DATEN(SCHUTZ) ALS NICHT-PREISBEZOGENER WETTBEWERBSFAKTOR

Arno Scharf

Universitätsassistent (prae doc), Universität Wien, Institut für Unternehmens- und Wirtschaftsrecht
Schottenbastei 10-16, 1010 Wien, AT
Arno.Scharf@univie.ac.at; https://unternehmensrecht.univie.ac.at

Schlagworte: ***Digitalökonomie, Datenschutz und Wettbewerb, Daten als Wettbewerbsfaktor, Privacy Fixing, Kartellverbot, Art 101 AEUV***

Abstract: *Daten stellen einen unerlässlichen Inputfaktor für Geschäftsmodelle der digitalen Wirtschaft dar. Neben verbraucher- und datenschutzrechtlichen Aspekten wirft der Umgang mit (Nutzer)Daten spannende Fragen des Wettbewerbsrechts auf. Der vorliegende Beitrag geht der Frage nach, ob Vereinbarungen zwischen Unternehmen über die Einhaltung derselben Datenschutzstandards – ähnlich wie Preisabsprachen – unter das Kartellverbot nach Art. 101 AEUV bzw. § 1 KartG fallen. Zu diesem Zweck wird untersucht, inwiefern die Datenschutzpolitik von Unternehmen einen Wettbewerbsfaktor darstellt und welche Auswirkungen die Ausgestaltung des Datenschutzrechts auf den Wettbewerb hat.*

1. Kartellverbot

Art. 101 AEUV[1] bzw. § 1 KartG[2] verbieten Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, die eine Beschränkung des Wettbewerbs bezwecken oder bewirken. Zur Konkretisierung wird das Kartellverbot um eine Liste von Beispieltatbeständen ergänzt. Die koordinierte Festsetzung von An- oder Verkaufspreisen ist Teil dieses Beispielkatalogs und ist unstrittig eine kartellrechtswidrige Absprache.[3]

Kündigen bspw. zwei führende Online-Datingplattformen an, ihre monatlichen Mitgliedsbeiträge gegenüber ihren Nutzern auf einen einheitlichen Betrag von jeweils EUR 10 festzusetzen, stellt dies eine *per se* unzulässige Preisabsprache nach Art. 101 Abs. 1 lit. a AEUV bzw. § 1 Abs. 2 Z. 1 KartG dar. Wie ist jedoch das folgende Szenario zu bewerten? Online-Datingplattformen schließen eine Vereinbarung, nach der zum Schutz der Privatsphäre gänzlich auf den Verkauf von Nutzerdaten verzichtet wird, um einen neuen einheitlichen (Datenschutz)Standard für die gesamte Online-Dating Industrie zu etablieren. Aus Sicht des Verbraucher- sowie Datenschutzes erscheinen solche Praktiken grundsätzlich begrüßenswert, weil hochsensible Nutzerdaten vor Werbetreibenden besser geschützt werden. Aus kartellrechtlicher Sicht stellt sich jedoch eine zentrale Frage: Stellt eine Reform der Datenschutzpraktiken im eben beschriebenen Sinn eine kartellrechtswidrige Vereinbarung über die Einhaltung derselben Datenschutzstandards dar (sog. *Privacy Fixing*)?[4] Wie diese Frage zu beantworten ist, hängt vor allem davon ab, ob der Schutz der Privatsphäre einen (nicht-preisbezogenen) Wettbewerbsfaktor darstellt, der dann Gegenstand einer kartellrechtswidrigen Vereinbarung sein kann.

---

1 Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung), ABl. C 2012/326, 1.

2 Bundesgesetz gegen Kartelle und andere Wettbewerbsbeschränkungen, BGBl. I 2005/61 i.d.F. BGBl. I 2017/56.

3 Schuhmacher in Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union[62.EL], C.H. Beck, München 2017, Art. 101 Rz 1.

4 Vgl. Dryden/Iyer, Privacy Fixing and Predatory Privacy: The Intersection of Big Data, Privacy Policies and Antitrust, in CPI Antitrust Chronicle 2017, The Digital Economy (Part 1) – Antitrust Risks, S. 53.

2. Geschäftsmodell digitaler Plattformen

Um Internetdienste kartellrechtlich zu beurteilen, ist es unerlässlich, ein Verständnis für das Funktionieren zwei- bzw. mehrseitiger Märkte zu entwickeln. Viele Geschäftsmodelle der digitalen Wirtschaft basieren auf dem Konzept mehrseitiger Plattformen. Dieses Phänomen beschreibt die gleichzeitige Bedienung mehrerer Gruppen von Nachfragern (durch einen Anbieter), die mittels indirekter (Netzwerk)Effekte aufeinander einwirken.[5] Ein Netzwerkeffekt wirkt dann indirekt, wenn der Nutzen der Plattform für eine Nutzergruppe (bspw. für die Händler oder Werbetreibenden) von der Größe einer anderen Nutzergruppe (bspw. der Verbraucher) abhängt.[6] Je attraktiver der auf der Plattform angebotene Inhalt, desto interessanter ist die Plattform für die Nutzer und desto attraktiver wird sie auch für Werbekunden.

Eine Besonderheit zweiseitiger Plattformen liegt darin, dass die Nutzer für die Inanspruchnahme der Plattformleistung regelmäßig keinen bzw. nur einen sehr geringen monetären Preis entrichten. Die eigentliche Bezahlung erfolgt durch die Preisgabe persönlicher Daten[7] oder indem den Inhalten und der Werbung der Plattform Aufmerksamkeit geschenkt wird.[8] Die aus den Daten gewonnenen Informationen versetzen den Plattformbetreiber in die Lage, zielgerichtet Werbung zu schalten sowie sein Produkt- bzw. Dienstleistungsportfolio zu erweitern und zu verbessern.[9] Überdies manifestiert sich bei zahlenden Nutzergruppen wie bspw Werbeanbietern die Bereitschaft zur Mehrbezahlung für nutzerorientierte Werbung. Die vom einzelnen Internetnutzer – mehr oder weniger freiwillig – zur Verfügung gestellten Daten fungieren im Internet als eine Art Zahlungsmittel.[10] Insofern stellen Daten einen unerlässlichen Inputfaktor für digitale Geschäftsmodelle dar[11] und spielen eine entscheidende Rolle für den wirtschaftlichen Erfolg von Unternehmen im Wettbewerb.[12]

3. Eigenschaften von Daten

Der Datenbegriff ist selbstverständlich nicht nur für die Internetökonomie von herausragender Bedeutung. Die Besonderheit der Digitalwirtschaft liegt allerdings in der Menge an Daten, auf der viele Geschäftsmodelle basieren. Aus diesem Grund sind Daten sowie damit verbundene Verhaltensweisen wohl erst durch die Erfassung von Internetsachverhalten in den Fokus wettbewerblicher Ermittlungen gerückt.[13]

Daten sind durch ökonomische Besonderheiten gekennzeichnet: Sie können zur gleichen Zeit durch mehrere Unternehmen erhoben und genutzt werden und sind damit nicht-rivalisierend.[14] Zudem sind Daten regelmäßig nicht exklusiv. Die Sammlung von Daten durch ein Unternehmen schließt andere Marktakteure grundsätzlich

---

5 Vgl dazu grundlegend Rochet/Tirole, Platform Competition in Two-Sided Markets, Journal of the European Economic Association 2003, S. 990; Armstrong, Competition in two-sided markets, Rand Journal of Economics 2006, S. 668; Caillaud/Jullien, Chicken & Egg – Competition among Intermediation Service Providers, Rand Journal of Economics 2003, S. 309; Evans, Some Empirical Aspects of Multi-Sided Platform Industries, Review of Network Economics 2003, S. 191.

6 Höppner/Grabenschröer, Marktabgrenzung bei mehrseitigen Märkten am Beispiel der Internetsuche, NZKart 2015, S. 162 (S.162).

7 Höppner/Grabenschröer, NZKart 2015, S. 162 (S. 164); Dewenter/Rösch/Terschüren, NZKart 2014, S. 387 (S. 389).

8 Kühling/Gauss, Expansionslust von Google als Herausforderung für das Kartellrecht, MMR 2007, S. 751 (S. 752); Babey, Kartellrechtliche Anforderungen an Suchmaschinen, Dissertation, Zürich 2010, S. 55; Ott, Ich will hier rein! Suchmaschinen und das Kartellrecht, MMR 2006, S. 195 (S. 197).

9 Dewenter, Digitale Ökonomie: Herausforderungen für die Wettbewerbspolitik, Wirtschaftsdienst 2016, S. 236 (S. 237).

10 Hoofnagle/Whittington, Free: Accounting for the Costs of the Internet's Most Popular Price, UCLA Law Review 2014, S. 606 (S. 626 ff.).

11 Monopolkommission, Sondergutachten 68, 2015, Rz 108; Acquisti/Taylor/Wagman, The Economics of Privacy, Journal of Economic Literature 2016, S. 442 (S. 444).

12 Kaben, Die Bedeutung von Daten für den Wettbewerb zwischen Suchmaschinen in Körber/Immenga (Hrsg.), Daten und Wettbewerb in der digitalen Ökonomie, Nomos, Baden-Baden 2017, S. 124.

13 Holzweber, Daten in der Fusionskontrolle, NZKart 2016, S. 104 (S. 105).

14 Nuys, «Big Data»: Die Bedeutung von Daten im Kartellrecht, WuW 2016, S. 512 (S. 513); Surblyte, Competition Law at the Crossroads in the Digital Economy – Is it All About Google? EuCML 2015, S. 170 (S. 175); Rubinfeld/Gal, Access barriers to Big Data, S. 37 ff., https://ssrn.com/abstract=2830586 (alle Websiten zuletzt aufgerufen am 10. Dezember 2017).

nicht davon aus, ebendiese Daten zu sammeln und einen korrespondierenden Datenbestand aufzubauen.[15] Daten sind ubiquitär und können in ihrer Gesamtheit von keinem Unternehmen ausschließlich besessen werden.[16] Darüber hinaus sind Daten nicht verbrauchbar. Von wenigen Ausnahmen abgesehen, sind Daten daher mehrfach nutzbar bzw anwendbar.[17] Zudem besteht die Möglichkeit, Daten von dritten Parteien (sog. *Data Broker*) zuzukaufen.[18]

Für den wirtschaftlichen Erfolg von Unternehmen dürfen Datenmenge, -qualität und -verfügbarkeit allerdings nicht überbewertet werden.[19] Zwar sind Daten eine notwendige Ressource für die Entwicklung datenbasierter Geschäftsmodelle. Sie stellen jedoch zunächst nur eine Abfolge von Zeichen (z.B. Zahlen, Buchstaben, Symbolen, etc.) dar, die nach bestimmten Regeln (Syntax) zusammengesetzt werden und auf einem beliebigen Datenträger (Papier, Festplatte, externer Server, etc.) niedergelegt sind.[20] Aus diesem Grund sind sie in unaufbereiteter Form für das Unternehmen im Wettbewerb meist wertlos oder von nur geringem wirtschaftlichen Nutzen.[21] Erst wenn Daten durch den jeweiligen Kontext ein Bedeutungsgehalt (Semantik) zugewiesen werden kann, spricht man von Informationen.[22] Maßgeblich ist insofern die Fähigkeit des Unternehmens – mithilfe entsprechender Technologien – die für das jeweilige Geschäftsmodell relevanten Informationen aus den gesammelten Datenbeständen zu extrahieren und diese anschließend gewinnbringend zu verwerten.[23] Dabei ist zu berücksichtigen, dass Daten bzw. die ihnen innewohnenden wirtschaftlich wertvollen Informationen eine relativ kurze Halbwertszeit aufweisen und angesichts der Dynamik digitaler Märkte schnell veralten.[24] Aktuelle Informationen sind demnach weit wertvoller als historische.

4. Datenschutzpolitik der Unternehmen als Wettbewerbsfaktor

Die Datenschutzpolitik von Unternehmen und damit der Umgang mit (Nutzer)Daten stellt – ähnlich wie die Produktqualität – einen nicht-preisbezogenen Wettbewerbsfaktor dar.[25] Die Qualität des Angebots von Internetplattformen kann u.a. daran gemessen werden, ob dieses datenschutzfreundlich ausgestaltet ist oder nicht.[26] Verbraucher, die besonderen Wert auf einen sensiblen Umgang mit ihren Nutzerdaten legen, sind geneigt, Anbieter zu wählen, die nur wenige Daten erheben. Insofern kann die Bereitstellung datenschutzfreundlicher

---

15 Sokol/Comerford, Antitrust and Regulating Big Data, George Mason Law Review 2016, S. 1129 (S. 1137).

16 Ebenda.

17 Nuys, WuW 2016, S. 512 (S. 513); Colangelo/Zeno-Zencovich, Online Platforms, Competition Rules and Consumer Protection in Travel Industry, EuCML 2016, S. 75 (S. 83).

18 Unter Hinweis auf die mit dem Ankauf von Daten verbundenen Nachteile BKartA/Autorité de la concurrence, Competition Law and Data, Mai 2016, S. 38 ff.

19 Körber, «Ist Wissen Marktmacht?» Überlegungen zum Verhältnis von Datenschutz, «Datenmacht» und Kartellrecht – Teil 1, NZKart 2016, S. 303 (S. 306).

20 Clement/Schreiber, Internetökonomie[2], Springer, Berlin 2013, S. 52; Specht, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, S. 288 (S. 290).

21 Nuys, WuW 2016, S. 512 (S. 515).

22 Clement/Schreiber, Internetökonomie[2], Springer, Berlin 2013, S. 52.

23 Kaben in Körber/Immenga (Hrsg.), Daten und Wettbewerb in der digitalen Ökonomie, Nomos, Baden-Baden 2017, S. 124 (S. 127, 131,146); Graef, Market Definition and Market Power in Data: The Case of Online Platforms, World Competition 2015, S. 473 (S. 479); Lambrecht/Tucker, Can Big Data Protect a Firm from Competition? in CPI: Internet Competition and Regulation of Online Platforms 2016, S. 155 (S. 159f); Sokol/Comerford, George Mason Law Review 2016, S. 1138 f.

24 Nuys, WuW 2016, S. 513; Schepp/Wambach, On Big Data and Its Relevance for Market Power Assessment, JECLAP 2016, S. 120 (S. 122); Rubinfeld/Gal, Access barriers to Big Data, S. 37 ff., https://ssrn.com/abstract=2830586.

25 Kommission 3. Oktober 2014, COMP/M.7217, *Facebook/WhatsApp*, Rz 87; Kommission 6. Dezember 2016, COMP/M.8124, *Microsoft/LinkedIn*, Rz 350, FN 330; BKartA, Big Data und Wettbewerb, Schriftenreihe «Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft», 12, http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_1.pdf?__blob=publicationFile&v=3; «Ist Wissen Marktmacht?» Überlegungen zum Verhältnis von Datenschutz, «Datenmacht» und Kartellrecht – Teil 2, NZKart 2016, S. 348 (S. 349); Schepp/Wambach, JECLAP 2016, S. 123 f.

26 Colangelo/Maggiolino, Data Protection in Attention Markets – Protecting Privacy through Competition? JECLAP 2017, S. 363 (S. 366).

Angebote Nutzer attraktivieren, weshalb Unternehmen um die Einhaltung hoher Datenschutzstandards miteinander in Wettbewerb treten.

4.1. Privacy Paradox

Nutzer von kostenlosen Internetplattformen legen ihre persönlichen Daten regelmäßig offen, um von den Vorteilen des digitalen Angebots möglichst schnell und unkompliziert profitieren zu können. Dabei nehmen die Internetnutzer die mit der Preisgabe ihrer persönlichen Daten einhergehenden (datenschutzrechtlichen) Risiken und Gefahren oft in Kauf.[27]

Gleichzeitig sind Verbraucher über die übermäßige Sammlung und Verwertung ihrer persönlichen Daten besorgt und fordern die Beachtung ihrer Privatsphäre (sog. *Privacy Paradox*).[28] Insofern spielt die Einhaltung von Datenschutzstandards eine entscheidende Rolle für die Bildung und Stärkung des Vertrauens der Öffentlichkeit in Staat und privatwirtschaftliche Unternehmen.[29] Anbieter, die datenschutzrechtliche Vorgaben einhalten, profitieren im Wettbewerb grds. von erhöhter Unternehmens- und Markenreputation.

4.2. Grenzen der wettbewerblichen Analyse

Im Bereich kostenloser Internetdienste werden datensparsame Angebote von den Nutzern allerdings nicht zwingend als qualitativ hochwertig eingestuft.[30] Studien[31] zeigen, dass Konsumenten bereits für einen kleinen (Preis-)Nachlass bereit sind, persönliche Daten preiszugeben. Wieder andere Forschungsergebnisse zeigen, dass Konsumenten unter bestimmten Voraussetzungen bereit sind, einen höheren Preis für mehr Privatsphäre zu bezahlen.[32]

Die Heterogenität der Studienergebnisse lässt sich darauf zurückführen, dass die Inhalte vieler Internetplattformen immer stärker am jeweiligen Nutzer orientiert sind, weshalb sich die Qualität eines digitalen Dienstes auch nicht verallgemeinern lässt. Zudem variiert die Sensibilität der Nutzer in Bezug auf den Umgang mit ihren Daten stark.[33] Manche Nutzer ziehen kostenfreie Dienste jenen vor, die mit weniger Daten auskommen und umgekehrt. Dies hat zur Folge, dass der Schutz der Privatsphäre als Qualitätsfaktor eines digitalen Dienstes von verschiedenen Nutzergruppen unterschiedlich bewertet werden kann.[34] Im Gegensatz zu Preissenkungen, die von den Konsumenten grundsätzlich als für sie vorteilhaft wahrgenommen werden, ist das Konzept einer «besseren» bzw. einer umfangreicheren Privatsphäre nicht immer klar.[35] Insofern erscheint die Ermittlung eines geeigneten Maßstabes problematisch, anhand dessen die Qualität der jeweiligen Datenschutzpolitik des Unternehmens (als Wettbewerbsfaktor) bewertet werden kann.

---

27 Colangelo/Maggiolino, JECLAP 2017, S. 368; Europäischer Datenschutzbeauftragter, Privacy and competitiveness in the age of big data, Preliminary Opinion 2014, Rz 74.

28 Brandimarte/Acquisti, The Economics of Privacy, in Peitz/Waldfogel (Hrsg.), The Oxford Handbook of the Digital Economy, New York 2012, S. 563; Norberg/Horne/Horne, The Journal of Consumer Affairs 2007, S. 100; Boston Consulting Group, The Value of our Digital Identity (2012), S. 12, 14, 26, 43 und 44, http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf.

29 Mantelero, Competitive value of data protection: the impact of data protection regulation on online behaviour, International Privacy Law 2013, S. 229 (S. 230).

30 Europäischer Datenschutzbeauftragter, Privacy and competitiveness in the age of big data: The Interplay between data protection, competition law and consumer protection in the digital economy, Preliminary Opinion 2014, Rz 74.

31 Preibusch/Kübler/Beresford, Price versus privacy: an experiment into the competitive advantage of collecting less personal information, Electron Comm Res 2013, S. 423; Norberg/Horne/Horne, The Journal of Consumer Affairs 2007, S. 100.

32 Shostack/Syverson, What Price Privacy (and why identity theft is about neither identity nor theft), in Economics of Information Security (2004) S. 129 ff.; Tsai/Egelmann/Cranor/Acquisti, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Information Systems Research 2011, S. 254.

33 Brandimarte/Acquisti, The Economics of Privacy, in Peitz/Waldfogel (Hrsg.), The Oxford Handbook of the Digital Economy, New York 2012, S. 562 f.; Tucker, The Proper Role of Privacy in Merger Review, CPI Antitrust Circle 2015 (2), S. 1 (S. 3).

34 Schepp/Wambach, JECLAP 2016, S. 124.

35 Tucker, CPI Antitrust Circle 2015 (2), S. 3.

4.3. Risiko eines «race to the bottom»

Der Versuch von Internetplattformen, mit datensparsamen Angeboten bzw. mit hohen Datenschutzstandards bei Verbrauchern zu punkten, ist bislang weitgehend erfolglos geblieben.[36] Dies ist u.a. darauf zurückzuführen, dass Verbrauchern aufgrund der hohen Marktkonzentration in der Digitalökonomie oft keine alternativen Ausweichmöglichkeiten zur Verfügung stehen, die die gleiche Qualität oder Nutzerdichte wie etablierte Unternehmen aufweisen. Zudem senken Netzwerkeffekte, die die Stellung marktstarker Unternehmen weiter verfestigen, den Anreiz für Unternehmen, datenschutzfreundliche Produkte, Dienstleistungen oder Technologien zu entwickeln.[37] Insofern besteht im Zusammenhang mit der Datenschutzpolitik der Unternehmen auch die Gefahr eines *race to the bottom*, wonach die Missachtung von datenschutzrechtlichen Standards sowie die wettbewerbswidrige Erschleichung von Daten ein Ausdruck von Marktmacht sein kann.[38]

5. Datenschutzrecht als Wettbewerbshindernis

Geht man von einem Konditionenwettbewerb zwischen Unternehmen um den besten Datenschutz aus (siehe Punkt 4.), kommt zwangsläufig auch dem Datenschutzrecht als gesetzgeberischer Begrenzung unternehmerischer Verhaltensspielräume maßgebliche Bedeutung zu. Datenschutzrecht zielt zwar grds. nicht auf die Regulierung von Märkten ab, kann dies aber unter Umständen bewirken und sich auf den Wettbewerb auswirken bzw. diesen verzerren.[39]

5.1. Unterschiedliche Datenschutzstandards als Wettbewerbsvor/-nachteil

Konkurrieren Unternehmen um den bestmöglichen Schutz der Privatsphäre, können sich unterschiedliche Datenschutzstandards verschiedener Staaten als problematisch erweisen. Plattformbetreibern aus weniger datensensiblen Jurisdiktionen kann ein Wettbewerbsvorteil gegenüber jenen Anbietern zukommen, die strengeren Datenschutzregelungen unterliegen.[40] Dieses Problem soll durch die neue EU-Datenschutzgrundverordnung[41] («EU-DSGVO»), die ab dem 25. Mai 2018 in der Europäischen Union gilt[42] und ein wettbewerblich einheitliches *level playing field* für Unternehmen der Internetbranche schaffen soll, zumindest auf europäischer Ebene gelöst werden.[43]

5.2. Datenschutz als (indirektes) Regulativ des Wettbewerbs

«*Wenn Daten so etwas wie die ‹Währung des Internets› sind, ist Datenschutz dann eine Art staatliche Preisregulierung?*»[44]. Dieser von Körber[45] aufgeworfene (plakative) Vergleich hat etwas für sich. Je mehr Konstellationen durch die Vorgaben des Datenschutzrechts und damit des Staats abschließend erfasst werden, desto weniger Raum bleibt für den unternehmerischen Wettbewerb um die Einhaltung hoher Datenschutzstandards. Das nationale Datenschutzrecht wirkt damit indirekt auch als Regulativ des Wettbewerbs um den besten Datenschutz.

---

36 So waren bspw. die datensparsame Suchmaschine *DuckDuckGo* oder das soziale Netzwerk *StudiVZ*, das mit hohen Datenschutzstandards versucht hat, *Facebook* Konkurrenz zu machen, nur mäßig erfolgreich.

37 Colangelo/Maggiolino, JECLAP 2017, S. 366.

38 Europäischer Datenschutzbeauftragter, Privacy and competitiveness in the age of big data, Preliminary Opinion 2014, Rz 74; Grunes, Another look at privacy, George Mason Law Review 2013, S. 1107 (S. 1112).

39 Körber, NZKart 2016, S. 349.

40 Monopolkommission, Sondergutachten 68, 2015, Rz 93.

41 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 2016/119, 1.

42 Art. 99 Abs. 2 EU-DSGVO.

43 ErwG. 9 ff. EU-DSGVO.

44 Körber, NZKart 2016, S. 349.

45 Körber, NZKart 2016, S. 349 f.

5.3. Datenschutz als Innovationsbremse

In Zeiten von *Big Data* ist es einerseits wichtig, die Daten der Bürger vor unbefugten Eingriffen Dritter zu schützen. Andererseits läuft ein besonders restriktives Datenschutzregime, das die ökonomische Dimension von Daten für Geschäftsmodelle der digitalen Wirtschaft verkennt, Gefahr, den technisch-innovativen Fortschritt zu bremsen und die Wettbewerbsfähigkeit der europäischen Wirtschaft zu beeinträchtigen.[46] Zu strenge Maßstäbe bergen das Risiko, Verbrauchern Geschäftsmodelle der digitalen Wirtschaft vorzuenthalten oder Internetnutzern einen monetären Preis aufzudrängen, obwohl diese bei freier Wahl die Offenlegung ihrer persönlichen Daten präferiert hätten.

Sog. *Opt-In*-Modelle ermöglichen Verbrauchern bessere Kontrolle über ihre Daten, weil die (rechtmäßige) Verwendung von Nutzerdaten dann von der ausdrücklichen Zustimmung der Nutzer abhängt.[47] Problematisch ist hierbei allerdings, dass eine obligatorische Einwilligung der Nutzer zu einer Bevorteilung bestimmter Geschäftsmodelle führen kann. So könnten bspw. Werbedienste, die mit dem Nutzer nicht direkt in Kontakt stehen und ihre Daten durch anonymisiertes *Tracking* erheben, gegenüber Anbietern mit Registrierungspflicht benachteiligt werden, die die Zustimmung der Nutzer im Rahmen des Registrierungsprozesses einholen.[48] Spontane kostenlose Geschäftsmodelle werden durch *Opt-In*-Ansätze, die die Nutzung eines Dienstes von der vorherigen Nutzerregistrierung abhängig machen, ausgeschlossen bzw. deren Nutzung zumindest wesentlich verkompliziert.[49] Alternativ sind für viele Internetdienste sog. *Opt-Out*-Modelle verfügbar, nach denen sich Nutzer bspw. von bestimmten Maßnahmen, die in deren Privatsphäre eingreifen (bspw. *Tracking*), ausnehmen lassen können.[50]

5.4. Datenschutz als Marktzutrittsschranke

Letztlich kann sich ein zu strenger Datenschutz als Marktzutrittsschranke für neue Marktakteure erweisen.[51] Dies gilt vor allem für Datenschutzstandards, die es Unternehmen verbieten, ihre Daten zu teilen[52] oder es neuen Anbietern auf andere Weise *de facto* unmöglich machen, Datenbestände in einem Ausmaß aufzubauen, die für die (Weiter-)Entwicklung von Geschäftsmodellen der digitalen Wirtschaft erforderlich sind.

Dasselbe gilt auch für datenschutzrechtliche Vorgaben, die Anbieter mit hohen Kosten belasten.[53] In diesem Zusammenhang ist auf das Recht auf Datenportabilität nach Art. 20 EU-DSGVO hinzuweisen.Unter bestimmten Voraussetzungen hat jede Person das Recht, «*die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten,* […].» Die Vorschrift dient dazu, die Übertragung von Kundendaten auf andere Unternehmen zu ermöglichen. Aus wettbewerblicher Sicht trägt die Bestimmung dazu bei, mögliche *Lock-In*-Effekte abzuschwächen, Wechselkosten zu senken sowie die Marktstellung jener Unternehmen, die auf der Sammlung und Verwertung von Daten aufbaut, angreifbarer zu machen.[54]

Problematisch ist allerdings die Kostenlast, die mit der Aufbereitung der Daten in einem den Vorgaben der Verordnung entsprechenden Format und deren anschließender Portierung verbunden sind. Gerade für *Start-*

---

46 Körber, NZKart 2016, S. 350.

47 Newman, Antitrust and Economics of the Control of User Data, Yale Journal on Regulation 2014, S. 401 (S. 448); Monopolkommission, Sondergutachten 68, 2015, Rz 103.

48 Monopolkommission, Sondergutachten 68, 2015, Rz 104.

49 Körber, NZKart 2016, S. 350.

50 Dewenter/Lüth, Big Data: eine ökonomische Perspektive in Körber/Immenga (Hrsg.), Daten und Wettbewerb in der digitalen Ökonomie, Nomos, Baden-Baden 2017, S. 18.

51 Dewenter/Lüth in Körber/Immenga (Hrsg.), Daten und Wettbewerb in der digitalen Ökonomie, Nomos, Baden-Baden 2017, S. 25.

52 Körber, NZKart 2016, S. 350.

53 Ebenda.

54 Europäischer Datenschutzbeauftragter, Privacy and competitiveness in the age of big data, Preliminary Opinion 2014, Rz 83; Monopolkommission, Sondergutachten 68, 2015, Rz 105; Schepp/Wambach, JECLAP 2016, S. 124.

Ups sowie für KMUs kann der Aufwand und die Kosten für die Entwicklung einer entsprechenden Portierungssoftware eine Hürde für den Markteintritt darstellen.[55] Einer Studie[56] zufolge zieht die Umsetzung der EU-DSGVO für kleine und mittlere Unternehmen jährliche IT-Mehrkosten nach sich, die – abhängig von der jeweiligen Industrie – zwischen EUR 3'000 und EUR 7'200 pro Unternehmen liegen und damit 16–40% des durchschnittlichen IT-Jahresbudgets ausmachen.

5.5. Exkurs: Datenschutz und Absprachen über die Aufteilung von Märkten

Während ein zu strenger Datenschutz zu Marktzutrittsschranken führen kann (siehe Punkt 5.4.), birgt ein zu geringer Datenschutz die Gefahr, dem Plattformbetreiber Verhaltensspielräume zu belassen, mit denen ebenfalls kartellrechtliche Probleme einhergehen können.[57] Mithilfe verschiedenster Technologien (*Internet-Cookies, Referral-Links, Tracking Bugs, Device-* oder *Browser-Fingerprinting*) ist es Unternehmen bspw. möglich, die Internetaktivitäten der Nutzer – insb. ihr Konsum- und Suchverhalten – zu verfolgen.[58] Auf diese Weise kann das Verhalten der Nutzer analysiert und deren Zahlungsbereitschaft bestimmt werden.

Es ist eine gängige Praxis vieler Internetplattformen, Preisniveaus in *Online-Shops* mit grenzüberschreitendem Zugang anhand der länderspezifischen Bonität bestimmter Bevölkerungsgruppen festzulegen und unterschiedliche Preise für dasselbe Produkt an Verbraucher verschiedener Herkunft zu verrechnen. Diese Handelspraxis wird – mithilfe von *Geo-Tracking-Tools* – regelmäßig durch Blockierung des Zugangs zu oder der unumkehrbaren Weiterleitung auf Websites anderer Mitgliedstaaten oder durch Verweigerung grenzüberschreitender Lieferung oder Zahlung realisiert.[59] Gleichermaßen kommen technische Vorkehrungen zum Einsatz, die die Zugehörigkeit des Nutzers zu einem anderen Mitgliedsstaat erkennen und ohne Weiterleitung im selben Shop automatisch einen anderen Gesamtpreis ausweisen.

Derartige Differenzierungen können neben der künstlichen Aufteilung des Binnenmarkts in den Anwendungsbereich des Kartellverbots nach Art. 101 AEUV fallen. Dies gilt insb. für *Geoblocking*-Maßnahmen, die auf Vereinbarungen oder abgestimmten Verhaltensweisen zwischen unterschiedlichen Unternehmen beruhen, die darauf abzielen, nationale Grenzen abzuschotten oder die gegenseitige Durchdringung der nationalen Märkte zu erschweren.[60] Darüber hinaus können nationale Preisdifferenzierungen in Online-Shops zulasten von Nutzern fremder Herkunft diskriminierend und damit missbräuchlich im Sinne des Kartellrechts sein. Das Verbot des Marktmachtmissbrauchs nach Art. 102 AEUV verbietet es Unternehmen nämlich, Abnehmer durch die Festsetzung unterschiedlicher Preise unmittelbar oder bloß mittelbar unbillig zu diskriminieren.[61] Ende November 2017 haben sich Unterhändler des Europäischen Parlaments, der Mitgliedstaaten und der Kommission

---

55 Swire/Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, Maryland Law Review 2013, S. 335 (S. 352); Vanberg/Ünver, The Right to Data Portability in the GDPR and EU Competition Law, European Journal of Law and Technology 2017; selbst *Facebook* als etabliertes Unternehmen spricht im Zusammenhang mit der Entwicklung und Aktualisierung entsprechender Portierungssoftware von einer «*technisch komplexen Herausforderung*» (*Facebook*, Response to European Commission Communication on personal data protection in the European Union, 5, http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/facebook_en.pdf.

56 Christensen/Colciago/Etro/Rafert, The Impact of the Data Protection Regulation in the EU, European Financial Review 2013, S. 72.

57 Dewenter/Lüth in Körber/Immenga (Hrsg.), Daten und Wettbewerb in der digitalen Ökonomie, Nomos, Baden-Baden 2017, S. 25.

58 Acquisti/Taylor/Wagman, Journal of Economic Literature 2016, S. 463.

59 Kommission, Abschlussbericht über die über die Sektoruntersuchung zum elektronischen Handel vom 10. Mai 2017, COM(2017) 229 final, Rz 45.

60 Kommission, COM(2017) 229 final, Rz 48.

61 Hüttenlauch/Lübbig in Loewenheim/Meessen/Riesenkampff/Kersting/Meyer-Lindemann, Kartellrecht[3], C.H. Beck, München 2016, Art. 102 AEUV Rz 205; Jung in Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union[61.EL], C.H. Beck, München 2017, Art. 102 Rz 189; Fuchs/Möschel in Immenga/Mestmäcker, EU-Wettbewerbsrecht I/2[5], C.H. Beck, München 2012, Art. 102 Rz 378 f.

darauf geeinigt, dass ungerechtfertigtes *Geoblocking* im Online-Handel in bestimmten Konstellationen verboten wird.[62]

6. Conclusio

Die wettbewerbliche Relevanz von Daten für Geschäftsmodelle der Digitalökonomie ist unbestritten.[63] Nutzer, die besonderen Wert auf den sensiblen Umgang mit ihren Daten legen, greifen vermehrt auf datensparsame Dienste zurück. Die Datenschutzpolitik von Unternehmen bzw. der Umgang mit (Nutzer)Daten stellt damit einen nicht-preisbezogenen Wettbewerbsfaktor dar. Unternehmen konkurrieren um den bestmöglichen Schutz der Privatsphäre und versuchen, sich durch datenschutzfreundliche Angebote von ihren Wettbewerbern abzugrenzen.

Der Wettbewerb um den bestmöglichen Schutz der Privatsphäre wird durch Vereinbarungen, wonach sich zwei Unternehmen verpflichten, dieselben Datenschutzstandards einzuhalten, beschränkt (sog. *Privacy Fixing*). Das trifft bspw. auf die eingangs beschriebene Angleichung der Datenschutzpolitik zweier Online-Datingplattformen zu. Vereinbarungen dieser Art sind im Ergebnis nicht anders zu bewerten als kartellrechtlich verpönte Preisabsprachen. Absprachen zwischen Unternehmen über die Einhaltung derselben Datenschutzstandards verstoßen damit – ebenso wie Preisabsprachen – gegen das Kartellverbot. Kartellrechtliche Verantwortlichkeit kann sich in diesem Zusammenhang auch insb. für Unternehmensvereinigungen ergeben, die Datenschutzstandards festlegen, die über bloß unverbindliche Empfehlungen hinausgehen.[64] Ob und inwiefern *Privacy Fixing* zukünftig Eingang in kartellrechtliche Verfahren findet, bleibt insofern mit Spannung abzuwarten. Aufgrund der fortschreitenden Digitalisierung rückt der Problemkreis rund um den Umgang mit Daten jedenfalls zunehmend in den Fokus der Wettbewerbsbehörden.

---

62 Kommission, Pressemitteilung 20. November 2017, IP/17/4781, http://europa.eu/rapid/press-release_IP-17-4781_de.htm; vgl auch Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 25. Mai 2016 über Maßnahmen gegen Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts sowie zur Änderung der Verordnung (EG) 2006/2004 und der Richtlinie 2009/22/EG, COM(2016) 289 final.

63 Colangelo/Maggiolino, JECLAP 2017, S. 369.

64 Dryden/Iyer in CPI Antitrust Chronicle 2017, The Digital Economy (Part 1) – Antitrust Risks, S. 61.