Germany

Thomas Hoeren and Hanna Hoffmann

Thomas Hoeren, Westfälische Wilhelms-Universität, Münster, Germany
E-mail: hoeren@uni-muenster.de

Hanna Hoffmann, Westfälische Wilhelms-Universität, Münster, Germany
E-mail: hanna.hoffmann@uni-muenster.de

1. Introduction

The development of artificial intelligence (AI) leads to new challenges in all legal fields. The application possibilities of the algorithms are becoming more and more extensive. While algorithms were once only used for recognizing patterns in data sets,[1] today they are increasingly making forecasting decisions and thus taking on human tasks.[2] From a competition law perspective, it is worth taking a look at the use of AI for marketing purposes, which often includes native advertising, and personal pricing, but the role of influencers is also in focus.

Firstly, this report examines the influence of algorithms on the customer's contractual freedom (section 2). Secondly, the relationship between competition law and data protection law is presented (section 3), referring in particular to current German and European case law. Thirdly, certain commercial practices that are currently of particular importance are examined, such as influencing, AI and marketing and personalised prices (section 4). Fourthly, the impact of personalised political campaigns on elections and democracy as a whole are discussed (section 5). Finally, future perspectives are outlined.

2. Algorithm's Influence on the Customer's Contractual Freedom

The infinite flood of information on the internet makes the use of certain tools such as search engines necessary. The mass of data can hardly be grasped by an individual, and could not be processed without a preselection of the search engine.[3] Therefore, the search algorithms of the search engines determine which offers and thus potential contractual partners are suggested to the customer.[4] A search engine often acts as a "gatekeeper".[5] The software's suggestion finding process remains hidden from the user, which becomes problematic, if external (third-party) factors such as advertising outweigh the user's interests when creating search results.[6] In order to get an objective selection of the best options, a user would have to do further research.[7] However, the average user only looks at the first two sides of results when using a search engine.[8] Therefore, it is no surprise that empirical studies show that the ranking has a considerable influence on

---

1 Bundesverband Digitale Wirtschaft e.V., Anwendungsgebiete. Available at https://www.bvdw.org/themen/kuenstliche-intelligenz/anwendungsgebiete/. Accessed 23 August 2021.
2 Fraunhofer Big Data AI, Potenzialanalyse »Künstliche Intelligenz«. Available at https://www.bigdata.fraunhofer.de/de/big-data/kuenstliche-intelligenz-und-maschinelles-lernen/potenzialanalyse--kuenstliche-intelligenz-.html. Accessed 23 August 2021.
3 C. Busch, Mehr Fairness und Transparenz in der Plattformökonomie?, GRUR 2019, pp. 788-796; J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.
4 J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.
5 S. Ott, Ich will hier rein! Suchmaschinen und das Kartellrecht, MMR 2006, pp. 195-202.
6 J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.
7 J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.
8 S. Ott, Ich will hier rein! Suchmaschinen und das Kartellrecht, MMR 2006, pp. 195-202.

consumers' purchasing decisions.[9] However, it is questionable whether it can be said that the customer's contractual freedom is being eroded by the use of search engines.[10] There is no denying that the customer's rights are affected. However, it should be noted that similar situations existed even before the search engines: If someone buys an item in a shop, one does not know whether it is possible to get it cheaper elsewhere. Search engines are the only way to sort the content of the Internet and the use of Internet itself offers chiefly a huge advantage in freedom of choice, which is greater than ever before.

However, in order to be fully informed the customer needs to know which criteria the search engine uses to create the ranking and how these criteria are rated. The primary concern is to prevent unfair influence using irrelevant ranking criteria,[11] which leads to worse results for consumers. Although the ranking algorithms are "black box systems" which are not transparent to the customer,[12] there are already regulations to ensure some transparency. According to Art. 5 (2) of Regulation 2019/1150,[13] "[p]roviders of online search engines shall set out the main parameters, which individually or collectively are most significant in determining ranking and the relative importance of those main parameters, by providing an easily and publicly available description, drafted in plain and intelligible language, on the online search engines of those providers. They shall keep that description up to date." If, for example, commission payments are considered for the ranking, the provider must indicate this and has to explain how such payments affect the ranking.[14] The more transparency there is on the market, the more informed the consumer would be. However, disclosing too much information (e.g. the entire algorithm) would make it possible to manipulate the rankings[15] and might also effect trade secrets. Therefore, this is correctly not required by the regulation.

Internet services as search engines affect the customer's contractual freedom not only by pre-arranging the information but also by using personalised advertisements. Since there is an increasing appearance of "non-monetary markets" on the internet,[16] some of those free service platforms have recently achieved very high market shares. Google for example, has about 90% of the search engine market in most countries of the European Economic Area.[17] From a financial point of view, customers, who are going to use services like search engines, are going to receive the information free of charge so that this business model is financed only through the advertising site, where advertisers pay a price to Google each time a search customer clicks on an ad.[18] The more information (data) about users is available, the more precisely this advertising can target the user.[19] If the advertisement fits the specific user well, the probability that he or she will click on it and ultimately purchase the advertised products increases.[20] In this respect, the user data has a value for platform companies such as Google or Facebook.[21] Therefore, the customers "pay" for the service by paying attention to the advertising displayed on the search page and the disclosure of their data.[22]

---

9 R. Ursu, The power of rankings: quantifying the effect of rankings on the online consumer search and purchase decisions, Marketing Science 37 (4), 2018, pp. 530-552.

10 With regard to the erosion of the free will in civil law by the internet see J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.

11 C. Busch, Mehr Fairness und Transparenz in der Plattformökonomie?, GRUR 2019, pp. 788-796.

12 C. Busch, Mehr Fairness und Transparenz in der Plattformökonomie?, GRUR 2019, pp. 788-796.

13 Regulation 2019/1150 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ 2019 L 186, p. 57–79.

14 C. Busch, Mehr Fairness und Transparenz in der Plattformökonomie?, GRUR 2019, pp. 788-796.

15 C. Busch, Mehr Fairness und Transparenz in der Plattformökonomie?, GRUR 2019, pp. 788-796.

16 T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, pp. 93-101.

17 European Commission, Antitrust: Commission sends Statement of Objections to Google on comparison shopping service, 15 April 2015. Available at https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_4781. Accessed 23 August 2021.

18 T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, pp. 93-101.

19 P. Hacker, Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht, ZfPW 2019, pp. 148-197.

20 T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, pp. 93-101.

21 T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, pp. 93-101.

22 P. Hacker, Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht, ZfPW 2019, pp. 148-197; T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, pp. 93-101.

It is obvious that the provision of data in certain constellations can have the character of a "fee" or a “payment” and therefore the relevant regulations regarding paid services should be applied.[23] The new Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services recognizes the disclosure of data as “remuneration” and treats it almost as other contracts for remuneration.[24]

However, while data can sometimes have the character of a remuneration, there is still a difference (from a financial point of view) between free services and paid services. On the one hand, unlike money, data is neither scarce nor exclusive and several companies can have access to the same data.[25] On the other hand, data can become outdated and obsolete.[26]

In December 2020, the EU Commission proposed its Digital Services Act (DSA).[27] The draft contains several rules and obligations concerning online advertising. According to Art. 24 DSA online platforms that display advertising on their online interfaces shall ensure that the recipients of the service 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 and meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed. In addition, according to Art. 30 DSA very large online platforms that display advertising on their online interfaces shall compile and make publicly available through application programming interfaces a repository containing certain information, until one year after the advertisement was displayed for the last time on their online interfaces. This repository shall include at least the content of the advertisement, the natural or legal person on whose behalf the advertisement is displayed, the period during which the advertisement was displayed, whether the advertisement was intended to be displayed specifically to one or more particular groups of recipients of the service and if so, the main parameters used for that purpose and the total number of recipients of the service reached and, where applicable, aggregate numbers for the group or groups of recipients to whom the advertisement was targeted specifically. Furthermore, according to Art. 26 DSA those very large online platforms shall identify, analyse and assess at least once a year any significant systemic risks stemming from the functioning and use made of their services in the EU. When conducting these risk assessments, the platforms shall consider, among other things, how their systems for selecting and displaying advertisement influence specific systemic risks, like negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child. According to Art. 27 DSA these very large online platforms shall additionally put in place reasonable, proportionate and effective mitigation measures aimed at limiting the display of advertisements in association with the service they provide. It remains to be seen whether these regulations will be adopted by the EU.

Besides that, in April 2021 the EU Commission proposed a regulation for harmonized rules on AI, the so-called Artificial Intelligence Act (AIA).[28] The AIA draft also provides certain transparency requirements, which are discussed in more detail in the following sections.

---

[23] T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, pp. 93-101.

[24] G. Spindler and K. Sein, Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen, MMR 2019, pp. 415-420.

[25] T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, pp. 93-101.

[26] T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, pp. 93-101.

[27] EU Commission, 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, COM(2020) 825 final of 15.12.2020.

[28] EU Commission, 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 of 21 April 2021.

2.1. Algorithmic Forecast and the Individual Autonomy

The customer's contractual freedom could also be affected by algorithmic forecast. Algorithms often undertake important forecast decisions and carry out contract negotiations while the customer remains an observer. Depending on the program, artificial intelligence has sometimes a broad and sometimes a limited scope of action.[29] However, often have a broad scope of action to take advantage of the benefits of artificial intelligence programs. Therefore, the customer cannot predict the outcome produced by the software and whether such outcome corresponds to his or her will, but he or she must allow himself or herself to be attributed any explanatory action of the software.[30] This is problematic because the result of the software may be objectively correct (based on mathematical calculations) but may not correspond to what the customer subjectively wanted.

Besides opaque algorithmic forecast, the ability of data collectors to manipulate users based on information collected about them, raises more and more public concerns.[31] The more information the data collector has, the better he can exercise considerable influence on the affected person.[32] The data collector can understand how he can influence the affected person best, by knowing his motives, weaknesses and vulnerabilities.[33] Some scholars say, that digital surveillance and the use of information to influence our decision making is not only about unfair commerce, since it does not just diminish our interests, but it threatens our autonomy.[34] Such an interference in our autonomy can only be assumed if the algorithm acts in a manipulative way. Manipulation only occurs if it is hidden influence. "Manipulating someone means intentionally and covertly influencing their decision-making, by targeting and exploiting their decision-making vulnerabilities."[35] Since "[t]he ruling idea behind the ideal of personal autonomy is that people should make their own lives",[36] we are only autonomous, if we act freely and can face the existing choices. And only if we can critically reflect our goals and desires, we can understand them authentically as our own.[37]

Nevertheless, this would not constitute a significant restriction of the individual autonomy if the customer could still terminate a contract which does not correspond to his will. However, under section 119 (1) of the German Civil Code (Bürgerliches Gesetzbuch, BGB) the right to contest is only available if the customer is in error. If a customer enters into a contract using a computer, a previous input error by the user can effect the declaration later made by the software. The error does not originate from the software: it can be traced back to the user.[38] The use of artificial intelligence, on the other hand, shifts the decision-making process significantly to the software itself.[39] If the software determined the content of the declaration and the user only gave a blanket declaration,[40] the error must have occurred within the software. However, a software generally does not make mistakes, but makes decisions based on a mathematically correct

---

29 J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.

30 J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.

31 M. J. Abramowitz, Stop the Manipulation of Democracy Online, The New York Times of 11 December 2017; J. Doubek, How Disinformation And Distortions On Social Media Affected Elections Worldwide, 16 November 2017. Available at https://www.npr.org/sections/alltechconsidered/2017/11/16/564542100/how-disinformation-and-distortions-on-social-media-affected-elections-worldwide?t=1624346148419. Accessed 22 June 2021; M. I. Vayena, Cambridge Analytica and Online Manipulation, 2018. Available at https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/. Accessed 22 June 2021.

32 N. M. Richards, The Dangers of Surveilllance, Harvard Law Rewiev 2013, 126 (7), pp. 1934-1965.

33 D. Susser, B. Roessler and H. Nissenbaum, Technology, autonomy and manipulation, Internet policy review 2019, 8 (2), pp. 1-22.

34 B. Frischmann and E. Sellinger, Re-Engineering Humanity, 1st ed, 2018, p. 271; S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 1st ed., New York: Public Affairs 2019, p. 347.

35 D. Susser, B. Roessler and H. Nissenbaum, Technology, autonomy and manipulation, Internet policy review 2019, 8 (2), pp. 1-22.

36 J. Raz, The Morality of Fredoom, Oxford: Clarendon Press 1986, p. 369.

37 D. Susser, B. Roessler and H. Nissenbaum, Technology, autonomy and manipulation, Internet policy review 2019, 8 (2), pp. 1-22.

38 BGH, Judgement of 16 October 2012 – X ZR 37/12, MMR 2013, pp. 296-298.

39 J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.

40 T. Nitschke and P. Sester, Software-Agent mit Lizenz zum…?, CR 2004, pp. 548-554; J. Grapentin, Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.

calculation.[41] If an unwanted result occurs, it is not an error in the legal sense.[42] Therefore, a right to contest on the grounds of error is generally precluded and the user cannot terminate the contract. This further limits the autonomy of the customer.[43]

2.2. The Instrument of the Informed Consent

Since there is an influence on the customer's contractual freedom, it can be compensated by the instrument of informed consent. The requirements for consent as a condition of lawfulness are present in various GDPR provisions. In addition to Art. 6 (1) lit. a GDPR, further requirements can be found in Art. 4 no. 11, Art. 7 and Art. 8 GDPR.[44]

The legitimacy of consent is the central requirement in data protection law.[45] Although the previous regulation, Art. 7 (a) of the Directive 95/46, unlike Art. 6 (1) lit. a GDPR, was referring to "unambiguously*"* consent of the user, this requirement also applies to the new regulation since Art. 4 no. 11 and recital 32, 42 and 43 have further specifications.[46]

By asking for "one or more specific purposes", Art. 6 (1) lit. a GDPR prevents the possibility of extending the purpose of processing after consent has been given.[47] Recital 42 specifies the requirements for consent by saying that the declaration of consent preformulated by the controller should be written in "clear and plain language and it should not contain unfair terms". These requirements ensure that the user is informed in a clearly understandable way[48] and is also informed about the specific intention.

However, some voices question the adequacy of consent to ensure an appropriate balance between data sovereignty of individuals and economic interests of businesses. Even if the user is aware of all circumstances of the data processing, he or she may be forced to accept the extensive processing of his or her personal data only because there are no comparable alternatives. The negligence of users represents another major risk. Some users may not take the time to read through data protection declarations, but may carelessly consent to the use of their data by clicking on them.[49] This risk could be reduced by the use of warning symbols or the implementation of a European uniform certification system, which classifies a website or app according to its truthfulness in terms of data processing.[50] Furthermore, these proposals would not constitute a one-sided consumer protection regulation to the disadvantage of the digital economy: if data protection and data security were correctly understood as a competitive strength, the European digital economy could gain an advantage over international competition precisely through transparent and user-oriented business models.[51]

Another issue is the expiry date of consent. Especially in the case of non-written requests, it might be difficult for the company processing the data to know when the consent is invalid or has been revoked,[52] and it might be even more difficult for the user to know whether the company is complying.

---

41 C. D. Müller-Hengstenberg and S. Kirn*,* Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems – Rechtliche Konsequenzen der "Verselbstständigung" technischer Systeme, MMR 2014, pp. 307-313; J. Grapentin*,* Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.

42 C. D. Müller-Hengstenberg and S. Kirn*,* Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems – Rechtliche Konsequenzen der "Verselbstständigung" technischer Systeme, MMR 2014, pp. 307-313.

43 J. Grapentin*,* Die Erosion der Vertragsgestaltungsmacht durch das Internet und den Einsatz Künstlicher Intelligenz, NJW 2019, pp. 181-185.

44 M. Albers and R.-D. Veit. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 6 DS-GVO, para. 23.

45 J. Masing, Herausforderungen des Datenschutzes, NJW, 2012, pp. 2305-2311; M. Albers and R.-D. Veit. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 6 DS-GVO, para. 19.

46 M. Albers and R.-D. Veit. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 6 DS-GVO, para. 7.

47 M. Albers and R.-D. Veit. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 6 DS-GVO, para. 23.

48 P.-L. Krüger, Datensouveränität und Digitalisierung, ZRP 2016, pp. 190-192.

49 P.-L. Krüger, Datensouveränität und Digitalisierung, ZRP 2016, pp. 190-192.

50 S. Kraska, Datenschutz-Zertifizierungen in der EU-Datenschutzgrundverordnung, ZD 2016, pp. 153-154; G. Hornung and K. Hartl, Datenschutz durch Marktanreize – auch in Europa? - Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit, ZD 2014, pp. 219-225.

51 P.-L. Krüger, Datensouveränität und Digitalisierung, ZRP 2016, pp. 190-192.

52 E. M. Frenzel. In Paal and Pauly (eds), Datenschutzgrundverordnung, Bundesdatenschutzkontakt, 2nd ed, C.H. Beck 2018, Art. 6 DS-GVO, para. 11.

Similar problems occur with the transparency requirements provided by the EU Commission's proposal for an Artificial Intelligence Act.[53] For example, according to Art. 52 AIA, AI systems that interact with natural persons must inform the natural person that he or she is interacting with such a system unless it is obvious. This exception offers much room for interpretation, which will have to be further determined by the responsible supervisory authorities and courts. Furthermore, it remains unclear how the duty to inform should look in practice. On the one hand, a too simple information to the affected person about the AI system does not help, since many people will ignore the information. On the other hand, it is generally assumed that only an informed person is able to take responsibility for him- or herself and take necessary protective measures. In the context of AI systems, often the persons concerned are not in the position to recognize the indirect consequences, which may lie in the future. Instead of referring to the use of an AI system, it would be preferable to provide information about criteria used by AI system and their possible consequences.

2.3. Improvement of Transparency

Besides the informed consent, an improvement of transparency reduces the algorithms influence on the customer's contractual freedom. The principle of transparency is included in several provisions of the GDPR (Art. 5 (1) lit. a, 12, 13, 14, 15, 22 GDPR and recital 58, 60, 71). According to Art. 15 (1) GDPR, the data subject shall have access to the personal data concerning him or her being processed, but at the same time the specific amount of the information to be communicated is highly controversial and equally relevant in practice.[54] The problem becomes obvious in the following example: According to Art. 15 (1) GDPR, a health insurance company must inform a policyholder requesting information of his "master data", such as name, date of birth, contact data, health data, medical statements, medical certificates. It is being discussed whether internal notes of the insurance company about the policyholder, internal reports, internal statements, past correspondence or the premium account at the insurance tariff must also be provided.

In the literature some voices say that Art. 15 (1) GDPR is not restricted within the limitations of section 826 BGB and therefore covers information on *everything* which contains personal data of the data subject, such as past correspondence from parties, internal memos on the data subject or internal opinions.[55] In individual cases, this can lead to a comprehensive provision of information.[56] The Cologne Higher Regional Court takes the same position: the term "personal data" under Art. 15 (1) GDPR is not limited to "master data", but also extends to electronically stored notes on telephone calls and other conversations with the customer.[57] In contrast, the Regional Court of Cologne takes the opposite view when it states that Art. 15 (1) GDPR does not refer to all internal transactions or correspondence, but is intended to ensure that the person concerned can assess the scope and content of the stored data.[58] This view could also be supported by Art. 15 (3) first sentence GDPR. According to this provision, the controller shall provide a copy of the personal data undergoing processing. It could be argued that the operator cannot be expected to make a copy of every piece of the data collection. In June 2021 the German Federal Court of Justice (Bundesgerichtshof, BGH) followed a comprehensive understanding of Art. 15 (1) GDPR.[59] The court ruled that Art. 15 (1) GDPR covers all "personal data" within the meaning of the broad definition of Art. 4 Nr.1 GDPR and therefore the data subject shall even have access to internal notes.

---

53 EU Commission, 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 of 21 April 2021.
54 F. Schmidt-Wudy, In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 15 DS-GVO, para. 52.
55 M. Riemer, Der Datenauskunftsanspruch als „discovery" im deutschen Zivilprozess, ZD 2019, pp. 413-415.
56 V. Scheepers, Der Umgang mit einem Auskunftsersuchen nach der DSGVO, DStR 2019, pp. 1109-1111.
57 OLG Köln, Judgement of 26 July 2019 – 20 U 75/18.
58 LG Köln, Judgement of 19 June.2019 – 26 S 13/18.
59 BGH, Judgement of 15 June 2021 – VI ZR 576/19.

In terms of time, it is not clear what the right covers. Art. 15 (1) GDPR does not address the problem raised in the "Rijkeboer" decision of the CJEU, according to which the right to information under data protection law does not only cover the data currently held by the responsible party, but also data from the past.[60] Some voices therefore say that the silence of the GDPR on this issue can only be understood to mean that there should be no claim to information on "past" data and only actually available data are to be considered.[61] Others say that the “Rijkeboer” principles would still apply.[62] It remains to be seen which view is supported by the case law.

Additionally, it becomes problematic for the consumers when the website operator does not know what data is collected from third parties on his website. In its judgement in the “Fashion ID” case, the CJEU disputed whether the operator of a website, who adds to that website a social plug-in which causes the browser of the visitor to ask for the content of the provider of that plug-in and, therefore, to transmit the visitor’s personal data to that provider, can be treated as a controller within the meaning of Art. 2 (d) of the Directive 95/46, even though that operator has no influence on the processing of the data which are transmitted to the provider. The data of the user is passed on to the provider of the plug-in no matter if the plug-in is clicked on or even whether the user is a member of the social network.[63]

The court found that the operator of a website placing the “Facebook-Like-button” (a social plug-in that causes the transmission to Facebook of website users’ personal data) and Facebook can be qualified as jointly responsible under EU data protection law. The term “controller” in Art. 2 (d) of Directive 95/46 is widely defined in order to ensure effective and comprehensive protection of data subjects.[64] The website operator is responsible within the meaning of Directive 95/46 even if, beyond the decision to use the social plug-in, he or she does not or cannot influence the processing of personal data. It is not necessary for each of the operators to have access to the personal data concerned. An operator may therefore be (jointly) responsible even if it does not process personal data itself, as long as the controller decides on the purposes and means of processing personal data with another operator that processes the data.[65]

The CJEU’s findings on shared responsibility in connection with social plug-ins can easily be transferred to the GDPR, as the definition of (jointly) responsible in Art. 4 no. 7 GDPR has not changed compared to the directive.[66] The GDPR contains specific legal consequences for joint controllership, such as the requirement of an agreement between the responsible parties, which defines, who is responsible for compliance with which obligations under the GDPR (Art. 26 (1) first sentence GDPR), without this agreement having any external effect (Art. 26 (3) GDPR).[67] According to Art. 26 (2) second sentence GDPR, "the essentials" of this agreement have to be made accessible to the data subject, for example in the context of providing the information according to Art. 13 and 14 GDPR.[68] The information that the operator of the website is required to provide to the data subject must relate only to operations involving the processing of personal data. In practice those joint controllers must agree on who and how they will fulfil of the relevant information obligations.[69]

Transparency is thus created due to the fact that the operator of a website that integrates social plug-ins from third-party providers such as Facebook, Google, Twitter and Microsoft (LinkedIn) must inform the data subject and obtain separate

---

60 CJEU, case C-553/07, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, Judgment of 7 May 2009, ECLI:EU:C:2009:293.

61 F. Schmidt-Wudy. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 15 DS-GVO, para. 52.2.

62 L. Franck. In: P. Gola (ed.), DS-GVO, 2nd ed, C.H. Beck 2018, Art. 15 DS-GVO, para. 8; A. Dix. In: Simitis, Hornung and Spiecker gen. Döhmann (eds), Datenschutzrecht, 1st ed, Nomos 2019, Art. 15 DS-GVO, para. 45.

63 CJEU, case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, Judgment of 29 July 2019, ECLI:EU:C:2019:629; Datenschutzrechtliche Verantwortlichkeit für Social Plugin auf Website, NJW 2019, pp. 2755-2760.

64 CJEU, case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgement of 13 May 2014, EU:C:2014:317, para. 34; CJEU, case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein gegen Wirtschaftsakademie Schleswig-Holstein GmbH, Judgement of 5 June 2018, ECLI:EU:C:2018:388, para. 28.

65 CJEU, case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, Judgment of 29 July 2019, ECLI:EU:C:2019:629, para. 85.

66 J. Spittka and R. Mantz, Datenschutzrechtliche Anforderungen an den Einsatz von Social Plugins, NJW 2019, pp. 2742-2745.

67 J. Spittka and R. Mantz, Datenschutzrechtliche Anforderungen an den Einsatz von Social Plugins, NJW 2019, pp. 2742-2745.

68 J. Spittka and R. Mantz, Datenschutzrechtliche Anforderungen an den Einsatz von Social Plugins, NJW 2019, pp. 2742-2745.

69 F. Moos and T. Rothkegel, „Gefällt mir“-Button von Facebook – Fashion ID, MMR 2019, pp. 579-587.

consent before collecting and transferring the data to the provider.[70] In addition, the shared responsibility operators are also both liable for the rights and compensation claims of the data subjects (Art. 26 (3), 82 (4) and (5) GDPR).[71]

Besides that, the AIA draft[72] also provides certain transparency requirements, but only applies to AI systems within the meaning of Art. 3 no. 1 AIA. Following a risk-based approach, the AIA draft differentiates between four risk categories: the first category of AI involves unacceptable risks and therefore are prohibited (Art. 5 AIA).

The second category covers the so-called high-risk AI systems. Those are either AI systems with a safety component of a product or itself products, which are covered by the Union harmonization legislation listed in Annex II or AI systems referred to in Annex III. In chapter 2 of the AIA draft there are specific requirements, which have to be fulfilled before or while using a high-risk AI system. According to Art. 13 AIA, AI systems should be designed and developed in such a way that their functioning is sufficiently transparent so that users can use the system appropriately and interpret its results correctly. The user is 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, Art. 3 no. 4 AIA. The call for transparency is reminding of the discussion about the existence of a so-called right to explanation of the GDPR[73]. Also here, the question of technical feasibility arises, as well as the resolution of possible conflicts with other rights. Technical barriers are encountered with deep learning, for example, because even if it is known what information the algorithm bases its decision on (input), there is no knowledge of how it reaches the result (output). According to the current state of research, in many fields of AI applications one has to decide between very well-functioning AI systems that provide hardly any insight into their functioning and more transparent, but then also less well-functioning AI systems. Furthermore, transparency obligations can come into conflict with other rights, especially the protection of trade secrets. Both the algorithm itself and the functioning of the algorithm can be subsumed under the concept of a trade secret according to Art. 2 no. 1 of the trade secrets directive[74]. The consequences are very extensive: The owner of the trade secret can object to almost any interference. The exceptions, regulated in Art. 5 of the trade secrets directive, are not likely to apply, so that the enforcement of transparency requirements could fail not only due to technical but also legal barriers.[75]

In addition to high-risk AI systems, Art. 52 of the AIA draft also names three groups of AI systems to which certain weakened information and transparency obligations apply. As mentioned before, the first group focuses on AI systems that interact with natural persons are covered unless it is obvious that they are facing an AI. The other two groups are emotion recognition and biometric categorisation systems as well as so-called deep fake applications. It is not quite clear why the Commission has decided to regulate these three groups in particular. Between the high-risk AI systems and the AI systems without a risk, there are likely to be other groups in addition to those listed in Art. 52 AIA. Therefore, a standard clause with sufficiently defined criteria would have been useful here as well.[76]

---

70 A. Sattler, Gemeinsame Verantwortlichkeit – getrennte Pflichten, GRUR 2019, pp. 1023-1026.

71 J. Spittka and R. Mantz, Datenschutzrechtliche Anforderungen an den Einsatz von Social Plugins, NJW 2019, pp. 2742-2745.

72 EU Commission, 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 of 21.4.2021.

73 B. Mittelstadt et al., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, Int. Data Priv. Law, 2017, 7 (2), pp. 76-99; B. Casey, A. Farhangi and R. Vogt, Rethinking explainable machines: The GDPR's "Right to Explanation" debate and the rise of algorithmic audits in enterprise, 34 Berkeley Tech. L. J. (2019), pp. 143-188; M. Kaminski, The Right to Explanation, Explained, 34 Berkeley Tech. L. J. (2019), pp. 189-218; S. Wachter and B. Mittelstadt, A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI, Colum. Bus. L. Rev. 2019 (2), pp. 494-620.

74 Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

75 H. Hoffmann, Regulierung der Künstlichen Intelligenz, K&R 2021, pp. 369-374.

76 H. Hoffmann, Regulierung der Künstlichen Intelligenz, K&R 2021, pp. 369-374.

However, it should be noted, that the transparency obligation only applies to the provider and user and not to the affected person.

2.4. The Right to Explanation

To improve transparency and therefore to reduce the algorithm's influence on the customer's contractual freedom, it is worth taking a deeper look on the so-called "Right to explanation".[77] There are three possible legal bases for a Right to explanation in the GDPR: safeguards against automated decision-making as required under Art. 22 (3) GDPR commented upon by recital 71; notification duties under Art. 13 and Art. 14 GDPR commented upon by recitals 60-62; or the right of access under Art. 15 GDPR commented upon by recital 63.

According to Art. 13 (2) lit. f and Art. 14 (2) lit. g GDPR, the controller shall provide the data subject with the existence of an automated decision-making and, at least in those cases, meaningful information about the logic involved, to ensure fair and transparent processing. Art. 15 (1) lit. h GDPR grants the corresponding right to information. Contrary to the still ambiguous opinion of the data protection authorities,[78] the wording "at least in these cases" is to be understood in such a way that the information obligations or the right to information also exist in such cases in which there is merely a decision supported by algorithmic systems.[79] A limitation to only automated decision-making would tempt controllers to avoid the rule by having a person formally confirm the decision.[80] Since Art. 13 (1) GDPR requires that the controller shall provide the information, at the time when personal data are obtained, the duty to inform cannot be focused on individual decision-making, as this has not even taken place at this point, but only on the general, global functioning of the system.[81] The same applies to Art. 14 (2) and Art. 15 (1) GDPR. On the one hand they have the same wording, on the other hand they both refer to "envisaged consequences".[82]

Another legal basis is Art. 22 (3) in conjunction with recital 71, fifth sentence, GDPR. According to Art. 22 (1) GDPR, the data subject has the right not to be subject to a decision based solely on automated processing which produces legal effects concerning them or similarly significantly affects them. Paragraph 2 provides three exceptional cases in which such an automated decision is nevertheless permitted. In the cases of Art. 22 (2) lit. a and c, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. These include at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. If these requirements are not met, the data processing is prohibited, irrespective of the data subject's exercise of any right under Art. 22 of the GDPR.[83] Recital 71, fourth sentence, GDPR requires an explanation of the decision reached after such an assessment. Although this obligation is just anchored in the recitals and not directly in the

---

77 For a comprehensive overview, see H. Hoffmann and J. Kevekordes, Das Right to Explanation, DuD 2021, (forthcoming).

78 See the contradictory statements of the Article 29 Data Protection Working Party in WP 251rev.01 v. 3.10.2017 on p. 25 and 31.

79 M. Bäcker, In: J. Kühling and B. Buchner (eds), DSGVO, 3rd ed., C.H. Beck 2020, Art. 13 DSGVO paras 52 f.; A. Dix, In: S. Simitis, G. Hornung and I. Spiecker gen. Döhmann (eds), Datenschutzrecht, 1st ed., Nomos 2019, Art. 13 DSGVO, para. 16; B.A. Mester, In: J. Taeger and D. Gabel (eds), 3rd ed., Fachmedien R&W 2019, Art. 13 DSGVO paras 27 f.; a different view is taken by M. Martini, Blackbox Algorithmus, Springer 2019, p. 183; M. Martini, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017 (21), pp. 1017-1025; F. Schmidt-Wudy, In: S. Brink and H. A. Wolff (eds), BeckOK-Datenschutzrecht, 35th ed., C.H. Beck 2021, Art. 15 DSGVO para. 77.

80 In result also S. Wachter, B. Mittelstadt and L. Floridi, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, Int. Data Privacy Law 2017, Vol. 7(2), pp. 76-99; A. D. Selbst and J. Powles, Meaningful information and the right to explanation, Int. Data Privacy Law 2017. Vol. 7(4), pp. 233-424; see also Article 29 Data Protection Working Party, WP 251rev.01, p. 21.

81 S. Wachter, B. Mittelstadt and L. Floridi, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, Int. Data Privacy Law 2017, Vol. 7(2), pp. 76-99; M. Martini, Blackbox Algorithmus, Springer 2019, p. 191.

82 See Article 29 Data Protection Working Party, WP 251rev.01, pp. 25-26; S. Wachter, B. Mittelstadt and L. Floridi, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, Int. Data Privacy Law 2017, Vol. 7(2), pp. 76-99; M. Martini, Blackbox Algorithmus, Springer 2019, p. 192; M. Bäcker, In: J. Kühling and B. Buchner (eds), DSGVO, 3rd ed., C.H. Beck 2020, Art. 15 DSGVO para. 27.

83 Article 29 Data Protection Working Party, WP 251rev.01, p. 19; B. Buchner, In: J. Kühling and B. Buchner (eds), DSGVO, 3rd ed., C.H. Beck 2020, Art. 22 DSGVO para. 12; M. Helfrich, In: G.Sydow (ed), Europäische Datenschutzgrundverordnung, 2nd editon, Nomos 2018, Art. 22 para. 38-41; M. Martini, In: B.P. Paal and D. A: Pauly (eds), DSGVO, 3rd ed., C.H. Beck 2021, Art. 22 para. 29b; the current state of the dispute: K. v. Lewinski, In: S. Brink and H. A. Wolff (eds), BeckOK-Datenschutzrecht, 35th ed. (1.2.2021), C.H. Beck 2021, Art. 22 DSGVO para. 2.1.

normative text, it must be considered when determining a Right to Explanation. Art. 22 (3) GDPR contains an exhaustive list of minimum measures, which is why in certain situations a Right to Explanation can still exist.[84] Since Art. 22 (3) GDPR uses the word "at least", it depends on the assessment of the individual case to decide whether a Right to Explanation exists.[85]

In addition, the AIA draft[86] also contains transparency obligations for high-risk AI systems (Art. 13) and mitigated transparency obligations for certain AI systems (Art. 52).

A comprehensive Right to Explanation, which the data subject can invoke, is currently not enshrined in the law. The existing provisions must be further specified by the legislator – or at least by the courts. However, both Art. 13 to 15 and Art. 22 GDPR and Art. 13 of the draft AI Regulation indicate that there is a duty to explain algorithmic decisions. Nevertheless, transparency obligations and a Right to Explanation conflict with other rights, especially the protection of trade secrets, and face technical barriers.

3. Unfair Commercial Practices and the GDPR

Data privacy is discussed in the context of the German Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen, GWB) as well as in the context of the German Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb, UWG). In the following section, we will deal with the issue of when data protection can amount to a competition law issue. It is also being dealt with the question whether the use of data requires consumer harm to become a competition law concern and if it requires the company to be in a dominant position.

The Higher Regional Court of Düsseldorf ruled in the “Facebook I” case[87] on the abuse of a dominant position on the German market for social networks. While the German Federal Cartel Office (Bundeskartellamt) justified the infringement against Facebook due to the abuse of a dominant market position by arguing that network users had to agree to contractual conditions which were inappropriate in terms of data protection law when registering and which enabled Facebook to collect, link and use data generated outside the network,[88] the court found, that the abuse of a dominant position by Facebook could not be clearly proven.

However, in its decision on June 23, 2020, the Federal Court of Justice (BGH) rejected this reasoning put forward by the Higher Regional Court and ruled that the exploitation of a dominant position does not always require a causal connection between the market dominance and the disapproved conduct (conduct causality) in the case of an abuse of conditions under section 19 (1) GWB.[89] At least a causal connection between the market dominance and the market result (causality of results) may be sufficient if, due to the special market conditions, the conduct of the dominant company leads to market results which would not be expected in the case of functioning competition and, moreover, the conduct not only constitutes exploitation, but is at the same time also likely to hinder competition. By receiving an indispensable service (the use of the social network) only in conjunction with another undesirable service (the provision of a personalised experience based on data generated by the user’s activity outside the network) users were forced into a service content and were no longer able to decide freely on the extent to which their data would be disclosed. The consent of the users was not actually

---

84 M. E. Kaminski, The right to explanation, explained, 34 Berkeley Tech. L. J. 2019, Vol. 34(1), pp. 189-218.

85 M. E. Kaminski, The right to explanation, explained, 34 Berkeley Tech. L. J. 2019, Vol. 34(1), pp. 189-218; S. Schulz, In: P. Gola (ed), DSGVO, 2nd ed., C.H. Beck 2018, Art. 22 para. 33; K. v. Lewinski, In: S. Brink and H. A. Wolff (ed), BeckOK-Datenschutzrecht, 35th ed. (1.2.2021), C.H. Beck 2021, Art. 22 DSGVO para. 47.; in result also S. Wachter, B. Mittelstadt and L. Floridi, Why a right to explanation of automated decision-making does not exist in the general data protection regulation, Int. Data Privacy Law 2017, Vol. 7(2).

86 EU Commission, 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 of 21.4.2021.

87 OLG Düsseldorf, Judgement of 26 August 2019 – VI Kart 1/19 (V).

88 German Federal Cartel Office, Case Report of 15 February 2019, B6-22/16 – NZKart 2019, pp. 178-184.

89 BGH, Judgement of 23 June 2020, KVR 69/19 – NZKart 2020, pp. 473-483.

voluntary within the meaning of Art. 6 (1) (a) GDPR. Thus, the disputed terms of use constituted a so-called “forced extension of service”. Contrary to the opinion of the Higher Regional Court, the assessment of such a forced extension of service remains unaffected by the fact that the provision of a personalised experience using data generated outside the network is free of charge in monetary ways. Rather, by imposing an undesirable service the consideration for the desired service (namely the use of the social network) is increased in form of disclosure of personal user data. Therefore, the Federal Court of Justice considered Facebook's exploitation of its dominant position to be abusive.

Furthermore, the Federal Court of Justice found no serious doubts that the disputed terms of use lead to an anti-competitive market result. This is underlined by the assumption that without Facebook’s dominant position there would be a usage offer linked to a lower level of data disclosure. Since there is no such an offer, the conditions used by Facebook leads to an impediment of competition both on the market for social networks dominated by the company and on the related market for online advertising. Besides the already existing direct network effects and the enormous economic value of personalised user data, the disputed terms of use further strengthened the market entry barriers for potential competitors and therefore hindered competition.

As pioneering case worldwide, the Federal Court of Justice’s decision states an important sign for competition on social platforms. However, the outcome of the principal proceedings remains to be seen. Currently, the proceedings have been suspended due to questions of interpretation submitted to the European Court of Justice (ECJ).[90]

In the draft and the explanatory memorandum of the 10th amendment of the GWB the Federal Ministry of Economics and Energy and the German Parliament already referred to the comments of the Higher Regional Court of Düsseldorf in order to clarify that no qualified requirements in the sense of a "strict causality" could be derived from the previous wording of section 19 (1) GWB.[91] The Federal Ministry of Economics and Energy explicitly mentioned that if the unjustified disclosure of personal data required the proof of strict causality, it would often encounter difficulties precisely in those cases where the exploitation of the market opponent is also favoured by other factors such as existing information asymmetries or rational apathy on the part of the demand side and where corresponding behaviour can therefore also be exhibited by non-dominant companies in individual cases.[92] Even after the decision of the Federal Court of Justice the legislator wanted to create legal certainty as clarification was still pending for other constellations.[93] Therefore the wording of section 19 (1) GWB no longer requires an abusive exploitation of a dominant position but rather just an abuse of a dominant position, which can be exclusionary.

The 10th amendment of the GWB also recognizes the increased importance of data and prepares for new challenges posed by advancing digitalization. Therefore, section 18 (3) no. 3 GWB now states that in particular the access of a company to data relevant to competition shall be taken into account when assessing the market position of a company in relation to its competitors. Moreover, section 19 (2) no. 4 GWB now expressly mentions that an abuse of market power may lie in refusing to grant access to data. The condition is that access must be objectively necessary for action on one of the previous or following markets and the refusal of access threatens to eliminate effective competition on that market, unless the

---

90 Request for a preliminary ruling from the Oberlandesgericht Düsseldorf lodged on 22 April 2021 – Facebook Inc. and Others v Bundeskartellamt, C-252/21 (OJEU 2021/C 320/20).

91 BMWi, Entwurf (RefE) eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz), pp. 70-71. Available at https://www.d-kart.de/wp-content/uploads/2019/10/GWB-Digitalisierungsgesetz-Fassung-Ressortabstimmung.pdf. Accessed 23 August 2021; BT-Drs. 19/23492 p. 71.

92 BMWi, Entwurf (RefE) eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz), p. 71.

93 BT-Drs. 19/23492 p. 71.

refusal of access is objectively justified. Admittedly, numerous consequential problems exist behind such a claim.[94] Nevertheless, it is a fall-back situation if there are no sector-specific data access obligations.[95]

Regarding companies in the area of data and platform markets, the new centrepiece of abuse control is section 19a GWB. While the application of competition law usually requires a company to be in a dominant position, the prerequisite for the application of section 19a GWB is not a dominant position in the traditional understanding (market power), but only a determination by the Federal Cartel Office that the company concerned has an "outstanding cross-market significance for competition". Among other things, the access of a company to competition-relevant data (section 19a (1) no. 4 GWB) but also the gatekeeper function of a company (section 19a (1) no. 5 GWB) must be considered while making this determination. It seems as if section 19a (2) no. 4 GWB is a direct reaction to the Facebook case, as the provision specifically contains the permission for the Federal Cartel Office to prohibit a company from using terms and conditions that make the use of services conditional on users consenting to the processing of data from other services of the company or a third party provider without giving users sufficient choice as to the circumstance, purpose and manner of the processing.

Since the changes made to competition law with regard to the digital companies entered into force on 19 January 2021, the Federal Cartel Office is extending the scope of its proceedings and examining whether Facebook is subject to the new rules applying to undertakings of paramount significance for competition across markets (section 19a German Competition Act, GWB) and whether linking the Oculus and the Facebook network is to be assessed on this basis.[96]

In May 2021, the Federal Cartel Office initiated a proceeding against Amazon based on the new rules for large digital companies. In addition to inspecting tying or bundling strategies the Federal Cartel Office examines whether Amazon creates or raises barriers to market entry by processing data relevant for competition.[97]

A few days later a proceeding against Google was also initiated where the Federal Cartel Office will undertake an in-depth analysis of Google's data processing terms.[98]

In June 2021, the Federal Cartel Office initiated a proceeding against Apple, the last of the four GAFA companies. Among other aspects, it will examine Apple's extensive integration across several market levels, the magnitude of its technological and financial resources and its access to data. A main focus of the investigations will be on the operation of the App Store as it enables Apple in many ways to influence the business activities of third parties.[99]

In May 2021, the French competition authority *Autorité de la concurrence* fined Google EUR 220 million for abusing its dominant position in the online advertising market. In the course of the settlement, Google also accepted a series of proposed commitments to settle the case, including promises to make it easier for competitors to make use of data and the online-ad tools.[100]

---

94 R. Podszun and F. Brauckmann, GWB-Digitalisierungsgesetz: Der Referentenentwurf des BMWi zur 10. GWB-Novelle, GWR 2019, pp. 436-438.

95 R. Podszun and F. Brauckmann, GWB-Digitalisierungsgesetz: Der Referentenentwurf des BMWi zur 10. GWB-Novelle, GWR 2019, pp. 436-438.

96 Bundeskartellamt, Press release of 28 January2021. Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/28_01_2021_Facebook_Oculus.html. Accessed 23 August 2021.

97 Bundeskartellamt, Press release of 18 May 2021. Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/18_05_2021_Amazon_19a.html?nn=3591286. Accessed 23 August 2021.

98 Bundeskartellamt, Press release of 25 May 2021. Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/25_05_2021_Google_19a.html?nn=3591286. Accessed 23 August 2021.

99 Bundeskartellamt, Press release of 21 June 2021. Available at https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/21_06_2021_Apple.html. Accessed 23 August 2021.

100 Autorité de la concurrence, Press Release of 7 June 2021. Available at https://www.autoritedelaconcurrence.fr/en/press-release/autorite-de-la-concurrence-hands-out-eu220-millions-fine-google-favouring-its-own. Accessed 23 August 2021.

In June 2021, the European Commission opened a formal antitrust investigation to assess whether Facebook violated rules on anticompetitive agreements between companies, Art. 101 TFEU, and on the abuse of a dominant position, Art. 102 TFEU, by using advertising data gathered in particular from advertisers in order to compete with them in markets where Facebook is active such as classified ads and by tying its online classified ads service "Facebook Marketplace" to its social network.[101]

4. Commercial Practices in the Debate

Since social media and AI-based systems become more and more important in online-marketing, commercial practices have changed enormously. Firstly, the significance and legal consequences of influencing in modern marketing will be presented. Afterwards, the relationship between AI and marketing and particularly their influence on data protection is examined as well as selected aspects of personalised prices. The current debate on the prohibition of sale products on platform as well as advertising them on search engines will be discussed afterwards. At the end of the section, the upcoming challenges concerning product liability are outlined and a future perspective is given.

4.1. Influencing

4.1.1. Introduction

Online-marketing is a central aspect of corporate management. In the last few years, in addition to classic advertising, advertising in social media channels has changed tremendously.

Social media platforms offer companies the possibilities of more or less conventional internet advertising. In addition to paid, static banner advertising or short video insertions, this can also be a sponsored posting.[102] Furthermore, a normal posting can also be an advertisement within the meaning of the relevant provisions.[103] According to section 5a UWG and section 6 TMG advertising and normal postings must actually be strictly separated from each other. In order not to violate the separation rule, advertising must be labelled as such. However, a certain additional problem is posed by any mandatory or clarifying information which often cannot be listed, or at least not completely, due to the limited size of such an electronic advertisement.[104]

So-called hashtags are used to tag articles in social media such as Twitter or Instagram and make them easier to find. These can contain characteristic terms of the posting, but also short sentences and are introduced by the diamond symbol "#". In comparison to the mere use of buzzwords, this further emphasizes their recognisability and thus reinforces their meaningfulness.[105] The use of hashtags in the context of commercial transactions may have consequences under trademark law or competition law.

In addition, on various social media platforms such as Facebook and Instagram, the photos uploaded by users can be tagged to products or companies.[106] This may also have consequences under trademark law or competition law.

Especially in social networks such as Instagram or YouTube the so-called "influencer marketing" becomes more and more important.[107] People with many followers in social media advertise for third parties and receive a service in return.

---

[101] European Commission, Opening of Proceedings caseAT.40684Facebook leveraging. Available at https://ec.europa.eu/competition/antitrust/cases/dec_docs/40684/40684_1812_3.pdf. Accessed 23 August 2021.
[102] F. Lichtnecker, Ausgewählte Werbeformen im Internet unter Berücksichtigung der neueren Rechtsprechung, MMR 2014, pp. 523-528.
[103] OLG Köln, Judgement of 19 May 2017 – 6 U 155/16.
[104] F. Lichtnecker, Neues aus dem Social Media-Marketing, MMR 2018, pp. 512-517.
[105] F. Lichtnecker, Neues aus dem Social Media-Marketing, MMR 2018, pp. 512-517.
[106] F. Lichtnecker, Neues aus dem Social Media-Marketing, MMR 2018, pp. 512-517.
[107] F. Suwelack, Schleichwerbung als Boombranche?, MMR 2017, pp. 661-665; U. Borsch, Der angemaßte Influencer – Markenpiraterie 2.0, MMR 2018, pp. 127-129.

They use their reporting to present the products to their loyal followers in a positive way and thus induce them to make a purchase decision. Generally, the advertising is part of a normal postings, so consumers cannot distinguish whether it is the actual opinion of the influencer or whether the influencer is presenting the product only on the basis of a contract with a company. The problem is that the ads are often not marked as advertising. Often the posts are only marked with "#ad", which is not really conclusive and does not solve the problem completely. National courts have already ruled on the first cases following this issue.[108]

If there is a contractual agreement between the company and the influencer, it is considered to be advertising, which in this respect is a commercial act pursuant to section 2 (1) no. 1 UWG.[109] If the contribution is (paid) advertising, it must also be recognisable as such and marked as such. Otherwise there would be a violation of section 6 (1) no. 1, 2 TMG, no. 11 of the annex to section 3 (3) UWG, section 5a (6) UWG, section 22 (1) or section 74 in connection with section 8 (3) of the Interstate Media Treaty (Medienstaatsvertrag, MStV).[110] If the advertising character is already obvious from the design of the post itself, there is usually no separate labelling necessary,[111] although one should be cautious here. As with other advertising campaigns, proper labelling includes the meaningful words such as "advertising" or "advertisement", possibly in combination with a hashtag, and should be used.[112]

4.1.2. Recent Case Law

However, it has been disputed for some time whether a declaration is necessary if the influencer just presents a product without having an advertisement contract with a company and without receiving remuneration. The Higher Regional Court of Karlsruhe (OLG Karlsruhe) ruled that commercial interests are also pursued with gratuitous contributions.[113] After all, the contributions are intended to contribute to increasing the value of the influencer's image and thus to obtain advantages for any future paid advertising contracts.[114] Therefore, labelling is necessary, especially when "tab links" are used.[115] The Higher Regional Court of Hamburg (OLG Hamburg) ruled that there is no need for advertising labelling, because with professionally designed posts and follower numbers in the millions, the commercial purpose is recognizable to consumers at first glance (section 5a (6) UWG).[116] In addition, there would also be a lack of consistency in comparison with the print media, because there are also personal product recommendations by individual editors in print media that do not have to be labelled as advertising if no service in return has been provided.[117] The Higher Regional Court of Munich (OLG München) went even further and denied the existence of a commercial act (pursuant to section 2 (1) no. 1 UWG), because the fact that influencers indirectly pursue the goal of making themselves more interesting for future advertising contracts with gratuitous contributions is fundamentally immanent to the actions of the media industry, which is dependent on advertising revenues.[118]

It seems more convincing, that if the influencer just presents a product without an agreement with a company and without using tab links this can´t be defined as advertisement and a declaration is not necessary. For the consumer it is crucial to know which products are recommended free of charge and which products are advertised in return for remuneration. However, if gratuitous contributions about a product also must be labelled as advertising, it becomes impossible for the

---

[108] LG Hannover, Judgement of 8 June 2017 – 3 U 53/17, C. Sobottka, Schleichwerbung durch Influencer-Marketing in sozialen Medien, MMR 2017, pp. 769-772; KG Berlin, Ruling of 11 October 2017, 5 W 221/17, Kennzeichnungspflicht bei Influencer Marketing, MMR 2018, pp. 98-99.
[109] F. Lichtnecker, Neues aus dem Social Media-Marketing, MMR 2018, pp. 512-517.
[110] M. Gerecke, Kennzeichnung von werblichen Beiträgen im Online-Marketing, GRUR 2018, pp. 153-159.
[111] T. Fuchs and C. Hahn, Erkennbarkeit und Kennzeichnung von Werbung im Internet, MMR 2016, pp. 503-507.
[112] LG Hagen, Judgement of 13 September 2017 – 23 O 30/17, GRUR-RR 2017, pp. 510-512.
[113] OLG Karlsruhe, Judgement of 9 September 2020 – 6 U 38/19, MMR 2021, pp. 159-164.
[114] OLG Karlsruhe, Judgement of 9 September 2020 – 6 U 38/19, MMR 2021, pp. 159-164.
[115] OLG Karlsruhe, Judgement of 9 September 2020 – 6 U 38/19, MMR 2021, pp. 159-164.
[116] OLG Hamburg, Judgement of 2 July 2020 – 15 U 142/19, MMR 2020, pp. 767-772.
[117] OLG Hamburg, Judgement of 2 July 2020 – 15 U 142/19, MMR 2020, pp. 767-772.
[118] OLG München, Judgement of 25 June 2020 – 29 U 2333/19, GRUR 2020, pp. 1096-1098.

consumer to distinguish between them. This would constitute over-labelling, which would be contrary to the protective purpose of section 5a (6) UWG. However, as the case law of the Higher Regional Courts is inconsistent, a decision by the Federal Court of Justice (BGH) remains to be seen. A decision of the Federal Court of Justice (BGH) is expected in the beginning of September 2021, where the court has the chance to provide clarity in three cases at once, as it will have to rule on the question of whether influencers are obliged to label their gratuitous Instagram posts as advertising.

On 2 December 2020, another important act concerning online-marketing and therefore also influencing came into force: The Act to Strengthen Fair Competition (Gesetz zur Stärkung des fairen Wettbewerbs), which modified the UWG. In particular, it was added to section 14 UWG that the court in whose district the infringement was committed does not have jurisdiction in disputes concerning infringements in electronic commerce or telemedia (section 14 (2) third sentence no. 1 UWG). In the case of infringements of unfair competition law committed on the internet, the place of infringement is the whole of Germany due to the fact that the infringement can be retrieved from anywhere on the internet, which means that under the old rules, any German regional court had jurisdiction and the competitor could choose a court (so called "Flying Jurisdiction"). Thus, he could choose the court which, according to previous decision-making practice, was favourably disposed towards his application. The amendment to the law has severely restricted this option for competitors in internet cases. Now, only the general place of jurisdiction at the defendant's registered address is to apply (section 14 (2) UWG). Since then, however, there has also been a decision by the Regional Court of Düsseldorf (LG Düsseldorf) that nevertheless assumed jurisdiction in the case of a YouTube advertisement, even though the defendant's registered address was not in its district.[119] According to the Regional Court of Düsseldorf, in order for jurisdiction to be excluded, the anti-competitive act must be an infringement that can only be committed in electronic commerce or in telemedia and is therefore already linked to these media. It argues, that the legislator's intention was only to abolish the "flying jurisdiction" in the case of abusive cease-and-desist letters, as in the case of violations of information and labelling obligations on the Internet.[120] This interpretation has already been the subject of much criticism, in particular because it contradicts the clear wording and, in the view of many, no contrary intention is apparent from the explanatory memorandum.[121] Moreover, the Higher Regional Court of Düsseldorf (OLG Düsseldorf) has already declared it unacceptable in an obiter dictum.[122] Since the Regional Court of Düsseldorf nevertheless continues to adhere to this interpretation and the Regional Court of Frankfurt (LG Frankfurt) has also followed suit, it remains to be seen how other courts will deal with this issue.[123]

4.1.3. German Bill to Strengthen Consumer Protection in Competition and Commercial Law

In addition to the court ruling, there were also legislative attempts to face the rising issues regarding online-marketing, social-media and influencing. On 4 November 2020, the German Federal Ministry of Justice and Consumer Protection published a ministerial draft bill to strengthen consumer protection in competition and commercial law.[124] The draft was followed by numerous comments from German associations as well as Instagram itself. Following on from this, a government draft for the modernization of consumer protection law was published in order to comply with the requirements of Directive 2019/2161 and in order to provide legislative clarification with regard to influencer

---

119 LG Düsseldorf, Judgement of 15 January 2021 – 38 O 3/21, GRUR-RS 2021, p. 402.
120 LG Düsseldorf, Judgement of 15 January 2021 – 38 O 3/21, GRUR-RS 2021, p. 402.
121 S. Wettig and G. Kiparski, Wiederaufleben des fliegenden Gerichtsstandes contra legem!?, CR 2021, pp. 177-182.
122 OLG Düsseldorf, Judgement of 16 February 2021 – I-20 W 11/21, GRUR-Prax 2021, p. 158.
123 LG Düsseldorf, Judgement of 26 February 2021 – 38 O 19/21, GRUR-RS 2021, p. 4044; LG Frankfurt, Judgement of 11 May 2021 – 3-06 O 14/21, GRUR-RS 2021, p. 11813.
124 Referentenentwurf eines Gesetzes zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht, Available at https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Staerkung_Verbraucherschutz_Wettbewerbs-_und_Gewerberecht.pdf?__blob=publicationFile&v=2. Accessed 23 August 2021.

marketing.[125] On 10 June 2021, the German parliament (Bundestag) passed this bill that will enter into force on 28 May 2022.[126]

The explanatory memorandum to the bill specifically addresses the problems of influencer marketing. It requires regulations to clarify the scope of application of the UWG and other changes to distinguish non-commercial communication from commercial actions:

First, the bill clarifies in section 1 (2) UWG that provisions regulating specific aspects of unfair business acts take precedence over the UWG when assessing whether an unfair business act has been committed. However, pursuant to section 1 UWG, the precedence only extends as far as the aspect in question is conclusively regulated in the more specific provision.[127] If, for example, the more specific provision only contains supplementary information requirements, the general information requirements of sections 5a and 5b UWG continue to apply.

At the same time, the UWG is applicable to regulations on specific aspects of unfair acts only with regard to those aspects that are not addressed in the specific regulations.

Additionally, it can sometimes be difficult to distinguish between commercial communication and private expression of opinion in social media or blogs. Therefore, the definition of the commercial act in section 2 (1) no. 2 UWG is supplemented to the effect that it must no longer only be objectively but also directly related to the promotion of sales.[128] In this regard, section 2 (2) no. 2 UWG explains that although the criterion "objectively" has to be interpreted in a way that it comprises "directly" in the case of actions towards consumers, a clarification is appropriate due to the importance of this central definition.[129] This is explained by the following example: In certain forms of promotion of one's own business there is no direct connection to sales promotion, for example, if an influencer recommends or mentions goods or services and has received no remuneration or similar consideration for doing so and the mention merely promotes his or her own notoriety.

Furthermore, section 5a (4) second sentence UWG clarifies that no commercial purpose is to be assumed in the case of an act in favour of another entrepreneur if the person acting does not receive any remuneration or similar consideration from the other entrepreneur or does not allow himself to be promised such consideration. This new amendment is intended to provide a secure legal framework for the actions of influencers when they recommend goods and services without themselves profiting from them by remuneration or a similar consideration.[130]

According to the comments on section 5a (4) second sentence UWG, it appears unreasonable to require a labelling as "commercial" for such actions.[131] The term "similar consideration" also includes commissions, products sent by the third-party company which the trader may use or keep, as well as press trips, provision of equipment or assumption of costs. The consideration may also be of a temporary nature. The mere increase of the own awareness, for example of influencers, through such actions, however, cannot be considered as consideration. The consideration does not have to take place in a direct temporal connection. The consideration must have been initiated by the entrepreneur for whose benefit the action is performed. If the consideration is provided by a third party, such as an agency, this is attributed to the entrepreneur according to general principles. In contrast, consideration provided by independent third parties that is not initiated by the entrepreneur is not included. This corresponds to the general assessment in the case of media companies from which employees also receive remuneration for the production of contributions.

---

[125] Regierungsentwurf eines Gesetzes zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht, BT-Drs. 19/27873.
[126] BGBl. I p. 3504.
[127] BT-Drs. 19/27873, p. 31.
[128] BT-Drs. 19/27873, p. 32.
[129] BT-Drs. 19/27873, p. 32.
[130] BT-Drs. 19/27873, p. 34.
[131] BT-Drs. 19/27873, p. 34.

However, according to the explanatory memorandum, it should be noted that sentence 2 is only applicable to the assessment of the question of whether there is an act for the benefit of a third party entrepreneur.[132] The question of whether a recommendation of an influencer made free of charge also constitutes a business act insofar as it pursues the purpose of promoting one's own company is assessed solely in accordance with section 5a (4) first sentence UWG and the definition of a business act in section 2 (1) no. 2 UWG. The question of whether an act in favour of one's own company exists does not depend solely on the receipt of a fee, since self-promotion is also generally subject to labelling requirements if it is not otherwise recognizable. In the case of recommendations made free of charge by influencers, therefore it should be taken into account, in accordance with the addition in section 2 (1) no. 2 UWG, whether there is a direct connection to the sale of products and services. In this context, it will also be necessary to consider the fact that influencers in this area could be assessed like media companies, which are also regularly financed by advertising revenues and are also particularly attractive for their clients if they reach a large number of people.

In addition, the freedom of expression and media freedom from Art 11 of the Charter of Fundamental Rights of the European Union must be included in the assessment. The effort to achieve advertising revenue according to a ruling of the Court of Appeal in Berlin (Kammergericht Berlin) does not justify to provide each statement with a reference, with which a subordinate or inferior value of the contribution is connected.[133]

4.2. AI and Marketing

In ages where online-marketing takes the leading role in commercial practices, the use of AI-based systems also increased and therefore became common practice. However, using personal data as foundation for forecast decision, contract negotiations and personalised advertisement, the upcoming popularity of AI-based systems in the field of online-marketing leads to higher requirements for data protection and the need of regulation. This is stressed even more by the fact, that the frequent use of AI-based systems also causes a discriminatory aspect.

4.2.1. Data Quality

For the creation of personalised advertising a high data quality of the underlying data sets has to be ensured. High quality of data is crucial for sustainable and valuable data use.[134] Therefore, guaranteeing high data quality is very important for the provision of algorithmic decisions. An incorrect data basis can lead to incorrect decisions, without the person concerned being aware of this. The evaluation of data quality is a complex task, as either the context of use, errors or distortions in data collection process or structural disadvantages of individual groups may cause errors. Data quality can be understood as readable and processable data or as accuracy of the data.[135] So one can differentiate between technical data quality and the quality of the information itself.[136]

Art. 5 (1) lit. d GDPR requires the controller to ensure that the data processed are accurate and, where necessary for the purposes of the processing, are kept up to date. He or she should not just act when the data subject exercises his right of rectification,[137] rather the controller must, on his own initiative, take appropriate measures to delete or correct inaccurate data without delay.[138] The appropriate steps to ensure accuracy and keeping the data up to date will be determined on a case by case basis, taking into consideration the purpose of the processing.[139] This is also shown in the wording by the

---

132 BT-Drs. 19/27873, p. 35.
133 Kammergericht (KG) Berlin, Judgement of 08.01.2019, Az. 5 U 83/18.
134 T. Hoeren, Data quality as a key issue for big data, MMR 2016, pp. 8-11; J. Stevens, Datenqualität bei algorithmischen Entscheidungen. In: David, Geihs, Lange and Stumme (eds), Informatik 2019, pp. 367-380.
135 P. Bitter and S. Uphues. In: Kolany-Raiser, Heil, Orwat and Hoeren (eds), Big Data, 1st ed, C.H. Beck 2019, p. 81.
136 P. Bitter and S. Uphues. In: Kolany-Raiser, Heil, Orwat and Hoeren (eds), Big Data, 1st ed, C.H. Beck 2019, p. 81.
137 P. Schantz. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 5 DS-GVO, para. 28.
138 H. Huber, Verbot der Diskriminierung aus Gründen der Staatsangehörigkeit – Ausländerzentralregister, NVwZ 2009, pp. 379-382.
139 P. Schantz. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 5 DS-GVO, para. 29.

limitation of the obligation to update by the word "if necessary": data which have become obsolete for their initial purpose may still be relevant for evidence purposes.[140]

As a general rule, higher standards must be set for the control of data in the context of their collection than for the control of the accuracy of stock data.[141] However, with regard to the data saved by the collector within the meaning of Art. 4 no. 7 GDPR, they must ensure that they take notice of information which calls into question the accuracy of the stored data and that subsequently, if necessary, the existing data is checked and corrected.[142] In addition, Art. 5 (1) lit. d GDPR says that the accuracy of the data must be guaranteed "in relation to the purposes for which they are processed".[143]

Data may also be inaccurate in the light of its purpose if it is incomplete and may therefore lead to a false impression or wrong decisions.[144]

The AIA draft[145] also provides requirements for data and data governance. According to Art. 10 (3) AIA, training, validation and testing data sets of high-risk AI systems shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. Nevertheless, a precondition for the applicability of Art. 10 AIA is that it is a high-risk AI system. Therefore, the provision will only apply in certain cases.

4.2.2. The Use of Incorrect Data

The algorithms create a profile of the customer, so that the advertisements correspond as closely as possible to the customer's wishes. Depending on the profile and the method used, the customer will be sorted into categories that do not correspond to his or her interests. Particularly, this danger exists if algorithms use incorrect or not up-to-date data or if they automatically combine several criteria. The customer may be confronted with advertisement that subjectively does not necessarily match his or her wishes. He or she has no possibility to contradict the classification into certain criteria.[146] Nevertheless, companies without algorithms display even more unsuitable ads. Whether this is a manipulation of the contractual freedom depends on whether the measures are carried out secretly or not.[147] It must always be remembered that our subconscious is regularly influenced in such a way that we do not even notice it.

4.2.3. Data Management

Especially when large amounts of data are used, there must be strict rules how they have to be encrypted, transmitted, stored and processed. The larger the amount of data, the higher the risk of abuse.

The accountability principle regulated in Art. 5 (2) GDPR is a real change from the previous legal situation: the data controller must prove compliance with the regulation.[148] This means that the controller must be able to prove at any time that he or she is processing personal data lawfully. This has significantly aggravated the situation for controllers, which is linked to high documentation requirements that must be implemented in practice.[149]

---

140 H. Heberlein. In: Ehmann and Selmayr (eds), Datenschutzgrundverordnung, 2nd ed, C.H. Beck 2018, Art. 5, para. 24.
141 P. Schantz. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 5 DS-GVO, para. 29.
142 P. Schantz. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 5 DS-GVO, para. 29.
143 E. M. Frenzel. In Paal and Pauly (eds), Datenschutzgrundverordnung, Bundesdatenschutzkontakt, 2nd ed, C.H. Beck 2018, Art. 5 DS-GVO, para. 41.
144 A. Roßnagel. In: Simitis, Hornung and Spiecker gen. Döhmann (eds), Datenschutzrecht, 1st ed, Nomos 2019, Art. 5 DS-GVO, para. 139.
145 EU Commission, 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 of 21 April 2021.
146 P. Scholz. In: Simitis, Hornung and Spiecker gen. Döhmann (eds), Datenschutzrecht, 1st ed, Nomos 2019, Art. 4 Nr. 4 DS-GVO, paras 9 ff.
147 D. Susser, B. Roessler and H. Nissenbaum, Technology, autonomy and manipulation, Internet policy review 2019, 8 (2), pp. 1-22.
148 A. Jung, Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018, pp. 208-213.
149 A. Jung, Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018, pp. 208-213.

Improvement can be achieved by using data management software that is designed for large amounts of data. In order to achieve the best application one should also check if there is a specially developed software for the branch in question. Furthermore, the software must be up to date and software updates must be carried out regularly.

Following on from this, Art. 15 of AIA draft[150] requires, that high-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle. According to Art. 15 (4) the technical solutions to 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.

4.2.4. National Restrictions on the Creation of User Profiles which also Use Data from International Third-Party Sources

Before the implementation of the GDPR, section 15 (3) of the German Telemedia Act (Telemediengesetz, TMG) was applicable. Section 15 (3) TMG allows the creation of pseudonymous user profiles for advertising purposes as long as the user has not objected. Section 15 (3) TMG does neither cover the use of data to create comprehensive personality profiles, nor does it cover the transmission of usage data to third parties.[151] However, it is precisely the creation of such a personality profile that AI often focuses on.

Since the GDPR became applicable, according to Art. 22 (1) GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. "Profiling" is defined in Art. 4 no. 4 GDPR as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person. This also applies to individual evaluations of usage profiles, but not to the collective evaluation of many usage profiles for statistical purposes.[152] However, the decision must have legal effect or affect the person in a similar way.

Art. 22 GDPR does not expressly regulate the special conditions under which a profile may be created and further processed unless it results in an exclusively automated decision. Instead, the general rules of justification, in particular Art. 6 and 9 GDPR regulate whether the data processing process is lawful. According to Art. 6 (1) lit. f GDPR, the creation of user profiles has to be „necessary for the purpose of the legitimate interests pursued by the controller or by a third party". It is therefore necessary to balance the interests in each individual case. This evaluation must consider the following factors: responsible expectation of the data subjects and foreseeability/transparency, the possibilities for intervention by the data subjects, chaining of data, players involved, duration of observation, types of data and the scope of data processing.[153] According to one view, as far as AI programs are used for the purpose of profiling measures that interact with cookies, there is a high risk for the data subject, so that his interests outweigh and Art. 6 (1) lit. f is not applicable.[154] Therefore, it would be necessary to obtain consent under Art. 6 (1) lit. a GDPR. Others argue using recital 47 of the GDPR, according to which direct marketing measures can be based on legitimate interests. If this is permitted, then tracking user behaviour beforehand should be even more so.[155] The interests of users are taken into

---

150 EU Commission, 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 of 21.4.2021.

151 A. Dix and P. Schaar. In: Roßnagel (ed), Beck'scher Komm. Zum Recht der Mediendienste, 1st ed, C.H. Beck 2013, § 15 TMG, paras 62 f.

152 S. Schleipfer, Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 2017, pp. 460-466.

153 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand May 2019, p. 16. Available at https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf. Accessed 23 August 2021.

154 F. Schmidt, Dynamische und personalisierte Preise – datenschutz-, wettbewerbs- und kartellrechtliche Grenzen. In: Taeger (ed), Tagungsband DSRI-Herbstakademie 2016, Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, DSRITB 2016, pp. 1007-1022; M. Albers and R.-D. Veit. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 6 DS-GVO, para. 49.

155 T. Gausling, Künstliche Intelligenz im digitalen Marketing, ZD 2019, pp. 335-341.

account by precisely matching advertising and avoiding advertisement that is not in line with their interests. And even if this is AI-based, Art. 21 (1) first sentence GDPR provides a right to objection to the provisions of Art. 6 (1) lit. f GDPR.[156] When user profiles use data from international third-party sources, the joint collectors have a shared responsibility according to Art. 26 GDPR. In this respect, the rights of the data subject are protected.

Whether more stringent restrictions are necessary depends on the understanding of the data protection authorities and courts. If they say that Art. 6 (1) lit. f GDPR is not applicable and it is rather necessary to obtain consent under Art. 6 (1) lit. a GDPR, there is no need for a stricter regulation.

The AIA draft[157] only prohibits AI-based social scoring for general purposes done by public authorities, Art. 5 (1) lit. c. According to the explanatory memorandum of the draft, 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.[158]

4.2.5. Unequal Competitive Conditions due to the Use of AI

The use of AI as such does not constitute an infringement of competition. The right to free competition allows each individual company to decide for itself whether to use AI. Even before AI came on the market, companies could decide to implement different strategies. Nevertheless, companies with large databases can often use AI more effectively. Instead of challenging competition law, it should therefore be decided whether access to data needs to be (re-)regulated.

4.2.6. Discrimination against Companies, which were not Subject to Previous Purchase Decisions

The evaluation of previous purchase decisions does not constitute discrimination against other companies, which were not yet subject to purchase decisions. The evaluation of previous purchase decisions is reflected in the profile created. Also new companies can get access to this profile and thus benefit from it. The fact that a new company has not evaluated its own purchasing decision yet does not conflict with the principle of fair competition, as it can also define the target group manually and still benefit from the profiling.

4.2.7. Legal, Social and Ethical Values to Prevent Discrimination

With increasing digitalization and widespread use of artificial intelligence, the value neutrality of the programs is of primary importance.[159] The algorithms make their decisions based on the underlying data sets and the programming of the code. As long as these data sets meet the wished social and ethical values, the algorithm will decide on the basis of these values. The question of what social and ethical standard the decision should be based on must nevertheless be answered, as the data set must be selected on the basis of this since it has to reflect this. In practice it is going to be problematic that it is hardly conceivable to find data sets that meet these standards. If the data set contains discriminatory elements, the decision of the algorithm will also be discriminatory. In order to prevent this from happening it is necessary to look carefully when selecting the training data.

---

156 T. Gausling, Künstliche Intelligenz im digitalen Marketing, ZD 2019, pp. 335-341.

157 EU Commission, 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 of 21.4.2021.

158 EU Commission, 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 of 21 April 2021, p. 13.

159 H. Steege, Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz, MMR 2019, pp. 715-721.

In this context, Art. 10 of the AIA draft[160] provides certain requirements for training, validations and testing data. According to Art. 10 (3) AIA draft, the data shall be representative and free of errors. The AIA draft does not solve the problem outlined above.[161]

4.2.8. Prohibition of AI Marketing in Certain Areas of Life

Moreover, there should be certain areas where AI advertising campaigns should either be prohibited or highlighted and regulated. These areas are the most sensitive and vulnerable to abuse, such as political campaigns, religions, medical care or culture-related ads.

4.3. Personalised Prices

Personalised pricing as a kind of sub-category of marketing is the subject of the following section addressing selected aspects such as data-protection issues, conflicts concerning competition law and consumer's individual disadvantage due to specific proposed higher prices. As counterweight to pricing algorithms, the development of algorithms for consumers increases.

4.3.1. Interference with Art. 22 (1) GDPR

Personalised advertising and personalised pricing are exclusively created by automatically generated user profiles based on automated processing. However, Art. 22 (1) GDPR only prohibits an automated individual decision, that has legal effects on the data subject or that has similarly significantly effects on him or her.

In principle, personalised advertising and personalised prices have no direct legal effect or do not similarly significantly affect the data subject[162], since advertising is not an offer to buy but rather an invitation to make an offer. They have no impact on the potential risk to which the European legislator refers in the norm.[163] This is justified by a reference to Art. 21 (2) GDPR and recital 70.[164] By providing a right of objection to direct advertising to the data subject, they connect it to lawful processing operations and assume that such processing is in principle lawful and not subject to the prohibition of Art. 22. Therefore, the possibility to offer different services and prices to different customers is an expression of the free market economy and finds its limits only in the standards of anti-discrimination law.[165]

However, some voices in the literature doubt whether this argumentation can still be maintained in the current era of „behavioural advertising" and "price discrimination".[166] They argue that a similar significant affect might occur in individual case if there were enormous deviations from the market price, the limited availability of the product or the degree of necessity for the person concerned.[167]

---

160 EU Commission, 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 of 21 April 2021.

161 H. Hoffmann, Regulierung der Künstlichen Intelligenz, K&R 2021, pp. 369-374.

162 M. Martini. In: Paal and Pauly (eds), Datenschutzgrundverordnung, Bundesdatenschutzkontakt, 2nd ed, C. H. Beck 2018, Art. 22 DS-GVO, para. 23; S. Schulz. In: Gola (ed), Datenschutz-Grundverordnung, 2nd ed, C. H. Beck 2018, Art. 22 DS-GVO, para. 28; S. Gierschmann, Gestaltungsmöglichkeiten bei Verwendung von personenbezogenen Daten in der Werbung, MMR 2018, pp. 7-12; K.-U. Plath and J. M. Grages, "Let's Stay in Touch" - Direktwerbung unter der DSGVO, CR 2018, pp. 770-782; R. B. Abel, Automatisierte Entscheidungen im Einzelfall gem. Art. 22 DS-GVO, ZD 2018, pp. 304-307.

163 M. Martini. In Paal and Pauly (eds), Datenschutzgrundverordnung, Bundesdatenschutzkontakt, 2nd ed, C.H. Beck 2018, Art. 22 DS-GVO, para. 23.

164 M. Martini. In: Paal and Pauly (eds), Datenschutzgrundverordnung, Bundesdatenschutzkontakt, 2nd ed, C.H. Beck 2018, Art. 22 DS-GVO, para. 23.

165 S. Schulz. In: Gola (ed), Datenschutz-Grundverordnung, 2nd ed, C.H. Beck 2018, Art. 22 DS-GVO, para. 28.

166 J. Hladjk. In: Ehmann and Selmayr (eds), Datenschutz-Grundverordnung, 2nd ed, C. H. Beck 2018, Art. 22, para. 9.

167 P. Schantz and H. A. Wolff, Das neue Datenschutzrecht, C.H. Beck 2017, para. 737; T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.

If an AI system is involved, the EU Commission's proposal for an Artificial Intelligence Act (AIA)[168] might also be applied soon. Depending on the risk of the AI system, different measures may be necessary. Most likely personalised prices created by an AI system only fall under Art. 52 AIA, which provides weakened transparency and information obligations.

4.3.2. Further Data Protection Requirements

As soon as personal data is processed, the processing has to comply with the principles of Art. 5 GDPR. Regarding the processing of personal data for the personalisation of content, advertising and prices the principles of "purpose limitation" and "data minimization" are of particular relevance.

According to Art. 5 (1) lit. b GDPR personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (principle of "purpose limitation").

According to Art. 5 (1) lit. c GDPR personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of "data minimization"). This principle is a concretization of the principle of necessity.[169]

At this point, the purpose of the data processing is particularly important. The purpose is the relevant point of reference for the principle of data minimisation.[170] In fact, it is even possible to process very large amounts of data, as long as there is a sufficient purpose to be achieved.[171] The principle of data minimisation does not call for an absolute reduction or limitation of the amount of data and therefore even "big data" analyses do not violate a priori the principle of data minimization.[172] In order to comply with the above-mentioned principles, it is ultimately only a question of the permissible definition of a broad purpose and compliance with the principle of compatibility of purposes.[173] The principle of data minimisation therefore only restricts the collection and use of data for the personalisation of content/advertising/pricing to a limited extent. The Vienna Regional Court, for example, found that the processing of data by Facebook for the personalisation of content and advertising was lawful and it did not address the plaintiff's argument that Facebook was violating the principle of data minimisation.[174]

While profiling for the purpose of the personalisation of advertising is not necessary to protect the legitimate interests of the controller and is therefore only lawful with the informed consent of the data subject.[175] However, consumers have long been aware of business models in which they "pay" for certain services with their data for the purpose of personalised advertising.[176] Accordingly, obtaining consent for processing for the purposes of personalised advertising is not such an obstacle in practice.

Profiling for the purpose of personalising prices is also not necessary to protect the legitimate interests of the controller.[177] Such legitimate interests may also be of an economic nature, but at least when weighing the interests, one will have to conclude that the fundamental rights of consumers outweigh the profit maximization interests of the controllers.[178] Therefore, with regard to personalised prices, data processing is also only lawful with the informed consent of the data

---

168 EU Commission, 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 of 21 April 2021.
169 A. Roßnagel, In: S. Simitis, G. Hornung and I. Spiecker gen. Döhmann (eds), Datenschutzrecht, 1st ed., Nomos 2019, Art. 5 DSGVO, para. 116.
170 T. Herbst, In: J. Kühling and B. Buchner (eds), DSGVO, 3rd ed., C.H. Beck 2020, Art. 5 DSGVO para. 22.
171 T. Herbst, In: J. Kühling and B. Buchner (eds), DSGVO, 3rd ed., C.H. Beck 2020, Art. 5 DSGVO para. 56.
172 T. Herbst, In: J. Kühling and B. Buchner (eds), DSGVO, 3rd ed., C.H. Beck 2020, Art. 5 DSGVO para. 56.
173 T. Herbst, In: J. Kühling and B. Buchner (eds), DSGVO, 3rd ed., C.H. Beck 2020, Art. 5 DSGVO para. 56.
174 LGZ Wien, Judgement of 30 June 2020 – 3 Cg 52/14k-91, ZD 2021, pp. 25-32.
175 A. Golland, Das Kopplungsverbot in der Datenschutz-Grundverordnung, MMR 2018, pp. 130-135.
176 L. Mischau, Daten als „Gegenleistung" im neuen Verbrauchervertragsrecht, ZEuP 2020, pp. 335-365.
177 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.
178 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.

subject.[179] This would require an explicit query as to whether the data subject consents to his or her data being used for the purpose of individual pricing.[180] In contrast to consent for personalised advertising, many companies are likely to shy away from this, especially since it is to be expected that such clauses would attract media attention.[181]

In December 2020, the EU Commission addressed this issue by proposing its Digital Markets Act (DMA).[182] According to Art. 5 lit. a DMA a gatekeeper shall refrain from combining personal data sourced from their core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of the GDPR.

4.3.3. Price Collusion due to the Use of the Same or Similar Algorithms

Intentional or unintentional price agreements may arise when companies use pricing algorithms and data sets of one and the same third-party supplier.[183] This can lead to the situation where all suppliers using the same system offer the same price to the individual, so that the customer has hardly any choice.[184] In this case, prices increase and the entire price acceptance of the customer can be absorbed.[185] The same scenario may also occur if many companies use personal prices and their algorithms are becoming very similar.[186] This is even likely, since there can be just one “correct” price that matches the customers’ willingness to pay.[187]

With regard to possible behavioural coordination in the context of pricing algorithms, an intentional collusion with the aid of algorithms would be the case, if algorithms are deliberately used by companies to achieve behavioural coordination.[188] This must be distinguished from unintentional algorithmic collusion, in which the coordination is brought about independently by the algorithms in the sense of "artificial intelligence" without any direct human intervention.[189]

Nowadays, an urgent need for legislative action regarding intentional price collusion cannot be identified. The current cases of intentional collusion using price algorithms can be handled adequately with the applicable competition law, as any form of explicit collusion based on communication using algorithms is legally treated in the same way as human collusion.[190] One example is the case pursued by the British antitrust authority (CMA) in which two Amazon Marketplace retailers implemented a price agreement for posters with the help of automatic pricing software (dynamic pricing algorithms). The companies themselves had clearly entered into a cartel agreement and the use of algorithms therefore only served to implement it.[191]

---

179 F. Hofmann and F. Freiling, Personalisierte Preise und das Datenschutzrecht - Anforderungen an die datenschutzrechtliche Einwilligung ZD 2020, pp. 331-335; T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.

180 F. Hofmann and F. Freiling, Personalisierte Preise und das Datenschutzrecht - Anforderungen an die datenschutzrechtliche Einwilligung ZD 2020, pp. 331-335.

181 F. Hofmann and F. Freiling, Personalisierte Preise und das Datenschutzrecht - Anforderungen an die datenschutzrechtliche Einwilligung ZD 2020, pp. 331-335.

182 EU Commission, 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 of 15 December 2020.

183 M. Ebers, Dynamic Algorithmic Pricing: Abgestimmte Verhaltensweise oder rechtmäßiges Parallelverhalten?, NZKart 2016, pp. 554-555; CJEU, case C-74/14, "Eturas" UAB and Others v Lietuvos Respublikos konkurencijos taryba, Judgement of 21 January 2016; Monopolkommission, XXII. Hauptgutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 1 GWB, Wettbewerb 2018, para. 167.

184 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.

185 M. Schleusener, Personalisierte Preise im Handel – Chancen und Herausforderungen. In: Stüber and Hudetz (ed), Praxis der Personalisierung im Handel, 1st ed, Springer 2017, pp. 71-89.

186 BGH, Judgement of 3 July 2003 – I ZR 211/01; BGHZ 155, 301, 305.

187 BGH, Judgement of 3 July 2003 – I ZR 211/01; BGHZ 155, 301, 305.

188 BeckOK InfoMedienR/Paal, 31st ed, C.H. Beck 1.2.2021, AEUV Art. 101 para. 133a.

189 BeckOK InfoMedienR/Paal, 31st ed, C.H. Beck 1.2.2021, AEUV Art. 101 para. 133a.

190 OECD, Directorate for Financial and Enterprise Affairs, Algorithms and Collusion – Note from the European Union, 14 June 2017, DAF/COMP/WD(2017)12; BeckOK InfoMedienR/Paal, 31st ed, C.H. Beck 1.2.2021, AEUV Art. 101 para. 137.

191 Competition and Markets Authority (CMA) 30 September 2016, case no. 50223, 19 (25 ff.) – Online sales of posters and frames. Available at https://assets.publishing.service.gov.uk/media/57ee7c2740f0b606dc000018/case-50223-final-non-confidential-infringement-decision.pdf. Accessed 23 August 2021.

Moreover, under the circumstances of the current state of the art and the existing market conditions, the occurrence of unintentional "algorithmic collusion" still appears to be comparatively remote.[192] Nevertheless, unintentional price agreements, like the ones described above, are not covered by section 1 GWB. If the circumstances in the future allow the occurrence of unintentional "algorithmic collusion" there should be a stricter regulation of the conditions of use of certain forms of algorithms to prevent companies from circumventing normal competition and thereby harming consumers.

In any case, it must be considered that algorithms significantly simplify price agreements and make it much more difficult to detect them.[193] Algorithms can thus promote collusion.[194]

Furthermore, it might become difficult to decide whether the price fixing was intentional or unintentional, if the price algorithms are able to observe each other and are able to match each other without leaving any traces.[195] As part of a stricter regulation some people suggest a reversal of the burden of proof: the operator of the algorithm would have to demonstrate to the verifying authority that the use of the algorithm did not contribute to infringements of competition law.[196] However, this is usually rejected with the argument, that such proof would be very difficult or even impossible for many companies with dynamic price algorithms.[197] This may be due to, for example, the structure of the algorithm or because the company would have to disclose its trade secrets.

4.3.4. Collusion of Algorithms to Achieve Higher Prices

Any form of explicit collusion based on communication using algorithms is legally treated in the same way as human collusion.[198] Entrepreneurs coordinate their prices or quantities with each other using algorithms. This enables companies to achieve higher prices and possibly higher profits than it would be possible in free competition.[199] As already explained above, an intentional collusion with the aid of algorithms is covered by section 1 GWB, while unintentional price agreements, in which the coordination is brought about independently by the algorithms, are not covered by section 1 GWB. The described scenario (deliberate use of algorithms to coordinate the behaviour of the entrepreneur involved) is therefore not lawful.

In order to prevent such actions, several countermeasures are requested: It is proposed that the competition authorities are better equipped with specialist staff and technical resources, that algorithms for consumers and interference algorithms are developed, that algorithms are used to detect collusion at an early stage, that transparency obligations are introduced for users and manufacturers of the algorithms and that the speed of price changes get limited.[200] Other voices suggest not to overestimate the possibilities of algorithmic collusion. Instead, antitrust and competition agencies should address the issue of blockchain-based collusion.[201]

---

192 BeckOK InfoMedienR/Paal, 31st ed, C.H. Beck 1.2.2021, AEUV Art. 101 para. 133a.

193 W. Kerler, Illegale Preisabsprachen: Drohen uns bald Algorithmus-Kartelle?. Available at https://www.wired.de/article/preisabsprachen-durch-kuenstliche-intelligenz-drohen-uns-algorithmus-kartelle. Accessed 23 August 2021; Monopolkommission, XXII. Hauptgutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 1 GWB, Wettbewerb 2018, para. 171.

194 BeckOK InfoMedienR/Paal, 31st ed, C.H. Beck 1.2.2021, AEUV Art. 101 para. 133a.

195 Monopolkommission, XXII. Hauptgutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 1 GWB, Wettbewerb 2018, para. 185.

196 L. Bernhardt, Algorithmen, Künstliche Intelligenz und Wettbewerb, NZkart 2019, pp. 314-317.

197 B. Paal, Missbrauchstatbestand und Algorithmic Pricing, GRUR 2019, pp. 43-53.

198 OECD, Directorate for Financial and Enterprise Affairs, Algorithms and Collusion – Note from the European Union, 14.6.2017, DAF/COMP/WD(2017)12.

199 M. Gal, Algorithms as Illegal Agreements, Berkeley Technology Law Journal 2018.

200 L. Bernhardt, Algorithmen, Künstliche Intelligenz und Wettbewerb, NZkart 2019, pp. 314-317.

201 T. Schrepel, Collusion by Blockchain and Smart Contracts, Harvard Journal of Law & Technology Vol. 33 (2019), pp. 117-166.

4.3.5. Promotion of the Stability of Cartels through the Use of Price Algorithms

Although supervision and assembly are not new problems, they are becoming more relevant as a result of the increased use of algorithms and the greater availability of market data.[202] If prices are set with the help of algorithms, possible agreements can be made more quickly. In addition, collusive behaviour can be stabilised through greater price transparency. This applies in particular to the possibility of quick price adaptations if deviations from the collusive agreement are found. This would make short-term deviations unprofitable, as companies would be able to analyse data on the price changes of their competitors in real time. As a result, mutual monitoring and sanctions are easier to enforce among cartel members and the companies involved have less incentive to break the agreement.[203]
As a result, the increasing utilization of price algorithms can help cartels to achieve greater stability.[204]

4.3.6. Combating Consumer Discrimination through Consumer, Competition and Unfair Competition Regulations

The prohibition of misleading advertising in section 5 UWG does not constitute a real obstacle to personalised pricing because of the principle of price freedom.[205] The amount of a price, price fairness and the underlying calculation are not subject to any legal control and do not have to be disclosed.[206] Therefore, prices set by the entrepreneur can be increased or decreased at any time if he or she considers it appropriate.[207]
An unfairness of personalised prices can result in interaction with the German General Equal Treatment Act (Allgemeines Gleichbehandlungsgesetz, AGG).[208] The provision in section 19 of the AGG constitutes a market conduct rule within the meaning of section 3a UWG, so that an infringement would be sanctionable under unfair competition law.[209] However, there is no general principle of equal treatment, so that prices do not have to be the same for everyone,[210] nor does an offer say that the goods will be offered to every customer for the same price.[211] Nevertheless, certain discriminations, such as those based on age, gender and religion, are prohibited (section 19 AGG). Although section 20 AGG contains a possibility of justifying different treatment, the higher willingness to pay does not justify different pricing.[212] In the case of personalised prices, the categories listed in section 19 AGG matter, but basically the aim is to charge the highest possible price: Women, for example, are not generally confronted with higher prices than men.[213] Thus, a man and a woman can be shown the same high price, although women would generally be more willing to pay for the underlying product.[214]
In general, the General Equal Treatment Act does not cover personalised prices in principle, although discrimination may well occur in individual cases, which are comprised. For this reason, at least the criteria on which pricing is based should be disclosed.[215] This is essential in order to identify and complain about any discrimination.[216] Such obligation does not

---

202 M. Gal, Algorithms as Illegal Agreements, Berkeley Technology Law Journal 2018.
203 L. Bernhardt, Algorithmen, Künstliche Intelligenz und Wettbewerb, NZkart 2019, pp. 314-317.
204 Monopolkommission, XXII. Hauptgutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 1 GWB, Wettbewerb 2018.
205 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.
206 F. Hofmann, Der maßgeschneiderte Preis, WRP 2016, pp. 1074 - 1081; D. Tietjen and F. Flöter, Dynamische und personalisierte Preise: Welche lauterkeitsrechtlichen Schranken gelten für Unternehmen?, GRUR-Prax 2017, pp. 546 – 548.
207 BGH, Judgement of 13 March 2003 – I ZR 212/00, BGHZ 154, 306.
208 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.
209 BT-Drs. 16/1780, 48/49.
210 E. I. Obergfell, Personalisierte Preise im Lebensmittelhandel – Vertragsfreiheit oder Kundenbetrug?, ZLR 2017, pp. 290-301.
211 F. Hofman, Der maßgeschneiderte Preis, WPR 2016, pp. 1074-1081.
212 F. Hofman, Der maßgeschneiderte Preis, WPR 2016, pp. 1074-1081.
213 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.
214 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.
215 H. Zander-Hayat, L.A. Reisch and C. Steffen, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, pp. 403-410.
216 H. Zander-Hayat, L.A. Reisch and C. Steffen, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, pp. 403-410.

currently exist and would have to be regulated by law.[217] However, the problems mentioned above with regard to the disclosure of an algorithm would then occur.[218]

4.3.7. Prohibition of the Use of Price Algorithms in Certain Areas of Life

Since personalised prices can be used by companies to maximise profits by making the consumer pay higher prices, the use of personalised pricing is particularly controversial in certain areas of life. Particularly, that applies in those areas that are a central component of basic services.

In the health sector, for example, there is a risk that personalised prices may undermine the principle of solidarity of statutory health and long-term care insurance. [219] Another area where the use of personalised pricing is highly problematic is food supply. The purchase of food is a key part of the basic supply. It is essential for everyone. Therefore, it is extremely important to provide consumers with maximum transparency in pricing policy.[220]

Sectors of basic need should therefore remain free of personalised prices. In order to achieve this, appropriate regulations should be laid down in special laws.[221]

4.3.8. Consumer-Friendly Algorithms

The development of algorithms for consumers, so-called algorithmic consumers, is suggested in order to provide a counterweight to the pricing algorithms used by companies. Examples of such applications are digital assistants such as Alexa (Amazon), Siri (Apple) or Cortana (Microsoft). Algorithmic consumers could compensate competitive disadvantages for consumers and prevent collusion. Algorithmic consumers could also reduce search and transaction costs, help consumers to avoid prejudice and make more rational and intelligent decisions, and create or strengthen buyer power. This of course presupposes that the algorithms act in the interest of the users and do not consider the interests of the companies or other third-parties.

However, such a possibility requires a high level of available data. Since companies would always have an information advantage, such an algorithmic consumer solution would be difficult to implement. Another problem is the cost that consumers would have to pay for the use of such algorithms. If there is also implicit or explicit coordination by algorithms, it is unclear how a consumer algorithm is supposed to protect consumers from the negative effects of this collusion, especially in terms of higher prices. Furthermore, it is questionable which institution should have the competence to support and verify consumer algorithms.

However, the common use of platforms for price comparison and price forecasting is a first approach. The German price regulation (Preisabgabenverordnung) is intended to strengthen the position of the consumer by creating an optimal price comparison and to promote competition. According to the legislator, correct and complete consumer information guarantees price clarity, price transparency and price truthfulness. The consumer must be able to obtain full information on the price level by comparing prices. In the end, this allows the consumer to decide on the most favourable purchase or service offer, thereby promoting competition and helping to reduce the increase in prices. Finally, there is also the question of how to ensure that they are independent and therefore neutral.

---

217 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.
218 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.
219 Verbraucherzentrale Bundesverband e.V., Personalisierte Preise Diskussionspapier des Verbraucherzentrale Bundesverbands, 23. September 2016, p. 7. Available at https://www.vzbv.de/sites/default/files/vzbv_position_preisdifferenzierung_16-09-21_pdf.pdf. Accessed 23 August 2021.
220 E. I. Obergfell, Personalisierte Preise im Lebensmittelhandel – Vertragsfreiheit oder Kundenbetrug?, ZLR 2017, pp. 290 -301.
221 T. J. Tillmann and V. Vogt, Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, pp. 447-455.

4.4. Prohibition of Online Distribution

In the past few years, rising online-marketing faces increasing concerns about online distribution which leads into a debate on the prohibition of the sale of products on certain platforms as well as the prohibition of advertising them on search engines.

4.4.1. Prohibition of the Sale of Products on Certain Platforms

The admissibility of marketplace bans has been the subject of a large number of court and authority decisions in recent years.[222] The German Federal Cartel Office (Bundeskartellamt) has considered such prohibitions to be generally inadmissible.[223] However, the EJC recently clarified in its *Coty*-ruling that platform bans do not in principle constitute a restriction of the customer group and they also do not constitute a restriction on passive sales to end users within the meaning of Art. 4 lit. b and lit. c of the Commission Regulation 330/2010.[224]

The court has ruled that a selective distribution network does not fall within the prohibition of Art. 101 (1) TFEU, if the selection resellers is made based on objective criteria which are determined uniformly for all eligible resellers and applied without discrimination. However, the characteristics of the product in question have to require such a distribution network in order to preserve its quality and the criteria cannot go beyond what is necessary. Regarding the question whether selective distribution may be necessary in respect of luxury goods, the Court held that the quality of such goods is not only based on their physical characteristics but also on their prestigious character which gives them an aura of luxury. That aura is an essential element in enabling consumers to distinguish the luxury good from other similar products, therefore, any damage to that aura also affects the quality of the goods themselves. A selective distribution system helps to preserve the aura of luxury. Therefore, a selective distribution system for luxury goods with the primary purpose of ensuring the luxury image of those goods, is compatible with Art. 101 (1) TFEU, provided that the conditions set out before are fulfilled.

4.4.2. Prohibition of Product Advertising on Search Engines

Fundamental legal questions remain unresolved both for platform bans and for AdWords restrictions.[225] In the 2017 annual report of the German Federal Cartel Office they assumed that "the discussion on the antitrust assessment of distribution restrictions on the Internet is far from complete".[226]

Only those constellations in which the respective distribution partner is a commercial agent in the sense of the EU Guidelines on Vertical Restraints should be largely unproblematic: in this case the ban on cartels does not apply to the relationship between suppliers and distributors.[227]

The ASICS distribution system prohibited dealers from using various forms of search engine advertising, including the use of ASICS trademarks as keywords. Adidas' distribution conditions also contained a ban on search engine advertising.[228] The German Federal Cartel Office considered the respective restrictions to be hard-core restrictions not exempted by the Regulation 330/2010. However, following the Coty judgment, this view may no longer be sustainable.

---

222 T. Reimers, S. Brack and C. Modest, Kartellrechtliche Compliance in Zeiten der Digitalisierung, NZKart 2018, pp. 453-459.

223 Bundeskartellamt, Case Summary B2-98/11, Unlawful restrictions of online sales of ASICS running shoes, 25 January 2016. Available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Kartellverbot/2016/B2-98-11.pdf?__blob=publicationFile&v=2. Accessed 23 August 2021; Bundeskartellamt, Case Summary B3-137/12, adidas abandons ban on sales via online marketplaces,19 August 2014. Available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Kartellverbot/2014/B3-137-12.pdf?__blob=publicationFile&v=2. Accessed 23 August 2021.

224 CJEU, case C-230/16, Coty Germany GmbH v Parfümerie Akzente GmbH, Judgement of 6 December 2017, ECLI:EU:C:2017:941.

225 T. Reimers, S. Brack and C. Modest, Kartellrechtliche Compliance in Zeiten der Digitalisierung, NZKart 2018, pp. 453-459.

226 Bundeskartellamt, Tätigkeitsbericht 2017, p. 11.

227 T. Reimers, S. Brack and C. Modest, Kartellrechtliche Compliance in Zeiten der Digitalisierung, NZKart 2018, pp. 453-459.

228 T. Reimers, S. Brack and C. Modest, Kartellrechtliche Compliance in Zeiten der Digitalisierung, NZKart 2018, pp. 453-459.

It follows from the ruling that restrictions on online distribution can no longer easily be classified as restrictions on passive sales – at least not if advertising on the Internet is not completely prohibited and customers continue to have access to the Internet offer of the distributors by means of "normal" searches.[229]

4.5. Product Liability

With regard to digital marketing, issues related to product liability have to be examined too. In a recent decision, the European Court of Justice has again held that the Product Liability Directive 85/347 does not apply to the defectiveness of intellectual content.[230] However in the future, at least software marketed and sold digitally might fall under the Directive. At their conference on May 7, 2021, the German consumer protection ministers unanimously decided that the current Product Liability Act (Produkthaftungsgesetz) which is a result of the directive no longer offers sufficient protection in an increasingly digitalized and technically interconnected world.[231] In their opinion, consumers need to be better protected against damage caused by software errors and therefore the provisions of product liability law should cover software that is not permanently integrated into a physical product.[232] This opinion was also already expressed by the German federal government.[233] In addition, product liability law should also cover digital damages, including data loss, in the future.[234] Furthermore, since digital products can change as a result of updates or machine learning, the ministers consider it necessary to review the definition of the term "placing on the market" in the context of product liability.[235] In view of the increasing complexity of "digital" products, they also believe that it is necessary to readjust the rules on the burden of proof as in many cases it remains unclear whether the cause of damage lies in the hardware, the software, faulty data or an application error.[236] In this respect, they reiterated the Federal Council's (Deutscher Bundesrat) statement that such uncertainties should not be to the detriment of consumers, who should be granted a simplification of the burden of proof.[237] The clarification of such questions and whether the directive should be transformed into a regulation had also already been demanded by the European Parliament.[238]

5. The Impact of Personalised Political Campaigns on Democracy

Through personalised political campaigns, also called microtargeting, a party can match its message to the specific interests and vulnerabilities of the voters. In terms of democracy, there are both advantages and disadvantages.
For citizens, such microtargeting may lead to more relevant advertising. It can reach citizens who ignore traditional media, and it can interest people in politics through tailored messages. Microtargeting might thus increase information, interest in politics, and electoral turnout.[239] For politicians, microtargeting can be efficient, effective, and – in some cases – cheap.[240] Microtargeting can benefit public opinion, as it can lead to more diverse political campaigns, and to more knowledge among voters about certain issues.[241]

---

229 T. Reimers, S. Brack and C. Modest, Kartellrechtliche Compliance in Zeiten der Digitalisierung, NZKart 2018, pp. 453-459.
230 CJEU, case C-65/20, Judegement of 10 June 2021, ECLI:EU:C:2021:471.
231 Ergebnisprotokoll der 17. Verbraucherschutzministerkonferenz am 7. Mai 2021, p. 84.
232 Ergebnisprotokoll der 17. Verbraucherschutzministerkonferenz am 7. Mai 2021, p. 84.
233 Stellungnahme der Bundesregierung der Bundesrepublik Deutschland zum Weißbuch zur Künstlichen Intelligenz, pp. 24 f.
234 Ergebnisprotokoll der 17. Verbraucherschutzministerkonferenz am 7. Mai 2021, p. 85.
235 Ergebnisprotokoll der 17. Verbraucherschutzministerkonferenz am 7. Mai 2021, p. 84.
236 Ergebnisprotokoll der 17. Verbraucherschutzministerkonferenz am 7. Mai 2021, p. 85.
237 BR-Drs. 95/20 (B), p. 6.
238 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), P9_TA(2020)0276.
239 F. J. Zuiderveen Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, Utrecht Law Review 2018, pp. 82-96.
240 F. J. Zuiderveen Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, Utrecht Law Review 2018, pp. 82-96.
241 F. J. Zuiderveen Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, Utrecht Law Review 2018, pp. 82-96.

At the same time, microtargeting also brings with it major disadvantages and risks for democracy. Unconscious manipulation and an undermining of democratic decision-making are the biggest dangers of big data applications.[242] It can invade people's privacy and can be used to exclude or manipulate people. Microtargeting can enable a political party to misleadingly present itself to various people as a different party with a different political program.[243] For politicians, microtargeting also brings with it threats. Some types of microtargeting are so expensive that large parties with more financial resources gain an unfair advantage. And new intermediaries, such as online marketing companies, become more powerful.[244] One risk for public opinion is that the priorities of political parties could become opaque. In addition, the political debate can be split if different groups of voters focus on different issues.[245]

These risks must be taken seriously, and if they occur, they threaten democracy. Nevertheless, microtargeting could have less influence in Europe than in the USA because of differences in the legal and electoral systems. The GDPR makes microtargeting more difficult in the EU than in the US.[246] In order to minimise the risks, the following approaches should be adopted: expanding the political education of citizens, expansion and strengthening of journalistic expertise, information obligation for data-based activities of parties, review legal conditions for data ownership, data transfer and data consolidation.[247]

Depending on the specific design of the AI systems, it is possible that the systems will be prohibited under Art. 5 (1) lit. a, b, c AIA draft or that they will be classified as high-risk AI systems and therefore subject to special safeguards. Due to the partially very vague formulations in the AIA draft,[248] no clear statements can be made today. In the recital 15 AIA draft, however, it is pointed out that the aim is to counteract the dangers to democracy.

6. Future perspectives

After highlighting the problems that society, the authorities and the legal system must deal with in the face of rapidly changing commercial practices and the implementation of algorithms in the marketing sectors, future perspectives are presented.

6.1. Specific Regulatory Instruments

As already shown, it is difficult to detect the use of algorithms if they are not labelled as such. A labelling requirement is therefore the first step towards creating transparency. In addition, transparency is required with regard to the understandability and verifiability of the algorithms used.[249] In order to control the application and use under the current legislation, public authorities must therefore be better provided with personnel and technical equipment.

Besides that, there are various points where regulatory instruments could be deployed:[250] an independent technical supervisory association could be established to verify the appropriate and correct use of decision-making systems and to address shortcomings at different stages. Input monitoring could check whether training data is adequate and of good

---

242 C. Pentzold and L. Fölsche, Die öffentliche Verhandlung von Big Data in politischen Kampagnen, p. 52. http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Digitaler%20Demos.pdf. Accessed 23 August 2021.

243 F. J. Zuiderveen Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, Utrecht Law Review 2018, pp. 82-96.

244 F. J. Zuiderveen Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, Utrecht Law Review 2018, pp. 82-96.

245 F. J. Zuiderveen Borgesius et al., Online Political Microtargeting: Promises and Threats for Democracy, Utrecht Law Review 2018, pp. 82-96.

246 B. Kolany-Raiser and T. Radtke, Microtargeting, Gezielte Wähleransprache im Wahlkampf, 2018, p. 6 ff. http://www.abida.de/sites/default/files/16_Microtargeting.pdf. Accessed 23 August 2021.

247 C. Pentzold and L. Fölsche, Die öffentliche Verhandlung von Big Data in politischen Kampagnen, p. 65 ff. Available at http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Digitaler%20Demos.pdf. Accessed 23 August 2021.

248 H. Hoffmann, Regulierung der Künstlichen Intelligenz, K&R 2021, pp. 369-374.

249 C. Husted, Algorithmen-Transparenz. Was steckt hinter dem Buzzword?, 6 May 2019. Available at https://algorithmenethik.de/2019/05/06/algorithmen-transparenz-was-steckt-hinter-dem-buzzword/. Accessed 23 August 2021.

250 K. Zweig, Wo Maschinen irren können, Bertelsmann Stiftung 2018. Available at https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WoMaschinenIrrenKoennen.pdf. Accessed 23 August 2021.

quality. An incorrectly designed decision system can be detected by black box experiments, which can be used to test the functionality of such systems. Professional ethics for data scientists could ensure that they are aware of certain principles in their work. A guidance document that helps users to interpret the results can contribute to a more competent use of decision systems. Last but not least, a better external researchability of algorithmic decision systems would generally ensure the independent evaluation of the overall process.

However, before considering the use of other regulatory instruments, one should ask where exactly these should be used. To do this, one must firstly clarify which algorithms should be made transparent, for whom and why.[251]

Some of these aspects are already mentioned in the EU Commission's proposal for an Artificial Intelligence Act (AIA).[252] Even though this is a good approach, the legal requirements must also take into account technical developments. Therefore, the progress of so-called *Explainable AI* (XAI) in particular must be considered.

6.2. No Need to Establish Special Units

In our view, it is not necessary to establish special units within the authorities. Special knowledge can be obtained by consulting experts and internal training of employees.

However, if this evaluation changes, consideration may be given to create special departments within the supervisory authorities. The establishment of special chambers at the courts does not appear to make sense, as there will be interfaces with algorithms in almost all areas of life.

6.3. Codes of Conduct

Up until now, codes of conduct have played a minor role in data protection. The GDPR wants to help the instruments for self-regulation gather steam: for this purpose, the legal basis of the codes of conduct, Art. 40 GDPR, was substantially expanded and is more detailed than section 38a of the former German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).[253]

Codes of conduct are guidelines for good data protection practice, which are developed by experts in the relevant field, are similar to technical standards: they standardize data processing in connection with typical services and products offered in an industry.[254] According to Art. 40 (2) GDPR, codes of conduct should "specify" the application of the regulation. The need for such a clarification arises from the fact that the regulation is in numerous places undefined and contains general clauses.[255] Codes of conduct can be used as interpretative aids and thus serve to create and maintain legal certainty.[256] It also follows, that codes of conduct are not a legal basis for the processing of personal data.[257] Codes of conduct are intended to make it easier to apply the regulation effectively. Recital 98 states that account should be taken of the specific nature of processing operations carried out in certain sectors and the special needs of micro, small and medium-sized enterprises.

---

[251] C. Husted, Algorithmen-Transparenz. Was steckt hinter dem Buzzword?, 6 May 2019. Available at https://algorithmenethik.de/2019/05/06/algorithmen-transparenz-was-steckt-hinter-dem-buzzword/. Accessed 23 August 2021.

[252] EU Commission, 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 of 21 April 2021.

[253] C. Herfurth and F. Engel, Codes of Conduct im Konzern?, ZD 2017, pp. 367-372.

[254] N. Raschauer. In: Sydow (ed), Europäische Datenschutzgrundverordnung, 2nd ed, Nomos 2018, Art. 40 DS-GVO, para. 3.

[255] V. Jungkind. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 6 DS-GVO, para. 23.

[256] B. Paal. In: Paal and Pauly (eds), Datenschutzgrundverordnung, Bundesdatenschutzkontakt, 2nd ed, C.H. Beck 2018, Art. 6 DS-GVO, para. 11.

[257] P. Laue. In: Laue and Kremer, Das neue Datenschutzrecht in der betriebsrechtlichen Praxis, 2nd ed, Nomos 2019, § 8, para. 7.

Codes of conduct can help to avoid uncertainty and legal disputes to a certain extent,[258] but the legal basis for data processing remains the regulation.[259] Self-regulation and codes of conduct can therefore not replace legal regulations.[260] The EU Commission's DSA draft contains provisions for a framework for the development of specific codes of conduct for online advertising. According to Art. 36 DSA the Commission shall encourage and facilitate the drawing up of codes of conduct at Union level between online platforms and other relevant 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 contribute to further transparency in online advertising. The codes of conduct shall pursue an effective transmission of information, in full respect for the rights and interests of all parties involved, and a competitive, transparent and fair environment in online advertising, in accordance with Union and national law, in particular on competition and the protection of personal data. The codes of conduct shall address at least the transmission of information held by providers of online advertising intermediaries to recipients of the service and the transmission of information held by providers of online advertising intermediaries to repositories containing certain information regarding the displayed advertisements.

6.4. A Vigilant and Learning Approach

New social media platforms with fresh or at least newly interpreted functions are constantly emerging. They offer special possibilities for advertising use to justify their special features and to stand out from other offers. Although new problems are always associated with this, the legal principles known from other, comparable constellations are usually transferable to these new types of questions.[261] However, the existing regulations must be regularly reviewed in the light of upcoming changes. Due to changing user habits and greater familiarity with new social media offerings, a certain adjustment of the requirements would be desirable in some constellations.[262]

The DSA and DMA drafts seem to try to learn from prior complications. A frequently raised criticism of antitrust supervision is that it is not fast enough to effectively stop abusive practices. Therefore, the DMA provides an ex-ante regulatory tool to control the behaviour of gatekeepers under Art. 5 and 6 DMA.[263] Furthermore, the findings of the evaluation report on the GDPR,[264] especially regarding the enforcement, have a direct impact on the DSA and DMA drafts: to address the different levels of enforcement across EU member states under the GDPR the DSA and DMA provide a modified enforcement regime. By involving the Commission, the lack of enforcement is supposed to be prevented.

7. Conclusion

In an overall assessment, Germany and the EU are taking different measures, which positively contribute to the new challenges. Nevertheless, AI regulation can only go hand in hand with the technical feasibility and the consideration of ethical and social circumstances and cannot be solved on a legal level alone. Therefore, the circumstances must regularly be assessed not only from a legal, but also an ethical perspective. In addition to economic aspects, the focus must be on

---

258 N. Raschauer. In: Sydow (ed), Europäische Datenschutzgrundverordnung, 2nd ed, Nomos 2018, Art. 40 DS-GVO, para. 7.

259 V. Jungkind. In: Wolff and Brink (eds), BeckOK Datenschutzrecht, 31st ed, C.H. Beck 2020, Art. 6 DS-GVO, para. 23; Landesbeauftragte für Datenschutz und Informationsfreiheit NRW, Verhaltensregeln und Akkreditierung von Überwachungsstellen nach der DS-GVO. https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Verhaltensregeln-_-Code-of-Coduct/Inhalt/Verhaltensregeln-und-Akkreditierung-von-Ueberwachungsstellen-nach-der-DS-GVO/Verhaltensregeln-und-Akkreditierung-von-Ueberwachungsstellen-nach-der-DS-GVO.html. Accessed 23 August 2021.

260 A. Roßnagel. In: Simitis,Hornung and Spiecker, Datenschutzrecht, 1st ed, Nomos 2019, Art. 40 DS-GVO, para. 20.

261 F. Lichtnecker, Neues aus dem Social Media-Marketing, MMR 2018, pp. 512-517.

262 F. Lichtnecker, Neues aus dem Social Media-Marketing, MMR 2018, pp. 512-517.

263 See N. Gielen and S. Uphues, Digital Markets Act und Digital Services Act, EuZW 2021, pp. 627-637.

264 EU Commission, COM(2020) 264 final.

the autonomy of the persons concerned, especially their informational self-determination, which is protected by Art. 8 CFR. Both economic and self-determination interests have to be fairly balanced.

The new legislative procedures at the EU and national level provide an insight into the new policy directions. With the help of harmonising legislation, the EU wants to make the EU internal market more competitive. In order to be able to effectively implement this goal, it is useful to seek solidarity with the US-partners.[265] Furthermore, the European Commission's proposal for an Artificial Intelligence Act as the world's first response to the issue of regulating AI is a step in the right direction but needs to be adapted in the further regulation process.

[265] See U. von der Leyen, Speech at the World Economic Forum in Davos 2021, "I want to invite our friends in the United States to join our initiatives. Together, we could create a digital economy rulebook that is valid worldwide." Available athttps://ec.europa.eu/commission/presscorner/detail/en/speech_21_221. Accessed 23 August 2021.