 makes it abundantly clear that there is no room for deviations:

> Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.

5. *Relationship to Substantive Private Law and Individual/Collective Remedies*

(44) The four regulations lay down mandatory requirements that should be respected by the different market players and supervised and monitored either by the European Commission (DMA), or by the Member States and the European Commission (DSA and AIA) jointly. In contrast, the Four Regulations do not introduce private law remedies, neither individual nor collective, neither for companies nor for consumers and their organisations. At the same time, the envisaged pieces of legislation include duties, for example on online platforms, that would seem to be apt for private enforcement, such as the duty to verify the trader's information on his name and address under Article 22 DSA, or the prohibition of harmful AI practices under Article 5 AIA.

(45) The chosen public law approach raises the question, well-known from the area of financial services,[43] to what extent the obligations imposed on the market players shall be exclusively supervised by public authorities or whether they also constitute private law obligations which open space for national private law remedies.

(46) In relation to the General Data Protection Regulation (GDPR), this has triggered the debate as to whether not only substantive law but also enforcement has been fully harmonised in that enforcement mechanisms that are not mentioned in the GDPR are not allowed.[44] On preliminary request by the German Federal Supreme Court (*Bundesgerichtshof*; BGH), this question is currently pending before the Court of Justice.[45] In relation to the proposed Digital Services Act, *Janal* has suggested that duties under that legislation should not be seen as duties of care under tort law.[46]

---

43 Gerald Spindler, loc. cit. who points to the lack of private law remedies. From a consumer law angle see Federico della Negra, MiFID II and Private Law, Enforcing EU Conduct of Business Rules, Hart Publishing 2019.

44 In favour of full harmonisation of enforcement: Helmut Köhler, Durchsetzung der DS-GVO - eine Aufgabe auch für Mitbewerber oder zumindest für Verbraucherverbände?, Wettbewerb in Recht und Praxis 2019, 1279, 1284 f. In favour of the possibility of private enforcement: Fabian Uebele, Datenschutzrecht vor Zivilgerichten, Gewerblicher Rechtsschutz und Urheberrecht 2019, 694, 699 f.

45 Case C-319/20 *Facebook Ireland Limited gegen Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.*.

46 See Ruth Janal, Haftung und Verantwortung im Entwurf des Digital Services Acts, Zeitschrift für Europäisches Privatrecht 2021, 227, 263.

(47) The question of an exclusion of private law remedies should be answered in the negative. The Court of Justice has always seen private enforcement as a useful if not necessary complement to public law enforcement even in areas where only public law enforcement was expressly required. In relation to the old Data Protection Directive 95/46/EC, the Court therefore accepted private law remedies by consumer organisations next to public law enforcement.[47] In the area of medical devices law, the Court of Justice left it to the Member States to foresee damage claims by victims of unsafe medicinal products (here: breast implants) against notified bodies that breached their duties under the Medical Devices Directive.[48] In the case of *Muñoz*, turning on quality standards for table grapes under Regulations (EEC) No 1035/72 and (EC) No 2200/96 on quality standards applicable to fruit or vegetables, which are public law regimes as well, the Court held that one of the aims of these regimes was to eliminate products of unsatisfactory quality from the market. Therefore, the full effectiveness of the rules on quality standards implied that it must be possible to enforce that obligation by means of civil proceedings instituted by a trader against a competitor. The Court argued that the possibility of bringing such proceedings strengthened the practical working of the Community rules on quality standards. As a supplement to the action of the authorities designated by the Member States to make the checks required by those rules it helped to discourage practices, often difficult to detect, which distort competition.[49]

III. The Regulatory Underground – Standardisation, Conformity Assessment and Certification

(48) An analysis of the Four would be incomplete without looking into the regulatory underground – the reliance on technical standards, on self- and third-party certification. There is a clear divide between the DGA and DSA on the one hand and the AIA on the other. In all three regulations, technical standards play a key role. However, within the DGA and DSA the European Commission relies on 'voluntary industry standards', that is, technical standards elaborated by CEN/CENELEC/ETSI in compliance with the Memorandum of Understanding which stood behind the new approach and which guides the NLF.

(49) In contrast, the AIA follows the regulatory logic of the NLF in the distinction between 'legally binding general requirements' and 'technical standards'. 'Technical standards' are not 'voluntary industry standards' but harmonised European standards as defined in Article

---

47 See CJEU, 29/7/2019, Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW e. V.*, ECLI:EU:C:2019:629.

48 See CJEU, 16/2/2017, Case C-219/15 *Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH*, ECLI:EU:C:2017:128. On damage claims under national law, see Carola Glinski and Peter Rott, Regulating certification bodies in the field of medical devices: The PIP breast implants litigation and beyond, European Review of Private Law 2019, 403 ff.

49 See ECJ, 17/9/2002, Case C-253/00 *Antonio Muñoz y Cia SA and others v Frumar Ltd and others*, ECLI:EU:C:2002:497, paras 29-31.

2(1)(c) of the Standardisation Regulation (EU) No. 1025/201,2 to which Article 3 (27) AIA refers: 'harmonised standard' means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation'. If the Commission makes such a request, it has to provide for funding, whereas voluntary industry standards are self-financed by the sectors concerned. The request necessarily combines the technical dimension with the legal dimension. The European Commission together with the European standardisation bodies have to assess compliance, and the European Commission shall publish the harmonised standard in the Official Journal, Article 10(5) and (6) Regulation (EU) No. 1025/2012. The regulatory technique implies that within the scope of the AIA, the European Commission is the master of the scene. It has a triple role: as instigator, it may make a request; as financier, it may influence the choice and, as compliance authority, it has to check whether the mandated standards respect the general requirements laid down in particular for high risk products.

(50) The AIA contains by far the most developed scheme on standardisation, on certification and on conformity assessment. The DGA and DSA with their trust in voluntary industry standards leave the elaboration to the self-set procedural rules of the European Standardisation Bodies in line with the Memorandum of Understanding. All three are only occasionally addressing the consumer directly. However, all three lay down the ground rules for the digital economy and the digital society. That is why there is at least an indirect impact on consumers which justifies the plea to integrate consumers and their organisations into the standardisation process.

1. DGA and the Consumer acquis

(51) At first glance, the DGA does not seem to be based to a comparable degree on standardisation, on conformity assessment procedures and on self- or third-party certification. There is nothing on harmonised standards, nothing on conformity, and certification is only mentioned in passing. However, a second look discloses that the core rules on data sharing are based on the availability of technical standards. Article 11(5) DGA sends the message: 'The provider shall facilitate the exchange of the data in the format in which it receives it from the data holder and shall convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union law or to ensure harmonisation with international or European data standards'. This is a necessary step to allow cross-border exchange. The European Data Innovation Board (Article 26 DGA) shall advise and assist the European Commission in promoting the development of appropriate technical standards which comply with the EU law, Article 27 DGA. As far as the data to be exchanged come under the scope of the GDPR, the European Standard Bodies are in charge of ensuring compliance with the legal requirements. Article 11 DGA imposes a set of obligations on the provider so as to ensure

compliance not only with the technical standards but also with the detailed set of safeguards. Third party certification is not foreseen.

(52) As is clear from the Memorandum,[50] there was disagreement between the Impact Assessment and the European Commission on how to deal with data altruism[51] and whether some sort of third-party control or even statutory control is needed. The impact assessment favoured a mandatory authorisation framework. The European Commission, because of 'additional concerns around the potential administrative burden', proposed as an alternative solution for organisation engaging in data altruism the possibility to register 'as a Data Altruism Organisation recognised in the EU'. This registry is believed to contribute to 'increasing trust', see Article 18 DGA.

2. *DMA and the Consumer Acquis*

(53) The DMA deals neither with standardisation nor with certification issues. However, Article 11 DMA makes it clear that the 'implementation shall not be undermined by any behaviour of the undertaking to which the gatekeeper belongs, regardless of whether this behaviour is of a contractual, commercial, technical or any other nature.'

(54) That is why technical standards, as far as they meet the requirements of Article 11 DMA, may be supervised and monitored by the European Commission which is the sole enforcement authority. This leads to the somewhat paradoxical result that the European Commission has to investigate, survey, monitor and even prohibit technical standards which the very same European Commission is promoting throughout its digital agenda and which in case of harmonised standards even require approval before they can be published in the Official Journal.

3. *DSA and the Consumer Acquis*

(55) The DSA is much more outspoken on the usefulness of technical standards. Throughout the document, the European Commission is speaking of 'voluntary industry standards'. There is not a single mention of harmonised standards. The spirit of the DSA is clearly formulated in recital 66:

> (66) ….To facilitate the effective and consistent application of the obligations in this Regulation that may require implementation through technological means, it is important to promote voluntary industry standards covering certain technical procedures, where the industry can help develop standardised means to comply with this Regulation, such as allowing the submission of notices, including through application programming interfaces, or about the interoperability of

50 Explanatory Memorandum p. 7.

51 On the difficulties, BEUC loc. cit.

advertisement repositories. Such standards could in particular be useful for relatively small providers of intermediary services. The standards could distinguish between different types of illegal content or different types of intermediary services, as appropriate.

(56) It light of the overall importance and to demonstrate the wide range of areas where technical standards are needed and relied upon, it might be worth quoting the respective Article 34 on standards in full:

1. The Commission shall support and promote the development and implementation of voluntary industry standards set by relevant European and international standardisation bodies at least for the following:

(a) electronic submission of notices under Article 14; (b) electronic submission of notices by trusted flaggers under Article 19, including through application programming interfaces; (c) specific interfaces, including application programming interfaces, to facilitate compliance with the obligations set out in Articles 30 and 31; (d) auditing of very large online platforms pursuant to Article 28; (e) interoperability of the advertisement repositories referred to in Article 30(2); (f) transmission of data between advertising intermediaries in support of transparency obligations pursuant to points (b) and (c) of Article 24.

2. The Commission shall support the update of the standards in the light of technological developments and the behaviour of the recipients of the services in question.

(57) In order to get an idea of the importance it would be necessary to check what kind of standardisation projects are already under way and to evaluate to what extent the list covers the relevant services provided under the DSA. The European Board for Digital Services, meaning the representatives of the Member States 'shall support and promote the development and implementation of European standards, guidelines, reports, templates and code of conducts as provided for in this Regulation'. A simple majority vote suffices, see Articles 47-49 DSA.

4. AIA and the Consumer Acquis

(58) The draft does not shy away in the recitals from using strong language so as to drive the risk-based approach home through extensive standardisation:

(61) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation..

(64) Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products.

(59) The AIA rules establish 'general requirements' in the meaning of the NLF with regard to 'high risk' AI systems on the creation of a risk management system (Article 9 AIA); on the quality

criteria for training, validation and testing data in relation to relevance, representativeness, accuracy and completeness (Article 10 AIA), inter alia to avoid biases and discrimination (Article 11, Annex IV AIA) and record-keeping (Article 12 AIA) provisions on transparency and user information (Article 13 AIA) on human oversight (Article 14) and obligations concerning the accuracy, robustness, and cybersecurity of systems (Article 15 AIA). These general requirements need to be concretised through harmonised technical standards. High-risk AI systems which are in conformity with harmonised standards and which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements of the AIA, Article 40 AIA. In case the general requirements or the harmonised standards are insufficient, or when there is a particular need to respect the safety and fundamental rights, the European Commission may, by means of implementing acts, adopt common specifications which concretise the general requirements, Article 41 AIA.

(60) By now, it looks as if the EU were a latecomer. The major international standardisation organisations, the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE) and the International Telecommunications Union (ITU), have already occupied the field. Martin Ebers[52] has given a thorough account on the initiatives taken; ISO/IEC on AI robustness, under development, e.g. standards relating to AI terminology, AI systems, trustworthiness, governance, ethics and machine learning, whilst ISO is working on software and system engineering, automatic identification and data capture, computer graphics, IT security, user interfaces, biometrics, cloud computing, IT Governance and Internet of Things. CEN/CENELEC may take over international standards provided they comply with EU legislation. The two European Standardisation Bodies have created a Focus Group which has developed a Road Map on Artificial Intelligence. Due to the temporal advance CEN/CENELEC as well as ETSI suffer from a strategic disadvantage. They have to 'upgrade' the international standards so as to make them compatible with the AIA requirements – health and fundamental rights. It is a well-known phenomenon in the drafting of the rules, that the institution which comes up first sets the tone, as each and every deviation requires justification. But a crucial question remains: can the NLF, which has a long-standing history in product regulation, be transferred *tel quel* from the world of engineers to the world of software scientists? Is standardisation contributing to the solution of problems that AI is creating?

(61) The AIA devotes particular attention to the conformity assessment procedure for high-risk AI systems in its two variations, self-certification and third-party certification. 'Conformity assessment' shows up 104 times in the document. The related rules (Article 43 AIA) are correspondingly extensive and comprehensive, providing legitimacy to the big players and

52 M. Ebers, loc. cit. 8-9.

make the lives of small companies and start-ups difficult'.[53] In the language of the AIA, high risk systems will have to comply with 'a set of horizontal requirements for trustworthy AI. Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle'.[54] As already said, these obligations provide legitimacy to the big players and turn into a burden for SMEs and start-ups. Whether this form of self-compliance provides for consumer protection is subject of controversy.

(62) When it comes to the distinction between self-certification and third-party certification, different rules apply to high-risk AI systems which are safety components of products or standalone AI systems. In the former group, the existing third party certification is extended beyond product safety towards the protection against physiological and psychological harm and respect for human rights.[55] This means that the so called notified bodies (Article 33 AIA) – the certification bodies – have to build competences far beyond product safety and enter into entirely new areas of skills to assess not only physiological harm which comes close to the protection against unsafe products but also to handle psychological harm. Here very different skills are needed. Are the notified bodies now required to hire psychologists and also human rights lawyers who are familiar with the growing intricacies of the Charter of Fundamental Rights? The AIA seems to take it for granted, although the European Commission is aware that additional resources are needed.[56] In the latter group – the stand-alone AI systems where little to no experience exists – self-certification is the rule, A The only exceptions are remote biometric identification systems, see Article 43 (1) and Annex VII AIA. Recital 64 states:

> Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for the remote biometric identification of persons, for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

(63) The design of the different conformity requirements for AI systems as safety components and standalone system lead to a paradoxical result: third-party assessment might have a role to play in the 'old' industries, where technology is an 'add-on' whereas third party assessment has practically no role in the world of the new risks – the physiological and

---

53 On this aspect in particular Palka, loc. cit.

54 Explanatory Memorandum p. 4.

55 Explantory Memorandum p. 5 and recital 30, where the products are listed.

56 Explantory Memorandum, 15 'The conformity assessment approach aims to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time.'

psychological harm and risks to fundamental rights. There is an obvious imbalance between the role of third-party assessment in product regulation and standalone technology. The overall idea is that the rather liberal self-assessment shall be compensated through appropriate enforcement mechanisms and the establishment of a European Commission run 'registry' (Art. 51): [57]

> A comprehensive ex-ante conformity assessment through internal checks, combined with a strong ex-post enforcement, could be an effective and reasonable solution for those systems, given the early phase of the regulatory intervention and the fact the AI sector is very innovative and expertise for auditing is only now being accumulated. After the provider has performed the relevant conformity assessment, it should register those stand-alone high-risk AI systems in an EU database that will be managed by the Commission to increase public transparency and oversight and strengthen ex post supervision by competent authorities.

(64) The AIA relies on a strong – these are the words - public enforcement mechanism. Member States are in charge of providing for the necessary resources. The regulation of enforcement and the potential implementation in Member States deserve a separate analysis. The experience with the GDPR demonstrates that common fully harmonised rules do in no way guarantee a uniform enforcement.[58] What matters though, non-governmental organisations, such as consumer organisations, have no role to play in the framework of the AIA.

(65) Despite its rather limited importance of third-party conformity assessment, the AIA contains a comprehensive set of rules on notified bodies, in Article 33 AIA for those located in the EU and in Article 39 AIA for those outside the EU. Out of the many detailed rules, two are of particular interest from a consumer perspective:

> Article 33 Notified bodies
>
> 5. Notified bodies shall be organised and operated so as to safeguard the independence, objectivity and impartiality of their activities. Notified bodies shall document and implement a structure and procedures to safeguard impartiality and to promote and apply the principles of impartiality throughout their organisation, personnel and assessment activities.
>
> 8. Notified bodies shall take out appropriate liability insurance for their conformity assessment activities, unless liability is assumed by the Member State concerned in accordance with national law or that Member State is directly responsible for the conformity assessment.
>
> 10. Notified bodies shall have sufficient internal competences to be able to effectively evaluate the tasks conducted by external parties on their behalf. To that end, at all times and for each conformity assessment procedure and each type of high-risk AI system in relation to which they have been designated, the notified body shall have permanent availability of sufficient

---

57 Explanatory Memorandum p. 15.

58 U. Pachl, Die Realität der Rechtsdurchsetzung im Datenschutz – bisher noch keine Erfolgsgeschichte für Verbraucher, Verbraucher und Recht 2020, 361.

> administrative, technical and scientific personnel who possess experience and knowledge relating to the relevant artificial intelligence technologies, data and data computing and to the requirements set out in Chapter 2 of this Title.

(66) There is a lot to say on the 'independence and impartiality'. The AIA uses similar language when it comes to legal requirements of regulatory agencies that control and supervise so-called regulated markets. Does it make sense at all to expect from profit-run companies to be 'impartial'? The AIA contributes to a further blurring of the limits between public and private responsibilities. A second, even more important weakness results from the lack of a mandatory liability insurance. The European Commission does not seem ready to learn the lessons from the PIP scandal,[59] let alone a debate on the insufficiencies of the product liability directive which does not cover certification bodies.[60] The AIA, similar to the new approach directives, delegates the responsibility for the availability of appropriate insurance and liability rules to the Member States – with disastrous effects for all those who have been affected by the insufficient and light-handed shaping of the conformity obligations in the Medial Devices Directive 93/42/EC.

5. The need for a Standardisation and Certification Governance Act (SCGA)

(67) The proposal of the European Commission to put the regulation of AI into the hands of standardisation bodies is comparable to the developments at the end of the 19th century. The tremendous industrialisation and the automation of production boosted the development of technical standards. This was the beginning of the outsourcing of knowledge from public administrations to private self-regulation.[61] The digitalisation of the economy is a kind of second wave. In theory the public authorities could gain comparable knowledge, However, this would require an enormous investment, the establishment of a 'digital agency'. The EU relies on 'strong' enforcement without clarifying what this means and implies. Due to the lack of competence, the insistence on strong enforcement is nothing more than programmatic language.

(68) This is to say that the AIA is more than a mere prolongation of the New Legislative Framework to new policy areas – in the EU language, the digital market and the digital agenda –the transfer of the new approach type of thinking to AI marks a break-even point in co-regulation. That is why there are serious doubts whether the proposed extension of the NLF

---

59 P. Rott, Certification – Trust, Accountability, Liability, 2018.

60 H.-W. Micklitz/ N. Reich/ L. Boucon, L'Action de la victime contre l'assureur du producteur RIDE, 2015, 37-68

61 K.-H. Ladeur, 'The Evolution of General Administrative Law and the Emergence of Postmodern Administrative Law' (2011) Comparative Research in Law & Political Economy. Research Paper No. 16.

is covered by the TFEU and the *Meroni*[62] doctrine of the European Court of Justice. One might argue that the move in 1985 to entrust standardisation bodies with the regulation of product safety was covered by the *Meroni* doctrine. However, the AIA grants the European Standardisation Bodies the mandate to develop technical standards far beyond product safety in order to protect the physical integrity. If the AIA will be adopted, the very same Standardisation Bodies have to handle psychological harm and to guarantee that the technical standards respect the fundamental rights. Such an extension is not covered by the *Meroni* doctrine.

(69) In terms of substance, the move is more than bold; it is naïve. Within the last decade, there has been a growing literature from legal experts and computer scientists on whether and how it is possible to build algorithms that respect fundamental rights. Whilst there is some agreement that we move into that direction and while there are opinions that explicitly ask for such type of algorithms,[63] the co-operation between legal experts and computer scientists has not yet led to seizable results. The AIA is delegating the unsolved problem to the standardisation bodies and the European Commission is expecting the results to be available in 3 to 4 years.[64]

(70) Where is the way out? Thinking at the limits of the *Meroni* doctrine, more is needed to ensure democratic control over the standardisation process. A short-hand solution could be to bring the European Parliament back into the approval procedure, that is to mobilise Article 291 TFEU. However, we need to go further: the elaboration of a Standardisation and Certification Governance Act, which puts the Memorandum of Understanding, the role of non-governmental organisations in the standard-making process and the supervisory function of the European Parliament into perspective. This is not a step backwards to return to parliamentary standard-making[65] but to democratise technical standardisation in the digital economy and not only there.

---

62 Meroni / Hohe Behörde, Rs. 10/56, p.75 lately extensively discussed in relation to the establishment of the European supervisory authorities on financial markets; see Takis Tridimas, Community Agencies, Competition Law, and ECSB Initiatives on Securities Clearing and Settlement January 2009 Yearbook of European Law 28(1) DOI:10.1093/yel/28.1.216

63 Advisory Council of Consumer Affaires to the German Ministry of Justice and Consumer Protection, Consumer Rights 2.0 Consumers in the Digital World https://www.svr-verbraucherfragen.de/en/wp-content/uploads/sites/2/Report-1.pdf

64 Explanatory Memorandum, thereto M. Ebers, loc. cit.

65 On the history behind the new approach, see Joerges, Ch., Falke, J., Micklitz, H.-W. and Brüggemeier, G. 'European Product Safety, Internal Market Policy and the New Approach to Technical Harmonisation and Standards' (1991) EUI Working Paper Law No. 10-14; (2010) 6 Hanse Law Review 109.

IV. The Four Regulations and the DV/DA

(71) What kind of concept of consumer protection is internalised in the Four Regulations? The following analysis is based on the questions, the findings and the recommendations of the main study.

1. Digital Fairness and Digital Vulnerability

(72) The Four are using all sorts of catch words to guide the proposed action: fairness, illegal content, systemic risks, manipulation, intention, risk, foreseeable misuse. Each of the regulations is guided by different value standards: DMA – fair competition, DSA – the removal of illegal content and responsible content moderation, and AIA – systemic risk for fundamental rights and society, while the DGA must create the conditions for innovation and trust in data sharing.

a) Digital Fairness

(73) DMA is extensively relying on *fairness in the sense of fair competition.* The term fairness appears 38 times. Article 6(k) might give a hint of the general philosophy behind. The DMA aims at the application of 'fair and non-discriminatory general conditions of access for business users to its software application store'. *Monti*[66] proposes a classification under four theories of harm: (i) addressing lack of transparency in the advertising market; (ii) preventing platform envelopment; (iii) facilitating the mobility of business users and clients; (iv) preventing practices that are unfair. Consumer interests are protected in the first place indirectly, through creating the conditions for fair competition and choice for consumers.[67] Accordingly most consumer-facing obligations in the DMA are aimed at improving the conditions for free choice and switching between platforms (e.g. the ability for third parties to offer products and services and conclude contracts with users of a particular platform in Art. 5 (b) and (c) DMA, allowing end users to uninstall pre-installed software applications in Art. 6 (b) respectively the installation of third party software in Art. 6(c), refrain the ability of end-users to switch between different services in Art. 6(d) as well as enabling data portability, Art. 6 (g). *Kerber and Specht-Riemenschneider*[68] use the reference to fairness as means to open the DMA towards data protection and consumer protection. They advocate a holistic perspective that breaks the boundaries between competition, data protection and consumer law.

---

66 Loc. cit. p. 3 under reference to CERRE, 'The European Proposal for a Digital Markets Act – A First Assessment' (19 January 2021), p. 19

67 See Recital 50 DMA: Gatekeepers should not restrict or prevent the free choice of end users by technically preventing switching between or subscription to different software applications and services.

68 Synergies between data protection and competition law, Gutachten für den Verbraucherzentrale Bundesverband, September 2021, will be available on the website www.vzbv.de

(74) The DSA takes a negative approach. The purpose is to fight '*illegal content*' which is mentioned more than 100 times. Art 2(g) provides for a definition: 'illegal content' means any *information*, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law. Recital (12) provides some clarification of what is meant by information:

> In order to achieve the objective of ensuring a safe, predictable and trusted online environment, for the purpose of this Regulation the concept of "illegal content" should be defined broadly and also covers information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal […] or that relates to activities that are illegal, such as […] activities involving infringements of consumer protection law.
>
> […]

(75) However, there is a second strand of value standards which runs across the DSA and which in a way competes with 'illegal content'. This is 'risk', as defined in Article 26 DSA. 'Very large online platforms shall identify, analyse and assess any significant *systemic risks* (*emphasis added*) stemming from the functioning and use made of their services in the Union'. The very same article provides for a definition of what the DSA understands as systemic risks.

- the dissemination of illegal content through their services, which covers unfair commercial practices as long as there is element of information. This implies that sales promotion measures are excluded as their purpose is generally not to carry information.
- any negative effects for the exercise of fundamental rights, respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively, but NOT Article 38 on consumer protection;
- *intentional manipulation* (*emphasis added*) e.g. inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.[69] Tying manipulation to 'intention' reduces potential systemic risks to situation of fraud and sets aside the architectural dimension of the digital vulnerability/asymmetry.

(76) It is worth noting that all the systemic risks that the DSA tackles are focused rather on the user as citizen and holder of fundamental rights than the user as consumers. Even the section about intentional manipulation is more targeted at forms of manipulation of the public

[69] See in the context of the advertising registry rec. 62 on the need of platforms to protect themselves against manipulative practices.

sphere and democratic discourse, rather than economic manipulation in the digital marketplace.

(77) The AIA is based on risks, broken down in the regulation to the distinction between 'prohibited practices', 'high risk' and 'certain risk'. The first two are distinct in the object of protection – 'prohibited practices' require physical or psychological harm or an infringement of fundamental rights. The proposal does not provide for a definition of risk, but concretises the concerned AI via annexes. However, 'certain risks' are defined (through the interaction between a human and an AI system). The AIA ties the risk assessment (Article 9), the information for users (Article 13) and human oversight (Article 14) to 'reasonably foreseeable misuse'. Article 3(13) AIA defines 'reasonably foreseeable misuse' as 'the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems'. In EU product safety law[70] the notion of risk is strongly related to the legitimate expectations of the consumer. The AIA goes even further than the recent proposal for a revision of the General Product Safety Directive 2001/95, which refers to 'reasonably foreseeable conditions'.[71]. It looks as if the professional users are subject to stronger requirements than the manufacturer of products which could potentially affect the health and safety of consumers.

(78) Just like the DSA, the AIA refers a couple of times to manipulation or manipulative practice. According to Article 1 c) AIA, AI systems used to generate or *manipulate* image, audio or video content are covered by the directive. Article 15(4) AIA states that the technical solutions of high-risk AI systems which address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to *manipulate* the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.' The AIA does not define manipulation but Recital 16, just like the DSA, links manipulation to intention.

> The placing on the market, putting into service or use of certain AI systems *intended* to distort human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of children and people due to their age, physical or mental incapacities. They do so with the *intention* to materially distort the behaviour of a person and in a manner that causes or is likely to cause harm to that or another person. The *intention* may not be presumed if the

---

70 With regard of the relevance and the difference between foreseeable use and foreseeable misuse, H.-W. Micklitz, in Ch. Joerges et al, loc. cit.

71 Proposal for a Regulation of the European Parliament and of the Council on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council, and repealing Council Directive 87/357/EEC and Directive 2001/95/EC of the European Parliament and of the Council, Brussels, 30.6.2021, COM(2021) 346 final, https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_general_product_safety.pdf.

> distortion of human behaviour results from factors external to the AI system which are outside of the control of the provider or the user (emphasis added HWM).

(79) The Recital is not very clear though, in particular when it comes to the burden of proof. The last sentence suggests that the burden of proof is presumed to lie with the supplier but it is unclear under what conditions this shall be the case.

b) Digital vulnerability/digital asymmetry

(80) None of the Four Regulations refers to digital vulnerability/digital asymmetry as a structural and relational phenomenon that is universal. Such language is deliberately avoided, which is in a way logical as it is in line with the philosophy of the Four Regulations. The most explicit mentioning of vulnerability in the context of algorithmic systems is Art. 5 (b) AIA, which, however, again adopts a narrow understanding of vulnerable groups in the sense of groups or persons that due to their age, physical or mental disability are not able to defend themselves against certain practices. The use of AI systems in a way that exploits the vulnerabilities of consumers that do not belong to that group(s) is consequently not prohibited under the AIA. Art. 7 (f) AI regulation determines that the extent to which consumers of AI systems find themselves in a disadvantaged position vis-à-vis professional users, in particular with respect to power asymmetries, knowledge economic or social circumstances, can be a reason to qualify that AI as high-risk AI. This seems to underpin a certain broadening of the vulnerability as proposed by the authors of this study.

(81) Veale and Borgesius (2021) conclude that the AIA explicitly excludes systems where distortion or harm arises not from the system itself but from dynamics of the user-base entwined with an AI system.[72] This is the result of the narrow definition of AI systems as essentially technological systems, not taking into account their broader socio-organisational context. The definition in Art. 3 (1) explicitly defines an AI system as software that is developed with particular techniques and that generates certain outputs. Therefore, the AIA does not address risks that are the result of the use of AI systems in a way that they create relational, situational or informational dependencies. Having said so, with its strong focus on making digital markets contestable, the DMA could develop into a potentially important legal framework to tackle the creation of digital choice architectures in a way that restricts users' free choices and create (lasting) relational dependencies. The scope of the DMA, however, is limited to a narrow category of users of AI or algorithmic systems, namely certain categories of information society services (search engines, social media, online market places, etc.) that qualify as gatekeepers in the sense of Art. 3 DMA.

---

[72] P. 21 loc. cit.

2. Prohibited (commercial) Practices

(82) The Four Regulations deal to a differing degree with specific practices. The analysis is complete in the sense that if the subcategories below do not contain information, there is nothing to report from the nearly 400 pages that make up of the four regulations. The preliminary question is whether Article 5 AIA precludes the possibility to prohibit AI practices to avoid consumer harm. This was discussed above.[73] Overall, the Four Regulations do not systematically connect to the consumer issues below. They contain rules and recitals randomly distributed all over the explanatory memorandum, the recitals and the rules (if any) are without any systemisation and without discussing the erratic rules against the background of the consumer acquis.

a) Advertising and Commercial Practices

(83) The DMA, DSA, and indirectly the AIA, deal with advertising and commercial practices, each within their particular regulatory ambit. However, none of the three discusses the potential interrelationship with the EU Directives on b2b (2006/114/EC) or b2c (2005/29/EC) advertising.

(84) The DMA does not deal with the regulation of advertising, but with the relationship between the gatekeeper and the provider of advertising services. Article 2(2)(h) DMA provides for a definition of advertising services, which cover advertising networks, advertising exchanges and any other advertising intermediation services, by a provider of any of the core platform services listed in points (a) to (g). Article 5 DMA lays down the obligations for gatekeepers in respect of each of its core platform services identified. Pursuant to Article 3(7)(g), a gatekeeper shall provide advertisers and publishers to which it supplies advertising services, upon their request, with information concerning the price paid by the advertiser and publisher, as well as the amount or remuneration paid to the publisher, for the publishing of a given ad and for each of the relevant advertising services provided by the gatekeeper.

(85) Art. 2 (n) DSA defines 'advertisement' in the following way: information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and displayed by an online platform on its online interface against remuneration specifically for promoting that information. The definition is broader than the UCPD in that it covers non-commercial practices such as political advertising, but also narrower, because non information-based sales promotion strategies are excluded from the scope.

(86) Article 24 and 30 DSA contain legal requirements for online platforms (Article 24) and large online platforms (Article 30) on 'Online advertising transparency'. Under the UCPD, advertisers are obliged to label advertisement so as to distinguish it from information, Article

[73] Under II. 4 a) and b).

7(2) UCPD. The DSA extends this obligations to online platforms.[74] The two articles must be read in connection with Recital 52:

> In addition to the requirements resulting from Article 6 of Directive 2000/31/EC, online platforms should therefore be required to ensure that the recipients of the service have certain individualised information necessary for them to understand when and on whose behalf the advertisement is displayed. In addition, recipients of the service should have information on the main parameters used for determining that specific advertising is to be displayed to them, providing meaningful explanations of the logic used to that end, including when this is based on profiling.

(87) Platforms shall ensure that the recipients - this includes consumers[75] - can identify, for each specific advertisement displayed to each individual recipient, 'in a clear and unambiguous manner and in real time: that the information displayed is an advertisement; the natural or legal person on whose behalf the advertisement is displayed; meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed.'[76] It is worth stressing that this provision applies equally to both commercial and political advertising. It is also equally worth pointing out that, seeing the complexity of algorithmic targeting practices it is still rather unclear if it is technically and practically feasible to pinpoint those main parameters and inform consumers in a meaningful way. Finally, the provision is limited to transparency and says nothing about the fairness of online advertising, respectively under which conditions it might be unfair.

(88) Last but not least, under Article 36 DSA the Commission shall encourage and facilitate the drawing up of codes of conduct between online platforms, service providers, such as providers of online advertising intermediary services, or organisations representing recipients of the service and civil society organisations or relevant authorities to concretise the transparency requirements. However, it is not clear what kind of incentives platforms should have to participate in the elaboration of such a Code.

(89) The AIA does not contain particular rules on advertising, sales promotion or commercial practices, though both, Art. 5 (2) AIA and 52 (2) (use of emotion recognition systems) could at least in theory become relevant for certain advertising practices, and psychographic advertising in particular. Art. 52(2) could become, for example, relevant in situations such as the famous Facebook emotional contagion experiment and instances of emotional targeting more generally. Having said so, seeing the fact that Art. 5(2) AIA does not address economic harm, and Art. 52 (2) only requires informing consumers that biometric categorisation systems or emotion recognition systems are being used, the level of consumer protection conveyed against psychographic marketing practices is very limited. One may wonder

---

74 Spindler GRUR 2021, 657.

75 Art. 2 b) 'recipient of the service' means any natural or legal person who uses the relevant intermediary service

76 See also on profiling under c).

whether simply informing users that they are subjected to emotion recognition systems can already offer sufficient protection from emotional manipulation, or what the provision actually adds to existing provisions under e.g. the GDPR and the UCP.[77] Unclear is also how Art. 5(2) and 52(2) AIA relate to each other. One of the key concerns about the use of emotion recognition software is the potential for manipulating consumers[78] and it seems at least contradictory that the regulation considers the risks from the use of emotion recognition manageable enough that a transparency obligation will suffice, while subjecting the use of sublimely techniques (e.g. using emotion detection) to an absolute ban.

b) Pervasive Tracking (traceability)

(90) Article 22 DSA defines standards for the traceability of traders. Online platform which enable consumers to conclude distance contracts need to make sure that they get minimum information from the trader that they can forward to the consumer. The rule has to be read in line with the overall purpose. The recipient shall be enabled to trace the trader in case of illegal content (hate speech and the like). However, as illegal content covers at least information-related advertising, Art. 22 DSA might have a certain impact on consumers.

c) Profiling

(91) The DMA and the DSA refer to profiling in a different context. Article 13 DMA obliges the gatekeeper to submit to the Commission an independently audited description of any techniques for profiling of consumers that the gatekeeper employs. One instance in which the DMA adds to the protection of consumers vis-à-vis profiling practices is Art. 5 (1) that obliges platforms to refrain from combining personal data that was acquired in the course of the operation of the core platform with personal data from any other service offered by the same provider.

(92) Article 24 DSA obliges platforms to disclose 'meaningful information on the 'main parameters' which have led to the selection of the respective recipients, here consumers. *Spindler*[79] argues that Article 24(c) DSA primarily aims at automated procedures, in that the recipients of the advertising should implicitly be facilitated in asserting their rights under Article 22(1) GDPR. Recital 52 DSA explicitly states that the data protection requirements under Article 22 GDPR and the ePrivacy Directive should remain unaffected. Having said so, it is unclear what Art. 24 (c) really adds to the transparency obligations already existing under the UCPD and the GDPR (including Art. 22 GDPR but also 13 (2) (f) that obliges data controllers to inform consumers about the logic involved as well as the consequences from profiling for the data subject).

---

77 Veale &Borgesius, 2021; Spindler 2021.

78 Clifford, D. (2017). Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side? CiTiP Working Paper Series, 31/2017.

79 Spindler GRUR 2021, 657, loc. cit.

d) Personalisation/Recommender Systems

(93) The DMA mentions choice between personalised and non-personalised systems. However, the related recital did not make it into Article 6(c) DMA.

- (36) 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.

(94) Article 29 DSA regulates recommender systems and brings in an element of choice similar to Recital 36 DMA: Very large online platforms are required to set out, in their terms and conditions, the main parameters used in their recommender systems as well as *at least one option which is not based on profiling*, within the meaning of Article 4(4) of the GDPR. Having said so, upon closer reading Art. 29 DSA is in the first place a transparency obligation – very large online platforms shall inform users in the situation that they offer different options for the recipient to modify or influence the main parameters of a recommendation, including one option that is not based on profiling. Art. 29 (1) DSA does not oblige platforms to offer such a choice, thereby leaving this entirely to the discretion of platforms. Seeing that the business model of social media platforms is essentially based on the ability to personalize individual information streams, it is difficult to see what incentives social media platforms would have to offer a non-profiling option. Also, note that offering an option not based on profiling does not mean that platforms would be obliged not to collect personal data or build personal profiles. In this context, it is a bit unclear what exactly consumers would be protected from.

(95) The AIA does not discuss the pros and cons of personalisation in any detail. The Explanatory Memorandum praises the opportunities,[80] just as Recital 3 does:

- By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, 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.

---

80 P. 2.

e) Non-discrimination

(96) The DMA refers to non-discrimination in the context of fair and non-discriminatory general conditions of access for business users, Article 6 (k), similar to the access rules in regulated markets and thus discusses discrimination in the first place from a b2b perspective. To the contrary, the DSA approaches discrimination as one possible systemic risk that can arise from the use of digital technologies from the perspective of the user/consumer in Art. 26 (1)(b). The AIA again addressed discrimination, or the danger of discrimination, from the perspective of those building and using AI systems (professionally). Particularly worth mentioning in this context is Art. 10 (2) (f) that requires an examination of (training) data sets in view of possible biases and Art. 10 (5) that introduces a new exemption from the protection of special categories of data pursuant Art. 9 GDPR specifically for the purpose of ensuring bias monitoring. Also, AI systems must be built in a way that those using and overseeing the system are made aware of, and can recognize and interfere in cases of discriminatory outcomes (Art. 14 (1) in combination with Art. 14 (2) (b) and (d).

(97) Art. 26 DSA obliges platforms to assess systemic risks, the AIA has the professional users of AI in mind. In both situations though the benchmark against which the risks are measured will be concretised through technical standards, to be developed by the European Standardisation Bodies. Consumers and consumer organisations would then need to know the technical standard in question, in order to find out whether the technical standards comply with the legal requirements of the DSA and the AIA.

f) Personalised Pricing

(98) Article 5 DMA deals with personalised pricing but through the eyes of the gatekeepers. Gatekeepers shall 'allow business users to offer the same products or services to end users through third party online intermediation services at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper'. One may read Article 5 DMA as invitation to offer consumer different prices. The link to personalisation is only implicit.

g) Transparency

(99) Ultimately, the most evidently consumer facing provisions in the Four are again transparency obligations, be that the provisions on online advertising transparency in Art. 24 or on potential choice options under Art. 29 DSA, be that the mitigation of risks emanating from low-risk AI in Art. 52 of the AIA. The message is clear: with the four regulations, the European Commission is seeking to lay down a framework for trustworthy AI, by imposing obligations on platforms and developers and professional users of AI and spurring innovation through promoting the sharing of data and market contestability. The role of users is making informed decisions.

(100) A critical analysis shows that the additional transparency requirements the draft regulations suggest are rather minimal, compared to the more far-reaching information obligations under the e.g. GDPR, the proposed DSA, the Unfair Commercial Practice Directive or provisions such as the California Bot Bill. Take the example of the transparency provision in Art. 52 AIA: informing users that they interact with a virtual agent, or that a piece of news content has been written by an AI may provide consumers with, but gives them little guidance on what this means for the quality or reliability of the information presented, whether the AI system has been designed to adhere to any editorial professional standards, whether it is biased, whether the information has been verified by a professional journalist, etc. Similarly, informing consumers that a selection of news contents is recommended through an AI system, rather than by a human editor, says in itself very little about the quality or editorial ambitions of that recommendation, the extent to which the responses of the AI have been checked for biases, prioritise the users' interest and are impartial, or even secured against hacking and other forms of malicious manipulation. Insofar, Art. 52 draft AI Regulation is dealing only with a very limited set of (ethical) concerns regarding the use of chatbots and virtual agents, and arguably not even the most pressing ones (compare e.g. Kaul, 2021; Danaeher, 2018).[81] And unlike the transparency obligations under the GDPR or the UCP, the transparency obligation under Art. 52 of the draft AI regulation is not actionable in the sense that it would give consumers concrete rights.

(101) And again, it is very unclear how transparency alone can help to protect consumers from the considerable potential psychological, financial and societal harms that deepfakes can cause.[82] Insofar, the Regulation's deepfake provisions cannot be seen separately from other regulatory initiatives to tackle the proliferation of disinformation and deepfakes (such as the Democracy Action Plan or the Code of Practice against Disinformation.

3. Standard terms

(102) The Four Regulations use similar or the same wording as the Unfair Contract Terms Directive 93/13/EEC in a bewildering way, again without any co-ordination with the consumer acquis.

(103) According to Article 6 DMA, a gatekeeper shall:… 'j) provide to any third party providers of online search engines, upon their request, with access on fair, *reasonable and non-discriminatory terms* to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data'. Such an

---

81 Danaher, J. (2018). Toward an Ethics of AI Assistants: an Initial Framework. *Philosophy & Technology,* Vol. 31, 629–653; Kaul, A. (2021). Virtual Assistants and Ethical Implications. In: Ali Soofastaei (2021). *Virtual Assistant*. Intech Open.

82 For an insightful overview see Van Huijstee, M. et al. 2021. *Tackling deepfakes in European policy*. Study for the European Parliament, Brussels.

obligation interferes with freedom of contract as it sets standards on how a contract might and should be formulated at least if one understands terms as contract terms. The DMA does not provide for a definition of 'terms'. However, if we assume that the European Commission aims at consistency between the Four, the definition of 'terms and conditions' in Article 2 (q) DSA suggests such an interpretation. 'Terms and conditions' under the DSA are 'all terms and conditions or specifications, *irrespective of their name or form, which govern the contractual relationship* (emphasis added) between the provider of intermediary services and the recipients of the services.

(104) Article 12 and 29 DSA are remarkable in that they set out a framework on the kind of provisions providers of intermediary services have to integrate into their 'terms and conditions': inter alia 'information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear and unambiguous language and shall be publicly available in an easily accessible format. According to paragraph 2, platforms are asked to ensure compliance, 'with due regard to the rights and legitimate interests of all parties involved, including the applicable fundamental rights of the recipients of the service as enshrined in the Charter'. Having in mind that consumers are recipients and that illegal content includes commercial practices, it is somewhat irritating that the Four provide for rules which affect the private law relations between b2b and b2c, but that the European Commission did not make any attempt to assess and discuss the potential implications.

4. Enforcement (individual and collective rights)

(105) Individual rights of consumers and collective rights of consumer organisations are completely left out. The reason is that the Four lay down rules which should be enforced by public authorities. In this top-down perspective, there is little room for private and individual enforcement. The potential preclusionary effects have been discussed under II. There is overlap between Directive 93/13/EEC and Article 6(j) DMA as well as between Directive 2005/29/EC on commercial practices and illegal content in the DSA. There is an overall lack of appropriate remedies to the benefit of consumers and business. *Spindler*'s analysis with regard to the DSA is more or less true for all Four Regulations. Even more surprising is the failure to connect the extensive rules on public enforcement to the recently adopted Directive (EU) 2020/1828 on representative actions. At the very minimum, the Four Regulations should be integrated into the Annex of Directive 2020/1828 so as to make clear that consumer organisations are empowered to undertake action against unlawful content under the DSA or prohibited practices under Article 5 AIA.

(106) The relevant rules in the DSA - Article 13 on trusted flaggers and Article 43 on the right to lodge a complaint - deserve particular attention. In theory, they could set a precedent for the DMA, the DGA and the AIA. However, none of the three contains similar rules.

(107) The DSA relies on trusted flaggers to assist law enforcement. Are consumer organisations trusted flaggers? Article 19(2) states: 'The status of trusted flaggers shall be awarded, upon application by any entities, by the national Digital Services Coordinator if the applicant has demonstrated that '(a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content; (b) it represents collective interests and is independent from any online platform; (c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner'. The registration procedure would have to be brought into compliance with the related rules for consumer organisations in Directive (EU) 2020/1828.

(108) Article 43 grants recipients of the service the right to lodge a complaint to the national Digital Services Coordinator against providers of intermediary services. Consumer organisations do not have such a right. Even more disturbingly, there is no obligation of the Digital Services Coordinator to respond to the applicant what kind of action has been taken and why. No remedy is foreseen in case the national authorities decide to decline the complaint.

V. Consequences for the Development of an Appropriate Consumer Law Approach

1. The hidden underground

(109) In the shaping of the digital market, the European Commission relies on the New Approach and the New Legislative Framework (NLF). This means that it does not suffice to look at the articles of the Four but one needs to read and interpret the Four having in mind the regulatory underground – the development and the making of technical standards, be they voluntary or be they requested by the European Commission and published as harmonized standards.

(110) This is true for all four pieces of regulation – the DMA does not discuss market closure effects through technology in general or through technical standards in particular. The DSA contains rules on data access for research, but what is really needed is access to the standardisation process – which is not discussed at all. The AIA requires the development of harmonised standards which have to take psychological harm and fundamental rights protection into account. Whatever solution is proposed, it has to have in mind that the European Standard Bodies are the key institutions.

2. Upgrading the Four Regulations or the Consumer Acquis?

(111) There is a strategic choice to make on whether it makes sense and is feasible to upgrade the Four Regulations and to systematically integrate consumer issues. The list of potential deficits is long as this addendum has documented.[83] It seems more appropriate, and perhaps also more realistic, to request

- a clarification that the Four do not deal with consumer concerns so as to avoid preclusionary effects. Article 1(5) DSA could serve as a model; and
- that there is room to upgrade the consumer acquis via targeted consumer law revisions, including a provision that must specifically tackle unfairness in digital commercial practices.

(112) Within the consumer acquis a holistic perspective is necessary. The Four mainly touch upon unfair commercial practices and standard terms, although they also affect the GDPR. The main report has demonstrated that problematic practices can take different forms, they can appear as standard terms, as commercial practices or as data privacy policies. EU law distinguishes between data policy, standard terms and commercial practices. In practice, national enforcement authorities use one of the three, usually the one they are most familiar with to fight against unfairness. Form shall not decide over substance.

[83] See the Position Papers of BEUC loc. cit.

Published in December 2021 by BEUC, Brussels, Belgium.

BEUC-X-2021-116

The European Consumer Organisation
Bureau Europeen des Unions de Consommateurs
Europaischer Verbraucherverband
Rue d'Arlon, 80 Bte 1, B - 1040 Bruxelles

BEUC The European Consumer Organisation