Die **essential facility doctrine,** nach der ein Unternehmen mit marktbeherrschender Stellung unter bestimmten Voraussetzungen Zugang zu Einrichtungen (gegebenenfalls auch Daten) gewähren muss,[262] hilft ebenfalls nicht weiter, da diese Doktrin nur unter „außergewöhnlichen Umständen" greift.[263]

Ein **Zugangsanspruch zu Daten** lässt sich auch aus dem **kartellrechtlichen Missbrauchstatbestand** (Art. 102 AEUV; §§ 18 f. GWB) nur in **Ausnahmefällen** ableiten. Dass eine dahin gehende Untersuchung aber an Bedeutung gewinnt, wird inbesondere durch die kartellrechtlich relevante Behördenpraxis[264] sowie die Tatsache deutlich, dass der deutsche Gesetzgeber im Rahmen der 10. GWB-Novelle den Zugang zu Daten nunmehr ausdrücklich bei der Missbrauchskontrolle berücksichtigt hat (§ 18 Abs. 3 Nr. 3 GWB und § 19 Abs. 2 Nr. 4 GWB und § 20 Abs. 1a GWB). In dynamischen, mehrseitigen Märkten ist es bereits schwierig, die Existenz einer marktbeherrschenden Stellung aufgrund der Kontrolle von Daten nachzuweisen[265] und klare Kriterien für die Feststellung eines Missbrauchs bei der Verweigerung des Datenzugangs festzulegen. Davon abgesehen greift das kartellrechtliche Durchsetzungssystem nur ex post; das Kartellrecht ist daher kein geeignetes Instrument, um die zahlreichen Fragen, die sich bei Annahme eines Zugangsanspruchs stellen (Zugangsmodalitäten; Vergütung für den Zugang; Berücksichtigung des Datenschutzrechts bei personenbezogenen Daten), systematisch zu lösen. **119**

b) Datenzugangsrechte nach dem Data Act

Neben einigen sektorspezifischen Regelungen[266] wurden mit dem im Januar 2024 in Kraft getretenen **Data Act**[267] nunmehr **gesetzliche Datenzugangsrechte im Unionsrecht** verankert, die ab dem 12.9.2025 bzw. 12.9.2026 greifen.[268] Ziel der Verordnung ist es, **120**

monopolize any part of the trade or commerce among the several States, or with foreign nations, shall be deemed guilty (…)".

262 Siehe für die USA MCI Commc'ns Corp. v. American Tel. & Tel. Co., 708 F.2d 1081, 1132-33 (7th Cir. 1983); Maurer/Scotchmer The Essential Facilities Doctrine; Pitofsky/Patterson/Hooks Antitrust Law Journal 70 (2002), 443 (448). Für die EU siehe EuGH Urt. v. 6.4.1995 – C-241/91 P und C-242/91 P, ECLI:EU:C:1995:98, GRUR Int. 1995, 490 – RTE und ITP/Kommission („Magill"); EuGH Urt. v. 29.4.2004 – C-418/01, ECLI:EU:C:2004:257, MMR 2004, 456 – IMS Health; EuG Urt. v. 17.9.2007 – T-201/04, ECLI:EU:T:2007:289 – Microsoft/Kommission; Evrard Columbia Journal of European Law 10 (2004), 491.

263 Zur Frage, ob Daten als essential facility angesehen werden können, vgl. aus US-amerikanischer Perspektive Sokol/Comerford Geo. Mason L. Rev. 23 (2016), 1129 (1158 ff.); Balto/Lane, Monopolizing Water in a Tsunami, 2016. Aus europäischer Perspektive vgl. Graef Data as Essential Facility; Lehtioksa Big Data as an Essential Facility; Telle Kartellrechtlicher Zugangsanspruch zu Daten nach der essential facility doctrine, 2017, S. 73–87.

264 Siehe zB BKartA Fallbericht v. 6.2.2019, B6-22/16 – Facebook; Kommission Pressemitteilung v. 20.3.2019, AT 40.411, IP/19/1770 – Google Search (AdSense); Kommission Pressemitteilung v. 18.6.2019, AT 40.099, IP/18/4581 – Google Android; Kommission, ABl. 2019 C 9, 11–14 – Google Search (Shopping). Schmidt Zugang zu Daten nach dem europäischen Kartellrecht S. 353 ff.

265 Der Zugang zu wettbewerbsrelevanten Daten bedingt allein noch keine besondere Macht; statt vieler Körber NZKart 2016, 303 (305 f.). Maßgeblich ist vielmehr der besondere Zugang zu Daten, durch den sich das Unternehmen dem Wettbewerbsdruck entziehen kann. Vgl. nur Paal/Hennemann Big Data as an Asset, 2018, S. 52: Für die Beurteilung von Marktmacht ist eine umfassende Einzelanalyse erforderlich, bei der (i) die Charakteristika und Kategorien der in Rede stehenden Daten, (ii) die konkrete Nutzung dieser Daten auf der Grundlage des verfolgten Geschäftsmodells sowie (iii) „externe" Faktoren wie insbes. die Interoperabilität der in Rede stehenden Daten zu betrachten sind.

266 Vgl. zB Art. 6–9 VO (EG) 715/2007, Art. 35 f. RL 2015/2366/EU, Art. 27, 30 VO (EG) 1907/2006, Art. 30, 32 RL 2009/72/EG und EG 11 RL 2010/40/EU. Auch das in Art. 20 DS-GVO geregelte Recht auf Datenportabilität basiert auf der Ratio, Lock-in-Effekte zu vermeiden und den Wechselprozess von einem Dienstleister zu einem anderen zu verbessern; vgl. dazu bspw. Hennemann PinG 2017, 5; Strubel ZD 2017, 355.

267 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), ABl. L 2023/2854 v. 22.12.2023.

268 Art. 50 Data Act.

harmonisierte Regeln für einen fairen Zugang zu Daten und deren Nutzung festzulegen.[269] Das Regelwerk soll das wirtschaftliche Potenzial der wachsenden Datenmengen freisetzen und einen wettbewerbsfähigen Datenmarkt fördern, indem es den Zugang zu Daten und deren Nutzung einheitlich regelt.[270]

121 Anders als die DS-GVO[271] erfasst der Data Act sowohl **personenbezogene** als auch **nicht-personenbezogene** Daten (Art. 2 Nr. 3 und 4 Data Act). Er bezieht sich allerdings nur auf **Rohdaten;** aufbereitete Daten fallen nicht unter den Anwendungsbereich.[272] Die Verordnung erfasst die **Datenverarbeitung vernetzter Produkte** und **verbundener Dienste,** also solche Geräte, die vernetzte Funktionen aufweisen und eine vollautomatisierte Datenverarbeitung ermöglichen. Darunter fallen vor allem **IoT-Geräte** (wie ein vernetztes Navigationsgerät).[273] Nicht unter den Anwendungsbereich fallen hingegen solche Geräte und Dienste, die einen menschlichen Beitrag zur Datengenerierung erfordern, wie zB Tablets oder Textscanner sowie Social-Media-Angebote oder Cloud-Dienstleistungen.[274]

122 Der Data Act räumt dem **Nutzer** vernetzter Produkte oder vernetzter Dienste **Rechte hinsichtlich der Datennutzung und -verbreitung** ein. Nach Art. 3 Abs. 1 Data Act müssen vernetzte Produkte und verbundene Dienste so konzipiert sein, dass die Produktdaten und verbundenen Dienstdaten für den Nutzer einfach, sicher, unentgeltlich in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format und, soweit relevant und technisch durchführbar, **direkt zugänglich** sind (sog. **„accessibility by design"**).[275] Da unter **„Nutzer"** jede natürliche oder juristische Person zu verstehen ist, die ein vernetztes Produkt besitzt oder der vertraglich zeitweilige Rechte für die Nutzung des vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nimmt (Art. 2 Nr. 12 Data Act), werden nicht nur **Unternehmer,** sondern auch **Verbraucher** erfasst, die ein vernetztes Produkt kaufen bzw. mieten oder einen verbundenen Dienst in Anspruch nehmen.[276] Ist ein direkter Zugang zu den Daten nicht möglich, kann der Nutzer nach Art. 4 Abs. 1 Data Act hilfsweise von der Person, die die faktische Kontrolle über die Daten hat (also in der Regel vom Gerätehersteller), verlangen, dass ihm die Daten unentgeltlich zur Verfügung gestellt werden. Darüber hinaus kann der Nutzer vom Dateninhaber nach Art. 5 Abs. 1 Data Act verlangen, die Daten an Dritte weiterzugeben. Flankierend hierzu haben **Hersteller** und **Anbieter** sowie **Dateninhaber** bestimmte Pflichten gegenüber den Nutzern. Art. 3 Abs. 2–3 Data Act regelt **vorvertragliche Informationspflichten** bezüglich Art, Format, Datenvolumen sowie Speicherung und Zugang zu Daten.

123 Der Data Act sieht darüber hinaus **gesetzliche Verwendungsbeschränkungen** hinsichtlich der erlangten Daten vor. Nach Art. 4 Abs. 13 Data Act darf der Dateninhaber nicht-personenbezogene Daten nur auf der Grundlage einer **vertraglichen Vereinbarung** mit dem Nutzer verwenden. Eine Weitergabe der Daten an Dritte ist nach Art. 4 Abs. 14 Data Act nur zur Erfüllung ihres Vertrags mit dem Nutzer gestattet. **Datennutzungsverträge** unterliegen nach Art. 13 Data Act zudem einer **Missbrauchskontrolle.** Darüber hinaus werden **vertragliche und organisatorische Wechselbarrieren verboten:** Der Nutzer soll künftig kostenlos zwischen verschiedenen Datenverarbeitungsdiensten (wie zB Cloud-Diensten) wechseln und alle seine exportierbaren Daten auf einen neuen Dienst

[269] Vgl. Erwgr. 5 und 6 Data Act.
[270] Vgl. Erwgr. 19 Data Act. Zur Anwendung neben anderen Rechtsakten Pathak Data Governance Redefined S. 14.
[271] Zum Anwendungsbereich siehe Schmidt-Kessel/Bomhard MMR-Beil. 2024, 69 (70); Schmidt-Kessel MMR-Beil. 2024, 122 (126 f.); vgl. Steinrötter GRUR 2023, 216; krit. Etzkorn RDi 2024, 116 (117).
[272] Erwgr. 15 Data Act; Wiebe GRUR 2023, 1569 (1570).
[273] Art. 1 Abs. 1 lit. a, Art. 2 Nr. 5 und 6 Data Act, Erwgr. 14 Data Act; siehe auch die dort aufgeführten Beispiele; vgl. auch Etzkorn RDi 2024, 116 (117).
[274] Dazu auch Schmidt-Kessel MMR-Beil. 2024, 75 (78).
[275] Schmidt-Kessel MMR-Beil. 2024, 75 (78); Podszun/Pfeifer GRUR 2022, 953 (956); Steinrötter GRUR 2023, 216 (220).
[276] Dazu Schmidt-Kessel MMR-Beil. 2024, 75 (76 f.).

übertragen können, ohne dass der Anbieter seinerseits den Wechsel behindert (Art. 23 S. 1 Data Act).[277]

Um die Integrität und Sicherheit von Daten und datenbezogenen Diensten zu sichern, werden durch **Regelungen zur Interoperabilität** (Art. 33 ff. Data Act) technische und sicherheitsrelevante Mindeststandards für Datenräume,[278] Datenverarbeitungsdienste sowie intelligente Verträge festgelegt.[279] **124**

c) Auswertung

Da der Data Act **kein Ausschließlichkeitsrecht an Daten** vorsieht,[280] sondern stattdessen Datenzugangsrechte regelt, ist die Diskussion um ein mögliches Dateneigentumsrecht (→ Rn. 104 ff.) weiterhin offen. Im Ergebnis bestehen gegen ein Ausschließlichkeitsrecht an Daten erhebliche Bedenken: Erstens gibt es **keine praktische Notwendigkeit** für ein solches Schutzrecht, da Unternehmen einen unbefugten Zugang zu „ihren" Daten durch technische Schutzmaßnahmen verhindern können. Zweitens werden Unternehmen bereits durch **delikts- und strafrechtliche Normen** vor einer Veränderung, Löschung oder unberechtigten Verwendung ihrer Daten geschützt.[281] Drittens zeigt die rechtliche Diskussion, dass sich der Schutzgegenstand und Schutzumfang eines solchen Ausschließlichkeitsrechts äußerst schwer bestimmen lassen.[282] Schließlich besteht bei Anerkennung eines absoluten Rechts auf Dateneigentum die Gefahr einer unangemessenen **Monopolisierung von Daten:** Unternehmen, die bereits jetzt eine markbeherrschende Stellung haben, könnten ihre Dominanz weiter ausbauen und zusätzliche Marktzutrittsbarrieren für Konkurrenten errichten.[283] Aus diesen Gründen erscheint ein Ansatz vorzugswürdig, der – wie der Data Act – für bestimmte Bereiche versucht, das Interesse von Personen, die ein berechtigtes Interesse am Zugang zu externen Daten haben, mit dem berechtigten Interesse der Datenerzeuger (oder Dateninhaber) am Schutz ihrer Investitionen und – soweit es um personenbezogene Daten geht – den Interessen sonstiger betroffener Personen in Einklang zu bringen. **125**

H. Algorithmische Manipulation und Diskriminierung

Lernende Algorithmen werden von Unternehmen, politischen Parteien und anderen Akteuren eingesetzt, um Vorhersagen über die Wahrscheinlichkeit künftigen Verhaltens treffen und darüber entscheiden zu können, wie ein bestimmter Trend oder eine bestimmte Neigung ausgenutzt, verstärkt oder beeinflusst werden kann. In der Praxis wird das Entscheidungsverhalten von Bürgern und Verbrauchern vor allem durch die Technik des **Online Behavioral Advertising** (OBA) bzw. **Microtargeting** beeinflusst. Dies wirft die Frage auf, inwieweit die (deutsche bzw. europäische) Rechtsordnung adäquate Schutzinstrumente zur Verfügung stellt, um einer solchen Manipulation entgegenzutreten (→ Rn. 144 ff.). Ein weiteres Problem, das bei der algorithmischen Entscheidungsfindung auftritt, ist das **Risiko der Diskriminierung:** Viele Studien zeigen, dass algorithmische Systeme nicht wertneutral, sondern häufig voreingenommen und diskriminierend sind. Demzufolge stellt sich auch hier die Frage, wie dem Problem der Diskriminierung rechtlich begegnet werden kann (→ Rn. 152 ff.). Das Phänomen der algorithmischen Manipulation **126**

[277] Schmidt-Kessel/Bomhard MMR-Beil. 2024, 69 f. mit den potenziellen Anwendungsfällen. Krit. Bomhard MMR-Beil. 2024, 109 ff.
[278] Krit. Siglmüller MMR-Beil. 2024, 112 (113 ff.).
[279] Siglmüller MMR-Beil. 2024, 112 ff.
[280] Erwgr. 5 Data Act; Hennemann/Steinrötter NJW 2022, 1481; Hoeren MMR 2023, 32 (33).
[281] Kerber GRUR Int. 2016, 989.
[282] Wiebe GRUR Int. 2016, 877 (881 ff.).
[283] MPI Positionspapier v. 16.8.2016 zur aktuellen europäischen Debatte, S. 6; Drexl NZKart 2017, 339 (343).

wirft darüber hinaus wichtige **wettbewerbsrechtliche Fragen** auf, wenn der Einsatz von (Preis-)Algorithmen zu einem kollusiven Marktergebnis führt (→ Rn. 126 ff.).

I. Profiling, Targeting, Nudging und Manipulation

1. Die Technik des Behavioral Microtargeting

127 Behavioral Microtargeting bzw Online Behavioral Advertising hat sich in den letzten Jahren zu einer neuen, erfolgsversprechenden Strategie entwickelt. Die Technik des Behavioral Microtargeting ermöglicht Unternehmen eine personalisierte Ansprache von Menschen auf der Grundlage **verhaltens- und persönlichkeitsbasierter Nutzerprofile,** die durch algorithmische Auswertung personenbezogener Daten erstellt werden.[284]

128 Behavioral Microtargeting basiert auf **drei Elementen.** Erstens setzt die psychometrische Analyse des Einzelnen die Erhebung großer Datenmengen voraus. Die so gesammelten Daten werden in einem zweiten Schritt im Wege der Big Data-Analyse durch Algorithmen und ML ausgewertet, um bestimmte persönliche Aspekte des Nutzers, seine Charakterstärken, aber auch seine kognitiven und voluntativen Schwächen zu analysieren oder vorherzusagen.

Beispiel 7:

Für besonderes Aufsehen haben mehrere Studien an der Universität Cambridge gesorgt,[285] die in den letzten Jahren die Facebook-Likes von mehr als 80.000 Nutzern analysierten und dabei zeigen konnten, dass man aus durchschnittlich (auf den ersten Blick „neutralen") 68 Likes weitgehende Aussagen über die Persönlichkeit eines Menschen treffen kann. So lässt sich beispielsweise mit 95-prozentiger Treffsicherheit die Hautfarbe bestimmen, mit 88 Prozent Wahrscheinlichkeit sagen, ob der Nutzer homosexuell ist und mit 85 Prozent, ob jemand Demokrat oder Republikaner ist. Berechnen lassen sich zudem Religionszugehörigkeit, Alkohol-, Zigaretten- und Drogenkonsum, aber auch, ob die Eltern einer Person bis zu deren 21. Lebensjahr zusammengeblieben sind oder nicht. Die so vorgenommene Analyse soll dabei nach Angabe der Wissenschaftler das menschliche Einschätzungsvermögen bereits bei wenigen Facebook-Likes übertreffen.[286]

129 Die auf diese Weise ausgewerteten Daten können in einem dritten Schritt vielfältigen Verwendungsmöglichkeiten zugeführt werden. Unternehmen können ihre **Werbung,** aber auch ihre Produkte und Preise gezielt auf das Kundenprofil abstimmen,[287] **Kreditinstitute** können auf dieser Grundlage Bonitätsanalysen erstellen,[288] **Versicherungsunternehmen** das zu versichernde Risiko besser einschätzen,[289] Personalabteilungen die Eignung von Bewerbern beurteilen,[290] Parteien die Wirksamkeit von Wahlwerbung verbessern[291] – eine

[284] Calo George Washington Law Review 82 (2014), 995 (1015 ff.); O'Neil Weapons of Math Destruction, S. 194 ff.; Chaimanowong et al. The Effects of Microtargeting on Conversion Rates and the Role of Information Asymmetry, S. 1.

[285] Kosinski/Stillwell/Graepel PNAS 110 (2013), 5802; Youyou/Kosinski/Stillwell PNAS 112 (2015), 1036.

[286] Zusammenfassend Grassegger/Krogerus, Das Magazin v. 3.12.2016, https://web.archive.org/web/20170127181034/https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/ (30.12.2024).

[287] Zum damit einhergehenden Problem der Preisdiskriminierung → § 13 Rn. 74; Hofmann WRP 2016, 1074; Zuiderveen Borgesius/Poort Journal of Consumer Policy 40 (2017), 347; Spiecker gen. Döhmann/Westland/Campos Demokratie und Öffentlichkeit im 21. Jahrhundert/Kelber/Leopold, 2022, S. 160 f.; Bijok Kommerzialisierungsfenster Datenschutz S. 100 f.

[288] Dazu Citron/Pasquale Washington Law Review 89 (2014), 1; Zarsky Washington Law Review 89 (2014), 1375; Taeger ZRP 2016, 72.

[289] Vertiefend Swedloff Connecticut Insurance Law Journal (21) 2014, 339; Helveston Washington University Law Review 93 (2016), 1.

[290] Dazu → § 7 Rn. 11, 36; O'Neil Weapons of Math Destruction, S. 105 ff.

[291] Vgl. nur den Vortrag von Alexander Nix, ex CEO von Cambridge Analytica, auf dem 2016 Concordia Annual Summit in New York, www.youtube.com/watch?v=n8Dd5aVXLCc (30.12.2024); ferner Ru-

Praxis, die bekanntermaßen zum **Cambridge Analytica-Skandal** geführt hat. In den USA setzen mittlerweile selbst die Gerichte Big Data-Analysen ein, um für Straftäter eine Rückfallprognose zu erstellen.[292]

2. Verhaltensökonomik und Behavioural Microtargeting

Von besonderem Interesse ist die Kombination von Big Data mit den Erkenntnissen der Verhaltensökonomik.[293] **130**

Schon seit geraumer Zeit haben sich die Wirtschaftswissenschaften von dem Paradigma der ökonomischen Neoklassik, dem **homo oeconomicus,** verabschiedet, dessen Leitbild bekanntlich auf der Annahme basiert, dass der Einzelne seine Entscheidungen grundsätzlich rational nach Kosten- und Nutzenaspekten mit dem Ziel der individuellen Nutzenmaximierung trifft. **131**

Die Verhaltensökonomik konnte demgegenüber zeigen, dass der Mensch nur eingeschränkt rational handelt, zum einen weil er nur über beschränkte Denk- und Vorstellungsfähigkeiten verfügt (beschränkte Rationalität – **bounded rationality**), zum anderen weil seine bewussten Entscheidungen von Vor- und Werturteilen geprägt werden (beschränkte Willensmacht – **bounded willpower**), die eine Orientierung am größtmöglichen Eigennutz verdrängen (beschränktes Eigeninteresse – **bounded self-interest**).[294] **132**

Die moderne Marktforschung macht sich diese Entscheidungsanomalien zunutze und kombiniert diese mit Big Data. Dabei gibt es Hinweise, dass suboptimales Entscheidungsverhalten von vielen Unternehmen ausgenutzt oder sogar hervorgerufen wird. **133**

Beispiel 8:

Ein Experiment mit knapp 700.000 Facebook-Nutzern hat zeigen können, dass Gefühle von Nutzern durch bestimmte Nachrichten bewusst manipuliert werden können (sog. Gefühlsansteckung – emotional contagion).[295]

Beispiel 9:

Anfang 2017 wurde bekannt, dass Facebook Australia seinen Werbekunden eine Software angeboten hatte, mit der treffsicher psychisch labile, depressive Teenager lokalisiert werden konnten.[296]

Auch andere Unternehmen machen sich die Erkenntnisse der Verhaltensökonomik zunutze. Microsoft ließ im Jahr 2012 ein Patent auf „Targeting Advertisements Based on Emotion" anmelden.[297] Und Samsung meldete 2013 das Patent „Apparatus und methods for sharing user's emotion" an.[298] **134**

---

binstein Wisconsin Law Review 2014, 861; Hoffmann-Riem AöR 142 (2017), 1 (14 f.); Hill/Hoffmann-Riem/Kugelmann/Martini, Digitalisierung in Recht, Politik und Verwaltung, 2018, S. 47 ff.; Richter/Hentschel/Hornung/Jandt Mensch – Technik – Umwelt S. 303 ff.

[292] Angwin et al., www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (30.12.2024).

[293] Dazu Hacker Verhaltensökonomik und Normativität.

[294] Simon The Quarterly Journal of Economics 69 (1955), 99; Kahneman/Tversky Econometrica 47 (1979), 263; Sunstein/Thaler The University of Chicago Law Review 70 (2003), 1159; dazu Eidenmüller JZ 2011, 814; Wiedemann/Wank JZ 2013, 340.

[295] Kramer/Guillory/Hancock PNAS 111 (2014), 8788–8790.

[296] Davidson Facebook targets ‚insecure' young people, The Australian v. 1.5.2017; vgl. auch www.news.com.au/technology/online/social/leaked-document-reveals-facebook-conducted-research-to-target-emotionally-vulnerable-and-insecure-youth/news-story/d256f850be6b1c8a21aec6e32dae16fd (30.12.2024).

[297] Microsoft Corporation, Targeting Advertisements Based on Emotion, 2012, US 20120143693 A1, www.google.com/patents/US20120143693 (30.12.2024).

[298] Samsung Electronics Co. Ltd., Apparatus and method for sharing user's emotion, 2013, US 20130144937 A1, www.google.com/patents/US20130144937 (30.12.2024).

3. Algorithmische Echokammern, Filterblasen und Fake News

135 Der Einsatz von Algorithmen und KI-Systemen in der Plattformökonomie, insbesondere in sozialen Netzwerken und Suchmaschinen, wirft angesichts der vielfältigen (häufig unbemerkten) Möglichkeiten der Einflussnahme auf Informationswahrnehmung, Meinungsbildung und -äußerung durch Auswahl und Filterung von Informationen, social bots und fake news, die Frage auf, wie in einer algorithmisch gesteuerten Gesellschaft die für eine demokratische Gesellschaft konstitutive **Meinungsbildungsfreiheit** und **Medienpluralität** aufrechterhalten werden können.

136 Algorithmenbasierte Dienste personalisieren, kanalisieren und steuern in zunehmendem Umfang meinungsbildungsrelevante Informationen. In vielen Fällen bestimmen Algorithmen (und Social Bots), welche Inhalte ausgewählt, verarbeitet und veröffentlicht werden; Algorithmen und social bots werden zudem dazu verwendet, gänzlich neue Inhalte zu generieren.[299] Wer den jeweiligen Algorithmus konfiguriert, trifft somit wesentliche Entscheidungen über die angezeigten Informationen und kann damit – wie vielfach hervorgehoben wird[300] – (auch) die für die demokratische Willensbildung wichtige Meinungsbildung beeinflussen.

137 Der Einsatz von Algorithmen kann in Verbindung mit der zunehmenden Monopolisierung von Marktmacht und Wissen in der Plattformökonomie (→ Rn. 135) insbesondere zu sog. **„Echokammern"** führen, in denen sich Menschen nur noch mit Gleichgesinnten austauschen, die ihre eigene (politische) Meinung bestätigen.[301] Ebenso bestehen Bedenken, dass **„Filterblasen"** entstehen, wenn dem Nutzer durch algorithmische Rankingsysteme nur diejenigen Informationen angezeigt werden, die mit seinen bisherigen Ansichten übereinstimmen, während andere Informationen ausgeblendet werden.[302] Vor diesem Hintergrund wird sowohl in den USA als auch in Europa die Befürchtung geäußert, dass es zu einer drastischen **Reduzierung der Medienvielfalt** kommen könnte[303] – ein Trend, der durch **KI-Suchmaschinen** erheblich verstärkt wird.[304] KI-Systeme begünstigen darüber hinaus die Verbreitung von **„fake news",** da mit ihrer Hilfe täuschend echt wirkende Bilder und Videos **(Deepfakes)** erstellt, journalistische Inhalte automatisch generiert und veröffentlicht und – über die Technik des Microtargeting – Bürger gezielt angesprochen werden können.[305]

138 Angesichts dieses Befundes werden eine Reihe (regulatorischer) Fragen diskutiert:[306] Sind **Informationsintermediäre** wie **Meta** und **Google** nur Vermittler von Meinungen oder sind sie bereits selbst zu **Medienunternehmen** geworden?[307] An welcher Stelle kann die

---

[299] Ausf. → § 34 Rn. 8 ff.

[300] Vgl. Paal/Hennemann JZ 2017, 641; Bogner/Decker/Nentwich/Scherz Digitalisierung und die Zukunft der Demokratie/Saurwein/Spencer-Smith/Krieger-Lamina, 2022, S. 243 ff.

[301] Sunstein #Republic. Divided Democracy in the Age of Social Media; Jaster et al. Fake News und Desinformation S. 250; Cinelli et al., The echo chamber effect on social media, 2021, https://doi.org/10.1073/pnas.2023301118 (30.12.2024); Talamanca/Arfini Through the Newsfeed Glass; Appel Die Psychologie des Postfaktischen/Messingschlager/Holtz S. 92 ff.

[302] Pariser The Filter Bubble: What the Internet is Hiding from You; vgl. OLG Karlsruhe Urt. v. 27.5.2020 – 6 U 36/20 Rn. 103; zu den Begrifflichkeiten Peukert WRP 2020, 391 (396 f.); Talamanca/Arfini Through the Newsfeed Glass; Kelly/François This is what filter bubbles actually look like; Appel Die Psychologie des Postfaktischen/Messingschlager/Holtz S. 92 ff.

[303] Epstein US News & World Report v. 9.6.2014; siehe auch Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to the 32nd session of the Human Rights Council (A/HRC/32/38): „search engine algorithms dictate what users see and in what priority, and they may be manipulated to restrict or prioritise content".

[304] Lewandowski, Integration von KI-Anwendungen, 2025.

[305] Brundage et al., The Malicious Use of Artificial Intelligence, 2018, S. 43 ff.; Vorberg The (Dis)informed Citizen S. 117.

[306] → § 32 Rn. 63 ff.; Helberger/Kleinen-v. Königslöw/van der Noll Info 17 (2015), 50.

[307] Die Datenethikkommission der Bundesregierung spricht in diesem Zusammenhang von „Medienintermediäre[n] mit Torwächterfunktion", denen sie ein „hohes Gefährdungspotential" für die Demokratie beimisst, Gutachten, S. 46 und 208.

derzeit übliche Unterscheidung zwischen traditionellen Medienunternehmen einerseits und Internetplattformen andererseits in Bezug auf Werberegulierung, Besteuerung, Programmstandards, Vielfalt und redaktionelle Unabhängigkeit nicht mehr aufrechterhalten werden? Welche Verantwortung tragen Informationsintermediäre für „fake news" und die Filterung von Informationen im Allgemeinen? Sollen bzw. müssen die Nutzer – gerade in Ansehung der demokratietheoretischen Implikationen – (besser) über die Personalisierung von Inhalten aufgeklärt werden? Ist die Personalisierung von Informationen bzw. deren Vermittlung gesetzgeberisch zu begrenzen? Muss womöglich gar der Algorithmus selbst reguliert werden, um eine angemessene Medien- und Meinungsvielfalt zu gewährleisten?

Wenngleich all diese Fragen berechtigt sind, sollte auf der anderen Seite auch bedacht **139**
werden, dass es immer noch **keine gesicherten wissenschaftlichen Erkenntnisse** über die Existenz von **Echokammern** und **Filterblasen** gibt. Einige Studien deuten darauf hin, dass der Einfluss personalisierter Medienangebote auf den Nutzer sehr viel geringer sein könnte als angenommen, da die meisten Menschen über Mediengewohnheiten verfügen, die ihnen dabei helfen, Echokammern und Filterblasen zu vermeiden.[308]

Der **Digital Services Act** (DSA)[309] will mit seinen Vorgaben zur Meldung, Kontrolle, **140**
Moderation und Streitbeilegung für Inhalte auf Online-Plattformen hier Abhilfe schaffen. Der DSA definiert dabei vor allem eine Reihe von **Sorgfalts- und Transparenzpflichten,** die Vermittlungsdienste bei der Inhaltemoderation und weiteren Beschränkungen von Nutzerinhalten beachten müssen. Dabei wird hinsichtlich der Pflichten nach Art und Größe des Dienstes differenziert. Besonders weitreichende Pflichten gelten für sehr große Online-Plattformen **(Very Large Online Platforms, VLOPs)** und sehr große Suchmaschinen, die eine durchschnittliche monatliche Zahl von mindestens 45 Mio. aktiven Nutzern im Monat haben. VLOPs müssen eine **jährliche Risikoanalyse** durchführen (Art. 34 DSA), so zB zu Hate-Speech-Kampagnen, Fake-News und die Beeinflussung von Wahlen, und Maßnahmen zur Risikominimierung ergreifen (Art. 35 DSA). Sie unterliegen zudem einmal jährlich einer **unabhängigen Prüfung** (Art. 37 DSA) und **Transparenzberichtspflichten** (Art. 42 DSA). VLOPs müssen ihren Nutzern zudem ermöglichen, Empfehlungssysteme zu nutzen, die nicht auf einem Profiling iSd Art. 4 Nr. 4 DS-GVO beruhen (Art. 38 DSA).

Zwar will der DSA der **Verbreitung rechtswidriger Online-Inhalte** und den gesell- **141**
schaftlichen Risiken, die die Verbreitung von **Desinformation** mit sich bringen kann, entgegenwirken (Erwgr. 9 DSA). Dennoch fällt die Erzeugung von **Inhalten durch generative KI (einschließlich Deepfakes)** nicht unter den **DSA,** da generative KI weder ein Vermittlungsdienst iSd Art. 3 lit. g i DSA, eine Caching-Leistung iSd Art. 3 lit. g ii DSA noch ein Hostingdienst iSd Art. 3 lit. g iii DSA ist.[310] Generative KI-Anwendungen sind auch keine Online-Suchmaschinen (Art. 3 lit. f DSA), denn solche liegen nach Art. 3 lit. f DSA ebenfalls nur dann vor, wenn es sich um einen Vermittlungsdienst handelt.[311]

Im Rahmen der **Verhandlungen zur KI-VO** wurde vom Europäischen Parlament **142**
vorgeschlagen, KI-basierte Empfehlungssysteme **(recommender systems),** die von VLOPs verwendet werden, als Hochrisiko-KI-Systeme einzustufen.[312] Dieser Vorschlag konnte sich jedoch nicht durchsetzen.[313] Die KI-VO stuft lediglich solche Systeme als **Hochrisiko-KI-Systeme** ein, die bestimmungsgemäß dazu verwendet werden sollen, um das **Ergebnis einer Wahl** oder eines Referendums oder das **Wahlverhalten** zu beeinflussen (Anhang III.8.b. KI-VO).

---

[308] Dubois/Blank Information, Communication & Society 21 (2018), 1; Moeller/Helberger Beyond the filter bubble, 25.6.2018; Appel, Die Psychologie des Postfaktischen/Messingschlager/Holtz S. 91 ff.

[309] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 277/1.

[310] Ausführlich hierzu Ebers/Quarch ChatGPT-Hdb/Ebers § 2 Rn. 42 ff.

[311] Hacker/Engel/Maurer Regulating ChatGPT and other Large Generative AI Models, 2023, S. 16.

[312] Abänderung 740 des EU-Parlaments P9_TA(2023)0236.

[313] Krit. Bayer TP 48 (2024) 102741; Martini/Wendehorst/Ruschemeier KI-VO Anh. III Rn. 88.

143 Auch die in **Art. 50 Abs. 4 KI-VO** vorgesehene **Regelungen zu Deepfakes** ist **unzureichend,** da die Vorschrift den Betreiber nur zur **Offenlegung** verpflichtet, dass Inhalte künstlich erzeugt oder manipuliert wurden. Nicht nur lässt sich diese Regelung leicht umgehen; sie ist zudem kaum durchsetzbar, da eine Überprüfung nicht praktikabel ist.[314] Insbesondere die vorsätzliche Verbreitung von Deepfakes wird auf diese Weise nicht verhindert.

4. Beeinflussung und Manipulation von Kunden

144 Der Einsatz von Microtargeting führt ferner zu einer **neuen Form der Macht- und Informationsasymmetrie** und zugleich zu einer **Erosion der Privatautonomie.**[315]

145 Big Data und Profiling eröffnen den Unternehmen die Möglichkeit, einen detaillierten, individuellen Einblick in die persönlichen Verhältnisse des Kunden, seine Verhaltensmuster und sein Persönlichkeitsprofil zu erhalten. Dies erlaubt den Unternehmen neue Formen des Einsatzes gezielter Werbestrategien und **Manipulationsmöglichkeiten.** Die Verhaltensökonomik konnte hunderte Effekte ausmachen, die allesamt zeigen, dass das menschliche Entscheidungsverhalten in vielen Situationen irrational, aber dennoch vorhersehbar ist und dementsprechend auch ausgenutzt werden kann.

Beispiel 10:

Produkte können einem Kunden genau dann angeboten werden, wenn dieser – beispielsweise aufgrund der Tageszeit oder eines vorangegangenen Ereignisses – nur suboptimale Entscheidungen treffen kann. Dieses sog. Emotional Targeting wird bereits von vielen Unternehmen gezielt eingesetzt. So hat zB das US-Werbeunternehmen MediaBrix[316] ein System entwickelt, das in Echtzeit die Emotionen von Computerspielern analysiert und diese dann in besonders geeigneten Momenten (während sog. Breakthrough Moments) direkt durch personalisierte Werbung anspricht.

146 Bereits dieses Beispiel zeigt, dass die Technik des Microtargeting ein **hohes Missbrauchspotenzial** aufweist. Unternehmen können durch die Auswertung personenbezogener Daten – gestützt auf die Erkenntnisse der Verhaltensökonomik – **kognitive und voluntative Schwächen der Kunden** systematisch ausnutzen oder durch sachfremde Anreize manipulieren.

147 Ob und inwieweit das geltende (europäische) **Verbraucherrecht** (→ Rn. 148) sowie das (nationale) **Zivilrecht** (→ Rn. 149) in der Lage sind, ein solches Verhalten wirksam zu sanktionieren, ist zweifelhaft. Neuere Entwicklungen im **Datenschutzrecht** haben demgegenüber dafür gesorgt, dass personalisierte Werbung nur noch unter sehr eingeschränkten Bedingungen möglich ist (→ Rn. 150).

148 Ob Microtargeting nach der **Richtlinie über unlautere Geschäftspraktiken 2005/29/EG (UGP-RL)** überhaupt als unlautere Geschäftspraktiken eingestuft werden kann, ist derzeit ungeklärt.[317] Probleme ergeben sich vor allem daraus, dass die Tatbestände der UGP-RL sehr eng gefasst sind und die ihr zugrunde liegenden **Leitbilder des „durchschnittlichen" und „verletzlichen" Verbrauchers** nicht dynamisch an die Eigenschaften des konkreten Adressaten anknüpfen, sondern statisch an die Zugehörigkeit zu einer bestimmten Gruppe, ohne die Erkenntnisse der Verhaltensökonomik und der Kognitionswissenschaften ausreichend zu berücksichtigen.[318] Das Phänomen des „Behavioral Micro-

[314] Dazu Becker CR 2024, 353 ff.

[315] IE auch Mik Law, Innovation and Technology 8 (2016), 1; SVRV Verbraucherrecht 2.0 S. 58 ff.; ferner → § 6 Rn. 28.

[316] Pritz Mood Tracking S. 140 f.

[317] Vgl. auch Europäische Kommission SWD(2024) 230 final S. 169: „EU consumer law cannot be considered sufficiently effective or clear in addressing the multifaceted concerns regarding commercial personalisation".

[318] Duivenvoorde Journal of European Consumer and Market Law 2 (2013), 69.