

# Datenkapitalismus – eine ökonomische Betrachtung

Im Datenkapitalismus sind neue Kommunikationsunternehmen entstanden, deren Angebot als „umsonst“ erscheint. Ihr Geschäftsmodell basiert darauf, dass die Nutzer (Kunden) ihre Daten preisgeben und dafür entweder ein nachgefragtes Gut (Kommunikation, Medien, Waren und Dienstleistungen) ohne oder für geringere monetäre Zahlungen erhalten. Wie die Unternehmen die Daten verwenden, wissen die Nutzer in der Regel nicht, auch der pekuniäre Wert ihrer Daten lässt sich nicht einfach ermitteln. Ganz wichtig sind also mehr Transparenz und Kontrolle. Die neue Datenschutz-Grundverordnung macht zwar Datenportabilität möglich und unterstützt damit den Wettbewerb innerhalb der EU, sie lässt sich aber in der Praxis schwer wirksam umsetzen.

Tobias Kretschmer

## Innovation und Datenschutz – von datenbasierten Geschäftsmodellen und deren Chancen und Gefahren

Datengetriebene Geschäftsmodelle beflügeln seit einigen Jahren die Phantasien der Anleger und Unternehmer, und auch etablierte Unternehmen suchen dieser Tage mit ständig wachsenden Datenanalyse-Abteilungen nach dem heiligen Gral der kommerziellen Verwendung von Daten. Zu Anfang profitierten datengetriebene Unternehmen noch von der vergleichsweise laxen Regulierung und insbesondere der Naivität der Verbraucher. In langen Allgemeinen Geschäftsbedingungen (AGB) waren weitreichende Einwilligungsklauseln enthalten, die Unternehmen das Recht gaben, nahezu unbeschränkt persönliche Daten zu speichern, kommerziell zu verwenden und schließlich an Drittunternehmen zu verkaufen. Im Zuge dessen sind junge Unternehmen mit innovativen Geschäftsmodellen und Diensten massiv gewachsen und haben auch etablierten Unternehmen zum Teil den Rang abgelaufen. Mittlerweile hat sich sowohl die öffentliche Meinung als auch die regulatorische Sichtweise auf datengetriebene Geschäftsmodelle und deren Chancen und Risiken geändert, und die vor kurzem in Kraft getretene Datenschutz-Grundverordnung (DSGVO) versucht, den Spagat zwischen Verbraucherschutz und Innovationsanreizen zu ermöglichen. In diesem Zusammenhang ergeben sich eine Reihe an Fragen, die es zu beantworten gilt.

„Daten sind das neue Öl“: Die EU-Politikerin Meglena Kuneva prägte im Jahr 2009 diese Aussage zur Bedeutung von Daten für die Weltwirtschaft. Wie zutreffend ist diese Aussage? Es gibt sicher eine Menge Parallelen zwischen den beiden – insbesondere die Tatsache, dass Öl seinerzeit zwingend notwendig für fortschreitendes Wirtschaftswachstum und für die Durchführung verschiedenartigster Transaktionen, insbesondere Firmenkundengeschäft (Business-to-Business) waren. Daten nehmen mittlerweile einen Teil dieser Rolle ein, zumal viele Produkte und Dienstleistungen digital angeboten und vertrieben werden, sodass Daten für diese Transaktionen ebenso wichtig sind wie früher Öl.

Allerdings gibt es auch einige entscheidende Unterschiede. So ist Öl ein sogenanntes privates Gut, dessen Besitz exklusiv ist – wenn mir ein Liter Öl gehört, kann er nicht gleichzeitig jemand anderem gehören. Daten hingegen sind prinzipiell nicht exklusiv, da ich sie auch mehreren Nutzern zur Verfügung stellen kann, ohne dass sie mir dadurch weniger gehören. Ein zweiter Unterschied ist, dass Daten im Verbund bzw. in größeren Mengen überproportional an Wert gewinnen, durch Netzeffekte. Das heißt, dass durch die Verbindung verschiedenartiger und großer Datenmengen deutlich mehr Wert geschaffen

wird, als durch gleichartige oder geringe Datenmengen. Ein dritter Unterschied, der eng mit dem zweiten in Verbindung steht, ist, dass persönliche Daten für den Verbraucher selbst verhältnismäßig geringen Wert haben, diese aber im Aggregat für Unternehmen sehr wertvoll sein können. Das hat in der Vergangenheit dazu geführt, dass Verbraucher bereitwillig Informationen preisgegeben haben, auf der anderen Marktseite aber ein enormer kommerzieller Wert entstand. Bei Öl bzw. irgendeinem anderen physischen Gut ohne derartige Netzeffekte wären Verbraucher nicht so großzügig.

Welche Geschäftsmodelle nutzen Daten und wie vollzieht sich die Transformation von Daten in Erlöse? Geschäftsmodelle, die Daten nutzen, sind natürlich sehr vielfältig. Generell kann man aber zwischen zwei großen Gruppen unterscheiden: Die eine Gruppe handelt mit Daten, die andere Gruppe nutzt Daten. In die zweite Gruppe kann man die klassischen „Tech-Giganten“ eingruppiieren. Unternehmen wie Amazon, Netflix etc. leben davon, dass sie bessere Empfehlungssysteme (Recommender Systems) haben als ihre konventionellen Mitbewerber und sie somit in der Lage sind, bessere und auf die Präferenzen des Kunden zugeschnittene Angebote zu machen. Diese Unternehmen verwenden die persönlichen Daten ihrer Kunden, um diese an sich zu binden und ihnen passgenaue Angebote zu machen. Das ist attraktiv, weil die Wahrscheinlichkeit eines Kaufs höher ist und natürlich auch die Zahlungsbereitschaft. Die erste Gruppe sind Datenhändler. Diese Unternehmen sammeln oftmals Daten durch Plug-ins oder Aggregationssoftware und verkaufen diese dann an Dritte. Die Transparenz in diesem Markt ist deutlich geringer, insbesondere da dem Verbraucher oft gar nicht bewusst ist, welches Unternehmen die Daten sammelt und wohin sie verkauft werden. Persönliche Daten an Werbetreibende zu verkaufen, ist da noch vergleichsweise harmlos. Aber beispielsweise können auch Anbieter von Finanzdienstleistungen oder Versicherungen derartige Daten beziehen und Risikoeinschätzungen vornehmen. Für solche Zwecke würden viele Verbraucher ihre persönlichen Daten wohl eher nicht bereitstellen – insbesondere in Deutschland.

### Funktionsweise

Wie lässt sich die Datenfreigabe durch die Verbraucher ökonomisch erklären? Solange sich die Verbraucher dessen bewusst sind, ist die Informationsübergabe als Akzeptanz eines Preises (in Form von Daten) zu interpretieren. Verschiedene Studien haben gezeigt, dass Verbraucher bereit sind, für Privatheit zu zahlen. Man kann sich hier eine Smartphone-App vorstellen, z.B. ein Spiel, das einmal in der kostenlosen Version erhältlich ist, die allerdings ein Einverständnis für die Datensammlung

durch die App verlangt. Die App mit derselben Funktionalität gibt es dann noch ohne dieses Einverständnis, aber mit einem Kaufpreis. Studien haben gezeigt, dass ein beträchtlicher Anteil der Verbraucher bereit ist, einen moderaten Preis für mehr Privatheit zu zahlen. Im Umkehrschluss heißt das dann, dass ein Verbraucher, der sich für die kostenlose Variante entscheidet, in Form von persönlichen Daten für den gleichen Service zahlt.

Entscheidend ist allerdings die Transparenz dieses „Preises“ für den Verbraucher. Wenn ich ein solches Einverständnis in ewig langen AGBs verstecke, ist dem Verbraucher mitunter nicht bewusst, wie viel und an wen er jetzt Daten preisgibt. Entsprechend haben gerade soziale Netzwerke, die oft von Jugendlichen genutzt werden und somit eine besondere Verantwortung tragen, den Prozess transparenter gestaltet. Die Aussagen, denen zugestimmt wird, sind zwar oft immer noch tendenziös („stimme zu, dass meine Daten zum Zweck des verbesserten Kundenerlebnisses genutzt werden“), aber insbesondere wird jetzt häufiger deutlich gemacht, ob die Daten vom Dienst selbst genutzt oder an Dritte weiterverkauft werden, also ob das eine oder das andere Geschäftsmodell hiermit verfolgt wird.

### Transparenz und Quantifizierung

Die DSGVO macht Datenportabilität möglich. Um mit Daten als ökonomischem Instrument umgehen zu können, muss der Verbraucher aber genau wissen, wer seine Daten zu welchem Zweck verwendet und verknüpft. Wie lässt sich das erreichen? Letztlich gibt es nur zwei Möglichkeiten: Entweder ich lege einen einzigen Standard fest und „erlaube“ somit nur bestimmte Geschäftsmodelle. Das ist transparent und leicht verständlich für den Verbraucher, läuft aber Gefahr, innovative Geschäftsmodelle zu bremsen. Zum Beispiel ist Onlinewerbung nur möglich geworden, weil die Clickstreamdaten kommerziell genutzt wurden, was vorher nicht möglich war. Mittlerweile wird der Großteil der Werbebudgets für Onlinewerbung ausgegeben. Die Alternative ist, dass Verbraucher selbst in der Verantwortung stehen und gegebenenfalls in standardisierter und übersichtlicher Form sehen können, für welche Zwecke der Anbieter die Daten verwenden möchte. Hier würden innovativen Geschäftsmodellen weniger Restriktionen auferlegt. Allerdings besteht dabei die Gefahr, dass Verbraucher sich nicht die Mühe machen (wie es jetzt bereits der Fall ist), die unterschiedlichen Verwendungszwecke zu verstehen und schließlich zwischen verschiedenen Modellen zu wählen. Somit muss, auch bei allen Zwischenformen, zwischen der Beschränkung innovativer Geschäftsmodelle und der Gefahr un- oder fehlinformierter Verbraucher, abgewogen werden.

Letztlich wissen die Verbraucher nicht, was ihre Daten tatsächlich wert sind. Wie kann der Wert der Daten quantifiziert werden? Verbraucher wissen das nicht, das ist richtig, aber sie kümmern sich ja auch nicht um die Monetarisierung. Am ehesten sind vermutlich Unternehmen in der Lage, den Wert von persönlichen Daten abzuschätzen. So kommen dann auch die exorbitanten Summen zustande, die bei Übernahmen in der Technologieindustrie geboten und letztlich auch gezahlt werden. Oft sind die Übernahmekandidaten ja wenig mehr als ein Datenfundus, die vom übernehmenden Unternehmen zu Erlösen gemacht werden. Der Wert persönlicher Nutzerdaten ändert sich ständig mit den möglichen Verwendungsmöglichkeiten. Mittlerweile wissen Unternehmen ziemlich genau, wieviel Nutzerdaten für personalisierte Werbung wert sind, aber inwieweit neue Dienste zu einem profitablen Geschäftsmodell gemacht werden können, ist oft höchst unklar.

### Wer profitiert?

Kommt es durch den Einsatz von Daten zu Verzerrungen der Marktverhältnisse, etwa dadurch, dass die Verbraucher in eine zunehmend ungünstige Position geraten? Zu-

## Autoren des Zeitgesprächs



**Prof. Dr. Tobias Kretschmer** ist Inhaber des Lehrstuhls für Strategie, Technologie und Organisation an der Ludwig-Maximilians-Universität München.



**Jun.-Prof. Dr. Lukas Wiewiorra** ist Inhaber der Juniorprofessur für Wirtschaftsinformatik in der Abteilung Wirtschaftsinformatik und Informationswirtschaft der Goethe-Universität Frankfurt am Main.



**Prof. Dr. Jan Krämer** ist Inhaber des Lehrstuhls für Wirtschaftsinformatik mit Schwerpunkt Internet- und Telekommunikationswirtschaft an der Universität Passau.



**Prof. Dr. Andreas Oehler** ist Inhaber des Lehrstuhls für Betriebswirtschaftslehre, insbesondere Finanzwirtschaft, an der Otto-Friedrich-Universität Bamberg, und Direktor der Forschungsstelle „Verbraucherfinanzen und Verbraucherbildung“.



**Matthias Horn, M. Sc.**, ist wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Betriebswirtschaftslehre, insbesondere Finanzwirtschaft, an der Otto-Friedrich-Universität Bamberg.



**Prof. Dr. Justus Haucap** ist Direktor des Düsseldorf Institute for Competition Economics (DICE) an der Heinrich-Heine-Universität in Düsseldorf.



**Prof. Dr. Stefan Klein** ist Inhaber des Lehrstuhls für Wirtschaftsinformatik und Interorganisationssysteme an der Universität Münster.



**Joschka Hüllmann** ist wissenschaftlicher Mitarbeiter des Lehrstuhls für Wirtschaftsinformatik und Interorganisationssysteme an der Universität Münster.

nächst eröffnen mehr Daten Möglichkeiten, einen Markt effizienter zu gestalten. Personalisierte Werbung, Empfehlungen, individualisierte Produkte etc. sind attraktiver für Verbraucher und Unternehmen als generische, One-size-fits-all-Angebote. Die entscheidende Frage ist aber, wie dieser Informations- und demnach Wohlfahrtsgewinn auf Verbraucher und Unternehmen verteilt wird. Wenn personalisierte Werbung oder Angebote zu weniger Wettbewerb führen, weil andere Angebote gar nicht an den speziellen Kunden herangetragen werden, geht der Hauptanteil an Unternehmen. Wenn hingegen weiterhin Wettbewerb und gegebenenfalls mehr Transparenz herrscht, können Verbraucher zu ähnlichen, wettbewerblich bestimmten Preisen, Güter oder Dienste beziehen, die besser auf ihre Bedürfnisse passen. Dann wäre der Hauptnutzen beim Verbraucher. Ich habe den Eindruck, dass das Pendel momentan eher in Richtung der Unternehmen ausschlägt, weshalb die DSGVO ja auch zum Zweck hat, mehr Transparenz und Informationen auf Seiten der Verbraucher zu schaffen.

### Wachstumspotenzial

Wie ist zusammenfassend die Rolle von Daten und deren Nutzung im Hinblick auf nachhaltiges Wirtschaftswachstum einzuschätzen?

Zunächst ist zu betonen, dass Daten ja schon im Zentrum der sogenannten Informations- und Kommunikationstechnologierevolution waren. Hier wurden durch die zunehmende Digitalisierung von Geschäfts- und Produktionsprozessen enorme Produktivitätsfortschritte und Wachstumsraten erzielt. Somit ist die kommerzielle und systematischere Verwendung von Daten lediglich eine Weiterentwicklung eines bereits früher begonnenen Trends. Allerdings ist in verschiedenen Studien belegt, dass der Wachstumsbeitrag von Informationstechnologien im Zeitverlauf zunimmt, und dass ein Teil dieser Zunahme der Expertise von Unternehmen, mit Informationstechnologien umzugehen, geschuldet ist. In diesem Wachstumsprozess enthalten sind allerdings tiefgreifende Umwälzungen der Wirtschafts- und Marktstruktur. Die eingangs erwähnten Datenanalyse-Abteilungen erfordern neue Fähigkeiten und somit neue Ausbildungsschwerpunkte, neue Unternehmen werden etablierte verdrängen, und manche Geschäftsfelder werden selbst für progressive Unternehmen nicht zu erschließen sein. Die Innovationskraft der Unternehmen ist allerdings immer in Verbindung mit den Verbraucherrechten zu bringen – ähnlich wie es Umweltstandards erst nach einer Phase der Experimente seitens der Unternehmen gab, werden sich auch Standards bezüglich der Datenverarbeitung im Zeitverlauf herausbilden und sich ähnlich schnell wie die Geschäftsmodelle selbst verändern.

Lukas Wiewiorra

## Transparenz und Kontrolle in der Datenökonomie

Bei der Nutzung von Internetangeboten, mobilen Applikationen und vernetzter Hardware werden von den bereitstellenden Unternehmen regelmäßig personenbezogene Daten gespeichert. Im Internet ermöglicht es die Kombination verschiedener Trackingverfahren und Indikatoren (z. B. Cookies, Tracking-Pixel, Fingerprinting etc.), das Nutzungsverhalten von Konsumenten zu protokollieren. Aus dieser Datenbasis können beispielsweise Rückschlüsse auf individuelle Vorlieben, Gewohnheiten, aber auch die Zahlungsbereitschaft von Nutzern gezogen werden. Großen Internetkonzernen (z. B. Facebook, Google) ist es durch die weit verbreitete Integration ihrer Funktionen möglich, Daten von Konsumenten auch über die Grenzen verschiedener Onlineangebote und Webdienste hinweg zu sammeln. Auch vernetzte („smarte“) Geräte wie z. B. Mobiltelefone, Fernsehgeräte, Lautsprecher und sogar Spielzeuge können Nutzungsdaten speichern und diese an den Hersteller übertragen. In Abhängigkeit vom jeweiligen Rechtsraum werden Anwender von Unternehmen in diesem Zusammenhang um ihre Zustimmung gebeten (opt-in), können widersprechen (opt-out) oder haben nur durch technische Gegenmaßnahmen (z. B. Tor-Browser) die Möglichkeit, die Datenerhebung einzuschränken bzw. auf bestimmte Funktionen oder die Verwendung zu verzichten.

Neben dieser passiven Datenerhebung stellen Nutzer aber auch aktiv Daten bereit, die sie auf digitalen Plattformen (z. B. sozialen Netzwerken) teilen oder bei der Verwendung von digitalen Diensten gegenüber dem Betreiber preisgeben (z. B. Online-Shop, Messenger). Dabei können die Dienstbetreiber auch personenbezogene Daten von Konsumenten speichern, die den betreffenden digitalen Dienst selbst nicht nutzen. So werden beispielsweise durch die Freigabe von Adressbuchdaten an einen Messenger-Dienst Informationen über Personen ohne deren Wissen bzw. Einverständnis gespeichert. Dadurch können von diesen Personen partielle Profile (Schattenprofile) erstellt werden. Darüber hinaus haben Unternehmen die Möglichkeit, Daten, die bei der Nutzung digitaler Dienste gespeichert werden, mit Informationen von Offline-Transaktionen zu verknüpfen. Dies kann beispielsweise durch den Einsatz von Kundenkarten, Coupons oder die Identifikation bzw. Ortsinformationen von Smartphones erreicht werden.

Individuelle Profile von Konsumenten erlauben es Unternehmen, kundenspezifische Angebote zu unterbreiten, sowie Produkte und Dienstleistungen zu personalisieren.

Aber auch in pseudonymisierter oder aggregierter Form können diese Daten genutzt werden, um beispielsweise die erwartete Nachfrage zu bestimmen, Trends genauer vorherzusagen und Produkte zu optimieren.

### Privacy

Privacy ist ein vielschichtiges Konzept. Es kann z. B. als Kontrolle über personenbezogene Daten sowie als Schutz gegen unerwünschten Zugriff auf diese verstanden werden, aber auch als Wahrung der eigenen Freiheit und Privatsphäre.<sup>1</sup> Konsumenten können Privacy also sowohl einen intrinsischen Wert beimessen als auch den Wert von Privacy über mögliche Vorteile einer Freigabe bzw. den Wert des Schutzes ihrer Daten bestimmen. Menschen haben dabei unterschiedliche Auffassungen darüber, welche Informationen sie als sensibel oder privat und damit schützenswert einstufen. Dazu zählen Aspekte wie das Gefühl beobachtet zu werden oder die Sorge vor Bloßstellung. Die Besorgnis von Konsumenten im Hinblick auf ihre Privacy hängt von verschiedenen Faktoren ab, wie z. B. der wahrgenommenen Gefährdung, wahrgenommener Kontrolle, Transparenz, dem Vertrauen in das beteiligte Unternehmen, negativen Erfahrungen und dem Kontext der Transaktion.

Konsumenten sind darüber besorgt, dass regelmäßig personenbezogene Daten von ihnen gespeichert und verarbeitet werden. 2014 gaben 80 % der durch das Pew Research Center befragten US-amerikanischen Nutzer sozialer Medien an, über den Zugriff von Werbetreibenden und Firmen auf ihre Daten besorgt zu sein, gleichzeitig stimmten 91 % der Befragten der Aussage zu, dass Konsumenten die Kontrolle darüber verloren haben, wie personenbezogene Daten über sie erhoben und verwendet werden.<sup>2</sup>

Im Hinblick auf die möglichen Konsequenzen einer Freigabe personenbezogener Daten (bzw. dem Verzicht auf ihren Schutz) spielt Transparenz eine entscheidende Rolle. Die Bereitstellung von Datenschutzerklärungen soll dazu beitragen, dass Konsumenten in diesem Kontext eine informierte Entscheidung treffen können. Dies ist

1 A. Acquisti, C. Taylor, L. Wagman: The economics of privacy, in: Journal of Economic Literature, 54. Jg. (2016), H. 2, S. 442-492.

2 Pew Research Center: Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014, [http://assets.pewresearch.org/wp-content/uploads/sites/14/2014/11/PI\\_PublicPerceptionsofPrivacy\\_111214.pdf](http://assets.pewresearch.org/wp-content/uploads/sites/14/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf) (9.7.2018).

für den Nutzer jedoch mit einem hohen Aufwand verbunden: Es wurde geschätzt, dass die Opportunitätskosten eines US-amerikanischen Konsumenten alle (als Privatperson relevanten) Datenschutzbestimmungen digitaler Dienste zu lesen im Jahr 2008 bei 743 US-\$ lagen; falls die Bestimmungen nur selektiv nach bestimmten Aspekten überprüft werden sollen, lagen die Kosten immer noch bei 468 US-\$.<sup>3</sup> Da nur ein sehr geringer Anteil der Konsumenten diese Erklärungen tatsächlich liest,<sup>4</sup> ließe sich daraus schlussfolgern, dass Konsumenten – im Gegensatz zu ihrer geäußerten allgemeinen Besorgnis – dem Schutz ihrer Daten keinen entsprechend hohen Wert beimessen. Andere Erklärungsansätze für dieses vermeintliche Paradoxon basieren auf begrenzter Rationalität, da es fraglich ist, ob Konsumenten diese Flut an Informationen überhaupt sinnvoll verarbeiten können.

Dabei sind die Folgen der Preisgabe von personenbezogenen Daten für Konsumenten nur schwer einzuschätzen und selten quantifizierbar. Im Gegensatz zu Unternehmen, die diese Daten verarbeiten, fehlt Konsumenten üblicherweise das Wissen, um das gesamte Ausmaß der Datensammlung und die Verfahren bei der Auswertung und Verarbeitung großer Datenmengen korrekt einzuschätzen. Daher existiert eine Informationsasymmetrie zwischen Unternehmen, die Daten sammeln und verarbeiten, und Kunden, die diese über sich preisgeben bzw. schützen.

Um über die Freigabe einer bestimmten Teilmenge von Daten zu entscheiden, müssten Konsumenten unter anderem beurteilen, welche(n) ...

- Wert die Preisgabe ihrer Daten für sie selbst erzeugt (z.B. Personalisierung, Verbesserung der Service-Qualität);
- Wert ihre Daten für verarbeitende Unternehmen haben;
- Rückschlüsse durch ihre Daten in Bezug auf sie selbst durch die Auswertung großer Datenmengen gezogen werden können (z. B. Zahlungsbereitschaft);
- Konsequenzen ihre Datenfreigabe und die darauf basierenden Rückschlüsse für sie haben können (z.B. Preisdiskriminierung);

3 A. M. McDonald, L. F. Cranor: The cost of reading privacy policies, in: *I/S: A Journal of Law and Policy for the Information Society*, 4. Jg. (2008), H. 3, S. 543.

4 V. C. Plaut, R. P. Bartlett III: Blind consent? A social psychological investigation of non-readership of click-through agreements, in: *Law and Human Behavior*, 36. Jg. (2012), H. 4, S. 293.

- Daten mit Dritten ausgetauscht und wie diese verarbeitet werden;
- Risiken bestehen, dass ihre Daten entwendet und missbraucht werden bzw. welche Konsequenzen sich daraus für sie ergeben können.

Darüber hinaus müssten Konsumenten berücksichtigen, welche Daten bereits über sie gespeichert wurden, also den Wertbeitrag der (zusätzlich) freigegebenen Daten bestimmen. Da die Preisgabe von personenbezogenen Daten oft untrennbar mit anderen Transaktionen (z.B. dem Einkauf in einem Online-Shop, der Kommunikation mit Freunden in einem sozialen Netzwerk) verbunden ist, müssten sie dabei von dem konkreten Kontext einer spezifischen Transaktion abstrahieren und die möglichen Konsequenzen der Datenfreigabe in anderen Kontexten beurteilen (z. B. Angabe des Wohnortes bei einer Bestellung, der ebenso in die Beurteilung der eigenen Bonität eingehen kann). Darüber hinaus müssten Erwartungen darüber gebildet werden, wie sich der Wert der gespeicherten Daten in der Zukunft entwickelt. Es ist unwahrscheinlich, dass Konsumenten die möglichen Konsequenzen ihrer Entscheidung über die Freigabe bzw. den Schutz ihrer personenbezogenen Daten und deren Wahrscheinlichkeiten bekannt sind, oder sie sich eine Vorstellung darüber bilden können.<sup>5</sup>

Zusätzlich können die Entscheidungen von Konsumenten durch behavioristische Effekte verzerrt werden. Beispielsweise bemessen Konsumenten den Wert ihrer Daten unterschiedlich, je nachdem, ob sie für deren Schutz zahlen oder für deren Freigabe eine Kompensation erhalten. Die Kompensation, die Konsumenten erwarten, damit sie Privacy aufgeben, fällt häufig höher aus, als ihre Zahlungsbereitschaft um ihre Privacy herzustellen.<sup>6</sup>

Darüber hinaus wird in einer Reihe von Studien geschlossen, dass Menschen angesichts kurzfristiger Vorteile (z. B. Rabattaktion) Schwierigkeiten haben, zeitkonsistente Entscheidungen unter Berücksichtigung langfristiger Konsequenzen vorzunehmen.<sup>7</sup> So wird durch zusätzliche Daten ein Kundenprofil reichhaltiger, was die Verhandlungsmacht des Unternehmens gegenüber einem Konsumenten in zukünftigen Transaktionen erhöht. Einer einmaligen Entschädigung stehen damit

5 A. Acquisti, J. Grossklags: What can behavioral economics teach us about privacy, in: A. Acquisti, S. Gritzalis, C. Lambrinouidakis, S. di Vimercati: *Digital Privacy: Theory, Technologies and Practices*, Kapitel 18, New York, London 2007, S. 363-377.

6 A. Acquisti, L. K. John, G. Loewenstein: What is privacy worth?, in: *The Journal of Legal Studies*, 42. Jg. (2013), H. 2, S. 249-274.

7 A. Acquisti: Privacy in electronic commerce and the economics of immediate gratification, in: *Proceedings of the 5th ACM conference on Electronic commerce*, Mai 2004, S. 21-29.

wiederkehrende Opportunitätskosten gegenüber. Da Konsumenten Vorteile in naher Zukunft (z. B. Rabatt) stärker gewichten als Vorteile, die sich erst in einer späteren Zeitperiode manifestieren (z. B. durch den Schutz der eigenen Daten), sind sie bereit, kurzfristige Bedürfnisse auf Kosten ihres zukünftigen Selbst zu befriedigen.

### Der Wert von Daten – Verfügbarkeit versus Schutz

Große Internetkonzerne führen an, dass sie durch die Verwertung großer Datenmengen ihre digitalen Dienste kostenfrei einer breiten Masse von Konsumenten zugänglich machen können. Diese Unternehmen sind durch die Auswertung dieser Daten beispielsweise in der Lage, gezielt Werbung anzuzeigen, individuell relevante Suchergebnisse auszugeben oder einschlägige Produkte zu empfehlen. Durch die gezielte Adressierung individueller Präferenzen können die Suchkosten für Konsumenten sinken und eine digitale Plattform kann theoretisch mit höherer Wahrscheinlichkeit ein erfolgreiches Matching (z. B. zwischen Käufer und Verkäufer, Mieter und Vermieter) herstellen. In der Literatur finden sich jedoch Beispiele, in denen Plattformbetreiber keine sozial optimalen Matching-Anreize haben, auch wenn ihnen ausreichende Informationen über die Beteiligten vorliegen. Solche Situationen können z. B. entstehen, falls eine digitale Plattform davon profitieren kann, wenn sie Konsumenten strategisch mit weniger präferierten Unternehmen zusammenführt. Gerade in diesen Fällen ist es hinderlich, dass Unternehmen in der Datenökonomie selten Preise für den Zugang zu ihren digitalen Diensten verlangen. Durch Zugangspreise bestünden für Betreiber Opportunitätskosten strategischer Matchings (bzw. eines sinkenden Nutzungsvolumens), wodurch das Problem zumindest abgeschwächt werden könnte.<sup>8</sup>

Ebenso wie die Freigabe von personenbezogenen Daten möglicherweise negative Effekte für Konsumenten nach sich zieht (z. B. durch Preisdiskriminierung), kann aber auch der Schutz personenbezogener Daten bzw. die Einschränkung von Tracking-Maßnahmen Opportunitätskosten auf Seiten von Unternehmen, Konsumenten und der Gesellschaft verursachen. Durch eine unzureichende Verfügbarkeit von Daten können Ineffizienzen entstehen und die Innovationskraft sowie der Wettbewerb eingeschränkt werden. Etablierte Unternehmen genießen z. B. durch eine überlegene Datenbasis einen Wettbewerbsvorteil gegenüber potenziellen Konkurrenten, da sie dadurch Produkte besser personalisieren und schneller (weiter-)entwickeln können. Eine entsprechende Datenbasis muss von mög-

lichen Wettbewerbern erst aufgebaut werden, um konkurrenzfähige Angebote bereitzustellen, von denen Konsumenten z. B. in Form von günstigeren Preisen profitieren könnten.

Zusammenfassend konnte bisher nicht festgestellt werden, dass die Verfügbarkeit bzw. der Schutz von personenbezogenen Daten unabhängig vom jeweiligen Kontext eine eindeutig positive oder negative Auswirkung auf die Wohlfahrt hat. Der unberechtigte Zugriff auf Datensammlungen hat für verantwortliche Unternehmen allerdings nachweisbar negative ökonomische Konsequenzen.<sup>9</sup> Darüber hinaus beeinflussen solche Vorkommnisse die Reputation und damit das Vertrauen in diese Unternehmen, was wiederum zu höheren Privacy-Bedenken bei Konsumenten führen kann. Dieser Zusammenhang legt nahe, dass Unternehmen, die der Datenökonomie zugeordnet werden, einen starken Anreiz haben, die Daten ihrer Kunden vor dem unbeabsichtigten Zugriff Dritter zu schützen. Fraglich bleibt aber, ob Konsumenten bisher das Ausmaß einschätzen können, in dem nicht nur die Betreiber digitaler Dienste selbst, sondern auch berechtigte Dritte ihre Daten sammeln, aggregieren, auswerten und monetarisieren.

In diesem Kontext stellt sich die Frage, ob Daten als eine Währung des digitalen Zeitalters angesehen werden können. Eine Währung hat verschiedene Eigenschaften. Sie dient als Tausch- bzw. Zahlungsmittel bei Transaktionen, als Recheneinheit und als Mittel zur Wertaufbewahrung. Daten werden offensichtlich als eine Art Tauschmittel verwendet, da Konsumenten diese für Gegenleistungen preisgeben. Personenbezogene Daten haben also offensichtlich einen Wert und können finanzielle Transaktionen ersetzen. Allerdings stellen Daten keine einheitliche Recheneinheit dar, da sich ihr Wert im Kontext der bereits gespeicherten und verfügbaren Daten ergibt und diese damit keine einheitliche Bezugsgröße darstellen. Darüber hinaus können Daten einfach kopiert bzw. erhoben werden und damit zu einem Zeitpunkt gleichzeitig von mehreren Unternehmen genutzt werden (Nicht-Rivalität). Im engeren Sinne sind Daten also keine Währung, können aber durch ihren Wert finanzielle Transaktionen ersetzen.

### Schlussbetrachtung

Die Nutzung vieler digitaler Dienste ist so selbstverständlich geworden, dass sie aus dem Alltag nicht mehr wegzudenken ist. Regulierung muss daher eine Balance fin-

<sup>8</sup> A. Hagiu, B. Jullien: Why do intermediaries divert search?, in: The RAND Journal of Economics, 42. Jg. (2011), H. 2, S. 337-362.

<sup>9</sup> Zum Beispiel A. Malhotra, C. Kubowicz Malhotra: Evaluating customer information breaches as service failures: An event study approach, in: Journal of Service Research, 14. Jg. (2011), H. 1, S. 44-59.

den, die sowohl die Vor- und Nachteile für Konsumenten, Unternehmen und die Gesellschaft in einem spezifischen Kontext bzw. einer Domäne berücksichtigt. Die neue europäische Datenschutz-Grundverordnung enthält daher beispielsweise Transparenzvorschriften für den Fall einer automatisierten Entscheidungsfindung sowie Regelungen zur Auskunftserteilung über die gespeicherten Daten eines Nutzers und einer Übertragung von Daten an Dritte. Mit Blick auf die vorgestellten Erkenntnisse und die Tatsache, dass Konsumenten ständig privacyrelevante Entscheidungen treffen, sollen diese Pflichten von

Unternehmen bzw. die Rechte der Verbraucher um bessere Kontrollmöglichkeiten ergänzt werden. In der Datenschutz-Grundverordnung verfolgt man in diesem Kontext die Konzepte „Privacy by Design & Privacy by Default“, also eine auf die Grundsätze des Datenschutzes ausgelegte Technikgestaltung bzw. Voreinstellungen. Fraglich bleibt, wie diese Konzepte und spezifische Formulierungen (z. B. berechtigtes Interesse) ausgelegt werden und ob zukünftig auch technische Kontrollmöglichkeiten unabhängig von anbieterzentrierten Systemen in Betracht gezogen werden.

Jan Krämer

## Datenschutz 2.0 – ökonomische Auswirkungen von Datenportabilität im Zeitalter des Datenkapitalismus

Nach einem langen politischen Tauziehen ist am 25.5.2018 die neue europäische Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Diese löst die bis dahin geltende europäische Datenschutzrichtlinie (95/46/EC) aus dem Jahr 1995 ab, die aus einer Zeit stammte, als Unternehmen wie Google, Facebook und Amazon nicht existierten oder nicht von Bedeutung waren. Angesichts der aktuellen Berichterstattung sowie der Flut an DSGVO-induzierten E-Mails, die man in den letzten Monaten erhalten hat, muss man eigentlich der Meinung sein, dass die DSGVO eine Revolution und nicht nur eine Evolution der bisherigen Datenschutzstandards in der EU ist: Datenschutz 2.0, maßgeschneidert auf die datenschutzrechtlichen Herausforderungen im Zeitalter des Datenkapitalismus.

### Datenportabilität kommt, Verbotsprinzip bleibt

In der Tat gibt es – aus ökonomischer Sicht – wesentliche neue Elemente in der DSGVO, die die Rechte der betroffenen Personen stärken. Hervorzuheben sind hier insbesondere das Recht auf Löschung („Recht auf Vergessenwerden“) nach Artikel 17 DSGVO sowie das Recht auf Datenübertragbarkeit gemäß Artikel 20 DSGVO. Einige ökonomische Implikationen dieser neuen Rechte werden im Folgenden genauer beleuchtet. Außerdem sieht die DSGVO bei Missachtung der geforderten Datenschutzstandards empfindliche Strafen von bis zu 4 % des weltweiten Jahresumsatzes bzw. einen Mindestbetrag von 20 Mio. Euro vor (Artikel 83 DSGVO). Das verleiht dem Datenschutz-Tiger erstmals Zähne.

Andererseits hält die DSGVO aber am althergebrachten Grundprinzip des europäischen Datenschutzes fest – dem Verbotsprinzip. Demnach ist es Unternehmen (und dem Staat) grundsätzlich untersagt, personenbezogene Daten zu verarbeiten, es sei denn bestimmte Ausnahmetatbestände oder eine explizite Einwilligung des Betroffenen liegen vor (siehe Artikel 6 DSGVO). In der Theorie erscheint dies als wirksames Instrument, um den Betroffenen Kontrolle darüber zu geben, wer personenbezogene Daten erheben darf. In der Praxis kann man jedoch in vielen Fällen infrage stellen, wie bewusst und freiwillig diese Einwilligung tatsächlich gegeben wird. Datenschutzklauseln werden oftmals nicht (sorgfältig) gelesen oder nicht verstanden. Gleichzeitig dehnen Unternehmen mithilfe weitreichender Einwilligungs-Formulierungen den Spielraum der Datenerhebung stark aus. Insbesondere bei marktmächtigen digitalen Diensteanbietern werden die Datenschutzklauseln aber gegebenenfalls schlichtweg nur deshalb akzeptiert, weil die Nutzung dieses Dienstes den Betroffenen alternativlos erscheint; z. B. weil sie befürchten, in die digitale soziale Isolation zu geraten, wenn sie nicht bei bestimmten sozialen Netzwerken vertreten sind. Hier muss sich die Rechtsprechung noch einpendeln und man wird sehen müssen, wie schlussendlich die Grenzen im Sinne des Verbotsprinzips genau gezogen werden.

Etwas grundsätzlicher kann man aber auch die Frage stellen, ob das Verbotsprinzip überhaupt zeitgemäß ist, da es bei der Erhebung und Verarbeitung der Daten und

nicht unmittelbar bei der Abwehr gesellschaftlich nicht wünschenswerter Anwendungsszenarien ansetzt. Aus ökonomischer Sicht ist grundsätzlich gegen die Erhebung von personenbezogenen Daten eigentlich nichts einzuwenden, wenn verantwortungsvoll mit ihnen und den darauf aufsetzenden Datenanwendungen umgegangen wird. Das Verbotsprinzip der DSGVO erhöht zunächst die Hürden (insbesondere für kleinere Unternehmen), Daten überhaupt zu erheben. Durch eine größere Datenverfügbarkeit kann in vielen Fällen aber ein positiver Mehrwert geschaffen werden, z.B. bei der Erkennung und Heilung von Krankheiten oder der Optimierung von Verkehrsflüssen. Oft ist bei der (Möglichkeit zur) Erhebung der Daten aber gar nicht klar, welche Datenverknüpfungen letztlich für eine neue Datenanwendung besonders wichtig sein werden. Der Gewinn von Big Data und Data Analytics liegt ja gerade darin, neue Muster in Daten zu erkennen. Der Grundsatz der Datensparsamkeit und der Zweckbindung nach Artikel 5 Absatz 1 DSGVO in Verbindung mit dem Verbotsprinzip steht aber im Konflikt mit einer zweckunabhängigen Datenerhebung für unbekannte zukünftige Zwecke. Das wird daher auch oft als Innovationshemmnis für europäische Firmen gesehen.

Als Rechtfertigung für das Verbotsprinzip werden oftmals die Dystopien à la Orwell angeführt, z.B. hinsichtlich der Befürchtung, dass Menschen mit gewissen statistischen Eigenschaften in Zukunft keine (bezahlbare) Kranken- oder Kfz-Versicherung mehr erhalten werden. Gleichzeitig werden nach der DSGVO aber keine bestimmten Datenanwendungen ausgeschlossen, sofern eine konkrete Einwilligung für diesen Zweck vorliegt. Eine Kfz-Versicherung basierend auf personenbezogenen Fahrdaten ist also grundsätzlich zulässig. Es liegt in der Verantwortung des Einzelnen und nicht der Gesellschaft, ob dies erwünscht ist. In den USA wird beispielsweise ein gänzlich anderer Ansatz des Datenschutzes gewählt. Hier existiert insbesondere das Verbotsprinzip nicht. Es werden jedoch bestimmte Anwendungsbereiche (z. B. bei der Ermittlung der Kreditwürdigkeit oder im Gesundheitswesen) konkreteren Regelungen unterworfen.<sup>1</sup> Darüber hinaus existieren Einzelfallentscheidungen (Case Law), z.B. Regelungen zum Abhören von Telefonverbindungen (Electronic Communications Privacy Act). Kurzum, es werden konkrete Datenanwendungen, aber nicht die Erhebungen von personenbezogenen Daten reglementiert.

Zukünftig sollte zumindest genauer ausgelotet werden, ob die Vorgehensweise, bei den Datenanwendungen und nicht bei der Datenerhebung anzusetzen – gegebenenfalls sogar in Kombination, in jedem Fall aber im Kontext

von zusätzlichen Datenschutz-Regelungen –, nicht auch in Europa denkbar wäre. Es wäre der ökonomisch sinnvollere, da innovationsfreundlichere Ansatz. Zudem könnten auf diese Weise die möglicherweise negativen Auswirkungen von zukünftigen Regelungslücken in den Datenschutzbestimmungen aufgrund von technischen Weiterentwicklungen (z.B. hinsichtlich der Möglichkeit zur De-Anonymisierung von Daten) abgeschwächt werden. Wenn die Verwendung von personenbezogenen Daten für bestimmte Anwendungen untersagt würde, verringerte dies gegebenenfalls auch die Anreize zur Datenerhebung und könnte gleichzeitig die Akzeptanz sinnvoller Anwendungen stärken.

### Ökonomische Wirkungen des Rechts auf Datenportabilität

Das Recht auf Datenportabilität ist, zusammen mit dem Recht auf Vergessenwerden, ein zentraler neuer Bestandteil der DSGVO. Beide, insbesondere in Kombination, sollen es Nutzern ermöglichen, mehr Kontrolle über ihre personenbezogenen Daten ausüben zu können. Vor allem soll es Nutzern ermöglicht werden, Lock-in-Effekten bei der Nutzung von digitalen Diensten entgegenzuwirken und somit einen Wechsel zu einem alternativen Anbieter wahrscheinlicher machen. Dies ist ein zentrales strategisches Instrument der DSGVO, um den Daten-Oligarchen Google, Facebook, Amazon und Co. etwas entgegenzusetzen und den Wettbewerb um Nutzer zwischen ihnen, aber besonders auch mit neuen Wettbewerbern, anzuhetzen. Diese vordergründigen ökonomischen Effekte, die mit dem Recht auf Datenportabilität (und dem Recht, diese Daten beim alten Anbieter auch wieder zu löschen) einhergehen, sind nachvollziehbar und scheinen zunächst auch im Sinne der Betroffenen. Weitere ökonomische Effekte offenbaren sich jedoch erst bei einem zweiten Blick:

1. Zunächst ergeben sich praktische Fragen der Machbarkeit (z. B., wenn ganze Profile in sozialen Netzwerken portiert werden sollen), nicht nur hinsichtlich des Bezugs auf verlinkte Datensätze, die nicht portiert werden, sondern auch hinsichtlich der Kompatibilität von Datenformaten. Es ist aus ökonomischer Sicht zu erwarten, dass Anbieter, die viel in den Lock-in ihrer Kunden investiert haben, sich bemühen werden, ihre Informationssysteme so zu gestalten, dass eine Datenportierung erschwert wird. Dies gilt insbesondere, da Artikel 20 Absatz 2 DSGVO den Vorbehalt der technischen Machbarkeit einräumt. Außerdem wird per Gesetz nur die Datenportabilität, aber nicht die Interoperabilität zwischen Diensten gefordert. Dennoch kann die Regelung bei weniger komplexen Daten (z. B. Reputationsprofile im eCommerce) greifen und Wettbewerb begünstigen.

<sup>1</sup> Diese sind z.B. im Fair Credit Reporting Act sowie im Health Insurance Portability and Accounting Act verankert.

2. Aus einem Recht auf Datenexport ergibt sich nicht zwangsläufig ein Recht auf Datenimport. Es ist durchaus denkbar, dass das Recht auf Datenportabilität dadurch ausgehebelt werden kann, dass konkurrierende Unternehmen eine stillschweigende Vereinbarung treffen, keine Importfunktion für die Daten des Konkurrenten bereitzustellen. Zwar ist ein Unternehmen zum Export der Daten verpflichtet, nur bringt dies dem Betroffenen im Sinne der Datenportabilität nichts, wenn die Daten nicht auch beim Konkurrenten wieder eingelesen und verarbeitet werden können. Ökonomisch gesehen kann das Recht auf Datenportabilität nämlich zu einer Situation ähnlich eines „Gefangenendilemmas“ führen. Jedes Unternehmen profitiert einseitig von diesem Recht, da es leichter Kunden des Konkurrenten gewinnt, aber letztlich stellen sich beide Unternehmen schlechter, da Datenportabilität die Konkurrenz unter den Unternehmen erhöht (was der beabsichtigte Effekt ist). Antizipieren die Firmen dieses Dilemma, so ist ein möglicher Ausweg, wechselseitig auf Datenimport zu verzichten. Solche stillschweigenden Vereinbarungen in Oligopolsituation sind in der Ökonomie wohlbekannt.
3. Erste ökonomische Arbeiten zu Datenportabilität zeigen, dass digitale Dienstleister nach der Einführung dieses Rechts dazu verleitet werden könnten, noch mehr personenbezogene Daten zu erheben als zuvor. Wohlfarth zeigt beispielsweise in einem spieltheoretischen Modell, dass Kunden mit dem Recht auf Datenportabilität gegebenenfalls eine geringere Konsumentenrente erzielen als dies ohne dieses Recht der Fall war.<sup>2</sup> Dies ist in dem Modell darin begründet, dass der neue Anbieter den durch den einfacheren Wechsel gewonnenen Spielraum zum Anlass nimmt, zusätzliche Kundendaten zu erheben. Ist eine solche Datenerhebung mit Privatheitskosten verbunden, sind Konsumenten am Ende schlechter gestellt. Die gute Nachricht ist jedoch, dass der etablierte, alte Anbieter durch das Recht auf Datenportierung grundsätzlich datensparsamer wird, da er eine stärkere Abwanderung der Kunden befürchten muss.
4. Durch Datenportabilität kann es auch zu Hold-up-Problemen kommen. Die Möglichkeit personenbezogene Daten zu einem Wettbewerber zu portieren, schmälert den Anreiz eines Unternehmens in die Gewinnung (und den Lock-in) von Kunden zu investieren. Konkret ist zu befürchten, dass die Qualität eines (z. B. werbefinanzierten) Angebots sinkt, da mit Datenportabilität nun

mehr Unternehmen Zugang zu den gleichen personenbezogenen Daten haben und somit die Wettbewerbssituation auf dem Daten- bzw. Werbemarkt verschärft wird. Mit anderen Worten, Drittunternehmen könnten als Trittbrettfahrer auf dem Datenmarkt auftreten, was letztlich dem Kunden ebenfalls schaden könnte.

Die obige Aufzählung stellt sicher keine abschließende Liste dar. Es lässt sich aber bereits feststellen, dass das Recht auf Datenportabilität komplexe ökonomische Prozesse auslöst, die weit über die vermeintlich positive Eigenschaft des „einfachen Wechsels“ des Anbieters hinausgehen. Aus theoretischer Sicht können sogar konkrete Nachteile für Kunden aufgezeigt werden, die das Recht auf Datenportabilität mit sich bringen kann. Dies bedeutet selbstverständlich nicht, dass dieses Recht in der Praxis nicht dennoch einen überwiegend positiven Effekt haben kann.

### Mögliche Wettbewerbsimplikationen freiwilliger Datenportabilität zwischen Anbietern

Abschließend soll exemplarisch ein weiteres ökonomisches Beispiel aufgezeigt werden, bei dem die zusätzliche Möglichkeit zur Datenportierung schlussendlich negative Konsequenzen haben kann – in diesem Fall für das kleine Unternehmen, das Daten vom großen Unternehmen importiert. Zusammen mit meinen Kollegen Daniel Schnurr und Michael Wohlfarth haben wir die ökonomische Wirkung des Datenteilens zwischen Dienstleistern mittels der „Login mit Facebook“-Funktion analysiert.<sup>3</sup> Diese Funktion erlaubt es unabhängigen Webseiten, auf die bei Facebook gespeicherten personenbezogenen Daten zuzugreifen, um auf diese Weise den Registrierungsprozess auf der eigenen Webseite zu vereinfachen. Im Gegenzug erhält jedoch auch Facebook wiederum Nutzungsdaten der Webseiten über die jeweiligen Login-Nutzer.

Das Teilen von Daten scheint zunächst attraktiv, da Facebook und die unabhängige Webseite nicht direkt miteinander in Konkurrenz um Nutzer stehen. Die Vereinfachung des Anmeldeprozesses erlaubt es der Webseite aber, sich von anderen, konkurrierenden Webseiten abzuheben und zusätzliche Nutzer zu gewinnen. Letztlich tritt aber auch hier aufgrund der Nicht-Rivalität von Daten in vielen Fällen ein Gefangenendilemma auf. Da die Webseiten und Facebook im Daten- und Werbemarkt doch in Konkurrenz stehen, wird durch das Teilen von Daten die Wettbewerbsfähigkeit von Facebook auf diesem Markt gestärkt. Für

2 M. Wohlfarth: Data Portability on the Internet: An Economic Analysis. Proceedings of International Conference on Information Systems (ICIS 2017), Seoul, Südkorea 2017.

3 Vgl. J. Krämer, D. Schnurr, M. Wohlfarth: Winners, Losers, and Facebook: The Role of Social Logins in the Online Advertising Ecosystem, in: Management Science, im Erscheinen.

die unabhängigen Webseiten ist es aber stets individuell rational, die Login-Funktion zu implementieren, sofern es die konkurrierenden Webseiten noch nicht getan haben. Letztlich implementieren alle Webseiten den Login, stellen sich damit aber schlechter als zuvor, da ihre Daten nun an Facebook abfließen.

Im Gegensatz zu der Argumentation zuvor, ist bei Unterstellung einer hinreichenden Zahl von konkurrierenden (kleinen) Webseiten eine stillschweigende Vereinbarung, den Login nicht zu implementieren, kaum vorstellbar. Die DSGVO hilft auch nicht unmittelbar weiter, denn Nutzer stimmen mit der Nutzung des Logins dem Teilen ihrer Daten zwischen Anbietern explizit zu. In diesem Fall hat Facebook also bereits freiwillig eine Datenportabilität bzw. sogar Dateninteroperabilität eingeführt, da es sich dadurch eine *bessere* Wettbewerbssituation verspricht.

Andreas Oehler, Matthias Horn

## Zur ungleichen ökonomischen Verteilung bei der Datennutzung oder: keine soziale Marktwirtschaft in der digitalen Welt!

Die Datensammlung und die Datenverwertung fokussiert längst nicht mehr nur auf Werbebotschaften oder personalisierte Produktangebote, sondern auf weitreichendes Profiling und Tracking aller erfassbaren Lebensumstände inklusive der finanziellen und gesundheitlichen Gesamtsituation der Einzelpersonen und der Haushalte sowie ihrer Verknüpfung mit Daten dritter Anbieter und Verwerter. Die originären und die verarbeiteten Daten sind also selbst entgeltliches Handelsgut. Dabei spielt es aus Sicht der Bürger weniger eine Rolle, ob die Datennutzung und die Datenverwertung ein anderes Sachgut oder eine Dienstleistung verbilligt (Rabatt). Vielmehr geht es um ein Entgelt für die in der Datenverwertung enthaltene Wertschöpfung, wie sie aus der Lizenzierung von immateriellen Vermögensgegenständen bekannt ist.<sup>1</sup>

1 Vgl. A. Oehler: Chancen der selbstbestimmten Datennutzung?!, in: Wirtschaftsdienst, 96. Jg. (2016), H. 11, S. 830-832, 831. Kerber kommentiert dies mit Bezug zur Literatur so: „But it might be helpful to think less in terms of markets for selling personal data and more in terms of markets for licensing the use of personal data. Such licensing agreements would also allow a much more precise specification for what kinds of uses and to whom the rights to use the data should be sold (and for how long).“ Vgl. W. Kerber: Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection, in: MAGKS Joint Discussion Paper Series in Economics, Nr. 14, 2016.

### Schlussgedanken

Die europäische Datenschutz-Grundverordnung ist sicher ein wichtiger und wesentlicher Schritt im Hinblick auf die Novellierung des Datenschutzes in Europa gewesen. Die ökonomischen Implikationen der neuen Datenschutzinstrumente, wie etwa dem Recht auf Datenportabilität, sind jedoch bisher nicht hinreichend erforscht. Durch die Nicht-Rivalität von Daten ergeben sich komplexe ökonomische Interaktionen, die gegebenenfalls auch zu kontraintuitiven Ergebnissen führen können. In vielen Fällen wird es schließlich aber eine empirische Frage sein, ob die geplanten Vorteile oder die (hier beispielhaft aufgeführten) Nachteile der neuen Regelungen überwiegen und ob diese Regelungen tatsächlich die erhoffte Wirkung entfalten, mehr Nutzerkontrolle und Wettbewerb im Zeitalter des Datenkapitalismus zu etablieren.

Viele Bürger haben erkannt, dass in der (sozialen) Marktwirtschaft kaum etwas tatsächlich unentgeltlich oder gratis angeboten wird, sondern z.B. der pekuniäre Gegenwert der eigenen Daten zur Bezahlung dient. Die Daten selbst sind dabei keine „Währung“, sondern ökonomisch betrachtet nur deren Gegenwert in Euro oder Dollar, also ihr Tauschwert. Umso mehr mag es überraschen, dass im juristischen Kontext z.B. des seinerzeitigen Referentenentwurfs der 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) 2016 und in der aktuellen Fassung des GWB weiterhin von „unentgeltlichen Märkten“ die Rede ist.<sup>2</sup> Dies sollte nicht vom klaren ökonomischen Sachverhalt ablenken. Aus ökonomischer Perspektive funktionieren die anbieterseitigen Geschäftsmodelle nachvollziehbarerweise ausschließlich pekuniär. Es soll schon der Gedanke aufgekommen sein, der eine

2 Referentenentwurf des Bundesministeriums für Wirtschaft und Energie: Entwurf eines Neunten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen (9. GWB-ÄndG), 1.7.2016, insbesondere S. 10, 37 und 47 f.: „Eine Trennung der unentgeltlichen von der entgeltlichen Seite bei der Marktabgrenzung wird der wirtschaftlichen Realität jedoch nicht gerecht.“ Gesetz gegen Wettbewerbsbeschränkungen (GWB) in der Fassung der Bekanntmachung vom 26.6.2013 (BGBl. I S. 1750, 3245), das zuletzt durch Artikel 10 Absatz 9 des Gesetzes vom 30.10.2017 (BGBl. I S. 3618) geändert worden ist, Artikel 18 Absatz 2a: „Der Annahme eines Marktes steht nicht entgegen, dass eine Leistung unentgeltlich erbracht wird.“

oder andere Online-Anbieter sei eher am Sammeln und Verwerten der Daten interessiert als am Vertrieb von Produkten. Die bisherige Nicht-Regulierung hat zur Folge, dass Bürger ihre „Datenspende“ zwar wahrnehmen, aber unter anderem nicht taxieren können, weder nach Umfang noch nach pekuniärem Wert.<sup>3</sup> Es verwundert daher auch nicht, dass die Datenindustrie quer (lateral) durch die juristisch definierten Märkte und damit besonders wenig kontrolliert und abseits einer Aufsicht in einem kleinen Oligopol agiert.

Aus der Perspektive von Verbrauchern geht es weniger um eine rechtsdogmatische Erörterung, ob und wenn ja an welchen originären oder verarbeiteten Daten ein Eigentum im Sinne eines immateriellen Sachgutes besteht. Vielmehr dürfte es – zusätzlich zu Aspekten der IT-Sicherheit der Daten – ganz pragmatisch darum gehen, ob Verbraucher in der digitalen Welt am pekuniären Wert ihrer Daten partizipieren dürfen und können, ob sie also für die Verwertung und Nutzung ausreichend pekuniär vergütet werden. Greift hier die neue Datenschutz-Grundverordnung (DSGVO)? Die personenbezogenen Daten von Bürgern bilden zusammen mit den neueren Techniken zur Datenspeicherung und -verarbeitung, wie beispielsweise Big Data und Profiling-, Scoring-, und Trackingmethoden, die Grundlage für die Geschäftsmodelle der sogenannten Datenindustrie (auch „Datenwirtschaft“).<sup>4</sup> Deren zunehmende Verbreitung und Industrialisierung war ein Anlass für die Überarbeitung der aus dem Jahr 1995 stammenden EU-Datenschutzrichtlinie. Die in diesem Zuge geschaffene EU-Datenschutz-Grundverordnung soll „zeitgemäße Antworten auf die fortschreitende Digitalisierung von Wirtschaft und Gesellschaft“<sup>5</sup> geben.

### Wie regulieren?

Die Verbraucherkommission Baden-Württemberg fasst mit ihren Empfehlungen zur Datensouveränität, -nutzung und -verwertung die Anforderungen für eine aus Sicht der Verbraucher zeitgemäße Regulierung in wenigen Punkten zusammen. Deren Ziel muss die Schaffung eines europaweit einheitlichen Wirtschafts- und Rechtsrahmens sein, der neben einer datenschutzrechtlichen Betrachtung auch die Nutzungsrechte von Massendaten und gegebenenfalls Individualdaten mit einhergehenden Verwertungsrechten enthält. Hierbei ist auf die Umsetzung einer praktikablen Datenverwertung mit einer fairen Partizipati-

on der Verbraucher an der Nutzung der Daten zu achten. Außerdem ist mit Hilfe von technischen Mindeststandards und Datenübertragbarkeitsrechten die Datenportabilität und Interoperabilität zu fördern.<sup>6</sup>

Eine zeitgemäße Regulierung sollte also Entgelte vorsehen, mit denen Verbraucher an der Wertschöpfung beteiligt werden, die überhaupt erst durch ihre Daten ermöglicht wurde. Diese Empfehlung scheint bisher allerdings kaum ins Bewusstsein der Rechtssetzung und der politischen Entscheidungsträger vorgedrungen zu sein. So schreibt die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, dass die DSGVO „der deutschen und europäischen Digitalwirtschaft ausreichend Spielraum [lässt], innovative und intelligente Geschäftsmodelle zu entwickeln, die das in den vorhandenen enormen Datenmengen liegende Potenzial ökonomisch verwertbar machen und dabei zugleich die datenschutzrechtlichen Vorgaben beachten.“<sup>7</sup> Eine Beteiligung der Verbraucher an der ökonomischen Verwertung der Daten wird hingegen nicht erwähnt. Dies verdeutlicht, dass im Rahmen der DSGVO ausschließlich die Datenwirtschaft als Profiteur der Datenverwertung gesehen wird. Den Verbrauchern wird hingegen lediglich ein Interesse am Datenschutz unterstellt. Daher verwundert es nicht, dass die DSGVO die ökonomischen Interessen der Verbraucher vollständig ignoriert und für die Thematik der Teilhabe an Datenprofiten nicht geeignet ist.

### Pekuniärer Wert von Daten

Die politischen Entscheider in Deutschland und Europa, die unter anderem die DSGVO initiiert und verabschiedet haben, bleiben eine Antwort schuldig, warum Verbraucher nicht an der ökonomischen Verwertung ihrer eigenen Daten beteiligt werden sollen. Dabei ist von einer Vielzahl an Untersuchungen dokumentiert, dass sie ihren Daten einen pekuniären Wert zumessen. Dieser Wert hängt unter anderem davon ab, wie sensibel die Daten sind,<sup>8</sup> wem die Daten zur Verfügung gestellt<sup>9</sup> und in welchem Kontext

3 Vgl. A. Oehler, a. a. O.

4 Vgl. A. Oehler: Grundsätze ordnungsgemäßer Bewertung durch Scoring, in: Wirtschaftsdienst, 97. Jg. (2017), H. 10, S. 748-751, 748.

5 Bundesministerium für Wirtschaft und Energie: Europäische Datenschutz-Grundverordnung, 2018, <https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html> (1.6.2018).

6 Vgl. Verbraucherkommission Baden-Württemberg: Datensouveränität, -nutzung und Datenverwertung – Forderungen nach einem „update“ der Wirtschafts- und Rechtsordnung als Chance für eine selbstbestimmte Datennutzung, Stellungnahme Verbraucherkommission Baden-Württemberg, Nr. 45, 2017 (Auslassungen von den Verfassern).

7 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Datenschutz-Grundverordnung, BfDI – Info 6, 2017, S. 7.

8 Vgl. J. Grossklags, A. Acquisti: When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information, Proceedings of Workshop on the Economics of Information Security, 7.6.2007, [http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags\\_Acquisti-WEIS07.pdf](http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags_Acquisti-WEIS07.pdf) (1.6.2018).

9 Vgl. D. Cvrcek, M. Kumpost, V. Matyas, G. Danezis: A Study on the Value of Location Privacy, Workshop on Privacy in Electronic Society (WPES'06), 2006, S. 109-118.

sie bereitgestellt werden.<sup>10</sup> Beispielsweise sehen Verbraucher Daten über ihren Aufenthaltsort als besonders wertvoll an, weil die Daten Rückschlüsse auf die täglichen Routinen zulassen.<sup>11</sup>

Obwohl sie eine Wertvorstellung hinsichtlich ihrer Daten haben, dürfte den Verbrauchern kaum klar sein, dass sie ihre personenbezogenen Daten theoretisch auf einem Markt handeln könnten. Ob sich ihre Preisvorstellungen dann mit denen der Datenwirtschaft decken, kann bisher kaum beantwortet werden, weil ihnen bislang – außer mit dem Verzicht auf die Dienste der Anbieter – kaum Möglichkeiten zur Verfügung stehen, um mit der Datenwirtschaft in Verhandlung zu treten.<sup>12</sup> Eine faire Teilhabe in einer sozialen Marktwirtschaft dürfte anders verstanden werden. Es wäre nicht überraschend, schon gar nicht unter dem politischen Leitbild der Bundesregierung der „selbstbestimmt handelnden“ Bürger, dass Verbraucher ihre Daten als noch wertvoller einschätzen, wenn sie darüber aufgeklärt würden, dass es einen Markt gibt, auf dem sie die Preise für ihre Daten aushandeln können.

### Daten-Anonymität

Gleiches dürfte gelten, wenn man die Erkenntnis ernst nähme, dass es zwar anonymisierte Daten geben mag, aber keine Anonymität bei personenbezogenen Daten. Hierzu stellen de Montjoye und Pentland unmissverständlich fest: „We have currently no reason to believe that an efficient enough, yet general, anonymization method will ever exist for highdimensional data, as all the evidence so far points to the contrary.“<sup>13</sup> Die Tatsache, dass auch anonymisierte Daten einzelnen Personen zugeordnet werden können, hat sowohl Auswirkungen auf den Schutz als auch auf den ökonomischen Wert der Daten von Verbrauchern.

Obwohl bei der Erstellung der DSGVO die grundsätzliche Möglichkeit, pseudonymisierte Daten einer Person zuordnen zu können, berücksichtigt wurde, wird die Existenz anonymer Informationen unterstellt. Im Erwägungsgrund 26 ist beispielsweise zu lesen: „Die Grundsätze des Datenschutzes sollten daher nicht für anony-

me Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.“ Die Einschätzung, ob anonyme Informationen vorliegen, erfolgt „nach allgemeinem Ermessen“<sup>14</sup>. Unklar ist, wie eine solche Einschätzung erfolgen soll, wenn ein Großteil der Daten an sogenannte „Third Parties“ weitergegeben wird, deren Geschäftsmodell ausschließlich aus dem Sammeln, Aggregieren, Auswerten und Weiterverkaufen von neu zusammengestellten Datensätzen besteht.<sup>15</sup> Daher kommen auch de Montjoye und Pentland zu dem Schluss „The current deidentification model, where the data are anonymized and released, is obsolete and should not be used for policy.“<sup>16</sup> Somit ist wohl kaum von einem wirkungsvollen Schutz durch die DSGVO auszugehen.

Durch die umfangreiche Verwendung von Daten in Algorithmen, z.B. in Scoring-Verfahren<sup>17</sup>, hat die fehlende Anonymität auch unmittelbare ökonomische Auswirkungen, nicht nur für Verbraucher in existenziellen Lebensbereichen wie Gesundheit oder Finanzen/Versicherungen. Die Datenverwertung kann und wird zum Aufbau von Markteintrittsbarrieren<sup>18</sup> und zur Preisdiskriminierung<sup>19</sup> verwendet werden.<sup>20</sup> Die rechtlichen und aufsichtlichen Handhabungsmöglichkeiten erscheinen eher sehr bescheiden angesichts des durch fortgesetztes Nichts-Tun entstandenen kleinen Oligopols der Datenindustrie. Eine Algorithmenkontrolle auf der Grundlage gesetzlicher Standards können Wirtschaftsprüfer im Rahmen einer Systemprüfung vornehmen, ohne mögliche Geschäftsgeheimnisse zu gefährden.<sup>21</sup> Allenfalls theoretisch könnte man sich vorstellen, dass Verbraucher, die sich durch die Weitergabe ihrer Daten dem Risiko einer Preisdiskriminierung ausgesetzt sehen, dem Wert ihrer Daten eine Risikoprämie aufschlagen werden. Dies könnte sich dann negativ für die Anbieter der Datenwirtschaft auswirken, wenn die Risikoprämie hoch genug ist, dass die Verbraucher die Dienste der Anbieter verlassen, um dem Risiko der Preisdiskriminierung auszuweichen.

10 Vgl. B. Huberman, E. Adar, L. R. Fine: Valuating Privacy; in: IEEE Privacy and Security, 3. Jg. (2005), H. 5, S. 22-25; vgl. auch S. Spiekermann, J. Korunovska: Towards a value theory for personal data; in: Journal of Information Technology, 32. Jg. (2017), H. 1, S. 62-84.

11 Vgl. A. Wagner, N. Wessels, P. Buxmann, H. Krasnova: Putting a Price Tag on Personal Information – A Literature Review, Proceedings of the 51st Hawaii International Conference on System Sciences, 2018.

12 Vgl. A. Oehler, M. Horn, S. Wendt: Digitale Zahlungsdienste: Chinese Walls 2.0 oder Trennung?, in: DIVSI Magazin, Oktober 2016, S. 23-25.

13 Y.-A. de Montjoye, A. Pentland: Response to Comment on „Unique in the shopping mall: On the reidentifiability of credit card metadata“; in: Science, 351. Jg. (2016), Nr. 6279, S. 1274.

14 DSGVO, Erwägungsgrund 26.

15 Vgl. S. Spiekermann, A. Acquisti, R. Böhmer, K.-L. Hui: The challenges of personal data markets and privacy; in: Electronic Markets, 25. Jg. (2015), H. 2, S. 161-167.

16 Y.-A. de Montjoye, A. Pentland, a. a. O.

17 Vgl. A. Oehler: Grundsätze ordnungsgemäßer Bewertung ..., a. a. O.

18 Vgl. C. Shapiro, H. Varian: Information rules, Boston 1998.

19 Vgl. A. Acquisti, H. Varian: Conditioning prices on purchase history; in: Marketing Science, 24. Jg. (2005), H. 3, S. 367-381.

20 Vgl. A. Oehler: Grundsätze ordnungsgemäßer Bewertung ..., a. a. O., S. 748.

21 Ebenda, S. 751.

Ganz praktisch sieht die digitale Welt heute dagegen vollkommen anders aus: Weder kann und soll die Datenverwendung und deren Preise bekannt sein, noch kann darauf von der Nachfrageseite adäquat reagiert werden, noch ist ein technisches oder inhaltliches Ausweichen möglich, da im 21. Jahrhundert in Deutschland und Europa noch nicht einmal die Basics der Interoperabilität und der Datenportabilität (siehe oben) umgesetzt sind.

Justus Haucap

## Daten als Wettbewerbsfaktor

Daten seien das Öl des 21. Jahrhunderts, wird manchmal gesagt.<sup>1</sup> Dies ist jedoch kein besonders treffendes Bild, denn Daten können – anders als Öl – von vielen Parteien zugleich oder auch nacheinander genutzt werden. Daten sind grenzkostenlos mehrnutzbar, d.h. die Nutzung von Daten durch eine weitere Person verursacht zunächst einmal keine zusätzlichen Kosten, wenn die Daten erst einmal vorliegen. Nur weil jemand bestimmte Daten nutzt, schließt dies – anders als eben beim Öl – nicht die parallele oder sequenzielle Nutzung derselben Daten durch andere aus.<sup>2</sup>

Sinnvoll ist der Vergleich von Daten und Öl als Antriebsmittel der Wirtschaft vielleicht insofern, als die enorme Reduktion bei Transport- und Mobilitätskosten durch die Erfindung des Automobils einen erheblichen Strukturwandel in vielen Bereichen ausgelöst hat, so wie er nun von datengetriebenen Geschäftsmodellen erwartet wird. Zudem gehören die sogenannten GAFA-Unternehmen (Google, Amazon, Facebook, Apple) heute zu den wertvollsten Unternehmen der Welt, so wie ehemals die großen Ölkonzerne. Eine mögliche Erklärung für die hohe Marktkapitalisierung der GAFA-Unternehmen ist die Erwartung der Märkte, dass diese Unternehmen sehr hohe Gewinnpotenziale haben. Solche Gewinnerwartungen könnten darauf beruhen, dass die Anleger davon ausgehen, dass diese Unternehmen erhebliche Marktmacht

Die Geschäftsmodelle der Datenindustrie dürften bis heute – und wahrscheinlich auch noch in der weiteren Zukunft – darauf vertrauen können, dass die zuständigen politischen Entscheider die bekannte ungleiche ökonomische Verteilung bei der Datenverwertung fortbestehen lassen und entgegen der Idee der sozialen Marktwirtschaft den Bürgern eine Beteiligung am Profit aus der Verwertung ihrer Daten verweigern.

haben oder erreichen werden.<sup>3</sup> Teilweise wird auch von einer dezidierten „Datenmacht“ gesprochen.<sup>4</sup> Dahinter steht die Annahme, dass der privilegierte Zugang zu Daten bzw. der Besitz bestimmter Daten Kern für Marktmacht sein kann und sich wirksamer Wettbewerb nicht entwickeln wird, wenn nicht konkurrierende Anbieter Zugang zu denselben oder funktionsäquivalenten Daten bekommen können.

Auch wenn sich Öl und Daten als Rohstoffe für die wirtschaftliche Wertschöpfung also erheblich unterscheiden, stellt sich die Frage, ob der Zugang zu Daten und ihre Verarbeitung für den Wettbewerb eine ebenso wichtige Rolle spielt wie der Zugang zu Transportmöglichkeiten, als vor rund 100 Jahren die Entwicklung des Transportwesens die Transportkosten erheblich reduzierte.<sup>5</sup> Der Koalitionsvertrag der Bundesregierung sieht daher eine erneute Überprüfung der kartellrechtlichen Bestimmungen mit Blick auf die Herausforderungen der Digitalisierung vor.<sup>6</sup> Darüber hinaus hat die Bundeskanzlerin jüngst in der Be-

1 Erstmals soll Clive Humby, britischer Mathematiker und Entwickler der Kundenkarte von Tesco, diese Analogie 2006 benutzt haben, vgl. M. Palmer: Data is the New Oil!, 3.11.2006, [http://ana.blogs.com/mastros/2006/11/data\\_is\\_the\\_new.html](http://ana.blogs.com/mastros/2006/11/data_is_the_new.html) (9.7.2018).

2 Vgl. auch R. Dewenter, H. Lüth: Big Data aus wettbewerblicher Sicht, in: Wirtschaftsdienst, 96. Jg. (2016), H. 9, S. 648-654; R. Dewenter, H. Lüth: Big Data: Eine ökonomische Perspektive, in: U. Immenga, T. Körber (Hrsg.): Daten und Wettbewerb in der digitalen Ökonomie, Baden-Baden 2017, S. 9-30.

3 Vgl. etwa U. Dolata: Volatile Monopole. Konzentration, Konkurrenz und Innovationsstrategien der Internetkonzerne, in: Berliner Journal für Soziologie, 24. Jg. (2015), H. 4, S. 505-529; ders.: Internetkonzerne: Konzentration, Konkurrenz und Macht, in: U. Dolata, J.-F. Schrape (Hrsg.): Kollektivität und Macht im Internet: Soziale Bewegungen, Open Source Communities, Internetkonzerne, Berlin u.a.O. 2018, S. 101-130.

4 Vgl. T. Körber: Ist Wissen Marktmacht? Überlegungen zum Verhältnis Datenschutzes, „Datenmacht“ und Kartellrecht, in: U. Immenga, T. Körber (Hrsg.), a. a. O..

5 Vgl. auch E. Brynjolfsson, A. McAfee: The Second Machine Age: Wie die nächste digitale Revolution unser aller Leben verändern wird, Kulmbach 2014; sowie A. Picot, Y. Berchtold, R. Neuburger: Big Data aus ökonomischer Sicht: Potenziale und Handlungsbedarf, in: B. Kolany-Raiser et al. (Hrsg.): Big Data und Gesellschaft, Technikzukünfte, Wissenschaft und Gesellschaft, Wiesbaden 2018, S. 309-416.

6 Vgl. CDU, CSU und SPD: Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land, Koalitionsvertrag zwischen CDU, CSU und SPD, 2018, S. 44.

steuerung und Bepreisung von Daten „das zentrale Gerechtigkeitsproblem der Zukunft“<sup>7</sup> erkannt.

Aus wettbewerbsökonomischer Perspektive ergeben sich mindestens fünf neue Problemkreise im Kontext datengetriebener Geschäftsmodelle:

- Erstens stellt sich die Frage, ob und wann der Zugriff auf bestimmte Daten eine notwendige Voraussetzung für die Teilnahme am Wettbewerb ist oder, anders gewendet, ob und wann das Erheben und Kombinieren bestimmter Daten einem Unternehmen solch einen Wettbewerbsvorsprung verschafft, dass es eine Monopolstellung erreichen und verteidigen kann oder zumindest erhebliche Marktkonzentration das Resultat ist.
- Zweitens ist der Austausch von Informationen und Daten durch Unternehmen sowie eine gegebenenfalls erhöhte Markttransparenz traditionell in der Kartellrechtspraxis und in der Wettbewerbsökonomie regelmäßig als kollusionsfördernd bewertet worden, sodass der Datenaustausch zwischen Unternehmen kartellrechtlich regelmäßig als problematisch bewertet wurde. Fraglich ist, ob diese Interpretation in einer datengetriebenen Ökonomie, in der Netzeffekte eine bedeutende Rolle spielen, auch richtig ist.
- Drittens ergeben sich Fragen, inwiefern im Kartellrecht Datenschutzbelange Berücksichtigung finden können bzw. inwiefern das (exzessive) Sammeln und Kombinieren von Daten ein Missbrauch einer marktbeherrschenden Stellung sein kann.
- Viertens stellen sich aufgrund der technischen Möglichkeiten zur stärkeren Preisdifferenzierung neue Fragen für Wettbewerbspolitik und Verbraucherschutz.
- Und fünftens wird unter Wettbewerbsökonomien und Kartellrechtlern aktuell intensiv diskutiert, ob auf Big Data Analytics beruhende Algorithmen zur Preissetzung Kartelle unterstützen oder sogar induzieren können.

## Daten und Wettbewerb

Für Wettbewerbsökonomien ist vor allem die Tatsache, dass Daten prinzipiell von vielen Personen ohne weitere Kosten parallel oder auch sequenziell genutzt werden können, zunächst einmal eine gute Nachricht, denn es

7 O.V.: Angela Merkel fordert Besteuerung von Daten, Zeit Online, 28.5.2018, <https://www.zeit.de/politik/deutschland/2018-05/steuerreform-angela-merkel-daten-eu> (9.7.2018).

gibt – anders als beispielsweise beim Frequenzspektrum im Mobilfunk – keine natürliche Ressourcenknappheit, die den Wettbewerb begrenzt. Gleichwohl kann der Zugriff auf bestimmte Daten essenziell für die effektive Teilnahme am Wettbewerb sein. Im Fall von Google wird etwa diskutiert, ob Wettbewerber wie Microsoft oder Yahoo! einen Zugriff auf historische Suchdaten von Google benötigen, um genauso gute Suchalgorithmen programmieren zu können.<sup>8</sup>

Auch wenn diese Forderung plausibel erscheinen mag, ist dies doch keineswegs klar. Letztlich ist dies eine empirische Frage. Google selbst nutzt nach eigenen Angaben nur einen Bruchteil der Daten zur Verbesserung des eigenen Suchalgorithmus, denn auch hier gilt die Logik der Äquivalenz von Grenzkosten und Grenznutzen im Optimum. Letztlich werden die Daten solange analysiert, bis die Grenzkosten der weiteren Analyse den Grenzertrag zu übersteigen drohen.<sup>9</sup> Gleichwohl ist nicht klar, inwiefern Google doch erhebliche Wettbewerbsvorteile bei der Optimierung der Suchalgorithmen und Erstellung der Trefferlisten hat, da Google auch auf andere Dienste wie Google-Mail, Google-Kalender etc. zugreifen kann, sofern ein Suchender diese Dienste nutzt. Da Suchergebnisse immer stärker individualisiert werden und viele Nutzer nur einen E-Mail-Dienst und einen Kalender nutzen, erschwert dies die Replikation der Datenbasis von Google durchaus. Das einfache Einlesen und Auswerten von öffentlichen Webseiten reicht dann nicht, um die bestmöglichen Suchergebnisse anzuzeigen. Selbst ein Zugang zu pseudonymisierten Daten von Google wäre nur begrenzt hilfreich, wenn die Qualität der Suchergebnisse etwa durch den Zugang zu persönlichen Daten im Kalender, den E-Mails oder anderen persönlichen Informationen beeinflusst wird.

Gleichwohl ist denkbar, dass der Zugriff auf Daten, die ein Wettbewerber erhoben hat, für die Teilnahme am Wettbewerb essenziell sein kann,<sup>10</sup> insbesondere, wenn individuelle Daten exklusiv vorliegen. Dies mag z.B. bei Ener-

8 Vgl. etwa O. Bracha, F. Pasquale: Federal Search Commission? Access, Fairness, and Accountability in the Law of Search, in: Cornell Law Review, 93. Jg. (2008), H. 6, S. 1149-1209; G. A. Manne, J. D. Wright: Google and the Limits of Antitrust: The Case against the Antitrust Case against Google, in: Harvard Journal of Law and Public Policy, 34. Jg. (2011), H. 1, S. 171-244; C. Argenton, J. Prüfer: Search Engine Competition with Network Externalities, in: Journal of Competition Law and Economics, 8. Jg. (2012), H. 1, S. 73-105.

9 Ausführliche Analysen des Google-Falls bieten Haucap und Kehder. Vgl. J. Haucap, C. Kehder: Suchmaschinen zwischen Wettbewerb und Monopol: Der Fall Google, in: R. Dewenter, J. Haucap, C. Kehder (Hrsg.): Wettbewerb und Regulierung in Medien, Politik und Märkten: Festschrift für Jörn Kruse zum 65. Geburtstag, Baden-Baden 2013, S. 115-154.

10 Vgl. etwa I. Graef: EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility, Alphen aan den Rijn 2016.

gieverbrauchsdaten in intelligenten Stromnetzen (Smart Grids) der Fall sein. Auch im Auto gesammelte Daten über Technik und individuelles Fahrverhalten können kaum dupliziert werden. Sollte etwa ein Pkw-Hersteller selbst Kfz-Versicherungen anbieten, hätten andere Versicherungen ohne Zugriff auf die Daten wohl einen erheblichen Nachteil. Dasselbe würde für freie Werkstätten bei der Reparatur gelten. Natürlich geht es hier im Grunde aus wettbewerbsökonomischer Sicht um eine klassische After-Markets-Problematik wie schon bei Pkw-Ersatzteilen, d. h., es stellt sich die (nur empirisch zu beantwortende) Frage, ob etwa Autokäufer in Zukunft schon beim Kauf eines Autos berücksichtigen werden, wer Zugang zu den in ihrem Auto gesammelten Daten hat oder bekommen kann.

In einigen Fällen wäre ein Zugriff auf Daten für Wettbewerber wohl in Zukunft eine unvermeidliche Vorbedingung, um den Wettbewerb zu schützen oder erst zu ermöglichen und das Aufkommen von „Datenmonopolen“, d. h. Monopolen, die aufgrund eines exklusiven Zugriffs auf bestimmte Daten bestehen, zu verhindern. Nun garantiert die Europäische Datenschutz-Grundverordnung (DSGVO) zwar die Portierung von persönlichen Daten für Privatpersonen, nicht aber für Gewerbe, sodass das Recht auf Portierung den Lock-in nur für Privatpersonen aufhebt, nicht aber für die oft wirtschaftlich sehr bedeutsamen Gewerbetreibenden, sofern die Portierung faktisch überhaupt möglich ist. Letzteres dürfte oft durch eine mangelnde Interoperabilität erschwert werden, denn für eine Portierung müssen Daten ja nicht nur abgegeben werden, sondern sie müssen auch aufgenommen werden können.

Um Wettbewerb zu ermöglichen und damit Auswahlmöglichkeiten für Nutzer zu schaffen, mag es somit manchmal notwendig sein, auf Daten zurückzugreifen, die ein Konkurrent originär erhoben hat. Bestimmte Daten haben dann die Eigenschaft einer sogenannten wesentlichen Einrichtung („essential facility“), ohne deren gemeinsame Nutzung Wettbewerb nicht möglich ist.<sup>11</sup> Tendenziell wird das in der DSGVO verankerte Recht auf die Portierung persönlicher Daten jedoch den Wettbewerb stärken, auch wenn die wettbewerblichen Auswirkungen nicht überschätzt werden sollten, gerade auch weil etwaige Probleme bei der Kompatibilität nicht unterschätzt werden sollten.

## Daten und Kartellrecht

Der Zugang zu wettbewerbsrelevanten Daten spielt zwar nach der 9. GWB-Novelle<sup>12</sup> in §18 Abs. 3 GWB eine Rolle

<sup>11</sup> Ebenda.

<sup>12</sup> Zur 9. GWB-Novelle vgl. detailliert C. Kersting, R. Podszun (Hrsg.): Die 9. GWB-Novelle, München 2017.

bei der Beurteilung von Marktmacht, es gibt aber – anders als etwa bei Netzinfrastrukturen – keinen kartellrechtlichen Zugangsanspruch zu wettbewerbsrelevanten Daten. Jedoch werden in §18 Abs. 3a GWB nun Kriterien definiert, die bei der Beurteilung von Marktmacht insbesondere bei Plattformen heranzuziehen sind. Wörtlich heißt es in §18 Abs. 3a GWB: „Insbesondere bei mehrseitigen Märkten und Netzwerken sind bei der Bewertung der Marktstellung eines Unternehmens auch zu berücksichtigen (1) direkte und indirekte Netzwerkeffekte, (2) die parallele Nutzung mehrerer Dienste und der Wechselaufwand für die Nutzer, (3) seine Größenvorteile im Zusammenhang mit Netzwerkeffekten, (4) sein Zugang zu wettbewerbsrelevanten Daten, (5) innovationsgetriebener Wettbewerbsdruck.“ Die Kriterien reflektieren direkt die Erkenntnisse der ökonomischen Theorie.<sup>13</sup>

Eine nach wie vor offen diskutierte Frage ist, ob kartellrechtliche Kontrollinstrumente auch dazu genutzt werden sollten, den Datenschutz zu unterstützen. Eine Möglichkeit etwa wäre, bei der kartellrechtlichen Kontrolle von Fusionen und Kooperationen auch die Gefährdungen in den Blick zu nehmen, die sich aus einer Kombination von Datenbeständen ergeben könnten. Sollte etwa bei einer völlig hypothetischen Fusion von E.ON, BMW, Facebook und einer Bank das etwaige, gegebenenfalls auch missbräuchliche Zusammenlegen von Daten eine Rolle spielen? Sollten Datenschützer gar ein eigenes Mitspracherecht bei Unternehmensfusionen bekommen?

Die beiden Vorschläge mögen vordergründig sinnvoll erscheinen, sind aber letztlich doch eher kritisch zu bewerten. Die Fusionskontrolle ist ein Instrument der Gefahrenabwehr, bei der präventiv die Entstehung von Marktconstellationen verhindert werden soll, die besonders anfällig für den unilateralen Missbrauch von marktbeherrschenden Stellungen, eine Kartellierung oder kollusives Verhalten und/oder eine andersartige erhebliche Minderung wirksamen Wettbewerbs sind. Diese Ex-ante-Kontrolle wird vor allem deswegen bevorzugt, weil sich die Ex-post-Kontrolle des Missbrauchs marktbeherrschender Stellungen oder kollusiven Verhaltens als sehr schwierig und oftmals fast unmöglich erweist. Die Fusionskontrolle ist somit ein imperfektes institutionelles Substitut angesichts der Unvollkommenheit der nachträglichen Missbrauchsaufsicht und der Kontrolle kollusiven Verhaltens.

<sup>13</sup> Vgl. etwa D. S. Evans, R. Schmalensee: Markets with Two-Sided Platforms, in: Issues in Competition Law and Policy, 2008, Nr. 1, S. 667-693; D. S. Evans, R. Schmalensee: The Antitrust Analysis of Multi-Sided-Platform Businesses, in: R. Blair, D. Sokol (Hrsg.): Oxford Handbook on International Antitrust Economics, 1. Jg. (2015), Oxford 2015, S. 404-449; J. Haucap, T. Stühmeier: Competition and Antitrust in Internet Markets, in: J. Bauer, M. Latzer (Hrsg.): Handbook on the Economics of the Internet, Cheltenham 2016, S. 183-210.

Für die Verletzung datenschutzrechtlicher Bestimmungen dürfte diese Logik jedoch nicht gelten. Eine Verletzung datenschutzrechtlicher Vorschriften sollte auch ex post entdeckt und abgestellt werden können, ohne dass dazu eine – sehr kostspielige – Entflechtung des fusionierten Unternehmens notwendig wäre.

Während in der Fusionskontrolle datenschutzrechtliche Aspekte keine Berücksichtigung finden, spielen sie in der kartellrechtlichen Missbrauchsaufsicht eine gewisse Rolle. Aktuell untersucht das Bundeskartellamt etwa, ob Facebook gegenüber seinen Nutzern zu sehr in die Privatsphäre eingreift und zu viele individuelle Nutzerdaten kombiniert und so den Nutzern schadet. Allerdings ist dies der weltweit erste Fall dieser Art, bei dem die Wahl des Datenschutzstandards kartellrechtlich untersucht wird. Schwierig ist die Untersuchung auch deshalb, weil die Kombination von Daten tendenziell zu Produktverbesserungen führt, wie etwa ein Newsstream, der näher an den individuellen Nutzerinteressen ist. Zugleich suggeriert die bisherige empirische und experimentelle Evidenz, dass ein Großteil der Verbraucher zwar öffentlich behauptet, sorgsam mit persönlichen Daten umzugehen und dafür auch Mühen in Kauf zu nehmen, dieselben Individuen jedoch gegen kleinste Anreize bereit sind, persönliche Informationen preiszugeben. In der Literatur wird dieses Phänomen auch als „Privacy Paradox“ bezeichnet.<sup>14</sup>

### Preisfindung durch Algorithmen und Kartellbildung

Unternehmen verwenden zunehmend Preisanpassungssoftware, denn dynamische Preisanpassungsalgorithmen versprechen Händlern eine verbesserte, d. h. gewinnsteigernde Preissetzung. Allerdings kann die Verwendung entsprechender Software auch wettbewerbliche Probleme und damit auch kartellrechtliche Risiken für die Unternehmen mit sich bringen.<sup>15</sup> Typischerweise sammelt eine Preisfindungssoftware diverse Markt- und Kundendaten (Konkurrenzpreise, Verbraucherverhalten, Saisoneinflüsse etc.) und empfiehlt dem Händler einen Preis oder legt diesen sogar selbst fest. Durch den Einsatz solcher Softwaretools kann es dann zu einer Kartellbildung kommen, wenn selbstlernende Algorithmen bei hinreichend vielen Händlern eingesetzt werden und diese lernen, dass Kartellpreise die höchsten Gewinne bringen.

14 Vgl. auch P. A. Norberg, D. R. Horne, D. A. Horne: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, in: *Journal of Consumer Affairs*, 41. Jg. (2007), H. 1, S. 100-126; A. Acquisti, C. R. Taylor, L. Wagman: The Economics of Privacy, in: *Journal of Economic Literature*, 54. Jg. (2016), H. 2, S. 442-492; V. Benndorf, H.-T. Normann: The Willingness to Sell Personal Data, in: *Scandinavian Journal of Economics*, 2018, im Erscheinen.

15 Zum Thema Preis- und Kartellbildung mit Hilfe von Algorithmen vgl. insbesondere A. Ezrachi, M. E. Stucke: *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge 2016.

Ein erster Fall der Kartellierung mit Hilfe von Algorithmen ist in den USA vor Gericht („USA versus Topkins“) behandelt worden, wenngleich der Mechanismus wesentlich plumper war als der oben vermutete Lernalgorithmus. Wie das amerikanische Department of Justice (DOJ) und die britische Competition and Markets Authority (CMA) ermittelt haben, hatten sich mehrere Händler von Postern zunächst über ein bestimmtes Preisniveau für ihre Produkte bei Amazon Marketplace verständigt. Die Einhaltung dieses Preisniveaus wurde anschließend durch die Programmierung einer allgemein erhältlichen Preisanpassungssoftware erreicht.<sup>16</sup>

Kartellrechtlich schwieriger wird es jedoch, wenn es gar nicht zu einem direkten Kontakt zwischen den Wettbewerbern kommt und der Kartellpreis allein auf der Nutzung von – gegebenenfalls sogar denselben – Preisanpassungsalgorithmen beruht. Die Verwendung von Preisanpassungssoftware kann kartellrechtlich problematisch sein, selbst bei jeglichem Fehlen direkter oder indirekter Kommunikation zwischen Wettbewerbern, da die Preisalgorithmen wettbewerbsfähig sensible Informationen sammeln und für die Preissetzung verwerten. Bekommt die Software solche Informationen unmittelbar von einem ebenfalls angeschlossenen Wettbewerber, ist das in jedem Fall kartellrechtlich heikel.

Aus ökonomischer Sicht kann selbst das unilaterale Einsammeln der Preisdaten von Wettbewerbern und die Nutzung für die algorithmische Preisfindung problematisch sein,<sup>17</sup> wenn dies zu kartellanalogen Preisen führt. Leicht vorstellbar ist, dass eine selbst lernende Software erkennt, dass Kartellpreise zu höheren Gewinnen führen als Wettbewerbspreise, sofern auch andere Händler Kartellpreise setzen. Gleichwohl gibt es bei dieser Art der automatisierten und gegebenenfalls sogar völlig unbewussten Abstimmung kartellrechtlich momentan kaum eine Eingriffsmöglichkeit, sodass für Verbraucher durchaus Risiken in der Preisbildung durch Algorithmen bestehen. Die oftmals im Kontext der dynamischen Preissetzung diskutierten Transparenzverpflichtungen wären aus wettbewerbsökonomischer Sicht gegebenenfalls sogar kontraproduktiv, sofern sie Kartellbildung und Kartellstabilität befördern. Die Monopolkommission hat in ihrem aktuellen Hauptgutachten nun eine Sektoruntersuchung von Preisalgorithmen durch das Bundeskartellamt angeregt.<sup>18</sup>

16 Vgl. dazu <https://www.justice.gov/atr/case-document/file/513586/download> (9.7.2018).

17 Vgl. dazu auch S. Schmidt: Webtracker und Kartellrecht, in: *Wirtschaft und Wettbewerb*, 66. Jg. (2016), H. 12, S. 572-580.

18 Vgl. Monopolkommission: *Wettbewerb 2018*, Bonn 2018, S. 63.

## Wettbewerbsprobleme der Plattformökonomie

Nahezu untrennbar mit dem Thema Daten und Digitalisierung verbunden ist das Aufkommen digitaler Plattformen. Diese bringen neue Wettbewerbsprobleme bzw. Herausforderungen in der Kartellrechtsdurchsetzung sui generis mit sich, wie etwa die deutlich komplexere Marktabgrenzung,<sup>19</sup> die bereits ausführlich in der Literatur diskutiert worden ist.<sup>20</sup> Zwei Phänomene sind jedoch bisher noch zu wenig beleuchtet worden: zum einen die auf Plattformmärkten verstärkten Anreize zur Marktabstottung, zum anderen das Zusammenspiel und die sich gegenseitig verstärkende Wirkung von Marktmacht und Informationsasymmetrien.

Sowohl die Anreize als auch die Möglichkeiten, in wettbewerbswidriger Weise einen Markt zu verschließen und Marktmacht auf benachbarte Märkte auszudehnen, sind bei Online-Plattformen tendenziell stärker ausgeprägt als auf „normalen“ Märkten. Zunächst gilt auch auf Plattformmärkten die von Segal und Whinston entwickelte Logik, dass bei steigenden Skalenerträgen (economies of scale) in Kombination mit Wechselkosten bzw. loyalen oder „gefangenen“ Kunden („captured customers“) ein etablierter Anbieter Markteintritte schon dadurch effektiv unterbinden kann, dass er nur einem Teil der Kunden (am besten den potenziell wechselwilligen) gezielt attraktive Angebote macht (und diese Angebote von den loyalen oder „gefangenen“ Kunden gewissermaßen „quersubventioniert“ werden).<sup>21</sup> Eine solche Strategie verhindert, dass ein Neuling hinreichende Skalenerträge realisieren kann, ihm fehlt die kritische Masse, um effizient anbieten zu können. Der etablierte Anbieter kann den Markt schon effektiv verschließen, wenn er lediglich einem Teil der Kunden attraktive Angebote unterbreitet. Da steigende Skalenerträge auf digitalen Märkten die Regel sind, gilt die von Segal und Whinston entwickelte Logik in besonderem Maße.

Direkte und indirekte Netzeffekte, die ebenfalls typisch für Online-Plattformen sind, verstärken diesen Mechanismus noch einmal. Während im vom Segal und Whinston entwickelten Ansatz der Marktverschluss allein durch den Kostenvorteil (aufgrund der steigenden Skaleneffekte) gelingt, hat etwa Vasconcelos theoretisch dargelegt, dass ein Marktverschluss durch eine große Plattform selbst dann gelingen kann, wenn ein Neuling

einen Kostenvorteil hat.<sup>22</sup> Grund sind die positiven Netzeffekte, die von der installierten Basis des etablierten Anbieters ausgehen. Kommen nun positive Netzeffekte und steigende Skalenerträge zusammen, was bei Online-Plattformen regelmäßig der Fall ist, so verstärken sich beide Effekte und ein Marktverschluss ist für eine etablierte Plattform relativ einfach möglich. Diese Logik lässt sich auch auf angrenzende Märkte erweitern, sofern Verbundvorteile (economies of scope) und/oder Netzeffekte auch über Produktgruppen hinweg eine Rolle spielen.

Michael Katz hat dies jüngst wie folgt zusammengefasst: „Although the issues are particularly difficult, there are also reasons to believe that two-sided markets may be particularly fertile ground for exclusionary behaviour.“<sup>23</sup> Ähnlich schlussfolgern Amelio, Karlinger und Valletti: „Traditional exclusionary practices carry over to platform competition and in some circumstances indirect network externalities accentuate the incentive to foreclose by incumbents.“<sup>24</sup> Eine schärfere kartellrechtliche Missbrauchsaufsicht speziell für Plattformen scheint daher angezeigt. Wie diese aussehen kann, erarbeiten Heike Schweitzer, Wolfgang Kerber und ich gerade im Auftrag des Bundesministeriums für Wirtschaft und Energie.

Zu wenig beleuchtet wurde bisher aber vor allem die Interdependenz zwischen Marktmacht und Informationsasymmetrien insbesondere bei Plattformen, auf denen Nutzer Preise oder Produkte vergleichen. Ein Beispiel wären etwa die Google-Rankings oder auch Rankings bei anderen Portalen, die sich immer wieder dem Vorwurf verzerrter Rankings der Suchergebnisse ausgesetzt sehen („search bias“), sodass konzerneigene Dienste bevorzugt werden, während zugleich konkurrierende Angebote – wie etwa Preisvergleichsportale im Fall von Google Shopping – strategisch nach hinten geschoben werden.

Sofern Nutzer nicht ohne bedeutende Anstrengungen eine solche Verzerrung erkennen können, wird eine solche Praxis auch nicht durch Wettbewerb sanktioniert. Ökonomisch betrachtet geht es hier um Vertrauensgüter, bei denen Nutzer auch nach dem Konsum/der Nutzung die Qualität einer Dienstleistung nicht erkennen können. Bei solchen Vertrauensgütern kann Wettbewerb nur schwer disziplinierend wir-

19 Dazu C. Kehder: Konzepte und Methoden der Marktabgrenzung und ihre Anwendung auf zweiseitige Märkte, Baden-Baden 2013.

20 Vgl. etwa J. Haucap, T. Stühmeier, a. a. O.

21 I. Segal, M. Whinston: Naked Exclusion: Comment, in: American Economic Review, 90. Jg. (2000), H. 1, S. 296-309.

22 H. Vasconcelos: Is Exclusionary Pricing Anticompetitive in Two-sided Markets?, in: International Journal of Industrial Organization, 40. Jg. (2015), H. C, S. 1-10.

23 M. Katz: Exclusionary Conduct in Multi-sided Markets, OECD Hearing on Re-thinking the use of traditional antitrust enforcement tools in multi-sided markets, OECD Document DAF/COMP/WD(2017)28/FINAL, 2017, Tz. 81.

24 A. Amelio, L. Karlinger, T. Valletti: Exclusionary Practices and Two-sided Platforms, OECD Hearing on Re-thinking the use of traditional antitrust enforcement tools in multi-sided markets, OECD Document DAF/COMP/WD(2017)34/FINAL, 2017.

ken. Dies gilt umso mehr, je weniger Vergleichsmöglichkeiten die Nutzer haben. In einem solchen Fall kann durch eine strategische Verzerrung von Rankings, indem eigene Dienste präferiert werden, die Marktmacht auf angrenzende Märkte ausgedehnt werden, was wiederum dort die Vergleichsmöglichkeiten reduziert und zum Erhalt der Marktmacht führt. Somit können fehlende Vergleichsmöglichkeiten (also Informationsasymmetrien) zum Ausbau von Marktmacht führen, während umgekehrt der Ausbau von Marktmacht wiederum Vergleichsmöglichkeiten reduziert und Informationsasymmetrien verschärft. Dieser sich selbst verstärkende Mechanismus induziert einen gesonderten Handlungsbedarf in der Wettbewerbsaufsicht.

### Implikationen der DSGVO und Fazit

Die Auswirkungen der DSGVO für den Wettbewerb dürften ambivalent sein. Zum einen reduziert die Harmonisierung des Datenschutzrechts in der EU die Kosten, geschäftlich in mehreren EU-Mitgliedstaaten aktiv zu

werden und somit die Markteintrittsbarrieren für Unternehmen. Zugleich wird durch die Stärkung der Verbraucherrechte, insbesondere die Portabilität von Daten, tendenziell auch der Wettbewerb befördert. Zum anderen sind jedoch gerade kleine Unternehmen oftmals mit – relativ betrachtet – höheren Umsetzungskosten konfrontiert als Großunternehmen. Dies verschafft großen Unternehmen tendenziell einen Vorteil und kann insbesondere für Start-ups und kleine und mittlere Unternehmen innovativshemmend wirken.

Allgemein ergeben sich bei datengetriebenen Geschäftsmodellen durchaus einige neue Wettbewerbsprobleme, wie etwa die Frage des Datenzugangs im Sinne einer wesentlichen Einrichtung, die potenzielle Kartellbildung durch Algorithmen sowie die Interdependenz zwischen Informationsproblemen und Marktmacht. Jedoch entstehen durch die prinzipiell mögliche parallele oder sequenzielle Nutzbarkeit von Daten auch Chancen für den Wettbewerb, die nicht übersehen werden sollten.

Stefan Klein, Joschka Hüllmann

## Datenkapitalismus akademischer Wissenschaftsverlage

Elsevier ist ein global führender akademischer Wissenschaftsverlag, der sich auf die Bereiche Wissenschaft, Bildung und Gesundheit spezialisiert hat. Wie die gesamte Medienbranche sind die Wissenschaftsverlage von der Digitalisierung unmittelbar betroffen. Während die physische Produktion von Büchern und Zeitschriften auf dem Rückzug ist, bauen die Verlage digitale Archive ihrer herausgegebenen Beiträge auf, die zugleich als Vertriebsplattformen dienen. Dabei sehen sich Unternehmen wie Elsevier zunehmend nicht mehr als Verlag, sondern als „global information analytics company“<sup>1</sup>. Die Analyse einiger Bausteine des Geschäftsmodells des Marktführers Elsevier veranschaulicht die Mechanismen dieser spezifischen Variante des Datenkapitalismus, der in ähnlicher Form auch von den anderen akademischen Verlagsgruppen praktiziert wird.<sup>2</sup>

### Geschäftsmodell

Aus ökonomischer Sicht betreibt Elsevier eine spezielle mehrseitige Plattform:<sup>3</sup>

1. Auf der einen Marktseite stehen Autoren, Herausgeber und Gutachter, welche die von Elsevier vertriebenen Inhalte produzieren (Produzenten).
2. Auf der anderen Seite stehen die Leser, die von den reichhaltigen, digital verfügbaren Informations- und Serviceangeboten profitieren. Da sie die Kosten der Nutzung in der Regel nicht tragen, führen der einfache Zugang, kombiniert mit personalisierten Empfehlungen zu steigender Nutzungsintensität, d. h. zum Aufruf oder Download von Beiträgen (Konsumenten).
3. Bibliotheken von Forschungsinstitutionen und Universitäten finanzieren die Produzenten (1) und bezahlen für den Zugang der Konsumenten (2).

Gemäß der Logik mehrseitiger Märkte subventioniert (3) die Leser (2) und finanziert die Medienproduktion (1). Seitenübergreifende positive Netzwerkexternalitäten gibt es zwischen Marktseite (1) und (2): (1) schafft Angebot für (2), (2) schafft positive Reputationseffekte für (1). Entgegen der Logik mehrseitiger Märkte finden allerdings keine direkten Transaktionen zwischen den Marktseiten statt, sondern nur zwischen Marktseiten und Plattform. Gruppe (3) gewährt den Zugang für die Leser (2) (soweit es sich um Angehörige der eigenen Institution handelt) als Teil ih-

1 Elsevier: Editor Welcome Package, September 2017, S. 5, [https://www.elsevier.com/\\_data/assets/pdf\\_file/0015/90123/EditorWelcomePack.pdf](https://www.elsevier.com/_data/assets/pdf_file/0015/90123/EditorWelcomePack.pdf) (9.7.2018).

2 Z. B. SpringerNature und Wiley.

3 Vgl. M. Kenney, J. Zysman: The Rise of the Platform Economy, in: Issues in Science and Technology, 2016, S. 61-69.

res Leistungsangebots, profitiert aber nur indirekt im Sinne der Abwendung negativer Reputationseffekte. Gruppe (3) profitiert durch positive Reputationseffekte von Publikationsleistungen von (1) aus der eigenen Institution. Insgesamt gibt es keine oder minimale Erträge für Gruppe (3) und negative seitenübergreifende Externalitäten durch die (auch) nachfrageorientierte Preispolitik der Plattformbetreiber (Verlage).

Digitale Archive wie ScienceDirect weisen starke Skaleneffekte auf: Die Betriebskosten pro Artikel sinken mit der Zahl der Beiträge, und die Attraktivität der Sammlung steigt mit ihrem Umfang (Bündelungseffekte). Nutzerzahl und Nutzungsfrequenz bilden die Basis von Empfehlungen, welche die Nutzungsfrequenz wiederum erhöhen und damit für Autoren, deren Institutionen und Zeitschriften den Impact-Faktor verbessern. Gold Open Access gegen Zahlung von Bearbeitungsgebühren (article processing charges, APC), ein Euphemismus für die Rückübertragung der Verwertungsrechte an publizierten Beiträgen, ist nicht nur äußerst lukrativ für die Verlage, es ist auch kompatibel mit dem Interesse der Autoren an erhöhten Downloadzahlen.

Die Verlage stellen den Bibliotheken nicht nur standardisierte Downloadstatistiken (COUNTER)<sup>4</sup> und über Nutzerabfragen nicht lizenzierter Inhalte (turn aways) zur Verfügung, sondern bieten darüber hinaus weitreichende, kostenpflichtige Nutzungsstatistiken, z. B. über SciVal (Elsevier), an. Aus Sicht der Bibliotheken entspricht dies der Auslagerung der Datenanalyse an den Leistungsanbieter. Die Nutzungsstatistiken kombinieren anonyme Abfragen aus der von Elsevier registrierten und freigegebenen IP-Adresse, z. B. der WWU Münster, mit personenbezogenen Informationen der Nutzer, sofern diese sich für irgendeinen Dienst von Elsevier registriert haben.

Die Nutzungsstatistiken der Verlage ermöglichen den Bibliotheken nutzungsbezogene interne Abrechnungen, z. B. gegenüber Fachbereichen. Gleichzeitig sehen die Verlage diese Statistiken jedoch als Rechtfertigung steigender Preise.

### Aufbau einer integrierten digitalen Plattform

Zwar bilden die digitalen Archive den Kern von Elseviers Plattform, sie werden aber erweitert durch ein Netzwerk digitaler Lösungen,<sup>5</sup> welches die Wertschöpfungskette akademischer Wissensproduktion unterstützt. Dieses

4 The COUNTER Code of Practice, <https://www.projectcounter.org/code-of-practice-sections/usage-reports/> (4.7.2018).

5 Elsevier: All Elsevier digital solutions, <https://www.elsevier.com/solutions> (4.7.2018).

Netzwerk an Lösungen, darunter SCOPUS (Referenzdatenbank und SCImago Journal Rank), Mendeley (Literaturverwaltung) und SSRN (Archiv für graue Literatur und Pre-Prints), unterstreicht die strategische Reorientierung vom Anbieter von Inhalten zu einem Anbieter von Tools und Informationsdienstleistungen entlang der Produktion, Analyse, Archivierung und Distribution akademischer Publikationen, mithin für Autoren, Leser, Herausgeber und Gutachter sowie Forschungsinstitutionen und Bibliotheken.<sup>6</sup> Die Dienstleistungen bedienen effizient die Bedürfnisse von Lesern und Autoren und ändern damit zugleich die akademische Wissensproduktion.

Für den Aufbau ihrer digitalen Archive akquirieren die Wissenschaftsverlage Verwertungsrechte der zu publizierenden Beiträge im Gegenzug und als Vorbedingung für die Veröffentlichung der Beiträge, d. h., zumeist ohne Vergütung der Autoren. Sie nutzen dabei die Bedeutung des Publikationserfolgs in namhaften wissenschaftlichen Zeitschriften als Bedingung akademischer Reputation und damit akademischer Karrierechancen aus. Die erzwungene Aufgabe der Rechte am intellektuellen Eigentum als Preis für die Publikation stellt dabei potenziell einen Missbrauch der Marktmacht dar.

Während die Reputation einer Zeitschrift in der akademischen Gemeinschaft und die damit einhergehende Bereitschaft von Herausgebern und Gutachtern erhebliche Arbeitszeit – ohne oder gegen marginale Vergütung – für die Publikation von Beiträgen zu investieren im Vordergrund der akademischen Aufmerksamkeit steht, sind Eigentum und Kontrolle an eben diesen Zeitschriften durch den Verlag im Hintergrund. So gelingt es den Verlagen, ein System freiwilliger und weitgehend unbezahlter Arbeit aufrechtzuerhalten<sup>7</sup> und Umsatzrenditen von 40 %<sup>8</sup> zu erzielen.

In dem Corporate-Responsibility-Bericht des Elsevier-Mutterkonzerns erhebt das Unternehmen Anspruch auf die Legitimität der Verwertungsrechte und bestätigt auch die strategische Neuausrichtung hin zu plattformübergreifender Datenanalyse: „... underpins our business strategy to deliver improved outcomes for our customers by combining content and data with analytics and technology across global platforms. It helps us build leading positions

6 R. C. Schonfeld: When is a Publisher not a Publisher? Cobbling Together the Pieces to Build a Workflow Business, in: The Scholarly Kitchen, 9.2.2017, <https://scholarlykitchen.sspnet.org/2017/02/09/cobbling-together-workflow-businesses> (4.7.2018).

7 G. Monbiot: Academic publishers make Murdoch look like a socialist | Comment is free, in: The Guardian, 29.8.2011, <https://www.theguardian.com/commentisfree/2011/aug/29/academic-publishers-murdoch-socialist> (9.7.2018).

8 RELX Group: Corporate Responsibility Report 2017, London 2017, S. 5, <https://www.relx.com/-/media/Files/R/RELX-Group/documents/responsibility/download-center/relx2017-cr-report.pdf> (9.7.2018).

in our markets by leveraging *our* skills and assets.“<sup>9</sup> Die Analyse von Soros trifft das sorgfältig aufgebaute Selbstbild: „The exceptional profitability of these companies is largely a function of ... avoiding paying for the content on their platforms. They claim they are merely distributing information. But the fact that they are near-monopoly distributors makes them public utilities and should subject them to more stringent regulations, aimed at preserving competition, innovation, and fair and open universal access.“<sup>10</sup>

### Datensammlung und -aggregation

Elsevier sammelt zunehmend umfassendere und detaillierte Daten über die Nutzer seiner digitalen Infrastruktur: über das Lese- bzw. Downloadverhalten, die Sammlung und Annotation von Quellen in Mendeley, die Nutzung von SSRN (Upload und Download), die Reviewtätigkeit (Inhalt der Reviews, Umfang der Reviewtätigkeit, Termintreue etc.), aber auch institutionelle Forschungsschwerpunkte. Die von Elsevier gesammelten Informationen sind potenziell für Wissenschaftsspionage (Wer forscht an welchen Themen?) wie für Überwachung (Welche Literatur wird gelesen und genutzt?) geeignet.<sup>11</sup>

Die Datenschutzerklärung von Elsevier dokumentiert Umfang und Zwecke der Datensammlungen über Nutzer, deren Verhalten und deren Weitergabe an Dritte: „We collect information about you in three ways: directly from your input, from third-party sources, and through automated technologies. ... Content that you upload and share or store in your account, such as annotations, comments, contributions and replies ... We are committed to delivering a relevant and useful experience to you. Depending on how you interact with us and the Service, we use your personal information to: ... Deliver targeted advertisements, promotional messages, and other information related to the Service and to your interests; ... Identify usage trends and develop data analysis, including for the purposes of research, audits, reporting and other business operations, such as to pay royalties and license fees to third-party content providers, ... evaluate our business performance.“<sup>12</sup> Dazu kommen „details and other information about you from other entities within the RELX Group and from third parties, including: Social networks ..., Service providers ..., Partners ... and/or publicly

available sources and data suppliers“ sowie technische Informationen wie IP-Adresse, Browser, Betriebssystem, benutztes Gerät, Referrer und mehr.

Die Menge und Reichhaltigkeit der Informationen lässt sich mit denen von Facebook oder Google vergleichen. Die Informationen werden aktuell verwendet, Elseviers eigene Angebote zu verbessern oder zu erweitern, etwa für Forschungsmonitoring und Impact-Analysen (z.B. Plum Analytics). Informationen über weitergehende Verwendung, z.B. Verkauf an Dritte, sind spärlich. Es gibt keine technische Transparenz oder Möglichkeit, interne Algorithmen nachzuvollziehen bzw. die gemachten Angaben zu überprüfen. Die Nutzer müssen den Aussagen Elseviers vertrauen oder auf die Nutzung der Dienste verzichten.

### Monopolisierung

Nach Einschätzung des Bundeskartellamts<sup>13</sup> ist Facebook ein marktbeherrschendes Unternehmen, sodass das Ausmaß der Sammlung und Verwendung von Nutzerdaten aus Drittquellen möglicherweise den Tatbestand des Missbrauchs einer marktbeherrschenden Stellung (in der Gestaltung der Nutzungsbedingungen) und Datenschutzverstöße erfüllt. Vergleichbar Elsevier: als Marktführer im Bereich akademischer Publikationen, für die es in den meisten Fällen keinen alternativen Zugang und keine Substitutionsmöglichkeit gibt, werden den Nutzern Bedingungen oktroyiert, denen sich die Nutzer, für deren Arbeit der Zugang zu spezifischen Beiträgen essenziell ist, kaum entziehen können. Sammlung und Nutzung von Fremddaten wie auch die Weitergabe von Nutzerdaten an Dritte sind intransparent und könnten Datenschutzverstöße darstellen. Viele Autoren haben angesichts der Reputation und Spezialisierung der von Elsevier vertriebenen Zeitschriften nur begrenzte Alternativen, z.B. Open-Access-Zeitschriften, ohne dabei Einbußen an ihren Karriereaussichten zu riskieren. Zwar ist diese Situation auch eine Folge von Fehlentwicklungen des akademischen Systems (einseitige Fokussierung auf Publikationserfolg in hoch gerankten Zeitschriften), aber sie wird durch das Geschäftsmodell von Elsevier systematisch gefördert, ausgenutzt und verschärft. Die potenzielle Interessenkollusion der Rollen Verlag und Rankingdienstleister widerspricht den Regeln guter Governance, ist aber Teil von Elseviers Geschäftsmodell.<sup>14</sup>

9 Ebenda, Hervorhebung nicht im Original.

10 G. Soros: Remarks delivered at the World Economic Forum, Davos, Schweiz, 25.1.2018, <https://www.georgesoros.com/2018/01/25/remarks-delivered-at-the-world-economic-forum> (9.7.2018).

11 S. Zuboff: Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, in: Journal of Information Technology, 30. Jg. (2015), H. 30, S. 75.

12 Elsevier: Privacy Policy, 22.5.2018, S. 1-2, [https://www.elsevier.com/\\_data/assets/pdf\\_file/0006/732795/Elsevier\\_Global\\_Privacy\\_Policy-2018-05-22.PDF](https://www.elsevier.com/_data/assets/pdf_file/0006/732795/Elsevier_Global_Privacy_Policy-2018-05-22.PDF) (9.7.2018).

13 Bundeskartellamt: Vorläufige Einschätzung im Facebook-Verfahren: Das Sammeln und Verwerten von Daten aus Drittquellen außerhalb der Facebook Website ist missbräuchlich, Pressemitteilung vom 19.12.2017, [https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2017/19\\_12\\_2017\\_Facebook.html](https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2017/19_12_2017_Facebook.html) (4.7.2018).

14 Ein aktuelles Beispiel einer Interessenkollusion: J. Tenant: Elsevier are corrupting open science in Europe, 29.6.2018, <https://www.theguardian.com/science/political-science/2018/jun/29/elsevier-are-corrupting-open-science-in-europe> (4.7.2018).

## Geschäftsgebaren

So wie Facebook die Datenintegration mit WhatsApp vorangetrieben hat, hat Elsevier Mendeley und SSRN, beides vormals eigenständige Lösungen, die sich den Zielen der Forschungscommunity verpflichtet sahen, integriert. Elsevier setzt die eigenen Rechte im Zweifel gegen die eigenen Autoren durch und sendet Abmahnungen, wenn Artikel auf Academia.edu oder ResearchGate verfügbar gemacht wurden.<sup>15</sup>

2016 haben Eve, Lawson und Tennant Anklage gegen die RELX-Gruppe bei der britischen Kartellbehörde (UK Competition and Markets Authority) wegen Missbrauchs einer dominanten Marktposition und wettbewerbswidriger Praktiken erhoben.<sup>16</sup> Hintergrund sind unter anderem die Geheimhaltungsklauseln in den Verträgen mit Bibliotheken, die den EU-Transparenzregeln bei öffentlicher Beschaffung widersprechen. Die Verhandlungen über ein wissenschaftsfreundliches Lizenzmodell für Bibliotheken in Deutschland im Rahmen des DEAL-Konsortiums haben auch nach zwei Jahren noch keine sichtbaren Fortschritte gemacht.

Das Ausmaß der Geheimhaltung und der Mangel an Transparenz widerspricht den Regeln und dem Geist einer kooperativen Beziehung zwischen Autor und Verlag, wie sie noch von Elseviers Logo symbolisiert und unter Verweis auf die Geschichte reklamiert werden: „Publishers and scholars cannot do it alone. They need each other. This remains as apt a representation of the rela-

15 S. Robinson: Elsevier issues academics thousands of takedown notices, doesn't want any friends anyway, 13.1.2014, <https://www.mh-pbooks.com/elsevier-issues-academics-thousands-of-takedown-notices-doesnt-want-any-friends-anyway> (4.7.2018).

16 M. P. Eve: Anti-competitive practices of RELX Group, 2016, <https://www.martineve.com/images/CMA-RELX.pdf> (4.7.2018).

onship between Elsevier and its authors today – neither dependent, nor independent, but interdependent.“<sup>17</sup>

## Notwendige Debatte

Die Situation der dominierenden Wissenschaftsverlage ist vergleichbar mit der von Facebook oder Google: Die Erstellung und Nutzung der Kernleistung (wissenschaftliche Veröffentlichungen) wird durch ein wachsendes Repertoire digitaler Tools erweitert; beides bildet die Grundlage zur Sammlung von Nutzerdaten, die aus externen Quellen ergänzt werden – angeblich im Interesse der Nutzer. Soweit erkennbar werden die Daten bisher überwiegend zur Verbesserung des Angebots, zur Intensivierung der Nutzung (Empfehlungen) und zum Aufbau kostenpflichtiger statistischer Informationen für Bibliotheken und akademische Institutionen verwendet. Die digitale Wissensproduktion ermöglicht so die „Datafication“ der Wissenschaft, die als analytisches Wissenschaftsmanagement vermarktet wird und zugleich ungeahnte Potenziale der Überwachung einzelner Wissenschaftler und des Wissenschaftsbetriebs erzeugt.

Systematische Intransparenz und das Geschäftsgebaren von Elsevier begründen die Sorge, dass Elsevier seine Marktposition missbraucht, Datenschutzregeln missachtet und sensible Nutzerdaten ausbeuten könnte. Mehr Transparenz und wirksamere Governancestrukturen der marktführenden Wissenschaftsverlage sind daher erforderlich, aber auch eine breitere Diskussion möglicher Regeln zur Begrenzung der Ausbeutung von Autoren und Gutachtern sowie zur Sicherstellung eines angemessen bezahlten Zugangs zu den Archiven der Wissenschaftsverlage sind im Interesse der Gesellschaft.

17 Elsevier: History, <https://www.elsevier.com/en-gb/about/our-business/history> (4.7.2018).

### Title: *Data Capitalism – an Economic Approach*

**Abstract:** *Companies aggregate, process and monetise data about consumers by leveraging actively shared information as well as the data they glean from tracking offline transactions. Data-driven business models come in two forms: Firms either use the personal data of users to tailor their own offerings to them, or they sell the data to others who use it for their own ends. These models have different implications for the protection of consumers. While they are typically reasonably well-informed about the data they transmit to a particular firm, they have less control about whom their data is sold on to. Consumers are regularly confronted with a lot of privacy-relevant information and choices, but they struggle to make decisions that are in line with their stated privacy preferences. Therefore, regulation should address privacy design concepts that actually foster control. The right to data portability is one of the fundamentally new elements of the General Data Protection Regulation. However, its economic implications are potentially very complex and, under certain circumstances, data portability may not even be in the interest of consumers. Nevertheless, the strengthening of consumer rights may likewise support competition. The monetary value of data is difficult to calculate. But if consumers are interested in a fair profit share of personal data markets, policy makers may disregard their claims. One article highlights the transformation in the academic publishing industry (STM) from a traditional focus on publishing services to a new emphasis on data analytics by reconstructing and illustrating the mechanisms of data capitalism. It offers an explanation for the growing profitability and concentration of the STM industry despite the growing open science movement.*

**JEL Classification:** D43, K24, L10, L40