Framing Algorithms: Competition Law and (Other) Regulatory Tools

Peter Georg PICHT* & Gaspare Tazio LODERER**

As other fields of law, competition law is put to the test by new technologies in general and algorithmic market activity in particular. This article takes a holistic approach by looking at areas of law, namely financial regulation and data protection, which have already put in place rules and procedures to deal with issues arising from algorithms. Before making the bridge and assessing whether the application of regulatory tools from these areas might be fruitful for competition law as well, the article discusses some recent competition cases involving algorithmic market activity. It concludes with policy recommendations.

1 INTRODUCTION

Although competition law may not be among the first topics one associates with algorithms[1] or Artificial Intelligence (AI),[2] it is certainly one area of law that starts to take a closer look at the phenomenon, and rightfully so. The use of algorithms does not only present great chances to economy and society, it might also lead to undesirable results. The algorithms used today can be surprisingly low in their level of sophistication. However, as they become more complex and move towards an 'intelligent' state, they are likely to disruptively change almost all areas of human life. Even simple algorithms widely deployed in many different industries today can have a far-reaching

* Prof. Dr, LL.M. (Yale), Chair for Business and Commercial Law, Center for Intellectual Property and Competition Law – CIPCO, University of Zurich; Affiliated Research Fellow, Max Planck Institute for Innovation and Competition, Munich. Email: peter.picht@rwi.uzh.ch.

** MLaw, Attorney-at-Law, PhD Candidate and Research Assistant to Prof. Dr Peter Georg Picht. Email: gaspare.loderer@rwi.uzh.ch.

1 An algorithm can be defined as a precise sequence of instructions to perform a task, *see* for instance https://dictionary.cambridge.org/dictionary/english/algorithm (accessed 13 June 2019).

2 The term AI was coined by John McCarthy in 1956 and now commonly refers to machines imitating human intelligence, *see* for the different definitions on AI Bernard Marr, *The Key Definitions of Artificial Intelligence (AI) That Explain Its Importance*, https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#3c01e9874f5d (accessed 13 June 2019); machine learning, a subfield of AI, refers to algorithms that learn from data and experience to build intelligent machines; deep learning, a subfield of machine learning, is based on faster and more accurate learning, although no information on the decision-making process will be known (OECD, *Algorithms and Collusion: Competition Policy in the Digital Age* 9–11 (14 Sept. 2017), www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm) (accessed 13 June 2019).

Picht, Peter Georg & Loderer, Gaspare Tazio. 'Framing Algorithms: Competition Law and (Other) Regulatory Tools'. *World Competition* 42, no. 3 (2019): 391–418.

impact on the forms of and conditions for competitive business conduct in these markets.[3] This fact in itself mandates competition law to scrutinize implications of algorithmic market conduct and to intervene where they risk distorting competition. The interaction of algorithms and their collusive potential is (at present) one focal point of this mandate,[4] another example being algorithm-driven resale price maintenance.[5] It seems not clear, though, that competition law has, in its present shape, the necessary rules and techniques to perform the task. Thus, it may be helpful to look at other areas of the law, which are more advanced in this respect, and to learn from their experience.

Against this background, the present article pursues a threefold, 'toolbox-oriented' task: Its second section assesses important examples of how other areas of law deal with algorithm-based market activity.[6] The third section sketches three prototypical competitive concerns algorithms may evoke.[7] In the article's last section, we ask whether competition law's present toolbox suffices to tackle these concerns, to which extent it may adopt tools used in other areas of the law, and whether, beyond mere adaptation, the development of new instruments seems necessary.[8]

2 THE LEGAL TOOLBOX FOR ALGORITHMS OUTSIDE COMPETITION LAW – EXAMPLES AND CATEGORIES

2.1 The ordering of algorithmic activity by financial markets and data protection rules – legal frameworks

Among the various legal areas which already contain specific provisions on algorithmic activity, this article focusses on financial markets regulation and data protection law, as their approaches seem particularly apt to inform competition law on ways to handle algorithmic market activity.

With the implementation of algorithmic trading, financial markets were among the first to broadly and intensely deploy algorithms as a technical basis for market activity. Financial markets regulation had thus to react and developed a comparatively detailed set of rules on algorithmic trading. As to the EU,[9] Germany pioneered with its 'Hochfrequenzhandelsgesetz'[10] and the EU followed suit,

---

3 OECD, *supra* n. 2, at 11–14.
4 Cf. *infra* s. 3.2.
5 Cf. *infra* s. 3.1.
6 Cf. *infra* s. 2.
7 Cf. *infra* s. 3.
8 Cf. *infra* s. 4.
9 Rules in other jurisdictions, such as Switzerland or the United States, are not being examined in this paper.
10 Hochfrequenzhandelsgesetz of 7 May 2013, Bundesgesetzblatt 2013 Teil I Nr. 23, 14 May 2013, 1162–66, http://dipbt.bundestag.de/extrakt/ba/WP17/479/47951.html (accessed 13 June 2019).

issuing the Directive 'on markets in financial instruments'[11] (MiFID II). Based to a large extent on the European Securities and Market Authority's (ESMA)[12] Guidelines on 'Systems and Controls in an Automated Trading Environment for Trading Platforms, Investment Firms and Competent Authorities',[13] the Directive deals in meticulous detail with several aspects of algorithmic trading (AT)[14] and high-frequency trading (HFT).[15]

AT, and HFT in particular, can have positive effects on financial markets, for instance by improving order execution, increasing market liquidity as well as trading volume, narrowing bid and ask spreads, and reducing short term volatility.[16] But they can also pose specific risks, for example an increased likelihood for duplicate or erroneous orders, potential 'automatic' overreactions to market events, or information asymmetries resulting from an inequality of technical (viz. mainly: algorithmic) equipment.[17] To fight these risks, MiFID II uses a combination of measures directed at firms engaging in algorithmic or high-frequency trading, at those providing electronic access, and at operators of trading venues.[18] In addition to MiFID II, the market abuse regulation (MAR)[19] prohibits some activities relating to algorithmic and high-frequency trading by qualifying them as market manipulation.[20]

Data protection law is another area that already has in place certain elements of a legal framework for algorithmic (market) activity. This is true for the EU's

---

11 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

12 https://www.esma.europa.eu (accessed 13 June 2019); *see* for Technical standards under Directive 2004/39/EC (MiFID I), Directive 2014/65/EU (MiFID II) and Regulation (EU) No 600/2014 (MiFIR): http://ec.europa.eu/finance/securities/docs/isd/mifid/its-rts-overview-table_en.pdf (accessed 13 June 2019).

13 Recital 63 MiFID II; *see* for the guidelines https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2012_122_en.pdf (accessed 13 June 2019).

14 According to MiFID II terminology, AT means the automatic determination of an order by a computer algorithm with minimal or no human intervention, Art. 4 para. 1 (39) and Recital 59 MiFID II.

15 HFT is considered to be a subset of AT in which 'a trading system analyses data or signals from the market at high speed and then sends or updates large numbers of orders within a very short time period in response to that analysis' (Recital 61 MiFID II, more precise definition in Art. 4 para. 1 (40) MiFID II). In fall 2018 and spring 2019, the Commission was supposed, according to Art. 90 MiFID II, to report on the impact of MiFID's AT/HTF requirements but these reports have been postponed due to ESMA's request to gain more time for evaluating MiFID's ramifications, *see* https://www.esma.europa.eu/press-news/esma-news/esma-writes-european-commission-mifid-iimifir-review-reports (accessed 13 June 2019).

16 Recital 62 MiFID II; *see also* Megan Woodward, *The Need for Speed: Regulatory Approaches to High Frequency Trading in the United States and the European Union*, 50 Vand. J. Transnatl. L. 1359, 1368–69 (2017).

17 Recital 62 MiFID II.

18 Recital 63 MiFID II.

19 Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 Apr. 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.

20 Art. 12 para. 2 lit. c MAR.

General Data Protection Regulation (GDPR)[21] which has replaced an earlier Directive in May 2018 and established a data protection framework of utmost relevance to economy and society not only in the EU but also in regions transacting with EU data subjects.[22] Roughly speaking, the GDPR aims to protect the processing of personal data of natural persons.[23] In doing so, it stipulates general principles and requirements for the processing of data,[24] rights and remedies[25] of persons subject to data collection and processing (data subjects), such as information, access, rectification or erasure,[26] and obligations on data controllers and processors, regarding, for instance, cooperation with supervisory authorities or the designation of data protection officers.[27] As to (cross-border) enforcement, the Regulation foresees requirements for the transfer of data,[28] the establishment of supervisory authorities,[29] and a mechanism for the cooperation between these authorities.[30] Terming the algorithm-based collecting or processing of data an 'automated' one, the GDPR stipulates technological neutrality in the sense that all rights and obligations safeguarding personal data apply to the manual and automated handling of data alike.[31]

As another pertinent piece of EU legislation, the ePrivacy Regulation, probably to be enacted sometime in 2019, forms a *lex specialis* to the GDPR.[32] It aims at protecting the fundamental rights and freedoms when using electronic communication[33] and at ensuring the free movement of electronic communication

---

21 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). On the Regulation in general, *see* Tobias Lettl, *Die Datenschutz-Grundverordnung (DSGVO)*, WM 1149 (2018).

22 Cf. Art. 3 GDPR.

23 Art. 1 para. 1 GDPR.

24 Art. 5 et seq. GDPR.

25 Art. 77 et seq. GDPR.

26 Art. 12 et seq. GDPR.

27 Art. 24 et seq. GDPR.

28 Art. 44 et seq. GDPR.

29 Art. 51 et seq. GDPR.

30 Art. 60 et seq. GDPR.

31 Recital 15 GDPR, cf. also Art. 4(2), (4) GDPR.

32 Art. 1 para. 3 of the proposed Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications (accessed 13 June 2019), (ePrivacy Regulation). The current draft of the Council of the European Union is from 13 Mar. 2019, https://iapp.org/media/pdf/resource_center/ePR_3-13-19_draft.pdf (accessed 13 June 2019).

33 Art. 1 para. 1 ePrivacy Regulation; including machine-to-machine communication, cf. Recital 12 of the proposed Regulation: 'Connected devices and machines increasingly communicate with each other by using electronic communications networks (Internet of Things). The transmission of machine-to-machine communications involves the conveyance of signals over a network and, hence, usually constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation should

data and services.[34] To this end, it stipulates a principle of confidentiality of electronic communications data[35] and restricts their storage and processing.[36] More specific provisions[37] address restrictions of calling and connected line identification, incoming call blocking, publicly available directories, and unsolicited communications. Compliance with the general and specific rules is enforced by remedies closely modelled after those in the GDPR.[38] The supervisory authorities established by the GDPR shall monitor compliance with the ePrivacy Regulation as well.[39]

2.2 Regulatory tools and categories

2.2[a] *Transparency and Documentation*

It is not the goal of this contribution to separately go into the details of each financial markets or data protection provision related to algorithms, but to highlight the main types of tools used by these legal areas. From this point of view, one can distinguish provisions aiming at transparency of[40] and documentation on the use of algorithms. Investment firms engaging in algorithmic trading, for instance, are required to notify this to the competent authorities of the trading venue and of its Member State.[41] The latter may require the investment firm to provide (regularly or ad-hoc) information, in particular on the trading algorithm it employs, its strategies and limits, as well as compliance and risk control measures.[42] At any time, the competent authority of the home Member State of the investment firm may request further information about the algorithmic trading and the systems used therefore.[43] Hence, such information has to be documented[44] and might also be forwarded to the competent authorities of a trading venue at which the investment firm undertakes algorithmic trading.[45] Moreover, an investment

apply also to the machine-to-machine communications whenever these are related to users. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications. Specific safeguards could also be adopted under sectorial legislation, as for instance Directive 2014/53/EU.'

34 Art. 1 para. 2 ePrivacy Regulation.
35 Art. 5 ePrivacy Regulation.
36 Art. 6 et seq. ePrivacy Regulation.
37 Art. 12 et seq. ePrivacy Regulation.
38 Art. 21 et seq. ePrivacy Regulation.
39 Art. 18 et seq. ePrivacy Regulation.
40 Transparency meaning not only perceptibility but also comprehensibility.
41 Art. 17 para. 2 subpara. 1 MiFID II.
42 Art. 17 para. 2 subpara. 2 MiFID II.
43 Art. 17 para. 2 subpara. 2 MiFID II.
44 Art. 17 para. 2 subpara. 4 MiFID II.
45 Art. 17 para. 2 subpara. 3 MiFID II.

firm engaging in HFT[46] must keep accurate and time-sequenced records of all orders and make them available to the competent authority upon request.[47] Further transparency measures include the duty to flag orders generated by algorithmic trading, the different algorithms used for the creation of orders, and the relevant persons initiating those orders.[48]

Turning to examples for transparency in data protection law, Article 17 of the draft ePrivacy Regulation requires the providers of electronic communications services to inform end users about security risks[49] and Article 13 paragraph 2 litera f[50] GDPR stipulates that the use of automated decision making based on Article 22 GDPR[51] shall be communicated to the data subject, including information about the involved logic and the consequences of the data processing. In this respect, it is disputed whether Article 13 GDPR constitutes a duty to disclose the algorithm itself, with the leading opinion answering this question in the negative because this would result in a forced disclosure of trade secrets.[52] Another prominent provision of the GDPR also aims at transparency and documentation: According to Article 20 GDPR and its corresponding Guidelines[53] and Recitals, the 'data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided'. This 'data portability right'

---

46 If they only engage in AT, they must also keep their transaction data due to the general provisions of Art. 25 MiFIR (Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012) and Art. 16 para. 6 MiFID II.

47 Art. 17 para. 2 subpara. 5 MiFID II.

48 Art. 48 para. 10 MiFID II.

49 'Where the risk lies outside the scope of the measures to be taken by the service provider', the latter has to 'inform end-users of any possible remedies, including an indication of the likely costs involved' (Art. 17 ePrivacy Regulation).

50 Cf. also Art. 14 para. 2 lit. g and Art. 15 para. 1 lit. h GDPR.

51 Cf. *infra* s. 2.2.2.

52 Boris P. Paal & Moritz Hennemann, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz,* Art. 13 para. 31 (Boris P. Paal & Daniel A. Pauly, 2nd ed., C. H.Beck 2018); Holger Greve, *Europäische Datenschutzgrundverordnung*, Art. 12 para. 7 (Gernot Sydow, 2nd ed., Nomos 2018); Marcus Helfrich, *ibid*., Art. 22 para. 79 (regarding Art. 15 para. 1 lit. h GDPR); Matthias Bäcker, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, Art. 13 para. 54 (Jürgen Kühling & Benedikt Buchner, 2nd ed., C. H.Beck 2018); Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 IDPL 76, 89–90 (2017).

53 The so-called 'Article 29 Data Protection Working Party', a body composed of representatives of the Member States' data protection authorities, of the European Data Protection Supervisor, and of the European Commission, issued Guidelines on Art. 20 GDPR, *see* Art. 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, 5 Apr. 2017, 16/EN WP 242 rev.01, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 (accessed 13 June 2019).

is rich in implications[54] and it conveys a far-reaching right to control and duplicate the use of the pertinent personal data.[55] At the same time, it is a means to increase transparency on which data has been collected regarding a specific data subject and to communicate this information to the person most concerned, namely to the data subject.

Transparency for data subjects, together with the control that the subjects can exercise due to this transparency, are also important elements of privacy by design and by default, one of the key elements of the GDPR. Implementing this concept, Article 25 GDPR requires data processors to implement, already in the design-phase, appropriate technical and organizational measures for the protection of data subjects' rights. Besides transparency and control, this encompasses the processing, by default, only of data necessary for the respective purpose, as well as pseudonymization and general restraint in the collection of data. Appropriate certification may be used to demonstrate compliance with these requirements (Article 25 paragraph 3 GDPR). In practice, a set of actionable guidelines in combination with documentation can form the basis for demonstrating data protection by design and default.[56]

2.2[b] *Prevention and Deterrence*

Prevention and deterrence of adverse effects generated by algorithmic market activity form the focus of another set of rules. Article 22 paragraph 1 GDPR[57] protects the data subject from decisions solely based on automated processing,[58]

---

[54] Among them are the questions of how to define 'personal data … provided to a controller', the only type of data subject to the portability right; of how a data subject may use its portability right as a basis for transacting over its data, e.g. by assigning to third parties a claim to access the data; of whether the data subject must wait until the controller has collected and assembled the data or whether Art. 20 GDPR implies a right to directly collect data regardless of the collector's business secrets being affected by such an act; of whether portability creates an ownership-like control over ported data; or of how to balance, mainly in the application of Art. 20 para. 4 GDPR, the portability right with intellectual property rights extending to the respective data. *See* on these aspects, Colette Cuijpers, Nadezhda Purtova & Eleni Kosta, *Data Protection Reform and the Internet: The Draft Data Protection Regulation* 558 (Andrej Savin & Jan Trzaskowski, Research Handbook on EU Internet Law, Edward Elgar 2014); Inge Graef, Martin Husovec & Nadezhda Purtova, *Data Portability and Data Control, Lessons for an Emerging Concept in EU Law*, 22 Tilburg Law School Legal Studies Research Paper Series 1, 9–13 (2017), https://ssrn.com/abstract=3071875 (accessed 13 June 2019); Hans-Georg Kamann & Martin Braun, *Datenschutz-Grundverordnung*, Art. 20, paras 33–37 (Eugen Ehmann & Martin Selmayr, 2nd ed., C. H.Beck 2018); Art. 29 Data Protection Working Party, *supra* n. 53, at 12.

[55] Graef, Husovec & Purtova, *supra* n. 54, at 5, 7, 19.

[56] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default (accessed 13 June 2019).

[57] The preceding Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data already contained a similar provision in Art. 15.

[58] Automated processing encompasses algorithms (Mario Martini, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, Art. 22 para. 21 (Boris P. Paal & Daniel A. Pauly, 2nd ed., C. H.Beck 2018)).

including profiling,[59] if these decisions have significant (legal) effects. As an addition to Article 22, Recital 71 paragraph 2 formulates some requirements for profiling algorithms, such as the use of appropriate mathematical or statistical procedures and the prevention of discrimination based on sensitive data (e.g. ethnicity). A decision based solely on automated processing is, as an exception, permissible, if it serves the entering or performance of a contract[60] or if the data subject has given its explicit consent.[61] In such cases, the 'data controller' has a duty to implement suitable procedures, with a minimum standard of protection consisting of a right of the data subject to obtain human intervention, to express his or her point of view as well as to contest the decision.[62] The definition of 'suitable measures' does, however, not seem to go as far as to require the algorithm to be disclosed.[63] While Article 22 GDPR tries to mitigate the risks associated with automated decision-making based on algorithms,[64] the provision's implications are limited[65] by its focus on automation without human interference. Nonetheless, it is at least an attempt at the ex ante protection of data subjects from uncontrolled algorithmic decision-making.[66]

Article 35 GDPR[67] seeks risk prevention by way of ex ante impact assessment for processing with a high risk for a natural person's rights and freedoms.[68] Regarding algorithmic data processing, the GDPR perceives such a risk where an extensive and systematic evaluation results from automated decision making including profiling.[69]

Ex ante-testing and impact assessment is a mechanism extensively employed by financial markets regulation as well. Regulatory Technical Standards 6 (RTS 6) set out important parts of the organizational requirements for the testing and monitoring exercises to be carried out by investment firms engaged in algorithmic trading.[70] The testing requirements include testing prior to deployment or update

---

59 Profiling is characterized in Art. 4(4) GDPR as using personal data to evaluate a natural person's specific personal aspects.

60 Art. 22 para. 2 lit. a GDPR.

61 Art. 22 para. 2 lit. b GDPR.

62 Art. 22 para. 3 GDPR.

63 Martini, *supra* n. 58, at Art. 22 para. 36; Benedikt Buchner, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, Art. 22 para. 35 (Jürgen Kühling & Benedikt Buchner, 2nd ed., C. H.Beck 2018); Wachter, Mittelstadt & Floridi, *supra* n. 52, at 94.

64 Martini, *supra* n. 58, at Art. 22, para. 8.

65 Ulrich Dammann, *Erfolge und Defizite der EU-Datenschutzgrundverordnung, Erwarteter Fortschritt, Schwächen und überraschende Innovationen*, ZD 307, 312–13 (2016).

66 OECD, *supra* n. 2, at 49; Martini, *supra* n. 58, Art. 22 para. 46.

67 On the applicability of this provision to algorithms, *see* Martini, *supra* n. 58, Art. 35 paras 18 & 77.

68 Art. 35 para. 1 GDPR.

69 Art. 35 para. 3 lit. a GDPR.

70 Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organizational requirements of investment firms engaged in algorithmic trading, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0589&from=EN (accessed 13 June 2019).

of the algorithms,[71] as well as a testing approach that secures the algorithm's conformance with the system of the trading venue or of the direct market access provider.[72] Some of the tests have to be undertaken in a sandbox-like testing environment.[73] An annual self-assessment and validation requirement[74] includes a stress testing of the algorithmic trading system.[75]

Similar to those for investment firms, Regulatory Technical Standards 7 (RTS 7) set out rules for trading venues.[76] They have to test their trading systems,[77] require their members and participants to test their algorithms, and provide an environment that allows for such testing.[78] These tests include a requirement for the members to conduct conformance testing in the testing environment of the trading venue,[79] so as to avoid disorderly trading conditions.[80] Overall, trading venues need to ensure that algorithmic trading does not lead to disorderly market conditions and to manage such conditions in case they arise nevertheless.[81]

More general rules stipulate that an investment firm engaging in AT or HFT[82] shall, in particular,[83] have in place[84] resilient trading systems with sufficient capacity, continuity agreements for trading system failures, and measures to avoid creating or contributing to a disorderly market (e.g. prevention of erroneous orders) as well as a use of trading systems contrary to the MAR or the rules of connected trading venues. Trading venues[85] shall, in general, establish resilient and tested trading systems and ensure their ability to deal with large order volumes and markets under stress.[86] A

---

71 Art. 5 RTS 6.

72 Art. 6 RTS 6.

73 Art. 7 RTS 6: 'an environment that is separated from its production environment and that is used specifically for the testing and development of algorithmic trading systems and trading algorithms'. For sandboxing in financial markets *see also* the regulatory sandbox of the Financial Conduct Authority in the UK, https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf and https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf (accessed 13 June 2019).

74 Art. 9 RTS 6.

75 Art. 10 RTS 6.

76 Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organizational requirements of trading venues, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R0584&from=EN (accessed 13 June 2019).

77 Art. 8 RTS 7.

78 Art. 48 para. 6 MiFID II.

79 Art. 9 RTS 7.

80 Art. 10 RTS 7.

81 Art. 48 para. 6 MiFID II.

82 Since HFT is a subset of AT, specific rules on AT also apply to investment firms engaging in HFT (Danny Busch, *MiFID II: Regulating High Frequency Trading, Other Forms of Algorithmic Trading and Direct Electronic Market Access*, 10 LFMR 72, 75 *in fine* (2016)).

83 Besides, i.a., requiring authorization (Art. 5 MiFID II).

84 Art. 17 para. 1 MiFID II.

85 Consisting of regulated markets, multilateral trading facilities (MTFs) and organized trading facilities (OTFs), cf. Art. 4 para. 1(24) MiFID II.

86 Art. 48 para. 1 MiFID II for regulated markets, in conjunction with Art. 18 para. 5 MiFID II for MTFs and OTFs.

deterring, or at least a steering rationale is particularly conspicuous in provisions on increased fees for unwanted practices[87] and on the allocation of responsibilities.[88]

2.2[c] *Ex post Intervention*

Where prevention has failed, ex post intervention can become necessary. To detect and satisfy the need for such intervention, financial markets rules require constant monitoring[89] of algorithmic transactions, 'kill functionalities' permitting the cancellation of such transactions as an emergency measure,[90] and the implementation of business continuity agreements[91] preventing the break-down of business in case of disruptive events.

As a stakeholder-driven combination of prevention and ex post intervention, the GDPR provides for 'binding corporate rules' specifying, inter alia, the remedies available to data subjects in case of a violation of GDPR rules. If approved by the competent supervisory authority, such binding corporate rules – a novelty in EU data protection law – can legitimize the cross-border transfer of data, in particular between the companies of a group.[92] Regarding, in particular, the rights of data subjects related to an automated decision-making, the competent supervisory authority shall approve binding corporate rules addressing the data subject's right to file a complaint and to seek remedies such as redress and compensation.[93] In the same vein, Articles 21–24 of the draft ePrivacy Regulation provide for compensation, administrative fines and – subject to Member State law – other penalties.

3 PROMINENT ALGORITHMIC ISSUES IN THE FIELD OF COMPETITION LAW

We cannot, today, foresee all the facets of AI and algorithmic market activity which may come under competition law scrutiny and this article cannot even attempt to

---

87 Art. 48 para. 9 subpara. 3 MiFID II.

88 Art. 5 para. 3 RTS 6; cf. also Art. 1 and Recital 3 RTS 6: 'As a part of its overall governance framework and decision making framework, an investment firm should have a clear and formalized governance arrangement, including clear lines of accountability, effective procedures for the communication of information and a separation of tasks and responsibilities'.

89 Arts 9, 10, 13, 16 RTS 6. Trading venues to which AT and HFT traders are connected have to meet specific requirements laid down, in particular, in Arts 7, 12, 14 RTS 7; Busch, *supra* n. 82, at 78; cf. also the decision *Autocomplete*, Az. VI ZR 269/12 (BGH 14 May 2013), on a potential duty to monitor the autocomplete feature of internet search algorithms.

90 Art. 12 RTS 6; Art. 18 para. 2 lit. c RTS 7.

91 Art. 14 RTS 6.

92 Thomas Zerdick, *Datenschutz-Grundverordnung*, Art. 47 paras 2–3 (Eugen Ehmann & Martin Selmayr, 2nd ed., C. H.Beck 2018).

93 Art. 47 para. 1 para. 2 lit. e GDPR.

detail the gamut of constellations whose relevance we already perceive. We therefore limit this section to three types of cases that are both much discussed at present and potentially prototypical for the intersection of algorithms and competition law.

3.1 Algorithmic resale price maintenance

In four recent decisions, the EU Commission dealt, for the first time since the Yamaha decision in 2003,[94] with resale price maintenance (RPM). This time, however, the RPM was algorithm-driven[95] and twofold: On the one hand, the four consumer electronics manufacturers Asus, Denon & Marantz, Philips and Pioneer ('Asus and others') used algorithms to monitor the resale prices of online retailers. In cases of price decreases,[96] they imposed sanctions or threatened to do so.[97] On the other hand, the retailers were using pricing algorithms themselves. Thus, pricing restrictions imposed by Asus and others had an effect on the online prices in general.[98] However, pricing algorithms can also benefit customers. The Pioneer decision, for instance, reveals that employees tried to identify 'who is the aggressor and who is the follower' in price adjustments.[99] A diagram in the Philips decision demonstrates that the price decreases by a 'maverick' were followed (in particular) by another competitor.[100] In spite of this evidence, both scholars and the EU Commission underline that unilateral price adjustments in algorithmic markets are not necessarily matched by (all) other players, for instance because algorithmic reactions to changes in price can heavily depend on the programming of the respective digital tools.[101]

---

94 Commission Decision of 16 July 2003, Case COMP/37.975 PO/Yamaha.

95 Similarly, Pat Treacy, Stephen Smith & Edwin Bond, *Maintaining Price Competition Between Retailers in E-Commerce Markets: The European Commission's Recent RPM Decisions*, 39 ECLR 470, 471 (2018), note that the novelty of the decisions lies in the control of resale pricing restrictions through software.

96 Cf. on possible incentives for higher resale prices: Clemens Graf York von Wartenburg, Craig G. Falls & Michael I. Okkonen, *Recent EU Fines for Resale Price Maintenance are Symptoms of Broader Challenges Faced by Today's Consumer-Goods Manufacturers*, 39 ECLR 495, 496 (2018).

97 EU Commission, Press Release of 24 July 2018, http://europa.eu/rapid/press-release_IP-18-4601_en.htm (accessed 13 June 2019).

98 *Ibid.; Asus*, Case AT.40465, decision of 24 July 2018, para. 58, http://ec.europa.eu/competition/antitrust/cases/dec_docs/40465/40465_337_3.pdf (accessed 13 June 2019); *Denon & Marantz*, Case AT.40469, decision of 24 July 2018, para. 95 http://ec.europa.eu/competition/antitrust/cases/dec_docs/40469/40469_329_3.pdf (accessed 13 June 2019); *Philips*, Case AT.40181, decision of 24 July 2018, paras 46–47 (with diagram), 64, http://ec.europa.eu/competition/antitrust/cases/dec_docs/40181/40181_417_3.pdf (accessed 13 June 2019); *Pioneer*, Case AT.40182, decision of 24 July 2018, paras 134–39, http://ec.europa.eu/competition/antitrust/cases/dec_docs/40182/40182_370_3.pdf (accessed 13 June 2019).

99 *Pioneer, supra* n. 98, para. 139.

100 *Philips, supra* n. 98, para. 47.

101 Treacy, Smith & Bond, *supra* n. 95, at 472; Directorate for Financial and Enterprise Affairs Competition Committee, *Algorithms and Collusion – Note from the European Union*, 14 June 2017, paras 9 & 16, https://one.oecd.org/document/DAF/COMP/WD(2017)12/en/pdf (accessed 13 June 2019).

Whether sustained by direct (agreement) or indirect means (e.g. threats, penalties, contract termination), RPM is prohibited as a 'restriction by object' under Article 101 paragraph 1 of the Treaty on the Functioning of the European Union (TFEU) and as a 'hardcore restriction' under Article 4 litera a of the Vertical Block Exemption Regulation (VBER).[102] The Guidelines on Vertical Restraints underline that RPM can be more effective when combined with price monitoring systems[103] and the Commission acknowledges in its Algorithm Report that algorithmic price monitoring systems can form part of RPM infringements as they contribute to their effectiveness.[104]

It is in line with these statements that, in the cases at hand, the conduct of assisting RPM by way of monitoring software was not exempted under the VBER or under Article 101 paragraph 3 TFEU.[105] Hence, companies need to be careful that their use of pricing algorithms and monitoring software is not 'infected', and turned into a competition law violation, by the parallel implementation of an anti-competitive practice such as RPM.[106] At the same time, though, the fact that the retailers themselves were not fined confirms that the use of algorithms for pricing or price level observation is not unlawful as such.[107]

As the companies were cooperative, the cases at issue required neither examination of the employed algorithms nor in-depth technical expertise. Nonetheless, they may foreshadow an era of EU 'algorithmic antitrust', in which algorithms will be closely scrutinized by competition authorities.[108] Additionally, the considerable reduction in the fines the companies had to pay,[109] while not in itself a novel feature of EU competition law,[110] may be the starting point for a process of working out, through pertinent case law, what effective cooperation between undertakings and competition agencies may look like with regard to algorithmic systems.

---

[102] Commission Regulation (EU) No 330/2010 of 20 Apr. 2010 on the application of Art. 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices.

[103] Guidelines on Vertical Restraints, 19 May 2010, para. 48; *Philips*, *supra* n. 98, para. 64; *Pioneer*, *supra* n. 98, para. 155.

[104] Directorate for Financial and Enterprise Affairs Competition Committee, *supra* n. 101, para. 14.

[105] *Asus, supra* n. 98, paras 115–17; *Denon & Marantz, supra* n. 98, paras 101–03; *Philips*, *supra* n. 98, paras 71–73; *Pioneer*, *supra* n. 98, paras 163–65.

[106] York von Wartenburg, Falls & Okkonen, *supra* n. 96, at 497–98.

[107] Cf. also Niccolò Colombo, *What the European Commission (Still) Does Not Tell Us About Pricing Algorithms in the Aftermath of the E-Comerce Sector Inquiry*, 39 ECLR 478, 480 (2018).

[108] Aurélien Portuese, *European Algorithmic Antitrust and Resale Price Maintenance: Asus, Denon & Marantz, Philips, and Pioneer Decisions*, https://www.competitionpolicyinternational.com/european-algorithmic-antitrust-and-resale-price-maintenance-asus-denon-marantz-philips-and-pioneer-decisions (accessed 13 June 2019).

[109] The cooperation resulted in reductions to the fines of 50% for Pioneer and 40% for Asus, Denon & Marantz and Philips, EU Commission, Press Release of 24 July 2018, http://europa.eu/rapid/press-release_IP-18-4601_en.htm (accessed 13 June 2019).

[110] Guidelines on the method of setting fines imposed pursuant to Art. 23(2)(a) of Regulation No 1/2003, para. 29.

3.2 Algorithmic collusion[111]

The competitive process risks suffering harm when competitors make arrangements regarding their market activity. Such arrangements are usually called 'collusion' if they serve to raise the coordinating parties' profits above the non-cooperative equilibrium.[112] 'Explicit collusion' rests on an agreement or some other form of concertation between the involved market players, while 'tacit collusion',[113] oftentimes leading to parallel behaviour, requires no such concertation and can, in particular, result from market players monitoring and reacting to each other's independent business decisions.[114] Both types of collusion are economically undesirable as they tend to result in supra-competitive prices, lower output, deadweight losses, and, ultimately, a reduction in (consumer) welfare.[115] Nonetheless, most competition law regimes presently prohibit only explicit collusion while tolerating tacit collusion and parallel behaviour, not least because banning tacit collusion might inhibit market players from intelligently adapting their business strategy to their competitors' prices or other market conditions – after all a key component of competitive behaviour.[116]

Algorithms can, in various ways, be tools for establishing explicit collusion.[117] The use of identical pricing algorithms by competitors, for instance, is, arguably, not unlawful as such[118] but it can help competitors to unlawfully align their prices as part of a joint and consented strategy reducing competitive pressure.[119] Instead of such a decentralized strategy, competitors

---

111 This section is based to a large extend on Peter Georg Picht & Benedikt Freund, *Competition (Law) in the Era of Algorithms*, 39 ECLR 403 (2018).

112 OECD, *supra* n. 2, at 19; cf. also Hal R. Varian, *Intermediate Microeconomics – A Modern Approach*, 531–32 (9th ed., W. W. Norton & Company 2014).

113 Cf. Richard A. Posner, *Antitrust Law*, 52–53 (2nd ed., University of Chicago Press 2001).

114 Picht & Freund, *supra* n. 111, at 404; Michael K. Vaska, *Conscious Parallelism and Price-Fixing: Defining the Boundary*, 52 U. Chi. L. Rev. 508, 517–26 (1985).

115 OECD, *supra* n. 2, at 19–20; Alison Jones & Brenda Sufrin, *EU Competition Law, Text, Cases and Materials* 650 (6th ed., Oxford University Press 2016).

116 For the EU: *Ahlström Osakeyhtiö and Others v. Commission*, C-89/85, para. 71 (ECJ 31 Mar. 1993); *Suiker Unie and Others v. Commission*, C-40/73, para. 174 (ECJ 16 Dec. 1975); cf. also Jones & Sufrin, *supra.* n. 115, at 694–98; for the US: *In re: Text Messaging Antitrust Litigation*, No. 14–2301, 10–11 (7th Cir. 9 Apr. 2015).

117 Cf. Ariel Ezrachi & Maurice E. Stucke, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, 2017 U. Ill. L. Rev. 1775, 1784–87 (2017).

118 *See* Advocate General Szpunar's remark in a footnote in the Uber case: 'the use by competitors of the same algorithm to calculate the price is not in itself unlawful, but might give rise to hub-and-spoke conspiracy concerns when the power of the platform increases' (Opinion of Advocate General Szpunar, 11 May 2017, *Asociación Profesional Elite Taxi*, C-434/15, fn. 23); Michal Gal sees possible unlawful conduct where competitors (1) start to consciously use similar algorithms, despite better algorithms being available, (2) feed the same or similar training data to the learning algorithm, despite better training data being available and despite the awareness of the possibility of similar pricing results, or (3) make the algorithm transparent to competitors without any procompetitive justification (Competition Lore Podcast by Caron Beaton-Wells, *Competition and Algorithms – Friend or Foe?*, Episode of 19 Sept. 2018, 55"13', https://overcast.fm/+N2zZD5F3Q/55:13) (accessed 13 June 2019).

119 *United States v. David Topkins*, Plea Agreement, No. CR 15 201 WHO (n. D. Cal. 30 Apr. 2015), https://www.justice.gov/atr/case-document/file/628891/download (accessed 13 June 2019); *United States v.*

may jointly implement[120] a 'hub and spoke' cartel, for instance[121] by delegating the setting of prices (and potentially other conditions) to a central, algorithmic agent.[122] The coordination necessary to establish the hub and spoke structure typically requires some form of explicit collusion. Another option, the 'signalling' strategy, employs algorithms to exchange concealed information about (planned) market behaviour by sending, for example, pricing data which is being registered and possibly agreed upon.[123]

Whatever the strategy, explicit collusion remains illegal, regardless of whether it is being implemented by traditional, analogue techniques or by cutting-edge algorithms.[124] The challenges algorithmic explicit collusion presents consist, hence, not in deciding whether such conduct should be banned but rather in assessing its likelihood, detecting it in specific cases, and assigning appropriate liability.[125] Compared to more old-fashioned scenarios, several factors can complicate the uncovering of algorithmic collusion. For instance, algorithms can run their direct interaction at much higher speed than humans,[126] and they can cloak it in patterns more complex than those of human communication.[127]

David Topkins, No. CR 15 201 WHO (n. D. Cal. 6 Apr. 2015), https://www.justice.gov/atr/case-document/file/513586/download (accessed 13 June 2019); according to the Commission's report on the E-commerce sector inquiry 67% of the 53% of respondents tracking competitor's prices do so by automated systems and 78% of those 67% adjust their prices (European Commission, *Preliminary Report on the E-Commerce Sector Inquiry*, 15 Sept. 2016, SWD(2016) 312, 56, http://ec.europa.eu/competition/antitrust/sector_inquiry_preliminary_report_en.pdf) (accessed 13 June 2019).

120 Hub and spoke settings are more likely to occur as the result of explicit collusion, although they may also result from implicit collusion.

121 For further variants and details, *see* Ezrachi & Stucke, *supra* n. 117, at 1787–88.

122 *Meyer v. Kalanick*, No. 15 Civ. 9796, Opinion and Order (S.D.N.Y. 31 Mar. 2016); *Eturas and Others,* C-74/14 (ECJ 21 Jan. 2016); *see also* Andreas Heinemann & Aleksandra Gebicka, *Can Computers Form Cartels? About the Need for European Institutions to Revise the Concertation Doctrine in the Information Age*, 7 JECLAP 431 (2016).

123 OECD, *supra* n. 2, at 29–31.

124 Monopolkommission, *XXII. Hauptgutachten: Wettbewerb 2018*, para. 201, https://www.monopolkommission.de/images/HG22/HGXXII_Gesamt.pdf (accessed 13 June 2019); cf. also EU Commission in its submission to the OECD: 'if pricing practices are illegal when implemented offline, there is a strong chance that they will be illegal as well when implemented online' (Directorate for Financial and Enterprise Affairs Competition Committee, *supra* n. 101, para. 38).

125 Cf. Monopolkommission, *supra* n. 124, para. 215, according to which algorithms represent the prior will of the user but a shift in liability may have to be considered regarding self-learning algorithms.

126 OECD, *supra* n. 2, at 22 with reference to the Autorité de la Concurrence & Bundeskartellamt, *Competition Law and Data* 14–15, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2 (accessed 13 June 2019). Humans can be involved in algorithmic collusion as well, of course, but more indirectly, as coders, implementers, beneficiaries, etc., not as those directly exercising the coordination.

127 Algorithms may be much better in devising and deciphering math patterns, but they may be much weaker in decoding the non-verbal and non-mathematical communication (a look, a wink of the eyes, a handshake, an ambiguous expression) with which humans are able to convey complex, multi-facetted messages.

Where competition law enforcers manage, nonetheless, to discover algorithmic collusion that violates the law, they must decide on the liability of and on sanctions for the humans having built, coded, implemented or profited from the colluding algorithm. The degree of complexity and independence with which the algorithm operates ought probably to matter in this respect. This is because humans, as the ultimate addressees of liability, exercise much more direct control over 'simple' algorithms that merely execute patterns initially coded into them[128] than over so-called 'deep learning' algorithms[129] which are able to make decisions based on their own artificial neural network. Currently, creators of such (deep learning) algorithms are only liable as 'assistants' if they knew about the possible collusive employment and condoned it.[130] The may escape liability if the algorithms produce a collusive outcome that the creators, but not the involved companies, knew about (possibly due to the algorithm's complexity).[131] In any case, their algorithms cannot be qualified as undertakings under the Höfner criteria (regardless of their degree of autonomy) and, consequently, cannot infringe on Article 101 TFEU.[132] Arguably, they are rather agents operating for someone else.[133] Given that these reflections indicate a certain risk of liability loopholes, some contributions seem to favour liability for the creators of algorithms to be based more strongly on collusive outcomes.[134]

Tacit collusion requires a more fundamental reflection: Besides other reasons, competition law has – so far and except for cases of joint market dominance – tolerated[135] the detrimental economic effects of tacit collusion because conventional wisdom has it that this type of conduct requires rather specific conditions to succeed. In a nutshell, these conditions are (1) an oligopolistic market structure,[136] (2) homogeneity of goods and services in the market,[137] (3) market transparency,[138] and (4) high barriers for market

---

128 Cf. Ezrachi & Stucke, *supra* n. 117, at 1787.
129 Cf. OECD, *supra* n. 2, at 32.
130 Monopolkommission, *supra* n. 124, para. 265.
131 *Ibid.*, paras 266–68.
132 *Höfner and Elser v. Macroton GmbH*, C-41/90, para. 21 (ECJ 23 Apr. 1991).
133 Nicolas Petit, *Antitrust and Artificial Intelligence: A Research Agenda*, 8 JECLAP 361, 362 (2017).
134 Cf. Monopolkommission, *supra* n. 124, para. 271.
135 Joint market dominance only partially covers tacit collusion, cf. Monopolkommission, *supra* n. 124, paras 217–24.
136 Jan Potters & Sigrid Suetens, *Oligopoly Experiments in the Current Millennium*, 27 J. Econ. Surv. 439, 448 (2013).
137 Marc Ivaldi, Bruno Jullien, Patrick Rey, Paul Seabright & Jean Tirole, *The Economics of Tacit Collusion, Final Report for DG Competition* 47, 66 (2013), http://ec.europa.eu/competition/mergers/studies_reports/the_economics_of_tacit_collusion_en.pdf (accessed 13 June 2019).
138 *See* Christian Schultz, *Transparency on the Consumer Side and Tacit Collusion*, 49 Eur. Econ. Rev. 279-82 (2003).

entry.[139] Since these conditions appear(ed) to be present in a few markets only, the economic harm from tacit collusion seemed limited as well.[140]

The use of algorithms may, however, change this assessment in several ways: Regarding market structure (condition 1 above), algorithms may facilitate collusion in less concentrated markets because they can rapidly analyse large amounts of data and, as a consequence, it is easier to coordinate the behaviour of several market players.[141] Moreover, if algorithms learn, by means of AI and past data, to detect changes in demand and ensuing price reductions, the importance of demand fluctuations as a traditional instability factor in oligopoly settings might be mitigated.[142] Other factors destabilizing collusion, such as human biases and errors, may be eliminated as well.[143] As to homogeneity (condition 2 above), algorithms facilitate personalized pricing and product offerings,[144] reducing the homogeneity of goods and services in a market, but also increasing the price points that need to be coordinated.[145] More generally, complex, differing algorithms may enable competitors to display a more *hetero*geneous set of market strategies than if their human representatives had to come up with creative strategies themselves, and this strategic variance may reduce the likelihood for collusion.[146] Regarding transparency (condition 3 above), algorithms tend to increase market transparency due to their ability to rapidly collect data from multiple sources.[147] This helps to detect deliberate deviations from a collusive equilibrium and to separate them from simple market adaptations, such as changes in demand.[148] As to entry barriers (condition 4 above), a market strategy that combines algorithms and (data generated on) digital platforms potentially heightens entry barriers related to platform-typical network effects, economies of scale, and big data-mining possibilities.[149]

---

139 OECD, *supra* n. 2, at 20–21; Michal S. Gal, *Algorithmic-Facilitated Coordination: Market and Legal Solutions*, 2 Antitrust Chronicle 22 (2017), https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/AC_May.pdf (accessed 13 June 2019).

140 Salil K. Mehra, *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, 100 Minn. L. Rev. 1323, 1328 (2016); Rolf H. Weber, *Disruptive Technologies and Competition Law*, Ch. 4.2.1 (Klaus Mathis & Tor Avishalom, New Developments in Competition Law and Economics, Springer 2019); *see also* Autorité de la Concurrence & Bundeskartellamt, *supra* n. 126, at 14–15.

141 Monopolkommission, *supra* n. 124, para. 182; OECD, *supra* n. 2, at 21.

142 Francisco Beneke & Mark-Oliver Mackenrodt, *Artificial Intelligence and Collusion*, 50 IIC 109, 126–27 (2019).

143 Cf. in detail Picht & Freund, *supra* n. 111, at 405.

144 Cf. also Ulrich Schwalbe, *Algorithms, Machine Learning, and Collusion* 4, https://ssrn.com/abstract=3232631 (accessed 13 June 2019).

145 Petit, *supra* n. 133, at 361.

146 *Ibid*.

147 Competition and Markets Authority, *Pricing Algorithms, Economic Working Paper on the use of Algorithms to Facilitate Collusion and Personalised Pricing*, 8 Oct. 2018, paras 5.26 and 8.3(b), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf (accessed 13 June 2019); Monopolkommission, *supra* n. 124, para. 181; OECD, *supra* n. 2, at 21–22.

148 Monopolkommission, *supra* n. 124, para. 181.

149 Schwalbe, *supra* n. 144, at 4, however, noting that algorithmic pricing as a service is provided by firms such as *Feedvisor, PricingPro* or *Intelligence Node* and might reduce market entry barriers.

Algorithm-based personalization strategies can create entry barriers as well if they strongly attach customers to the personalizing incumbent.[150] On the other hand, availability of data resulting from widespread use of algorithms may reduce entry costs for new market players.[151]

As these reflections show, the influence of algorithms on the traditional conditions for tacit coordination does not appear fully settled yet.[152] In spite of ambiguities, however, it may be argued that algorithms are a catalyst for the establishment of collusion in markets already prone to such coordination.[153] If, in addition, (deep learning) algorithms were to make tacit collusion less dependent on its traditional preconditions[154] and, overall, more likely, competition law's present approach towards tacit collusion may have to be reassessed. Factors to potentially consider in this exercise are the extent to which competitors are using identical algorithms, as this can indicate the reach of hub and spoke cartels, and the source of the data sets on which these algorithms were based and trained, as using data from several competitors may increase the risk for tacit collusion.[155]

In fact, a recent article[156] seems to confirm that algorithmic markets put the traditional conditions for tacit collusion to their test. In a controlled, market-simulating environment, relatively simple algorithms learned to collude by trial and error, with their initial instruction stating only that the algorithms maximize profits, but not specifying how to do so.[157] The algorithms came to their collusive results with no prior knowledge of the environment in which they operated, without communicating with one another, and without being specifically designed or instructed to collude.[158] Notably, collusion prevailed even in simulations with up to four algorithms[159] and inhomogeneity in cost and demand had only a limited effect or, respectively, did not prevent collusion entirely.[160]

---

150 Competition and Markets Authority, *supra* n. 147, para. 8.4(b); cf. also Monopolkommission, *supra* n. 124, para. 183.

151 OECD, *supra* n. 2, at 21.

152 Schwalbe, *supra* n. 144, at 4; Monopolkommission, *supra* n. 124, para. 197; OECD, *supra* n. 2, at 23-24.

153 Monopolkommission, *supra* n. 124, para. 197; Ashwin Ittoo & Nicolas Petit, *Algorithmic Pricing Agents and Tacit Collusion: A Technological Perspective* 2–3, https://ssrn.com/abstract=3046405 (accessed 13 June 2019).

154 Michal Gal, *Algorithms as Illegal Agreements*, 34 Berkeley Tech. L.J. 67, 116 (2019); OECD, *supra* n. 2, at 24.

155 Competition and Markets Authority, *supra* n. 147, paras 8.7(b) and (c).

156 Emilio Calvano, Giacomo Calzolari, Vincenzo Denicolò & Sergio Pastorello, *Artificial Intelligence, Algorithmic Pricing and Collusion* 3, https://cepr.org/active/publications/discussion_papers/dp.php?dpno=13405 (accessed 13 June 2019).

157 https://www.law.ox.ac.uk/business-law-blog/blog/2019/02/artificial-intelligence-algorithmic-pricing-and-collusion (accessed 13 June 2019).

158 Calvano, Calzolari, Denicolò & Pastorello, supra n. 156, at 3, 39.

159 *Ibid.*, at 31–32.

160 *Ibid.*, at 32–33, 35.

3.3 Google Shopping: Paving the way for a 'results-based algorithmic approach'?

Cases relating to the use of algorithms by dominant market players are slowly moving into the antitrust spotlight. Two prominent examples are the German Bundeskartellamt's Lufthansa case[161] and the EU Commission's Google Shopping case. In the context of this article, the Google Shopping case is of particular interest because the EU Commission's approach focused on the market results of Google's conduct rather than on the (in) appropriateness of the algorithmic design which brought them about.[162]

In this prong of Google's confrontation with competition agencies,[163] the EU Commission had to assess whether Google was abusing its dominance[164] on the search engine market and held the company did so by demoting rival comparison shopping services in its search results whilst prominently placing its own ('Google Shopping').[165] The demotion was attributed to several criteria in Google's search algorithm and the fact that Google Shopping itself was not subject to the workings of the algorithm, resulting in significant gain in traffic for Google Shopping and corresponding losses for its competitors.[166] The decision raises several interesting

---

[161] In the context of the insolvency of Air Berlin, the German Bundeskartellamt started a preliminary investigation to assess the initiation of proceedings against Lufthansa due to abusive pricing. After Air Berlin's insolvency, Lufthansa's algorithmically determined ticket fares skyrocketed (+ 25–30%) on certain – now monopolistic – routes. In the end, the Bundeskartellamt did not initiate proceedings because of competitor easyJet's quick entry into the market which resulted in a market structure comparable to the one before Air Berlin's insolvency. Nonetheless, the case brings up the important question as to what extent the insolvency of a competitor or similar changes in market structure have to be considered in the price determination parameters of an algorithm and whether there is a duty to monitor and adjust (potentially after a grace period) the algorithm in the event of such structural changes. This issue gains in significance if insolvency leads to a dominant position of the remaining market participant, subjecting the latter to the stricter requirements for dominant companies. Cf. Bundeskartellamt, *Press Release of 29 May 2018* (https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/29_05_2018_Lufthansa.html) (accessed 13 June 2019), Bundeskartellamt, *Fallbericht B9-175/17 – Lufthansa*, 29 May 2018, 3 (https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2018/B9-175-17.pdf?__blob=publicationFile&v=4) (accessed 13 June 2019), Interview with the president of the Bundeskartellamt Andreas Mundt with in Neue Osnabrücker Zeitung (http://www.bundeskartellamt.de/SharedDocs/Interviews/DE/2018/180127_NOZ.html) (accessed 13 June 2019), Andreas Mundt, *Sixty Years and Still Exciting – The Bundeskartellamt in the Digital Era*, 6 Journal of Antitrust Enforcement 1, 3 (2018); Lufthansa-subsidiary Austrian Airlines might also be facing an inquiry involving pricing algorithms (https://kurier.at/wirtschaft/ueberteuert-behoerde-hat-fluege-wien-bruessel-im-visier/400051874) (accessed 13 June 2019).

[162] Cf. in detail Nicolo Zingales, *Antitrust Intent in an Age of Algorithmic Nudging*, Ch. 3.1, https://ssrn.com/abstract=3266624 (accessed 13 June 2019).

[163] Among the other prongs are Google Android (http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40099) and Google AdSense (http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40411).

[164] The EU Commission found Google dominant in general internet search markets in all thirty-one countries of the European Economic Area (EEA) since 2008 (except in the Czech Republic since 2011) and abusing its dominance in all thirteen EEA countries in which it offered Google shopping.

[165] *Google Search (Shopping)*, Case AT.39740, decision of 27 June 2017, http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.

[166] Cf. Commission Press Release IP/17/1784, http://europa.eu/rapid/press-release_IP-17-1784_en.htm (accessed 13 June 2019).

questions, i.a. related to two-sided markets,[167] on how to categorize Google's abusive conduct,[168] and what an appropriate implementation of the EU Commission's remedies would look like.[169]

Evidence in the case included 5.2 terabytes of search result data from Google. However, judging from the publicly available information, the EU Commission does not seem to have had any special insight into the functioning of Google's search algorithms. In order to establish that Google's algorithms, including one called 'Panda', demoted competing shopping comparison services[170] according to certain criteria,[171] the EU Commission relied on blogposts and documents,[172] as well as the fact that the visibility of competing comparison shopping services was at the highest before the launch of Panda and dropped afterwards with no sustainable recovery.[173] The fact that Google Shopping was not subject to the same ranking mechanism as its competing services was apparently established based on emails, replies to the Commission's request for information, and other data.[174]

Furthermore, the Commission did not attempt to meddle in the design or workings of Google's search algorithm. The Commission stated, for instance, that Google's search algorithm would not be examined[175] nor interfered with.[176]

---

[167] Rupprecht Podszun, *Der grosse Donner – hat sich Alphabet vergoogelt?*, https://www.d-kart.de/der-grosse-donner-hat-sich-alphabet-vergoogelt (accessed 13 June 2019).; on two- and multi-sided markets: Thomas Hoppner, *Defining Markets for Multi-Sided Platforms: The Case of Search Engines*, 38 WC 349 (2015); Stefan Holzweber, *Market Definition for Multi-Sided Platforms: A Legal Reappraisal*, 40 WC 536 (2017)

[168] For example, discrimination (Anca Chirita, *Google's Anti-Competitive and Unfair Practices in Digital Leisure Markets*, 11 The Competition L. Rev. 109, 120, 122 (2015); Renato Nazzini, *Google and the (Ever-Stretching) Boundaries of Art. 102 TFUE* [sic], 6 JECLAP 301, 307–10 (2015)), tying (pro: Chirita, *ibid.*, at 121; Benjamin Edelman, *Does Google Leverage Market Power Through Tying and Bundling?*, 11 J. Competition L. & Econ. 365, 369–78 (2015)), refusal to supply (contra: Chirita, *ibid.*, at 123; Nazzini, *ibid.*, at 307–10), margin squeeze (contra: Nazzini, *ibid.*, at 307–10) or lack of any abuse and theory (John Lang, *Comparing Microsoft and Google: The Concept of Exclusionary Abuse*, 39 WC 5, 27–28 (2016); Torsten Körber, *Common Errors Regarding Search Engine Regulation – and How to Avoid Them*, 36 ECLR 239 (2015)).

[169] The EU Commission specified the remedies in its corrected Tender Specification of 17 July 2017 for Technical Expertise in the case, 4–5, https://etendering.ted.europa.eu/cft/cft-documents.html?cftId=2629 (accessed 13 June 2019); *see* for case law on access remedies and Google's implementation: Bo Vesterdorf & Kyriakos Fountoukakos, *An Appraisal of the Remedy in the Commission's Google Search (Shopping) Decision and a Guide to Its Interpretation in Light of an Analytical Reading of the Case Law*, 9 JECLAP 3 (2018); calling this a 'magic stroke' and favouring the EU Commission not to fumble with any algorithms: Rupprecht Podszun, *The Google Case: First Comments by Haucap, Kersting, Podszun*, https://www.d-kart.de/the-google-case-first-comments.

[170] *Google Search (Shopping), supra* n. 165, para. 349.

[171] *Google Search (Shopping), supra* n. 165, paras 352, 358.

[172] *Google Search (Shopping), supra* n. 165, para. 358.

[173] *Google Search (Shopping), supra* n. 165, para. 361.

[174] *Google Search (Shopping), supra* n. 165, paras 380–83.

[175] Commitments in Case COMP/C-3/39.740, 3 Apr. 2013, Annex 4, s. A, para. 6, ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_8608_5.pdf. (accessed 13 June 2019).

[176] EU Commission Statement on the Google Investigation, 5 Feb. 2014, http://europa.eu/rapid/press-release_SPEECH-14-93_en.htm (accessed 13 June 2019).

On the remedies side, the proposed remedy of equal treatment[177] was not supposed to interfere with the search algorithm[178] or object to its fundamental structure either.[179] In this sense, the decision rather takes on a result-based approach, holding Google liable for the outcome the algorithm produced.[180]

4 WHERE COMPETITION LAW MIGHT LEARN AND IMPROVE

There are many lessons and proposals for the development of competition law that one might – and should – draw from the previous sections of this contribution. On a fundamental level, competition law must be designed so as to protect the dynamic, innovation-enhancing efficiency of algorithmic markets. Learning from other areas of the law will help competition law to frame – by combining transparency, prevention, deterrence, intervention, and systemic tools – algorithmic market activity towards a beneficial, dynamically efficient state. As concrete steps on this way, we want to highlight the following:

(1) So far, it has been possible to tackle cases involving algorithms largely with the existing tools of competition law (enforcement), without delving too deep into technical details.[181] However, this is likely to change, especially if further economic and empirical research confirms that algorithmic markets host a high potential for collusion. This will force competition authorities to improve the **factual and analytical foundation** on which they base their decisions and policies.[182] This suggests not only additional inquiries into sectors on which digitalization and 'algorithmization' have a strong impact.[183] The above-sketched 'transparency prong' of MiFID II,[184] for

[177] Cf. on this duty Eduardo Aguilera Valdivia, *The Scope of the 'Special Responsibility' upon Vertically Integrated Dominant Firms After the Google Shopping Case: Is There a Duty to Treat Rivals Equally and Refrain from Favouring Own Related Business?*, 41 WC 43 (2018).

[178] Commission MEMO/15/4781, http://europa.eu/rapid/press-release_MEMO-15-4781_en.htm (accessed 13 June 2019).

[179] Commission MEMO/17/1785, http://europa.eu/rapid/press-release_MEMO-17-1785_en.htm (accessed 13 June 2019); Aguilera Valdivia, *supra* n. 177, at 66.

[180] S*ee* in more detail Zingales, *supra* n. 162, at Ch. 3.1. Google's appeal of the decision is pending (Case T-612/17, Action Brought on 11 Sept. 2017 – Google and Alphabet *v.* Commission OJ C 369, 30 Oct. 2017, 37–38).

[181] Cf. however the screening tool of the Swiss Competition Commission to detect price fixing in procurement, David Imhof, Yavuz Karagök & Samuel Rutz, *Screening for Bid Rigging – Does It Work?*, 14 J. of Competition L. & Econ. 235 (2018).

[182] Rupprecht Podszun, *The More Technological Approach: Competition Law in the Digital Economy*, 101, 107 (Gintarė Surblytė, Competition on the Internet, Springer 2015); cf. also Monopolkommission, *supra* n. 124, para. 240; the German Bundeskartellamt and the French Autorité de la concurrence launched a joint project on algorithms and their implications on competition aiming at analysing challenges resulting from algorithms and trying to identify any approaches, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2018/19_06_2018_Algorithmen.html?nn=3591568 (accessed 13 June 2019).

[183] Cf. Monopolkommission, *supra* n. 124, paras 233–37, also evaluating the right of consumer protection organizations to request sector inquiries by amending § 34a of the German Act against Restraints of Competition (Competition Act – GWB).

[184] Cf. *supra* s. 2.2.1.

instance, shows that algorithm users' duties to inform and document can contribute a lot to keeping authorities (at least theoretically) up-to-date. Corroborating this approach, the UK Digital Competition Expert Panel considered in its March 2019 report that businesses should understand and be able to explain their algorithms and their interactivity with other firm's algorithms as well as any measures undertaken against potential biases and anti-competitiveness.[185]

When specific issues arise, authorities should be able and willing to carry out testing exercises regarding algorithms or AI systems, be it alone or in cooperation with the involved undertakings. As Article 7 RTS 6 and the respective experience of Financial Conduct Authorities show, it can be helpful to design these tests in a 'sandboxing' style, i.e. in a protected model environment.[186] Sandboxing may become especially important, if algorithmic collusion turns out to be a frequent reality.[187] For such endeavours, competition authorities may need additional resources (know-how, tools, skilled staff, etc.).[188] In the aftermath of the Google Shopping decision, for instance, the EU was looking for a technical expert[189] to monitor compliance with and implementation of the decision.[190] The expert's tasks were rather challenging and included the assessment – depending also on Google's approach for remedy implementation – of how Google's and its competitors' comparison shopping services are positioned and displayed on the search results page, as well as the standards, algorithms, mechanism and parameters used therefore.[191]

Some suggest, inter alia with regard to Swiss competition law,[192] that firms may submit their algorithms to the respective competition law authority for analysis and clearance.[193] A positive result of such an 'ex ante audit' could mitigate the risk of being

---

185 Digital Competition Expert Panel, *Unlocking Digital Competition, Report of the Digital Competition Expert Panel*, Mar. 2019, para. 3.171, https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel (accessed 13 June 2019).

186 Cf. *supra* s. 2.2.2.

187 Cf. Calvano, Calzolari, Denicolò & Pastorello, *supra* n. 156, at 41.

188 In Switzerland, the Competition Commission has mentioned the possibility to employ technical specialists (https://www.nzz.ch/wirtschaft/das-anliegen-der-fair-preis-initiative-ist-berechtigt-ld.1391008) and is at least building on its technical expertise (https://www.nzz.ch/wirtschaft/wenn-algorithmen-kartelle-bilden-ld.1415028); Margrethe Vestager publicly discussed employing algorithms to detect collusion (https://www.reuters.com/article/us-eu-antitrust-algorithm/eu-considers-using-algorithms-to-detect-anti-competitive-acts-idUSKBN1I5198); Michal Gal is suggesting that competition authorities build on technical expertise, also considering that possible remedies may include orders to stop using the algorithm, to not disclose the algorithm to competitors or to amend the algorithm (Competition Lore Podcast by Caron Beaton-Wells, *supra* n. 119, at 58"04', https://overcast.fm/+N2zZD5F3Q/58:04); Schwalbe, *supra* n. 144, at 22; cf also *infra* n. 193.

189 https://ted.europa.eu/TED/notice/udl?uri=TED:NOTICE:244258-2017:TEXT:EN:HTML&tabId=1.

190 Tender Specifications, Corrected Version of 17 July 2017, 3, https://etendering.ted.europa.eu/cft/cft-document.html?docId=27867.

191 *Ibid.*, at 5-6.

192 Picht & Freund, *supra* n. 111, at 408.

193 The FTC, for instance, established the Office of Technology Research and Investigation (https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-

sanctioned for unwanted effects the respective algorithms generate when used in a real-world environment. This option may be particularly attractive regarding undertakings which have already violated competition law and subsequently altered their algorithmic conduct in order to (purportedly) terminate the violation. Such preventive monitoring should, however, not gravitate towards a highly impracticable and anti-innovative scenario in which new algorithms or AI systems (legally or factually) require ex ante authorization to be put on the market.[194]

(2) Privacy by design and by default (Article 25 GDPR) was advocated by EU Commissioner Vestager as a standard of conduct under competition law as well, stating that '[w]hat businesses can – and must – do is to ensure antitrust compliance by design. That means pricing algorithms need to be built in a way that doesn't allow them to collude. Like a more honourable version of the computer HAL in the film 2001, they need to respond to an offer of collusion by saying "I'm sorry, I'm afraid I can't do that."'[195] This would mean that undertakings should structure their digital tools in a way that promises these tools to operate in a procompetitive manner (**pro-competitiveness by design**). Furthermore, the procompetitive configuration of a tool should form the pre-installed standard configuration (**pro-competitiveness by default**).[196]

One might reject this policy element due to the different regulatory purposes of privacy law and competition law. Another difference lies in the fact that the concept of a 'ban with permit reservation', i.e. the general unlawfulness of data-relevant measures unless they are justified by statutory reason or permission, is a principle from EU data protection regulation and alien to competition law.[197] However, the stronger reasons weigh in favour of a pro-competitiveness by design and by default approach. Given that not only data protection but also financial markets rules revert to systemic, design and default approaches, competition law should consider doing the same. Algorithmic markets are a rapidly evolving reality. Approaches that try to

---

investigation) (accessed 13 June 2019) that will also play an important role in helping the FTC understand how algorithms and AI software work in particular markets (remarks of former FTC Commissioner Terrell McSweeny, *Algorithms and Coordinated Effects*, 22 May 2017, 6, https://www.ftc.gov/system/files/documents/public_statements/1220673/mcsweeny_-_oxford_cclp_remarks_-_algorithms_and_coordinated_effects_5-22-17.pdf); similarly, to deal with algorithms, AI and big data, the UK's Competition and Markets Authority is building a technology team (https://www.ft.com/content/349103ba-c631-11e7-b2bb-322b2cb39656; https://www.gov.uk/government/news/cma-appoints-stefan-hunt-to-top-digital-role); cf. also *supra* n. 188.

194 For example, Google made 3'234 improvements to its search algorithm in 2018 (https://moz.com/blog/how-often-does-google-update-its-algorithm).

195 https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017_en.

196 Privacy by default (Art. 25 para. 2 GDPR) requires companies to process personal data with the highest privacy protection in a way that by default personal data is not accessible to an indefinite number of persons.

197 Sebastian Louven, *Antitrust by Design – Kartellrechtliche Technik-Compliance für Algorithmen, Blockchain und Plattformen?*, InTeR 180–81 (2018).

safeguard their pro-competitiveness ex ante, based on technology design, promise to be more effective than ex post enforcement via fines and conduct commitments. More than that, antitrust compliance by design and by default seems more apt to mitigate the risk that competition law violations escape notice altogether because they are committed by undertakings technologically superior to enforcement authorities.[198] On a conceptual level, this reflects the fact that privacy by design and default can be characterized as a principles-based regulation (as opposed to rules-based regulation),[199] a type of regulation typically more capable to cope with a fast-developing technical and economic environment.[200] Finally, giving pro-competitive rules of action to digital agents is, in a way, not so different from establishing a competition law-compliant code of conduct for human employees, and the latter is a well-known element of competition law compliance.[201]

The real intricacy is, of course, to identify what the design and the default should be in complex scenarios.[202] Some authors suggest that, regarding simple pricing algorithms, this may mean that the algorithms ought to be set not to react to price changes when they result from certain companies[203] or not to follow and match price *increases* by competitors but only their price decreases.[204] Others, like the German Monopolies Commission, point to the risk that very rigid regulatory

---

198 *Cf. also* Simonetta Vezzoso, *Competition by Design*, Ch. 3, https://ssrn.com/abstract=2986440 (accessed 13 June 2019).

199 Tilen Čuk & Arnaud van Waeyenberge, *European Legal Framework for Algorithmic and High Frequency Trading (Mifid 2 and MAR) – A Global Approach to Managing the Risks of the Modern Trading Paradigm*, 9 EJRR 146, 152 (2018). Principles-based regulation focusses on the outcomes and requires firms to take responsibility in conceiving measures realizing these outcomes, whereas rules-based regulation specifies rules of conduct, obliges firms to adhere to these rules and attempts to thereby realize the desired outcomes (Pascal Frantz & Norvald Instefjord, *Regulatory Competition and Rules/Principles-Based Regulation*, 45 JBFA 818, 819 (2018)). Although this dichotomy has been prominently discussed mainly in financial markets regulation, it seems noteworthy that both data protection and financial markets law employ a combination of rules and principles for framing algorithmic market activity. This suggests that it could be wise for other areas of the law – including competition law – to pursue a similar approach, setting rules where the *dos* and *don'ts* seem reasonably clear while reverting to principles-based provisions in case of uncertainty over what detailed rules should look like. An adapted principle of competition law compliance by default and design, for instance, could induce market players to shape their algorithmic market activity in a way that restricts the unwanted, uncontrolled exchange of sensitive market data between competitors.

200 Winston J. Maxwell, *Principles-Based Regulation of Personal Data: The Case of 'Fair Processing'*, 5 IDPL 205, 212, 214 (2015).

201 Cf., for instance, *British Sugar*, Com OJ. 1999 L 76/1, para. 208.

202 *See also* Vezzoso, *supra* n. 198, at Ch. 4.

203 Antonio Gomes, *Disruptive Innovation, Big Data and Algorithms*, OECD Presentation of 31 Aug. 2017, 40, http://www.sic.gov.co/sites/default/files/documentos/092017/antonio-ferreira-gomes-disruptive-innovation-big-data-and-algorithms.pptx (accessed 13 June 2019); Vezzoso, *supra* n. 198, at Ch. 4, also considering excluding collecting certain categories of data altogether.

204 The CMA identified this as a topic for further research while also pointing out that the underlying rationale of maximizing firm profit might make this 'too interventionist and damage the competitive process to restrict firms' ability to set its own prices' (Competition and Markets Authority, *supra* n. 147, para. 9.1(b)); *see also* Ariel Ezrachi & Maurice E. Stucke, *Two Artificial Neural Networks Meet in an Online Hub and Change the Future (Of Competition, Market Dynamics and Society)*, University of Tennessee Legal Studies Research Paper 1, 43 (2017), https://ssrn.com/abstract=2949434 (accessed

stipulations may block legitimate algorithmic pricing strategies and create barriers to market entry by raising regulatory cost.[205] The OECD also highlights the threat for innovation and underlines that such rules place considerable supervising burdens on the agencies in charge.[206]

The design of regulatory stipulations for pricing algorithms will be particularly challenging with regard to deep learning algorithms.[207] While scrutinizing the code of an algorithm (static testing) might be an option for simple algorithmic scenarios, it will fail for deep learning due to its inherent complexity.[208] In such cases, a viable option might be dynamic testing, whereby the deep learning system's output is compared with the input previously received.[209] Sometimes, such testing will tell that a particular input has a tendency to produce non-compliant output and that it should not, therefore, form the input training basis, even though the (growing) complexity of deep learning and its inherent mutability tend to complicate predicting correlations between input and output.[210] Moreover, it will not be possible to properly assess the risk of algorithmic collusion based on the features of individual algorithms, without also looking at their interactions with each other.[211] Here, economic theory or sandboxing exercises[212] could be capable of singling out design/default-worthy configurations.

The setting of standards for compliant, beneficial algorithm design by stakeholder-based organizations, potentially including certification to demonstrate compliance by design and default (cf. Article 25 paragraph 3 GDPR), could be a promising mechanism, as the success of standards for digital communication shows. Data protection and financial markets law have, so far, not pushed it very strongly.[213] Competition law, however, has already gained considerable experience on how to establish a workable, pro-competitive legal framework for standard-setting organizations, i.a. by securing open access to these organizations for all relevant stakeholders.[214] It can therefore, possibly,

---

13 June 2019), exploring the option of allowing immediate price decreases, while implementing a time lag for price increases.

205 Monopolkommission, *supra* n. 124, para. 251; *see also* Gomes, *supra* n. 203, at 40.

206 OECD, *supra* n. 2, at 50.

207 *See also* Vezzoso, *supra* n. 198, Ch. 4.

208 Joseph E. Harrington, *Developing Competition Law for Collusion by Autonomous Artificial Agents*, 14 J. Competition L. & Econ. 331, 354–55 (2019).

209 *Ibid.,* at 355.

210 *Ibid.*, at 355-56.

211 Emilio Calvano, Giacomo Calzolari, Vincenzo Denicolò & Sergio Pastorello, *Algorithmic Pricing What Implications for Competition Policy?,* 55 Review of Industrial Organization 156, 165 (2019).

212 Cf. *supra* s. 2.2.2; proposing an 'algorithmic collusion incubator': Ezrachi & Stucke, *supra* n. 204, at 42-43.

213 Cf., however, the discussion on standard-setting for the technologies underlying data portability according to Art. 20 GDPR, Inge Graef, Jeroen Verschakelen & Peggy Valcke, *Putting the Right to Data Portability into a Competition Law Perspective* 5, https://ssrn.com/abstract=2416537 (accessed 13 June 2019).

214 *See* for instance on the framework setting for the European Telecommunications Standards Institute (ETSI) by the European Commission: Christian Koenig & Ana Trias, *Some Standards for*

take a lead in the joint attempt of several legal regimes[215] to establish an appropriate standard-setting regime for algorithmic market activity. Where previous experience, clear results from testing or theory, convincing standards or similar guidance is not at hand, though, competition law enforcement must be careful not to place excessive liability burdens on the market players[216] by considering every undesirable market outcome as the result of a design/default violation.

(3) A conceptual alternative to the aforementioned antitrust compliance by design and by default could be a, less intrusive,[217] '**results-based approach**'[218] which entitles authorities to intervene where they detect anticompetitive market outcomes, even if they do not (immediately) manage to prove flaws in algorithmic design or the presence of subjective elements, such as knowledge or intention.[219] This seems to be the tendency in the Google Shopping decision and the system of ex post intervention measures in MiFID II shows that such an approach can be viable longterm, even with regard to markets as complex and fast-moving as financial markets.[220]

The results of complex, even self-learning algorithms and their interactions with other (algorithmic) market forces can be very hard for undertakings to predict and control.[221] One result from the Google Shopping decision might be that companies with algorithmic intermediary services will, therefore, conduct monitoring in order to proof their 'compliance by design'[222] or at least their appropriate care to avoid anti-competitive algorithmic results. It remains to be seen whether such exercises effectively shield from liability.[223] If the Google Shopping decision were taken (even pending appeal[224]) to establish a rigorous

---

Standardisation: A Basis for Harmonisation and Efficiency Maxmisation of EU and US Antitrust Control of the Standard-Setting Process, 32 EIPR 320, 325 (2010); Michael Fröhlich, *Standards und Patente – Die ETSI IPR Policy*, GRUR 205 (2008).

215 This would involve not only competition, data protection and financial markets law, but also other legal regimes, for instance on product liability, ethical considerations or contracts.

216 Nicolo Zingales, *Google Shopping: Beware of 'Self-Favouring' in a World of Algorithmic Nudging*, https://www.competitionpolicyinternational.com/google-shopping-beware-of-self-favouring-in-a-world-of-algorithmic-nudging (accessed 13 June 2019).

217 Calvano, Calzolari, Denicolò & Pastorello, *supra* n. 211, at 15.

218 *See also* Gal, *supra* n. 154, at 117.

219 Picht & Freund, *supra* n. 111, at 408; this approach also has the advantage of clearly distributing liability among the involved players, in a digital world consisting of developer, implementers and users of algorithms/AI systems. Incentivizing parties to clearly document who decided on the specifications for a system may be worthwhile as well, for instance by granting developers a 'client's choice defence' if a (anticompetitive) setting was requested by the implementer.

220 Cf. *supra* s. 2; *see further* Čuk & van Waeyenberge, *supra* n. 199, at 152.

221 Monopolkommission, *supra* n. 124, para. 170; Picht & Freund, *supra* n. 111, at 408.

222 Zingales, *supra* n. 162, Ch. 3.1.

223 *Ibid*.

224 Case T-612/17, Action Brought on 11 Sept. 2017 – Google and Alphabet *v*. Commission OJ C 369, 30 Oct. 2017, at 37–38.

results-based approach, this may generate excessively strict liability absent limiting concepts.[225] These could include a predictability defence, a 'notice and readjustment' mechanism, potentially including an obligation to establish 'kill switches'[226] as an emergency tool against anticompetitive algorithmic dynamics, or even possibly an exculpatory defence where an algorithm was designed according to compliance by default and design.[227]

(4) Undoubtedly, algorithms provide demand-side efficiencies by helping consumers to judge prices, quality and variety, for example by means of price comparison websites or rating portals. They can thus reduce search transaction costs or help avoid biases.[228] However, consumers can have great difficulties to detect algorithmic practices patronizing or harming them and to defend their interests against such practices. To take a seemingly mild, but potentially far-reaching example, Amazon's recently patented 'anticipatory shipping' might predict what customers want and deliver it to them before an order is even placed.[229] The introduction of such 'algorithmic consumers'[230] could well come at the price of reduced consumer autonomy.[231] Balancing such risks may require specific **customer information rights and company transparency duties** similar to those stipulated by the GDPR.[232]

A core element of such duties could be the obligation to thoroughly explain the workings of an algorithm, not on a technical level but regarding its impact on the customer, especially where it is designed to replace customer choice. Furthermore, it has been suggested that companies employing algorithms should display a notice including the requirements of competition law and how the firm deals with them.[233] A duty to disclose source code, on the contrary, may impair legitimate confidentiality interests and innovation incentives too strongly, while being of limited help to those affected by the source code's workings.[234] A further

---

225 Zingales, *supra* n. 162, Ch. 4. This issue will be much aggravated as growing sophistication increasingly turns algorithms into 'black boxes' not only for competition law enforcers but also for the market players using them.

226 On the use of 'kill functionalities' in financial markets regulation, *supra* s. 2.2.3; on the danger of learning algorithms overcoming such a kill-switch, *see* Laurent Orseau & Stuart Armstrong, *Safely Interruptible Agents*, http://intelligence.org/files/Interruptibility.pdf (accessed 13 June 2019).

227 *See also* Zingales, *supra* n. 216.

228 OECD, *supra* n. 2, at 17, 18.

229 Praveen Kopalle, *Why Amazon's Anticipatory Shipping Is Pure Genius*, https://www.forbes.com/sites/onmarketing/2014/01/28/why-amazons-anticipatory-shipping-is-pure-genius/#3928d2ed4605 (accessed 13 June 2019).

230 Gal and Elkin-Koren coined this term for algorithms bypassing genuine consumer choice, *see* Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 Harv. J.L. & Tech. 309, 310 (2017).

231 *Ibid.*, at 322–23.

232 Art. 13 para. 2 lit. f, Art. 14 para. 2 lit. g and Art. 15 para. 1 lit. h GDPR.

233 Vezzoso, *supra* n. 198, at Ch. 4.

234 This is not only true for non-technological users, but also for more tech-savvy users: after *reddit* disclosed its ranking code, programmers and developers were disagreeing on its functioning (https://

line must be drawn where transparency would substantially facilitate (tacit) collusion.[235]

All in all, a duty to disclose whether an algorithm was involved in the decision-making process and to explain its logic in basic terms, i.e. an obligation similar to the requirements made by Article 22 GDPR, could increase companies' incentives to design their algorithmic tools in a way that is both legally compliant and attractive from the viewpoint of consumers' interests. Not only law enforcement but also market dynamics could thus generate a push towards a beneficial design of algorithms.

---

www.businessinsider.com/two-programmers-claim-reddits-voting-algorithm-is-flawed-2013-12?r=US&IR=T); in deep learning applications, even its developers and engineers are often unaware of the specific decision-making processes (https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai) (accessed 13 June 2019).

[235] Cf. in detail Gal, *supra* n. 154, at 84-88.