Schweitzer, Heike; Peitz, Martin

Working Paper

Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?

ZEW Discussion Papers, No. 17-043

Provided in Cooperation with:
ZEW - Leibniz Centre for European Economic Research

Suggested Citation: Schweitzer, Heike; Peitz, Martin (2017) : Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?, ZEW Discussion Papers, No. 17-043, Zentrum für Europäische Wirtschaftsforschung (ZEW), Mannheim, https://nbn-resolving.de/urn:nbn:de:bsz:180-madoc-436113

This Version is available at:
https://hdl.handle.net/10419/170697

Discussion Paper No. 17-043

Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?

Heike Schweitzer und Martin Peitz

ZEW
Zentrum für Europäische Wirtschaftsforschung GmbH
Centre for European Economic Research

Discussion Paper No. 17-043

Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?

Heike Schweitzer und Martin Peitz

Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?[1]

Heike Schweitzer, Freie Universität Berlin

Martin Peitz, Universität Mannheim und MaCCI

18. Oktober 2017

Kurzzusammenfassung: Die Autoren untersuchen die Funktionsweise von Datenmärkten. Besonderes Augenmerk wird dabei auch auf Substitute zu einem „Handel mit Daten" im engeren Sinne gelegt. Die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten ist für die Analyse der Funktionsweise und möglicher Funktionsdefizite von Datenmärkten von zentraler Bedeutung. Die Funktionsweise von Märkten für personenbezogene Daten kann insbesondere durch das Recht auf Datenportabilität (Art. 20 DSGVO) nachhaltig geprägt werden. Dies hängt allerdings von der konkreten Ausgestaltung des Rechts auf Datenportabilität ab. Funktional kann dieses Recht unter anderem als eine Abhilfe für eine durch das Datenschutzrecht bedingte partielle Marktbehinderung verstanden werden. Die Einführung eines - allerdings nur bei Marktmachtlagen zwingenden – Rechts auf Datenportabilität kann auch für nicht personenbezogene Daten sinnvoll sein. Es würde dann auf eine andere Form von Marktversagen reagieren. Im Übrigen sehen die Autoren weder bei personenbezogenen noch bei nicht personenbezogenen Daten einen gesetzgeberischen Handlungsbedarf zur allgemeinen Förderung des Datenhandels.

Stichworte: Datenhandel, personenbezogene Daten, nicht personenbezogene Daten, Datenportabilität

[1] Die Autoren danken den Teilnehmerinnen und Teilnehmern der Workshops im Rahmen des Fachdialogs Ordnungsrahmen für die Digitale Wirtschaft für Kommentare und Hinweise. Die Studie wurde im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) angefertigt. Sie gibt nur die Meinung der Autoren wieder und nicht zwingend Positionen des BMWi.

Data markets in the digitized economy: Functional deficiencies and the need for regulation?

Heike Schweitzer and Martin Peitz

Abstract: The authors examine the functioning of data markets. Particular attention is paid to substitutes for "data trading" in a narrow sense. In the analysis of the functioning and possible functional deficiencies of data markets, it is necessary to distinguish between markets for personal data and markets for non-personal data. In the functioning of markets for personal data, the right to data portability (Article 20 of the GDPR) may play an important role. Functionally, the right to data portability can be understood as a remedy for the restrictions to trade that follow from data protection law. There may be a good case for introducing a right to data portability also for non-personal data. However, it would react to a different form of market failure and should be mandatory only in the presence of market power. Apart from this, the authors currently do not see a need for legislative action to promote data trading—this holds for personal as well as for non-personal data.

Keywords: data trading, personal data, non-personal data, data portability

Inhaltsverzeichnis

Data markets in the digitized economy: Functional deficiencies and the need for regulation?

Heike Schweitzer and Martin Peitz

Executive Summary

Machine data as well as user-generated data are an important raw material in the data driven economy. If companies have access to this raw material, these data can contribute significantly to improved production and sales processes, product development and innovation, and to more successful marketing. From today's point of view, access to data is often not the limiting factor, however, but the ability of firm to make good use of the data and to develop innovative application ideas.

Companies that do not have sufficient access to relevant data themselves can try to obtain access to data on "data markets". However, a study of data markets should not be confined, from the outset, to certain types of markets (e.g., "secondary markets" for data). Access to data is possible either through the primary market—i.e., the collection of data directly from the data producer—or secondary data markets in a narrow sense—here we distinguish between bilateral negotiations and more standardized market relations (including platforms). In addition, access is possible via data sharing. An alternative to accessing data may be the use of data services (markets for data derivatives). Depending on the intended use, these various forms of data access may be substitutes from a data user perspective.

In the analysis of the functioning and possible functional deficiencies of data markets, it is necessary to distinguish between markets for personal data and markets for non-personal data. Data protection law decisively influences the functioning of markets for personal data. A clarification how the General Data Protection Regulation (GDPR) will influence the functioning of primary markets, where data are collected directly from consumers, is urgently needed. It depends on the requirements that the GDPR places on the effectiveness of consent, especially where consumers "pay" with data. Moreover, data protection law does not exclude data trading on secondary markets altogether. Yet, the legal limits of such data trading will need to be clarified, too.

The access to personal data is currently carried out mainly through the primary market—i.e., data are collected in direct contact with the consumers. Other companies may benefit indirectly from the existence of personal data through the use of data services (e.g., targeted advertising) offered by particularly "data-rich" companies. Finally, data sharing is also important for personal data. “Data trading” in the narrower sense on secondary markets is of very limited importance. One reason is the often limited interest of "data-rich" market players in the trading of personal data: the data are then understood as a key competitive advantage. Besides, data protection law also limits “data trade” in a

narrow sense. The further development of a data trade in a narrow sense for personal data would arguably require the involvement of the affected parties. This can be done via Personal Information Management Systems (PIMS)—for example, Industrial Data Space, MyData. But their market success is not yet a given.

The introduction of a right to data portability (Article 20 of the GDPR) seems to be of much more immediate importance to make sure that a company can gain access to personal data. A data subject may request the transfer of the data related to her, thus facilitating the change of supplier. Specialized forms of data portability in the area of smart metering and in payment services, for example, show that the avoidance of an aftermarket lock-in and the promotion of competition is the real function of data portability, rather than the protection of the general personality right. Functionally, the right to portability of personal data can be regarded as a compensation for the weakening of the secondary markets for personal data by data protection law.

The current structure of “trade” in personal data (in a broader sense) does not ensure a positive equality of opportunity for enterprises in accessing data: the great importance of the primary market for data access can lead to a competitive advantage for large and successful market players. Network effects that promote concentration in platform markets can also lead to a certain concentration of data access. However, this competitive advantage does not systematically prevent market entry, nor does it systematically lead to market foreclosure. Smaller companies can frequently use other forms of (direct or indirect) data access.

In the opinion of the authors, there is currently no apparent need for legislative action to promote the general trading of personal data beyond the applicable legal framework. However, it is important to clarify the prerequisites and limitations of data access on the primary market. Also, in certain constellations competition law may play a role: In the B2B area, there are complaints that large platforms such as Apple and Google hinder the access of app providers to user data or prevent others from obtaining data access. In addition, exclusivity agreements regarding data access must be critically examined, in case they involve dominant companies.

In the case of non-personal data, as in the case of personal data, self-use and vertical integration play an important role. Data sharing is relevant where companies have an interest in cooperating with others (e.g., autonomous driving, mobility data, and parallel data access by machine manufacturers and machine users). To a limited extent, a bilateral data trade in the strict sense takes place. Bilaterally negotiated contracts are the basis of this trade. Data trading via platforms can be observed mainly with a view to public data. However, there are few examples of a platform trading with private (in the sense of non-public) data. Such trading is not precluded by any legal requirements. Furthermore, it is not a lack of data ownership rights that prevents such a "trade": The access of "data buyers" to the data, which typically remain on the server of the "data vendor", can be technically prevented or limited, such that the de facto data owner retains control. Rather, as in the case of personal data, there is a considerable interest of the companies in the exclusive use of data as a competitive advantage.

A few platforms provide centralized access to data sets. Several factors are conducive to data trading via a platform: (a) the data are standardized products / the compatibility of the data is ensured; (b) there are reliable technical possibilities for effectively limiting accessibility and securing the data; and

(c) trust in the reliability of the business partners. While platforms can affect these factors, it is not clear whether any standardization of data accesses can satisfy the variety of users' interests. It is also not clear whether the technical safeguards currently allow a de facto anonymized trade. Beyond the limited self-interest of many data-rich companies in an open trade with datasets via platforms, these specific requirements imply further boundaries for the provision of data on platforms.

In markets for non-personal data, on the basis of the information available to the authors, there is no systematic market failure across sectors. The focus on self-use and bilateral trade or data sharing, which is currently being observed, does not lead to perfect solutions. The transaction costs in “data trading” tend to be high. A lack of data access can—depending on the context—lead to obstacles to market entry. Constellations are also conceivable in which new "aftermarket" problems arise. These problems are, however, fundamentally to be mastered by means of competition law. In Germany, the prohibition of the abuse of relative market power (§ 20 GWB) is available in addition to the prohibition of abuse of dominant positions (Article 102 TFEU, § 19 GWB).

New property rights are unlikely to improve the functioning of the markets for non-personal data. In view of the uncertainties regarding the proper specification and the correct allocation of these rights, they are not likely to reduce transaction costs in data markets. In addition, property rights are not suitable for counteracting market imbalances.

The EU Commission is considering the creation of a new data producer’s right. Such a right need not necessarily constitute a property right. Its function is primarily to ensure the access of the machine or service users to the usage data. While it seems plausible that machine manufacturers or service providers will regularly have de facto control over the usage data resulting from machine or service use, the assumption that there will be a market failure with regard to data access for machine or service users independent of a position of market dominance on the part of the manufacturer or service provider lacks sufficient validation. In a competitive setting, machine or service users with a sufficient interest in—for example, maintenance and value-added services—may be able to negotiate access rights to data. Conversely, legitimate interests of machine manufacturers or service providers in an exclusive data access are also conceivable—for example, based on product safety or secrecy concerns. Thus, a general "data producer’s right" in the sense of a property right-like data access right of the machine or service user irrespective of the manufacturer’s or service provider’s market power is not called for. However, it may be useful to consider positions of relative market power in addition to market dominance. Moreover, it may be useful to differentiate according to the type of data and uses. These considerations also argue against a full extension of the right to data portability (as set out in Article 20 GDPR with respect to personal data) to non-personal data. We should keep in mind that the former—beyond combating lock-in effects—is meant to compensate for the weakening of data traffic by data protection law.

Finally, data sharing between competitors—whether in markets for personal data or for non-personal data—must not violate the ban on cartels. Hence, the limits of Article 101 (1) TFEU / § 1 GWB must be kept in mind.

Zusammenfassung

Maschinendaten wie auch von Nutzern erzeugte Daten sind in der datengetriebenen Ökonomie ein wichtiger Rohstoff. Haben Unternehmen Zugang zu diesem Rohstoff, können diese Daten maßgeblich zu verbesserten Produktions- und Vertriebsabläufen, zur Produktentwicklung und –innovation und zu einem erfolgreicheren Marketing beitragen. Aus heutiger Sicht ist häufig allerdings nicht der Zugang zu Daten der beschränkende Faktor, sondern die Fähigkeit der Unternehmen, die Daten für die eigenen Zwecke zu nutzen und innovative Anwendungsideen zu entwickeln.

Unternehmen, die selbst keinen oder keinen hinreichenden Zugang zu den Daten haben, können versuchen, sich Zugang zu Daten auf „Datenmärkten" zu beschaffen. Eine Untersuchung von Datenmärkten sollte sich aber nicht von vornherein auf bestimmte Erscheinungsformen von Märkten (z.B. „Sekundärmärkte" für Daten) verengen. Ein *Zugriff auf Daten* ist entweder über den Primärmarkt möglich – d.h. über eine Erhebung von Daten unmittelbar beim Datenerzeuger, oder über sekundäre Datenmärkte im engeren Sinne, wobei hierbei zwischen durch bilaterale Verhandlungen geprägte Marktbeziehungen und stärker standardisierte Marktbeziehungen (einschließlich solcher, die über Plattformen zustande kommen) unterschieden werden kann. Ferner kommt ein Zugriff über Data Sharing in Betracht. Eine Alternative zum Zugriff auf Daten kann die *Nutzung von Datendienstleistungen* sein (Märkte für Datenderivate). Je nach dem verfolgten Zweck können diese verschiedenen Formen des Datenzugriffs aus Nachfragersicht Substitute sein.

In der Analyse der Funktionsweise und möglicher Funktionsdefizite von Datenmärkten ist zwischen Märkten für personenbezogene Daten und Märkten für nicht personenbezogene Daten zu unterscheiden. Die Funktionsweise von Märkten für personenbezogene Daten wird maßgeblich durch das Datenschutzrecht beeinflusst. Wie die Datenschutzgrundverordnung (DSGVO) die Funktionsweise von Primärmärkten beeinflussen wird, auf denen Daten direkt bei Konsumenten erhoben werden, gilt es dringend zu klären. Es hängt von den Anforderungen ab, welche die DSGVO an die Wirksamkeit der Einwilligung stellt – gerade auch dort, wo Daten als „Entgelt" fungieren. Das Datenschutzrecht schließt im Übrigen auch einen Datenhandel auf Sekundärmärkten nicht gänzlich aus. Ein solcher Datenhandel – wie auch ein Data Sharing – kann aber nur in engen rechtlichen Grenzen stattfinden.

Der Zugriff auf *personenbezogene Daten* erfolgt derzeit vor allem über den Primärmarkt – Daten werden im direkten Kontakt mit den Konsumenten gesammelt. Mittelbar profitieren Unternehmen von der Existenz personenbezogener Daten bei der Inanspruchnahme von Datendienstleistungen (z.B. Targeted Advertising), die von besonders „datenreichen" Unternehmen angeboten werden. Schließlich ist auch Data Sharing bei personenbezogenen Daten von Bedeutung. Eine sehr begrenzte Bedeutung hat demgegenüber der Datenhandel im engeren Sinne. Ein Grund hierfür ist das oftmals begrenzte Eigeninteresse „datenreicher" Marktakteure am Handel mit personenbezogenen Daten: Die Daten werden dann als zentraler Wettbewerbsvorteil begriffen. Aber auch das Datenschutzrecht zieht dem Datenhandel im engeren Sinne enge Grenzen. Die Fortentwicklung eines Datenhandels im engeren Sinne für personenbezogene Daten ist praktisch wohl nur unter Einbeziehung der Betroffenen möglich. Diese kann über Personal Information Management Systeme (PIMS) erfolgen (zum Beispiel Industrial Data Space; MyData) – allerdings ist deren Markterfolg bislang nicht absehbar.

Eine praktisch größere Bedeutung für die Gewährleistung des Zugriffs von Unternehmen auf personenbezogene Daten hat die Einführung eines Rechts auf *Datenportabilität* (Art. 20 DSGVO). Es beinhaltet eine Ermächtigung der Betroffenen zur wirtschaftlichen Nutzung der auf sie bezogenen Daten, und erleichtert so den Anbieterwechsel. Spezialgesetzliche Ausformungen der Datenportabilität zum Beispiel im Bereich „Smart Metering“ und bei Zahlungsdiensten zeigen, dass hierin – und nicht im Schutz des Allgemeinen Persönlichkeitsrechts – die eigentliche Funktion der Datenportabilität liegt. Funktional ist das Recht auf Portabilität personenbezogener Daten zugleich als Kompensation für die Schwächung der Sekundärmärkte für personenbezogene Daten durch das Datenschutzrecht zu sehen.

Die derzeitige Struktur des Handels mit personenbezogenen Daten (im weiteren Sinne) gewährleistet zwar keine positive Chancengleichheit von Unternehmen im Zugriff auf Daten: Die große Bedeutung des Primärmarktes für den Datenzugriff kann zu einem Wettbewerbsvorteil großer und erfolgreicher Marktakteure führen. Netzwerkeffekte, welche die Konzentration in Plattformmärkten begünstigen, können zugleich zu einer gewissen Konzentration des Datenzugriffs führen. Dieser Wettbewerbsvorteil verhindert aber nach derzeitigem Erkenntnisstand neue Marktzutritte nicht systematisch beziehungsweise führt nicht systematisch zu Marktabschottung. Kleineren Unternehmen sind andere Formen des (unmittelbaren oder mittelbaren) Datenzugriffs möglich.

Ein gesetzgeberischer Handlungsbedarf zur allgemeinen Förderung des Handels mit personenbezogenen Daten über den geltenden Rechtsrahmen hinaus ist aus Sicht der Autoren zurzeit nicht ersichtlich. Sinnvoll wäre allerdings eine Klärung der Voraussetzungen und Grenzen des Datenzugriffs am Primärmarkt. Auch kann in bestimmten Konstellationen eine Anwendung des Wettbewerbsrechts zu prüfen sein: Im B2B-Bereich gibt es Beschwerden, dass große Plattformen wie Apple und Google den Zugriff von App-Anbietern auf Nutzerdaten behindern beziehungsweise sich den Datenzugriff selbst vorbehalten.[2] Auch Ausschließlichkeitsvereinbarungen bzgl. eines Datenzugriffs unter Beteiligung marktbeherrschender Unternehmen sind kritisch zu prüfen.

Auch bei *nicht personenbezogenen Daten* spielt Eigennutzung und vertikale Integration eine große Rolle. Data Sharing spielt dort eine Rolle, wo Unternehmen ein Eigeninteresse an der Zusammenarbeit haben (zum Beispiel autonomes Fahren; Mobility Data; denkbar auch: paralleler Datenzugriff durch Maschinenhersteller und Maschinennutzer). In eingegrenztem Umfang findet ein bilateraler Datenhandel im engeren Sinne statt. Grundlage dieses Handels sind Verträge, die bilateral ausgehandelt werden. Ein Datenhandel über Plattformen findet vor allem mit öffentlichen Daten statt. Wenige Beispiele finden sich dagegen für einen Plattformhandel mit privaten Daten. Dem stehen zwar keine rechtlichen Vorgaben entgegen. Auch ist nicht davon auszugehen, dass fehlende Dateneigentumsrechte einen solchen „Handel“ verhindern – denn der Zugriff von „Datenkäufern“ auf die Daten, die typischerweise auf dem Server des „Datenverkäufers“ verbleiben, kann technisch wirksam verhindert beziehungsweise begrenzt werden. Wie schon bei personenbezogenen Daten, so besteht aber auch bei nicht personenbezogenen Daten ein erhebliches Eigeninteresse der Unternehmen an der Nicht-Weitergabe der Daten und an der Nutzung des exklusiven Datenzugriffs als Wettbewerbsvorteil.

[2] European Innovators Open Letter to the EU Commission on DSM and Platforms, 4 May 2017.

Einige wenige Plattformen bieten einen zentralisierten Zugang zu Datensätzen an. Mehrere Faktoren sind für einen Plattformhandel mit Daten förderlich: (a) Bei den Daten handelt es sich um standardisierte Produkte / die Kompatibilität der Daten ist gewährleistet; (b) es bestehen zuverlässige technische Möglichkeiten zur effektiven Begrenzung von Zugriffsmöglichkeiten und zur Sicherung der Daten; und (c) es besteht Vertrauen in die Zuverlässigkeit der Geschäftspartner. Plattformen können zwar diese Faktoren beeinflussen, es ist aber nicht eindeutig, ob eine etwaige Standardisierung von Datenzugängen der Vielfalt der Verwendungsinteressen der Nachfrager entspricht. Es ist auch nicht klar, ob die technischen Sicherungsmöglichkeiten derzeit einem de facto stärker anonymisierten Handel ermöglichen. Jenseits des begrenzten Eigeninteresses vieler datenreicher Unternehmen an einem offenen Handel mit Datensätzen über Plattformen folgen aus diesen spezifischen Anforderungen weitergehende Grenzen für die Bereitstellung von Daten auf Plattformen.

In Märkten für nicht personenbezogene Daten lässt sich auf der Grundlage der den Autoren dieser Studie zur Verfügung stehenden Information sektorübergreifend kein systematisches Marktversagen feststellen. Der Fokus auf Eigennutzung und bilateralen Handel beziehungsweise Data Sharing, der derzeit zu beobachten ist, führt nicht zu perfekten Lösungen. Die Transaktionskosten im Datenhandel sind tendenziell hoch. Ein fehlender Datenzugang kann – je nach Kontext – zu Marktzutrittshindernisse führen. Ebenso sind Konstellationen denkbar, in denen neue „Aftermarket"-Probleme entstehen. Diese Probleme sind aber grundsätzlich mit Mitteln des Wettbewerbsrechts zu bewältigen – wobei in Deutschland neben dem Verbot des Missbrauchs marktbeherrschender Stellungen (Art. 102 AEUV; § 19 GWB) auch das Verbot des Missbrauchs relativer Marktmacht zur Verfügung steht (§ 20 GWB).

Neue Eigentumsrechte werden die Funktionsweise der Märkte für nicht personenbezogene Daten voraussichtlich nicht verbessern. Angesichts der Unsicherheiten hinsichtlich des richtigen Zuschnitts und hinsichtlich der richtigen Allokation dieser Rechte sind sie nicht geeignet, die Transaktionskosten in Datenmärkten zu senken. Eigentumsrechte sind ferner von vornherein ungeeignet, Machtungleichgewichten im Markt zu begegnen.

Die EU-Kommission erwägt die Schaffung eines neuen *Datenerzeugerrechts*. Dieses Recht muss nicht als Eigentumsrecht gedacht werden. Seine Funktion soll vor allem in der Gewährleistung des Zugangs der Maschinen- beziehungsweise Dienstenutzer zu den Nutzungsdaten liegen. Zwar besteht Grund zur Annahme, dass Maschinenhersteller beziehungsweise Diensteanbieter im Ausgangspunkt regelmäßig eine de facto-Kontrolle über die bei der Maschinen- oder Dienstenutzung anfallenden Nutzungsdaten haben. Das von der Kommission marktmachtunabhängig angenommene Marktversagen in der Gewährleistung eines Datenzugangs der Maschinen- oder Dienstenutzer ist aber bislang nicht hinreichend validiert. Zwar kann ein Interesse an der Offenhaltung etwa von Wartungs- und Mehrwertdienstemärkten und damit auch ein Interesse an Datenzugangs- und Weitergaberechten der Maschinen- oder Dienstenutzer bestehen. Umgekehrt sind aber auch legitime Interessen von Maschinenherstellern beziehungsweise Diensteanbietern an einem exklusiven Datenzugriff denkbar – etwa mit Blick auf Produktsicherheitsbedenken beim Datenzugriff oder mit Blick auf legitime Geheimhaltungsinteressen. Ein allgemeines „Datenerzeugerrecht" im Sinne eines marktmachtunabhängigen Datenzugangsrechts der Nutzer ist daher nicht opportun. Ausgangspunkt muss die Feststellung einer regelungsbedürftigen Machtlage sein – wobei auch relative Marktmacht zu berücksichtigen ist. Im Übrigen kann es sinnvoll sein, nach der Art der Daten und Verwendungszwecke zu differenzieren. Das Recht auf Datenportabilität bei personenbezogenen Daten (Art. 20 DSGVO) lässt sich schon deswegen nicht pauschal auf nicht personenbezogene Daten

übertragen, weil ersteres – jenseits der Bekämpfung von lock-in-Effekten – gerade auch die Schwächung des Datenhandels durch das Datenschutzrecht kompensiert.

Ein Data Sharing zwischen Wettbewerbern – ob in Märkten für personenbezogene Daten oder für nicht personenbezogene Daten – darf das *Kartellverbot* nicht verletzen. Die Grenzen des Art. 101 Abs. 1 AEUV / § 1 GWB sind daher im Blick zu halten.

A. Einleitung

Zu den zentralen Merkmalen der digitalen Ökonomie zählen die neuen Bedingungen der Verfügbarkeit und Verarbeitung von Daten. Neu sind vor allem die technologischen Möglichkeiten des Zugriffs auf sowie der Speicherung, Kombination und systematischen Auswertung von häufig unstrukturierten und nebenbei erzeugten Daten in Echtzeit. Sie schaffen Potentiale für Produkt- und Prozessverbesserung und -innovation, für Logistik, Trendvorhersage und Marketing. Sowohl der Zugang zu relevanten Daten als auch die Fähigkeit zur Datenanalyse werden damit zu wichtigen Wettbewerbsparametern. Gesprochen wird von einer sich neu entwickelnden „Datenwirtschaft".[3]

Angesichts der mit der neuen Datenwirtschaft verbundenen Chancen ist die Frage aufgeworfen, ob die europäische und die deutsche Rechtsordnung die für ihr Funktionieren beziehungsweise ihre Weiterentwicklung erforderlichen Regeln bereitstellen. Grundlage der Beurteilung muss ein besseres ökonomisches Verständnis der Datenwirtschaft sein. Wie gelangen Unternehmen an diejenigen Daten, die sie für ihre unternehmerische Tätigkeit benötigen? Was sind die wirtschaftlichen und rechtlichen Funktionsbedingungen von Datenmärkten in ihren verschiedenen Erscheinungsformen? Wie unterscheiden sich die Funktionsbedingungen der Märkte für personenbezogene und nicht personenbezogene Daten? Gibt es Anlass für die Annahme eines Marktversagens? Falls ja: was sind die Ursachen dieses Marktversagens? Handelt es sich um systematisches Marktversagen oder tritt es nur in einem bestimmten Marktumfeld auf? Und was sind mögliche Abhilfen? Ist etwa die Schaffung neuer Zugangsrechte sinnvoll? Benötigen wir anderweitige Anpassungen des rechtlichen Rahmens, um die Potentiale der neuen Datenwirtschaft zu realisieren?

Diese Fragen stehen derzeit hoch auf der rechtspolitischen Agenda der EU-Kommission. Der Aufbau einer wettbewerbsfähigen Datenwirtschaft ist – so die EU-Kommission in ihrer Mitteilung vom Januar 2017[4] – ein zentrales politisches Ziel der EU. Für die Datenwirtschaft sei ein „Strategie- und Rechtsrahmen zu schaffen, indem noch bestehende Hindernisse für den Datenverkehr abgebaut und die von den neuen Datentechniken aufgeworfenen rechtlichen Fragen geklärt werden".[5] Der EU-Kommission schwebt dabei ausweislich ihrer Mitteilung die Stärkung eines „sekundären" Datenhandels zwischen Unternehmen mit bereits vorhandenen Daten vor, denen zu einer stärkeren Verbreitung und damit Nutzung verholfen werden soll; also ein Datenhandel zwischen Unternehmen, die über Daten verfügen, und Unternehmen, die diese Daten verwenden möchten. Schwerpunkt der Überlegungen der Kommission sind dabei die nicht personenbezogenen Daten.

Ein „sekundärer" Datenhandel auf anonymen Märkten ist allerdings nur eine von vielen Möglichkeiten, Zugang zu Daten zu erhalten. Insoweit es um personenbezogene Daten geht, zieht das Datenschutzrecht dem „sekundären" Datenhandel überdies enge Grenzen. Auch bei nicht personenbezogenen Daten wird ein standardisierter Datenhandel auf anonymen Märkten häufig nicht den Interessen der Dateninhaber entsprechen. Statt von „Datenhandel" sprechen Unternehmen regelmäßig von „Datenökosystemen" und bringen damit zum Ausdruck, dass Daten nicht standardisiert, sondern in konkreten geschäftlichen Beziehungen weitergegeben werden, wenn dies einem gemeinsamen Interesse entspricht, und wenn gegebenenfalls konkrete „Governance"-

[3] Siehe Kommission, Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin.
[4] Kommission, Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin.
[5] Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 5

Mechanismen vereinbart wurden, um vereinbarte Nutzungsbeschränkungen überwachen und durchsetzen zu können.

Für ein Verständnis der Funktionsweise von „Datenmärkten“ und etwaiger Defizite solcher Märkte – einschließlich der skizzierten Datenökosysteme – ist es zunächst geboten, einen Überblick über die verschiedenen Möglichkeiten des Zugangs zu Daten zu gewinnen. Hierzu zählen neben dem Datenhandel im engeren Sinne die Möglichkeit einer unmittelbaren Datenbeschaffung, die Möglichkeit des Data Sharing und die Inanspruchnahme von datenbasierten Diensten.

Die vorliegende Studie versucht, existierende Datenmärkte und ihre Funktionsprinzipien in einer solch breiteren Perspektive zu systematisieren. Die Funktionsweise und Grenzen von Datenmärkten werden dabei maßgeblich von den rechtlichen Rahmenbedingungen mitbestimmt. Bei der Analyse eines etwaigen Marktversagens sind die geltenden rechtlichen Rahmenbedingungen stets in Rechnung zu stellen. Insoweit es um personenbezogene Daten geht, haben etwa die Unterschiede zwischen US-amerikanischem „privacy law“ und unionsrechtlichem Datenschutzrecht erheblichen Einfluss auf die Zugänglichkeit von Daten. Die Rückschlüsse, die aus US-amerikanischen Untersuchungen zu „Datenmärkten“ für den europäischen Markt gezogen werden können, sind begrenzt. Die vorliegende Studie beschränkt sich auf eine Untersuchung der Funktionsweise von Datenmärkten in Europa.

B. Die Bedeutung von Daten in der neuen Datenökonomie

I. Veränderungen der Informationsbedingungen in der digitalen Welt

Die Bedeutung von Information in Wirtschaft und Gesellschaft ist nicht neu.[6] Kunden- oder produktbezogenes Wissen ist für viele Unternehmen seit jeher zentraler Bestandteil ihres ideellen Firmenwerts („Goodwill“) und Grundlage ihrer Geschäftsstrategie. Volkswirtschaftlich ist die bestmögliche Nutzung des in der Gesellschaft dezentral vorhandenen Wissens eine der grundlegenden Herausforderungen für jede Wirtschaftsordnung, wie bereits Friedrich A. v. Hayek in seinem einflussreichen Aufsatz „The Use of Knowledge in Society“[7] festgestellt hat.

Verändert haben sich in den letzten Jahrzehnten allerdings die technischen Grundlagen der Informationssammlung beziehungsweise -gewinnung. Ausgangspunkt sind die neuen Möglichkeiten der Datenerhebung, -speicherung und -verarbeitung: Unter den Bedingungen einer technisch limitierten und kostenträchtigen Informationsgewinnung, -speicherung und -verarbeitung wurden früher im Wesentlichen strukturierte Kundendaten mit relativ zeitstabilen Informationen etwa über Namen, Adressen, Alter, Geschlecht und Transaktionen erhoben. Die neuen Technologien ermöglichen heute demgegenüber die systematische Speicherung und Verarbeitung von Daten in Echtzeit, die maschinell häufig als Nebenprodukt einer anderweitigen Aktivität erzeugt werden – etwa über Sensoren oder unter Verwendung von Tracking-Technologien im Internet. Die Mengen von digital erfassten, unstrukturierten Massendaten wachsen seit Jahren exponentiell. Die Möglichkeiten der

[6] Siehe auch Autorité de la Concurrence and Bundeskartellamt, Competition Law and Data, 10.05.2016, S. 8-9.
[7] *v. Hayek*, The Use of Knowledge in Society, American Economic Review 35(4), 1945, S. 519-530.

Datenspeicherung sind ebenfalls exponentiell gewachsen und deren Kosten drastisch gesunken. „Big Data“ steht als Schlagwort für die neuen Technologien der Datenverarbeitung: Möglich ist nunmehr eine systematische Auswertung von Datenmengen, die lange Zeit als zu groß, zu komplex, zu schnelllebig und/oder zu unstrukturiert galten, um einer systematischen, kontinuierlichen Auswertung zugänglich zu sein. Mittels neuer Datenanalyseverfahren können sehr große Datensätze („volume“) unterschiedlicher Art („variety“) miteinander verknüpft und systematisch statistisch auf bislang unbekannte Zusammenhänge hin untersucht werden.

Mit diesen neuen Technologien hat sich zugleich die Art der unternehmerisch relevanten Informationen erweitert. Eben die Daten, die durch Computeranwendungen oder Internetdienste als Nebenprodukt anderer Aktivitäten automatisch anfallen oder durch Sensoren erfasst werden, sind in der digitalen Ökonomie zu einer „Kernkomponente für neue, innovative Dienste“ geworden. Sie können genutzt werden, „um Produkte oder Produktionsprozesse zu verbessern und die Entscheidungsfindung zu unterstützen“.[8] Der Zugang von Unternehmen zu solchen Daten kann maßgeblich zur Optimierung von Produktions- und Vertriebsabläufen einschließlich Einkauf, Lagerhaltung und Transport (Logistik),[9] zur Produktentwicklung und -innovation und zu einem effizienten, kundenspezifischen oder kundengruppenspezifischen Marketing[10] beitragen. Im Kontext der sog. „Industrie 4.0“ können Sensorinformationen Auskunft darüber geben, wann eine Maschinenwartung geboten ist, und somit helfen, Ruhezeiten zu optimieren und Kosten zu senken. Daten über das Kauf- und evtl. Suchverhalten von Nutzern können für eine effizientere Lagerhaltung eingesetzt werden. Des Weiteren können Daten auch bei langfristigen strategischen Entscheidungen helfen, beispielsweise bei der Frage, ob und welche neuen Märkte oder Geschäftsfelder erschlossen werden sollen, und sie können die Verifizierung von Identitäten und Betrugserkennung[11] und damit die „Risk Mitigation“ unterstützen.[12] Schließlich benötigen selbstlernende Algorithmen große Datensätze, auf deren Grundlage sie trainiert werden können.

Für all diese Anwendungen reicht allerdings der Datenzugang allein nicht aus. Hinzutreten muss die Fähigkeit, die Daten für die jeweiligen Ziele nutzbar zu machen. Mithilfe von Datenanalyse („data analysis“ oder „data analytics“) können Zusammenhänge in den Daten aufgedeckt werden. Mit dem Schlagwort „data mining“ wird die Suche nach Korrelationen in großen Datenmengen bezeichnet – häufig in Datenbeständen aus unterschiedlichen Quellen. Hierbei wird relativ ergebnisoffen nach Korrelationen gesucht, wohingegen bei anderen Datenanalysen zunächst Hypothesen gebildet und im Anschluss überprüft werden. Für die Durchführung von Datenanalysen (einschließlich „data mining“)

[8] Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 9.

[9] Siehe dazu auch Fraunhofer Gesellschaft, Industrial Data Space – Digitale Souveränität über Daten, White Paper, 2016, S. 10: Verbreitung von datengetriebenem Manufacturing Resource Planning und Enterprise Resource Planning seit den 1980er/1990er Jahren.

[10] Für eine nützliche Übersicht zur praktischen Relevanz von Daten für das Marketing siehe FTC-Report, Data Broker. A Call for Transparency and Accountability, 2014, S. 23 ff.: Unterscheidung zwischen Direktmarketing (Post, e-mail, Telefon – hier wiederum unterschieden zwischen „Data appends“, bei denen der Kunde den Personenkreis bezeichnet, zu dem er mehr Informationen will, und die benötigte Information spezifiziert, der Datenhändler dann diese Information ergänzt; und „marketing lists“, bei denen der Datenhändler Informationen zu Personen bereitstellt, die bestimmte Eigenschaften haben); Online Marketing („registration targeting“, „collaborative targeting“, „onboarding); und „Marketing Analytics“.

[11] Allgemein zu den Verwendungsmöglichkeiten von Daten, siehe FTC, Data Brokers. A Call for Transparency and Accountability, 2014, S. 23-35.

[12] Näher: FTC, Data Brokers. A Call for Transparency and Accountability, 2014, S. 23ff, insbesondere S. 32ff.

bedarf es in der Regel keiner personenbezogenen Daten. Vielmehr kann mit anonymisierten oder pseudonymisierten Daten gearbeitet werden. Die aus den Korrelationen folgenden Erkenntnisse über typische Verhaltensweisen verschiedener Nutzergruppen können allerdings später genutzt werden, um Neigungen einer Person, die – womöglich nur spärliche – personenbezogene Daten übermittelt, mit hoher Treffgenauigkeit vorherzusagen. Voraussetzung ist in einem solchen Fall, dass das Unternehmen die personenbezogenen Daten mit den aus der Datenanalyse gewonnen Erkenntnissen kombinieren darf.

Neben von Programmierern erstellten spezifischen Algorithmen zur Datenanalyse kommt zunehmend auch Artificial Intelligence zum Einsatz, die eine selbständige Anpassung von Algorithmen über die Zeit ermöglicht – sogenannte selbstlernende Algorithmen. Bei solchen selbstlernenden Algorithmen werden Variationen von „Treatments", also eine mit dem Ziel der Verbesserung des Algorithmus vorgenommene exogene Variation der Bedingungen, unter denen beispielsweise Konsumenten eine Entscheidung treffen, nicht mehr vorprogrammiert. Die Intensität und Art des Experimentierens wird vielmehr an Artificial Intelligence delegiert. Den Algorithmen werden lediglich Ziele vorgegeben. Für einen solchen Selbstlernprozess sind große Datenmengen erforderlich. Artificial Intelligence kann zu erheblichen Kostensenkungen führen. Ein konkretes Beispiel ist der Einsatz von Artificial Intelligence beim Onlinehändler Otto.[13] Hier wurden 3 Milliarden Transaktionen und 200 Variablen wie beispielsweise Wetterinformation und Produktsuche, auf dem Portal von Otto mithilfe selbstlernender Algorithmen analysiert, um vorherzusagen, welche Produkte Konsumenten kaufen werden. Aufgrund dieser Analysen konnte Otto den überschüssigen Lagerbestand um ein Fünftel reduzieren.

Aus dem Zusammenspiel des Zugriffs auf den „Rohstoff" Daten und der Fähigkeit zu ihrer „Veredelung" oder Verwertung können wichtige Wettbewerbsvorteile für Unternehmen folgen. Dies gilt für die unternehmensinterne Datenverwertung, für den B2B-Bereich und für das B2C-Geschäft, das in der öffentlichen Diskussion – nicht zuletzt angesichts der Verarbeitung personenbezogener Daten – eine besondere Rolle spielt.

Die Bedeutung der Datenverwertung im B2C-Geschäft hat stark zugenommen, seit mit der Verbreitung mobiler Endgeräte große Mengen an Echtzeitdaten über das Nutzerverhalten zur Verfügung stehen.[14] Daten können aber auch durch Videoaufnahmen und Smartphone-Daten in Geschäften generiert werden, um Kenntnisse über die momentanen Gefühle von Käufern zu gewinnen und darauf zu reagieren.[15] Big Data ermöglicht es den Unternehmen, Nutzervorlieben – und damit auch die individuellen Zahlungsbereitschaften – besser einzuschätzen. Konsumenten können (und müssen)

[13] The Economist, Automatic for the people, 15. April 2017, Business Section, S. 55-56.

[14] Siehe Fraunhofer Gesellschaft, Industrial Data Space – Digitale Souveränität über Daten, White Paper, 2016, S. 10.

[15] So berichtet der Economist: „Thermal-imaging cameras can detect the heart rate. Wirelessly captured data from smartphone accelerometers can suggest when shoppers become fascinated (movement often stops) or are fretting over prices (a phone is repeatedly raised to search for cheaper products online)." – siehe The Economist, How retailers are watching shoppers' emotions, 8 June 2017, Business Section. Auch wenn sich vieles noch im Experimentierstadium findet, ist manches schon Praxis in Deutschland. „Die Zeiten, in der Verbraucher ziellos und unbehelligt durch einen Supermarkt laufen können, sind vorbei. Wer gedankenlos auf einen Bildschirm mit Werbung blickt, bekommt in vielen Märkten bereits heute das zu sehen, was ihn vermeintlich interessiert. Kameras analysieren, wie lange jemand den Filmen zusieht und wer vor ihnen steht: Mann oder Frau, alt oder jung das System wählt zielgruppengerechte Spots aus. In Hunderten Filialen deutscher Supermärkte stehen schon Tausende solcher Geräte."- siehe Nicolai Kwasniewski, So rüsten Supermärkte im Kampf mit dem Onlinehandel auf, Spiegel Online, 5. Juni 2017.

daher mit stärker individualisierten Angeboten – z.B. personen- oder gruppenspezifischen Preisnachlässen (beispielsweise über Coupons) – und individualisiertem Marketing („targeted advertising“) rechnen.[16] Daneben wächst der Bereich neuer datengetriebener Mehrwertdienste („smart services“).[17] Ein Kennzeichen dieser neuen Dienste ist die Ausrichtung der Produkte oder Dienstleistungen an individuellen Kundenpräferenzen und -bedürfnissen. Zunehmend verschwimmen dabei die Grenzen zwischen physischen Produkten und digitalen Dienstleistungen (Hybridität).[18] Auch klassische Dienstleistungen werden digital angereichert (z.B. mytaxi, AirBnB u.a.). Für all dies ist der Zugriff auf (personenbezogene) Daten und die Möglichkeit, diese zu „bewirtschaften“, zentral.[19]

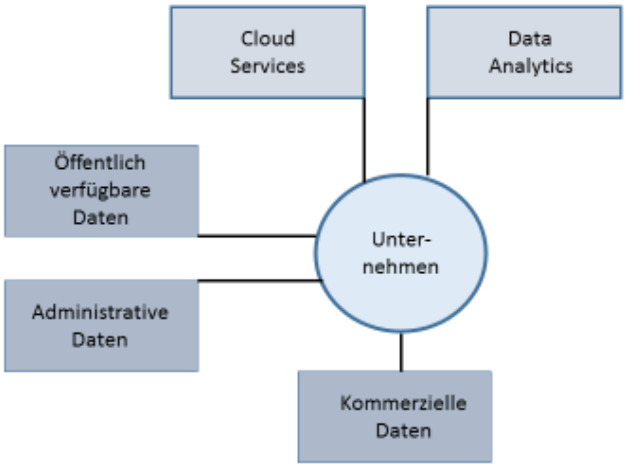

Schaubild 1: Datennutzung durch ein Unternehmen

Wertschöpfungskette bei Daten

Das Umfeld eines Unternehmens, das sich Daten bedient, ist in Schaubild 1 illustriert. Das Unternehmen generiert und sammelt im Geschäftsablauf eigene Daten. Diese kommerziellen Daten, die personenbezogen oder nicht personenbezogen sein können, können gegebenenfalls mit öffentlich verfügbaren und/oder mit Daten der öffentlichen Verwaltung kombiniert werden. Wie weiter unten erläutert, können diese kommerziellen Daten selbst erzeugt oder in einem Primär- oder Sekundärmarkt erworben werden. Zur Speicherung der Daten kann das Unternehmen Cloud Services benutzen, die auf kommerzieller Basis von mehreren Dienstleistern kompetitiv angeboten werden (beispielsweise Amazon, Google, Microsoft und Deutsche Telekom). Alternativ können Daten auf eigenen Servern bereitgehalten werden.

[16] In ihrer Analyse der Ökonomie mit Big Data und deren Nutzung, legen Ezrachi und Stucke den Schwerpunkt ihrer Betrachtung auf die Gefahren, die für Konsumenten aufgrund der Nutzung von personenbezogenen Big Data entstehen. Siehe *Ezrachi/Stucke*, Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy, 2016, insbesondere S. 85-130.

[17] Fraunhofer Gesellschaft, Industrial Data Space – Digitale Souveränität über Daten, White Paper, 2016, S. 8.

[18] Dazu unter anderem: Perzanowski / Schultz, The End of Ownership. Personal Property in the Digital Economy, 2016.

[19] Fraunhofer Gesellschaft, Industrial Data Space – Digitale Souveränität über Daten, White Paper, 2016, S. 9

Um die Daten auszuwerten, kann das Unternehmen entweder eigene Data Analytics-Kompetenz aufbauen oder auf die Dienste externer Data Analytics-Anbieter (beispielsweise IBM, SAS oder SAP) zurückgreifen. Die Märkte für Data Analytics-Dienste entwickeln sich gegenwärtig schnell.[20] Data Analytics-Anbieter stellen selbst keine Daten bereit, sondern spezialisieren sich auf die Auswertung vorhandener Daten. Entweder verkaufen Analytics-Anbieter Data Analytics Pakete oder sie treffen zeitlich befristete Lizenzvereinbarungen, bei denen die Konditionen bilateral verhandelt werden. Die Data-Analytics-Angebote stehen nicht nur großen, sondern auch kleineren Unternehmen zur Verfügung, so dass hier keine für kleine Unternehmen unüberwindbaren Marktzutrittsschranken existieren. Unabhängig davon, wie die vertragliche Beziehung zwischen Analytics-Anbieter und dem Unternehmen als Analytics-Nutzer im Einzelnen ausgestaltet wird, verbleiben die analysierten Daten typischerweise im Unternehmen.

Schaubild 2: Datenwertschöpfungskette

Der Wert der Daten für ein Unternehmen folgt erst aus der Gesamtheit der Wertschöpfungskette von Datenerfassung über Speicherung bis zu Data Analytics. Entscheidend für die Generierung eines Wertes ist stets eine konkrete Anwendungsidee. Wie in Schaubild 2 dargestellt, unterscheiden wir fünf Komponenten innerhalb der Wertschöpfungskette bei Daten: Datenerzeugung; Datenspeicherung; Datenaufbereitung; Datenanalyse; und die Anwendungsidee. In einem statischen Umfeld ergibt sich die natürliche Sequenz Datenerzeugung, -speicherung, -aufbereitung und -analyse. An welche Stelle die Entwicklung einer Anwendungsidee oder Nutzungsidee tritt, hängt vom Einzelfall ab. Wenn Daten mit einer bestimmten Nutzung im Sinne gesammelt werden, steht die Anwendungsidee am Anfang. Wenn dagegen erst Korrelationsergebnisse zu einer Anwendungsidee führen, steht diese am Ende. Ein statisches Umfeld ist aber atypisch. Häufig werden Daten über die Zeit hinweg fortlaufend gesammelt. Zu einem bestimmten Zeitpunkt werden dann bestehende Daten ausgewertet auf Basis einer

[20] Laut IDC werden 2017 die weltweisen Erlöse für Big Data Analytics und Business Analytics bei etwa 150 Milliarden US$ liegen, was einen Anstieg von etwa 12% gegenüber dem Vorjahr bedeutet. Auch in den Folgejahren wird ein zweistelliges Erlöswachstum erwartet. Siehe Mitteilung des IDC, Big Data and Business Analytics Revenues Forecast to Reach $150.8 Billion This Year, Led by Banking and Manufacturing Investments, According to IDC, 14. März 2017; https://www.idc.com/getdoc.jsp?containerId=prUS42371417

Anwendungsidee. Mit fortlaufendem Sammeln von Daten werden Analysen angepasst. Ebenso werden Anwendungsideen angepasst oder neue Anwendungsideen kommen hinzu, die sich wiederum auf Datenerhebung und –verarbeitung auswirken können.

Aufgrund von Komplementaritäten zwischen Datenerzeugung, -speicherung, -aufbereitung, -analyse und Anwendungsidee, kann keinem einzelnen dieser Komplemente eindeutig eine Wertschöpfung zugewiesen werden. Wir illustrieren das anhand eines Zahlenbeispiels. Unterstellen wir, dass mit einer bestimmten Anwendungsidee ein zusätzlicher Erlös für die gesamte Industrie von 10 Mio. Euro in den fünf Komponenten gemeinsam erzeugt wird. Welcher Teil der Wertschöpfung soll nun jeder Komponente zugeordnet werden? Jede Komponente muss mindestens mit ihren Opportunitätskosten entlohnt werden. Wenn die Datenerhebung zu anderen Zwecken erfolgt, so sind deren Opportunitätskosten mit Null anzusetzen. Wenn andererseits die Daten speziell mit der Anwendungsidee im Sinne erhoben wurden und keine weiteren Anwendungen erkennbar sind, so sind diese mindestens mit den Kosten der Erhebung zu entlohnen, sagen wir 1 Mio. Euro in unserem Zahlenbeispiel. Für die Speicherung sind die Kosten anzusetzen, die für die Bereitstellung der erforderlichen Speicherkapazität anfallen. Insbesondere kann bei Nutzung von Angeboten vollständig kompetitiver externer Cloudanbieter der Preis, den diese Anbieter verlangen, als Opportunitätskosten angesetzt werden, beispielsweise 0,5 Mio. Euro. Entsprechendes gilt bei der Nutzung von Angeboten für Datenaufbereitung und –analyse von Data Analytics-Firmen, wobei hier näher zu prüfen wäre, inwieweit deren Angebote kompetitiv sind. Falls dies nicht der Fall ist, liegen die ökonomischen Kosten unterhalb des Preises und bei den Opportunitätskosten des Data Analytics Anbieters. In unserem Beispiel veranschlagen wir 0,5 Mio Euro. Bei der Berechnung der ökonomischen Kosten der Anwendungsidee einschließlich deren Implementierung ist zu prüfen, ob hier spezifische Vorleistungen notwendig sind. Ist das nicht der Fall, so liegen die ökonomischen Kosten bei Null – davon gehen wir in unserem Zahlenbeispiel aus. Die Differenz aus zusätzlichem Erlös und der Summe der ökonomischen Kosten entlang der Wertschöpfungskette stellt die Wertschöpfung dar. In unserem Zahlenbeispiel ergibt sich somit eine Wertschöpfung von 8 Mio. Euro. Keiner der Komponenten kann eine bestimmte Zahl zugeordnet werden.

Wenn also von einem ökonomischen Wert von Daten gesprochen wird, so ist darunter die Wertschöpfung der gesamten Wertschöpfungskette zu verstehen. Die Frage der Zuordnung erübrigt sich bei vertikal integrierten Modellen. Ein Beispiel hierfür ist Amazon. Amazon beobachtet das Such- und Kaufverhalten von Konsumenten. Die erzeugten Daten werden in der eigenen Cloud gespeichert. Mit firmeneigener Data Analytics werden die Daten ausgewertet, insbesondere um damit zielgenauere Produktempfehlungen zu geben, die dann zu einem erhöhten Transaktionsvolumen der auf Amazon bereits aktiven Konsumenten oder einer verstärkten Nutzung durch andere Konsumenten führen. Der (private) Wert der Daten liegt dann im Gewinnzuwachs, den Amazon langfristig aufgrund der Daten erzielt.

Die Wertschöpfung – d.h., der private ökonomische Wert von Daten – unterscheidet sich möglicherweise vom gesamtwirtschaftlichen Wert der Daten. Letzterer ist größer, wenn beispielsweise Konsumenten langfristig aufgrund der zielgenaueren Produktempfehlungen eine höhere Konsumentenrente erzielen; er ist kleiner, wenn das Gegenteil der Fall ist. A priori ist unklar, welcher von beiden Fällen eintritt. Eine weitere Differenz besteht, wenn andere Unternehmen von der Datennutzung eines Unternehmens betroffen sind; dies kann darin begründet sein, dass Unternehmen

im Wettbewerb zueinander stehen. Die Unterscheidung zwischen privatem und gesamtwirtschaftlichem Wert von Daten ist insofern von Bedeutung, als regulatorische Eingriffe sich am gesamtwirtschaftlichen und nicht am privaten Wert von Daten ausrichten sollten. Das bedeutet, dass Aktivitäten außerhalb der Datenwertschöpfungskette mit zu berücksichtigen sind. Ineffizienzen können in zwei Hinsichten auftreten: (1) wenn die realisierte Wertschöpfung unterhalb der potentiell Möglichen liegt und (2) wenn zwar der maximal mögliche private ökonomische Wert erwirtschaftet wird, dieser sich aber vom gesamtwirtschaftlichen Wert der Daten unterscheidet, beispielsweise wenn es zu Ineffizienzen in einem nachgelagerten Markt kommt (siehe auch G.I).

Die erste Art von Ineffizienz kann in einer idealisierten Welt – d.h., einer Welt mit vernachlässigbaren Transaktionskosten und anderen Friktionen entlang der Wertschöpfungskette – ausgeschlossen werden. Vernachlässigbare Transaktionskosten sind bei vertikaler Integration denkbar. Die zweite Art von Ineffizienz kann ausgeschlossen werden, wenn es keine Transaktionskosten und andere Friktionen in den nachgelagerten Märkten der Datennutzung gibt. Bevor wir mögliche Ineffizienzen näher thematisieren, ist es sinnvoll den „Handel“ mit Daten zu thematisieren.

II. Der „Handel“ mit Daten

Datensätze enthalten Informationen, die potentiell und in Abhängigkeit von der jeweiligen Anwendungsidee in ganz vielfältiger Weise im Interesse Einzelner und der Gesellschaft genutzt werden können. Da derjenige, der die Daten erhoben hat, im Zweifel nicht über ein umfassendes Wissen über alle möglichen nutzbringenden Einsatzmöglichkeiten verfügt, kann es die Wohlfahrt erhöhen, wenn auch Dritte auf die Daten zugreifen können. Zusätzlicher Nutzen kann aus der Zusammenführung oder Verknüpfung verschiedener Datensätze im Lichte spezifischer Anwendungsideen folgen.[21]

Anders als beispielsweise Güter des täglichen Gebrauchs sind digitale Daten nicht rivalisierend im Konsum. Sie können zu vernachlässigbaren Kosten repliziert beziehungsweise vielfach verwendet werden. Die Tatsache, dass eine Person die Daten nutzt, schließt die Nutzung durch andere Personen nicht aus. Andererseits kann ein allgemeiner offener Datenzugriff Dritter zu Anreizproblemen hinsichtlich der Investition in die Sammlung und Speicherung von Daten führen. Damit ist ein freier Zugang aus gesellschaftlicher Sicht nicht notwendigerweise optimal.

Es liegt daher nahe, die Entscheidung über die Einräumung eines Datenzugriffs im ersten Schritt – und vorbehaltlich von Wettbewerbsproblemen, die sowohl aus der mit einem offenen Datenzugriff verbundenen Gefahr von Verhaltensabstimmungen im Wettbewerb als auch aus der Gefahr eines Marktverschlusses bei Verweigerung des Datenzugriffs folgen können – den Unternehmen selbst zu überlassen. Die Kontrolle über den Zugang zu den jeweiligen Speichermedien (verbunden mit einer Verschlüsselung der Datenübertragung) ermöglicht Unternehmen im Regelfall den Ausschluss Dritter

[21] Zur möglichen Komplementarität von Datenquellen siehe auch *Duch-Brown/Martens/Mueller-Langer*, The Economics of Ownership Access and Trade in Digital Data, JRC Digital Economy Working Paper 2017-01, Europäische Kommission, 2017, S. 9.

von der Nutzung der dort angesammelten Datenmengen[22] – allerdings keineswegs notwendigerweise den Ausschluss vom Zugriff auf vergleichbare Daten.

Wenn es sich bei den fraglichen Daten also um Kollektivgüter *mit* Ausschließbarkeit handelt,[23] ist grundsätzlich zu erwarten, dass hier ein Markt für Big Data oder ein „Handel" mit Big Data entstehen kann. Der Handel muss (und wird regelmäßig) nicht in einer tatsächlichen Übertragung von Datensätzen bestehen. Häufig werden die Daten auf dem Server des ursprünglichen Dateninhabers verbleiben, der Dritten aber – gegebenenfalls technisch auf bestimmte Verarbeitungsvorgänge beschränkte – Zugriffs- und Nutzungsmöglichkeiten einräumen kann. Unternehmen, die über größere Datenmengen verfügen, lehnen die Verwendung des Begriffs des „Datenhandels" für diesen Vorgang regelmäßig ab. Sie sprechen stattdessen von „Datenökosystemen",[24] in denen dort, wo ein Interesse an einer gemeinsamen Datennutzung besteht, selektiv, nach Maßgabe individueller Vereinbarungen und auf der Grundlage mehr oder weniger ausdifferenzierter „data governance"-Systeme Zugriff auf Daten gewährt wird.[25]

Die EU-Kommission hat zwar den Begriff der „Datenökosysteme" aufgegriffen,[26] spricht daneben aber weiter von einem Datenhandel.[27] Von einem intensivierten Datenhandel verspricht sie sich ausweislich ihrer Mitteilung zum Aufbau einer europäischen Datenwirtschaft einen deutlich verbesserten Zugriff

[22] Koutroumpis et al. schlagen vor, Big Data als gesellschaftliche Ressourcen zu betrachten, also davon auszugehen, dass es Rivalität im Konsum, aber keine Ausschließbarkeit gibt, siehe *Koutroumpis/Leiponen/Thomas*, The (unfulfilled) potential of data marketplaces, unveröffentlichtes Manuskript, 22. März 2017, S. 23. Koutroumpis et al. schreiben (auf S. 23): „For example, valuable data can be shared within a community of users, but if some users extensively share the resource with outsiders, its distinctive market value may be diminished or lost." Worin könnte eine solche Verringerung des Marktwertes der Daten begründet sein? Wenn die Nutzer Unternehmen sind und die Unternehmen, die in einer Gruppe (community) organisiert sind, nicht miteinander im Wettbewerb stehen, so kann die Weitergabe durch ein Unternehmen in dieser Gruppe an andere Unternehmen, die zwar nicht mit diesem Unternehmen aber mit anderen Unternehmen in dieser Gruppe im Wettbewerb stehen, eine oben beschriebene Verringerung des Marktwerts begründen. Hierbei handelt es sich allerdings um negative Externalitäten im Konsum zwischen potentiellen Nutzern, die in bestimmten Fällen vorliegen mögen, aber nicht um eine gesellschaftliche Ressource. Insbesondere steht die mögliche wiederholte Nutzung digitaler Daten außer Zweifel. Deshalb betrachten wir Big Data als Kollektivgüter, aus denen Nachfrager dann einen Nutzen ziehen können, wenn sie komplementäre Komponenten wie Data Analytics und Speicherung in Verbindung mit einer Nutzungsidee einsetzen. Zur Wertschöpfungskette siehe weiter oben. Ob Dritte von der Nutzung ausgeschlossen werden können, hängt von den technologischen und rechtlichen Rahmenbedingungen ab. Selbst wenn ein Ausschluss technisch und rechtlich möglich ist, kann derjenige, der die Daten kontrolliert, sich natürlich dagegen entscheiden.

[23] Wir unterscheiden hierbei zwischen Kollektivgütern mit Ausschlussmöglichkeit und reinen Kollektivgütern, bei denen niemand vom Konsum ausgeschlossen werden kann. Erstere werden häufig Clubgüter und letztere öffentliche Güter genannt (so z.B. *Mankiw/Taylor*, Grundzüge der Volkswirtschaftslehre, 6. Aufl., 2016). Bei Open data hat jeder Zugang zu den Daten, allerdings ist damit die Ausschlussmöglichkeit trotzdem möglicherweise gegeben, so dass für den Zugang oder die Nutzung ein Entgelt verlangt werden kann.

[24] Siehe z.B. Fraunhofer, White Paper: Industrial Data Space, S. 4.

[25] Ein Beispiel für eine Initiative, die den Datenaustausch auf dieser Grundlage erleichtern und fördern soll, ist der von der Fraunhofer Gesellschaft entwickelte Industrial Data Space – siehe Fraunhofer, White Paper: Industrial Data Space.

[26] EU-Kommission, Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., z.B. S. 2.

[27] EU-Kommission, Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., z.B. S. 3.

von Marktteilnehmern zu großen und möglichst vielfältigen Datensätzen.[28] Damit soll eine erhebliche Stärkung des europäischen Innovationspotentials im digitalen Zeitalter einhergehen. Die Datenbeschaffung im Wege eines freiwilligen Datenhandels ist aus Sicht der Kommission die bevorzugte Option, um unter den neuen Bedingungen der Digitalwirtschaft die Wettbewerbsfähigkeit europäischer Unternehmen zu stärken.[29]

Gleichzeitig geht die Kommission in ihrer Mitteilung von der Möglichkeit eines Marktversagens in Datenmärkten aus. Diese könnten, so die Kommission, einen Grund in fehlenden Eigentumsrechten an Daten sowie in Machtungleichgewichtslagen in Datenmärkten haben.

Grundlage der Untersuchung eines etwaigen Marktversagens (dazu näher Teil E) muss ein besseres Verständnis der Datenmärkte sein (dazu im Folgenden Teil C).

C. Datenmärkte: Funktionsweise und Erscheinungsformen

Die Innovationspotentiale der neuen Datenökonomie hängen unter anderem von der Vielfalt und Qualität unternehmerischer Ideen über mögliche Anwendungsfelder ab, sowie von der Fähigkeit von Unternehmen, diese Ideen umzusetzen. Die Umsetzung der Ideen kann von einem Zugriff auf relevante Daten abhängen. Im Übrigen ist die Fähigkeit entscheidend, diese bestmöglich im Dienste der verfolgten unternehmerischen Zwecke zu verwerten.

Einen Zugriff auf relevante Daten können Unternehmen – je nach dem konkreten Markt- und Anwendungskontext – auf unterschiedliche Weise erlangen. Für ein adäquates Verständnis der Funktionsweise von Märkten ist es wichtig, diese unterschiedlichen Möglichkeiten des Datenzugriffs in ihrem Zusammenhang zu sehen und die Substitutionsbeziehungen zu verstehen.

Möglichkeiten des Datenzugriffs bestehen direkt bei „Open Data“ und selbst erzeugten Daten. Außerdem kann ein Datennutzer über Primär- und Sekundärmarkte sowie Data-Sharing-Vereinbarungen auf Daten zugreifen. Alternativ kann es in manchen Fällen Dienstleistungen anderer „datenreicher“ Unternehmen in Anspruch genommen werden. All diese Datenzugriffsmöglichkeiten sind in Schaubild 3 dargestellt und werden im Anschluss ausführlicher erörtert.

[28] Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 9.

[29] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 12: “Companies (especially SMEs and start-ups) that do not wish to or cannot generate all the data they need for their products or services should be able to obtain data like any other (physical) resource. At the same time, such data trading allows companies to monetise certain data they hold (e.g. anonymised data), opening additional sources of revenue”.

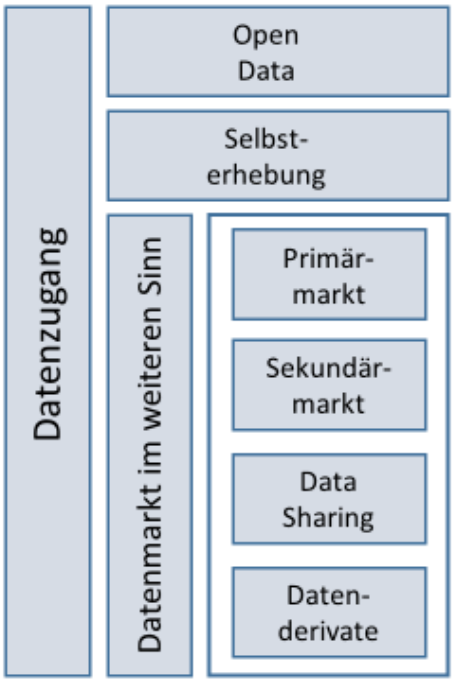

Schaubild 3: Datenzugriffsmöglichkeiten

Wenn Daten frei zur Verfügung stehen (als Open Data), sprechen wir nicht von einem Handel, da es zu keiner Gegenleistung für die Nutzung der Daten kommt. Dasselbe gilt, wenn Daten selbst erzeugt werden.

Bei einem Handel mit Daten unterscheiden wir zwischen Handel auf einem Primärmarkt und einem auf einem Sekundärmarkt (näher siehe unten). Eine Kombination aus beidem (oder eine Kombination aus Selbsterhebung und sekundären Märkten) stellt Data Sharing dar (näher siehe unten).

Hybride zwischen exklusivem Primärmarkt (oder Eigennutzung selbsterzeugter Daten) und Data Sharing sind ebenfalls möglich. Wir sprechen von Datenhandel im weiteren Sinne auch dann, wenn „Datenderivate" gehandelt werden, wenn also datenbasierte Dienstleistungen angeboten werden – die gegebenenfalls als Substitut für einen direkten Datenzugang dienen können. Insbesondere dort, wo Daten nicht offen – oder nur zu nachteiligen Bedingungen – an Sekundärmärkten gehandelt werden und der Zugriff auf datenbasierte Dienste nicht ausreicht, bleibt die Möglichkeit des Aufkaufs von „datenreichen" Unternehmen.

Open Data

Unternehmen können auf Open Data zugreifen. Hierbei handelt es sich um Daten, die ohne Einschränkung zur freien Nutzung, zur Weiterverbreitung und zur freien Weiterverwendung verfügbar sind. Zum Teil wird von Open Data nur gesprochen, wenn die Daten strukturiert und maschinenlesbar verfügbar sind und sich somit durchsuchen und weiterverarbeiten lassen.[30] Solche Daten werden vom Staat[31] sowie von Privaten bereitgestellt. Ein Beispiel für Letztere ist WikiData (www.wikidata.org), das

[30] Siehe beispielsweise http://opendatahandbook.org/guide/en/

[31] Siehe dazu Art. 1 Abs. 1 RL 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. 2003 Nr. L 345/90; § 1 Abs. 1 Informationsweiterverwendungsgesetz vom 13. Dezember 2006 (BGBl. I S. 2913), geändert durch Art. 1 des

seine Datensätze unter der Creative-Commons-Lizenz zur Verfügung stellt. Die Daten können in einem Standardformat heruntergeladen und weiterverarbeitet sowie mit anderen Daten – einschließlich anderen Open Data – verknüpft werden.

Selbsterhebung und Primärmärkte für Daten

Unternehmen können versuchen, die für sie relevanten Daten selbst zu erheben. Insoweit es dem Unternehmen um eine Optimierung eigener Produktions- und Vertriebsabläufen geht, kann es im Zweifel auf unternehmensinterne Maschinendaten zurückgreifen. Es ist dabei nicht auf Daten Dritter angewiesen. In einem solchen Fall besteht kein Datenmarkt, weil weder direkt noch indirekt ein Vertragsverhältnis besteht, das Daten zum Gegenstand hat. Geht es demgegenüber etwa um die Entwicklung neuer „smart services", liegt es häufig nahe, die Daten über individuelle Kundenpräferenzen und -bedürfnisse bei den eigenen Dienstenutzern zu erheben. Auch zahlreiche digitale Plattformen, die Nutzern ihre Dienste unentgeltlich anbieten, sammeln im Gegenzug personenbezogene Daten („Dienste gegen Daten"). Insoweit Unternehmen relevante (häufig personenbezogene) Daten unmittelbar von ihren Dienstenutzern beziehen, kann man von einem „Primärmarkt" für Daten sprechen.

Sekundärmärkte für Daten

Unternehmen können versuchen, gegen Zahlung eines Entgelts Zugriff auf Daten anderer Unternehmen zu erlangen, um diese für eigene unternehmerische Zwecke zu nutzen. Wir sprechen in diesem Zusammenhang von „Sekundärmärkten" für Daten – unabhängig davon, ob der Datenanbieter mit selbst erzeugten oder mit erworbenen Daten handelt. Auf solchen Sekundärmärkten können – gegebenenfalls über zwischengeschaltete Datenhändler[32] – mehr oder weniger standardisierte Datenpakete gehandelt werden; insoweit stark standardisierte Datenpakete gehandelt werden, und unter der Bedingung eines gut implementierbaren technischen Schutzes des Dateninhabers vor einem unerwünschten Zugriff Dritter, kann der Datenhandel zu einem Massengeschäft werden. In Betracht kommt dann grundsätzlich auch ein Handel von Daten über zwischengeschaltete Plattformen, die nicht selbst über handelbare Daten verfügen, sondern durch Bereitstellung spezieller Such- und Matchingfunktionen und eine Standardisierung der Schnittstellen für den Datentransfer den Handel zwischen Datenanbieter und Datennutzer vereinfachen. Der Handel kann aber auch dezentral organisiert sein – häufig dann, wenn auf der Anbieterseite nicht genuine Datenhändler, sondern Unternehmen stehen, welche die fraglichen Daten auch für eigene unternehmerische Zwecke nutzen. Individuell ausgestaltete Bedingungen des Datenzugriffs werden dann bilateral ausgehandelt.

Data Sharing

Gesetzes vom 8. Juli 2015 (BGBl. I S. 1162); §§ 3, 12, 12a E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749), geändert durch Art. 1 des Gesetzes vom 5. Juli 2017 (BGBl. I S. 2206).

[32] Eine besondere Rolle spielen Datenbroker und Ad networks, die Daten unterschiedlichen Typs erwerben, speichern, weiterverkaufen oder selbst auswerten und damit verbundene Dienstleistungen (wie die Platzierung von Werbung) anbieten. Während Ad networks zielgerichtete Werbeangebote anbieten und damit nicht als Anbieter von Daten auftreten, sind Datenbroker Anbieter von Daten. Die weltweit operierende Acxiom ist einer der großen Datenbroker. Für B2C-Anwendungen verfügt Acxiom auch in Deutschland über eine Adressdatenbank, die 35 aus 40 Millionen deutscher Haushalte erfasst (siehe Thomas Jüngling, Was die Datenbroker alles über uns wissen, in: Die Welt, 13.06.2013) und diese 14 Kundensegmenten zuordnet (siehe http://www.acxiom.de/personicx-zielgruppensegmentierung/, zuletzt aufgerufen am 30.07.2017).

In bestimmten Zusammenhängen sind „datenreiche“ Unternehmen bereit, einander einen (regelmäßig begrenzten) Zugriff auf eigene Daten zu erlauben (sog. Data Sharing[33]). Anders als bei einer Gewährung von Datenzugang gegen Entgelt geht es den Parteien hier regelmäßig um die Realisierung komplementärer Zwecke. Das Data Sharing kann unterschiedliche Formen annehmen. So werden sich häufig Maschinenhersteller und Maschinennutzer auf eine Form des Data Sharing, nämlich eine gemeinsame Nutzung der Maschinendaten, einigen. Dem Maschinennutzer können die Daten gegebenenfalls nutzen, um konkrete Störfälle besser vorherzusehen. Dem Maschinenhersteller können die gesammelten Maschinendaten bei der Produktverbesserung helfen. Smart Service-Anbieter, die ihren Kunden bestimmte Zusatzdienste von Drittanbietern zugänglich machen wollen, sind unter Umständen bereit, für diese Zwecke Kundendaten mit Drittanbietern zu teilen. Mitunter werden auch Daten-Konsortien gebildet – insbesondere dann, wenn in bestimmten Märkten die Realisierung des vollen Nutzens von Daten davon abhängt, dass die Marktakteure auf einen möglichst breiten Datenpool zugreifen können. Denkbar ist dies künftig etwa im Bereich des autonomen Fahrens, wenn bei Zugriff auf die gesammelten Mobilitätsdaten selbstfahrender Autos in Gefahrsituationen besser reagiert werden kann, als wenn die Reaktion alleine auf Basis der Sensoren des einzelnen Fahrzeugs erfolgt. Ähnlich wie bei dem bekannten Phänomen der Patent Pools kann es für Unternehmen dann sinnvoll sein, ihre jeweiligen Daten in einen gemeinsamen Pool einfließen zu lassen, auf den sämtliche Pool-Mitglieder Zugriff haben. Diese Art des „Daten-Pooling“ bietet sich für die Nutzung von komplementären Daten an, wenn alle Beteiligten einen direkten Nutzen aus einem erweiterten Datensatz ziehen. In bestimmten Fällen ist die gemeinsame Nutzung von Informationen regulatorisch vorgegeben.[34]

Märkte für Datenderivate

Für bestimmte Anwendungszwecke – etwa im Bereich des individualisierten Marketing, aber auch bei Identitäts- und Bonitätsprüfungen – benötigen Unternehmen unter Umständen keinen eigenen Datenzugriff, sondern können die Dienstleistungen „datenreicher“ Unternehmen (z.B. Google, Facebook) in Anspruch nehmen. Wir sprechen dann im Folgenden von einem Markt für Datendienstleistungen oder „Datenderivate“. Die Konsumenten solcher Datendienste erlangen zwar keinen Zugriff auf die Daten, wohl aber auf die für sie in einem bestimmten Kontext relevanten Ergebnisse einer Datenauswertung. Sie können die Datenauswertung dabei unter Umständen auch selbst steuern. Gut entwickelte Datendienste-Märkte existieren etwa für den Bereich des Targeted Advertising. Für andere Bereiche – etwa die Entwicklung neuer, datengetriebener Produkte – wird es hingegen keine Datendienste-Märkte geben.

[33] Für Beispiele siehe EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 14

[34] Siehe z.B. Art. 27, 30 Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), ABl. 2006 Nr. L 396/1. Bis zum 31.3.2017 war ferner der Informationsaustausch zwischen Versicherern und Rückversicherern in Form von gemeinsamen Erhebungen, Statistiken und Studien per Gruppenfreistellungsverordnung vom Kartellverbot ausgenommen – siehe Verordnung (EU) Nr. 267/2010 der Kommission vom 24. März 2010 über die Anwendung von Artikel 101 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union auf Gruppen von Vereinbarungen, Beschlüssen und abgestimmten Verhaltensweisen im Versicherungssektor, ABl. 2010 Nr. L 83/1. Die GVO ist nunmehr außer Kraft getreten. In Zukunft müssen die Versicherer prüfen, ob ein Informationsaustausch dem Kartellverbot unterfällt, und ob er ggfs. nach Art. 101 Abs. 3 AEUV vom Verbot ausgenommen ist.

Substitutionsbeziehungen zwischen Datenzugangs- beziehungsweise Datennutzungsmöglichkeiten

Wie die EU-Kommission in ihrer Mitteilung zum Aufbau einer europäischen Datenwirtschaft und dem Begleitpapier festgestellt hat, dominiert bislang die Eigenbeschaffung und -nutzung von maschinengenerierten Daten.[35] Erhebliche Bedeutung kommt daneben dem Data-Sharing zu. Der Handel von Daten über Intermediäre auf „sekundären" Datenmärkten ist bislang hingegen nur von eingeschränkter praktischer Bedeutung.[36] Dies gilt insbesondere für den Handel standardisierter Datenpakete über Datenplattformen oder elektronische Daten-Marktplätze.[37] Zwar wird gegenwärtig mit solchen Plattformen (insb. für Industriedaten) experimentiert.[38] Es existieren vertikal integrierte Modelle mit entweder einem Anbieter oder einem Nachfrager. Alternativ kann eine Datenplattform von einer Marktseite (oder einer Teilgruppe davon) als Konsortium geführt werden. Ähnlich der vertikal integrierten Lösung übernimmt hier ein einzelnes Unternehmen auf einer Marktseite die Führungsrolle und bietet eine integrierte Lösung für alle Anbieter und Nachfrager an. Ein Beispiel ist die Reiseauskunft für eine Reise, bei der ein Endnutzer die Angebote unterschiedlicher Verkehrsunternehmen abfragt und möglicherweise kombiniert.[39] Eine Datenplattform kann schließlich auch als zweiseitige Plattform von Dritten betrieben werden.[40] Insgesamt ist die Zahl und Bedeutung solcher Daten-Plattformen bislang jedoch begrenzt.

Hierin muss jedoch nicht notwendig ein korrekturbedürftiges Marktversagen liegen. Für die Entwicklungsperspektiven der Datenökonomie ist entscheidend, dass es sich bei den verschiedenen Formen des Datenzugriffs aus Nachfragersicht potentiell um Substitute handelt. Von welcher Möglichkeit des Datenzugriffs ein Unternehmen Gebrauch macht, hängt davon ab, welche konkreten Formen des Datenzugriffs mit Blick auf die Ziele, die das Unternehmen verfolgt, tatsächlich zur Verfügung stehen, über welche Daten das Unternehmen bereits verfügt beziehungsweise auf welche es selbst am Primärmarkt Zugriff erlangen kann; von der Fähigkeit des Unternehmens zur wertsteigernden Auswertung dieser Daten; und davon, welche Produkte von Datendienstleistern

[35] Siehe EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 15

[36] Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 11.

[37] Für eine Definition elektronischer Daten-Marktplätze siehe *Stahl/Schomm/Vossen/Vomfell*, A Classification Framework for Data Marketplaces, Working Paper No 23, 2015, S. 9.: "the concrete agency or infrastructure that allows participants to meet and perform the market transactions, translated into an electronic medium". Die Europäische Kommission macht sich diese Definition in EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 17, zu eigen.

[38] Siehe EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 18. Dort werden Daten-Marktplätze definiert als „virtual environments facilitating the exchange and connection of data among different companies and organisations through a shared reference architecture, common governance rules and within a secure business econsystem. The common governance rules in particular could technically implement an open, generally recognized process and a standardised data ecosystem for the transfer of property and possession of data assets". Auch Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 11. Für den Versuch einer Klassifikation nach der Zahl der Anbieter und Nachfrager von Daten siehe *Stahl/Schomm/Vossen/Vomfell*, A Classification Framework for Data Marketplaces, Working Paper No 23.

[39] Ein konkretes Beispiel hierzu ist die Plattform der Schweizerischen Bundesbahnen, die standardisierte Schnittstellen bereitstellt, um Daten einzupflegen, die dann von Endnutzern abgerufen werden können. Die Plattform ist daneben auch ein Buchungsportal und liefert den teilnehmenden Unternehmen Verkaufs- und Abrechnungsdaten. Siehe https://company.sbb.ch/content/dam/sbb/de/pdf/sbb-konzern/sbb-als-geschaeftspartner/partnervertrieb/webserviceB2P_factsheet_d.pdf

[40] Ein Beispiel für eine zweiseitige sektorübergreifende Datenplattform ist DAWEX – siehe www.dawex.com/en/

angeboten werden und gegebenenfalls zu welchem Preis. Die Verfügbarkeit von Daten an sekundären Datenmärkten ist in der modernen Datenwirtschaft mithin nur einer von verschiedenen Faktoren.

So können Datendienste ein Substitut für echte Datenmärkte sein – und eine effiziente Antwort von Unternehmen auf die rechtlichen Beschränkungen für die Weitergabe personenbezogener Daten. Will beispielsweise ein Unternehmen bestimmte potentielle Kundengruppen gezielt durch Werbung ansprechen, so kann es versuchen, dies auf Basis von selbst erworbenen Daten zu tun. Es kann aber auch ein Unternehmen mit der Schaltung zielgruppengenauer Werbung beauftragen, das seinerseits über aussagekräftige Daten verfügt. Ebenso können Data Sharing-Vereinbarungen ein Substitut für sekundäre Datenmärkte sein. Dort, wo Nutzerdaten für die Produktgestaltung und –weiterentwicklung benötigt werden, können die primären Datenmärkte – also die Möglichkeit der Beschaffung von Daten direkt von den Nutzern – einen Ausweg bieten.

Ein korrekturbedürftiges Marktversagen liegt mithin erst dann vor, wenn Unternehmen, die für die Umsetzung ihrer Ideen beziehungsweise für ihre Wettbewerbsfähigkeit auf Daten angewiesen sind, auf keinem der genannten Wege auf Daten zugreifen können, oder wenn für Datennachfrager wegen des Verschlusses bestimmter vorzugswürdiger Datenzugriffsoptionen vermeidbare und hohe Transaktionskosten entstehen.

D. Personenbezogene vs nicht personenbezogene Daten – Rechtliche Weichenstellung für die rechtliche Zulässigkeit und Grenzen des Datenhandels

Für die Funktionsweise von Märkten für Daten ist die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten von zentraler Bedeutung. Für die ganz oder teilweise automatisierte Verarbeitung von personenbezogenen Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, gilt ab 25. Mai 2018 unionsweit die DSGVO (Art. 2 Abs. 1 DSGVO). Wann immer personenbezogene Daten automatisiert erhoben werden, Dritten Zugriff auf solche Daten gewährt beziehungsweise diese in der Folge verarbeitet werden, ist mithin dem Datenschutzrecht Rechnung zu tragen. Der Schutz der Vertraulichkeit und Privatsphäre im Bereich elektronischer Kommunikation richtet sich derzeit noch nach der ePrivacy-RL 2002/58/EG in der Fassung der RL 2009/136/EG[41] (Art. 95 DS-GVO). Gegenwärtig läuft auf europäischer Ebene ein Gesetzgebungsverfahren zur Ersetzung der ePrivacy-RL durch eine Verordnung über Privatsphäre und elektronische Kommunikation. Die Verordnung soll gelten für Betreiber elektronischer Kommunikationsdienste, für Software, die elektronische Kommunikation ermöglicht, und für natürliche und juristische Personen, die mithilfe elektronischer Kommunikationsdienste an Endnutzer gerichtete gewerbliche Direktwerbung betreiben oder auf Endnutzergeräten gespeicherte Informationen sammeln, und sie soll die DSGVO in ihrem Anwendungsbereich bereichsspezifisch ergänzen.[42]

[41] Umgesetzt in §§ 91 ff. TKG.

[42] Siehe Art. 2 des Vorschlags für eine Verordnung über Privatsphäre und elektronische Kommunikation v. 10.1.2017, COM(2017)10 fin. sowie Begründungserwägung 8-9. Für den räumlichen Anwendungsbereich Art. 3 des Entwurfs.

Unternehmen, die personenbezogene Daten „tauschen“, „teilen“ oder mit ihnen „handeln“ wie auch Unternehmen, die personenbezogene Daten erwerben, benötigen nach bisherigem wie künftigem Datenschutzrecht stets eine auf den spezifischen Zweck der Datenverarbeitung bezogene – oder jedenfalls mit diesem Zweck vereinbare – Erlaubnis,[43] die grundsätzlich entweder aus einer Einwilligung oder aus einem gesetzlichen Erlaubnistatbestand folgen kann. Gerade dem „sekundären“ Datenhandel sind damit von vornherein Grenzen gezogen (näher: Teil E). Beim Handel mit nicht personenbezogenen Daten entfällt diese Regelungsebene. Die Vertragsfreiheit der an einer Datentransaktion beteiligten Unternehmen hat daher beim Handel mit nicht personenbezogenen Daten größeren Raum.

Die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten ist allerdings mit erheblichen Schwierigkeiten verbunden. Nicht hilfreich ist dabei die Kennzeichnung bestimmter Daten als „maschinengenerierte Daten“: Auch Maschinendaten können personenbezogen sein,[44] wie etwa die Beispiele „smart metering“, „connected cars“,[45] wearable-Computing (Computer- und sensorgestützte Geräte, wie Smart-Watches oder Quantified-Self Geräte),[46] Patientendaten von M2M-Medizinprodukten oder location data[47] zeigen. Die Abgrenzung zwischen personenbezogenen und nicht personenbezogenen Daten muss anhand anderer Kriterien erfolgen.

Art. 4 lit. a DSGVO definiert personenbezogene Daten als

> „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Auch die Verarbeitung von Daten, die erst durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können, unterfällt damit der DSGVO. Anonyme[48] und anonymisierte Information, die nicht oder nicht mehr auf identifizierbare Personen bezogen ist, fällt demgegenüber aus dem Anwendungsbereich der DSGVO heraus.

---

[43] Siehe Art. 5 Abs. 1 lit. b DSGVO. Eine Weiterverarbeitung der einmal erhobenen personenbezogenen Daten ist künftig zulässig, wenn sie nicht in einer mit dem Erhebungszweck „nicht zu vereinbarenden Weise“ erfolgt. Die Datenverarbeitung zu einem anderen, mit dem ursprünglichen Zweck zu vereinbarenden Zweck ist ohne neue Einwilligung zulässig, wenn der Verantwortliche die Voraussetzungen des Art. 6 Abs. 4 DSGVO erfüllt.

[44] Siehe EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 49 und Erwägungsgrund 30 der DSGVO. Aus der Literatur: *Duch-Brown/Martens/Mueller-Langer*, The Economics of Ownership Access and Trade in Digital Data, JRC Digital Economy Working Paper 2017-01, Europäische Kommission, 2017; ebenso für Machine2Machine Communication: *Grünwald/Nüssing*, MMR 2015, 378, 382.

[45] Siehe *Schulze*, BB 2013, 195, 199.

[46] Siehe hierzu Artikel 29 Datenschutzgruppe, Stellungnahme 8/2014 zu den neuesten Entwicklungen im Internet der Dinge, 16. September 2014, S. 5ff.

[47] Dazu *Arning/Moos*, ZD 2014, 126, 129ff.

[48] Typischerweise nicht menschlichem Verhalten zugeordnet werden können demgegenüber Daten über die Auslastung oder einen Defekt einer Maschine, Daten über Temperatur, Luftfeuchtigkeit oder die Bodenfeuchtigkeit eines Ackers oder Satellitenaufnahmen von der Erdoberfläche. Hierbei handelt es sich um tatsächlich anonyme Daten.

Entscheidend für die Abgrenzung zwischen personenbezogenen und nicht personenbezogenen Daten ist damit der Bezug von Daten auf eine zumindest identifizierbare Person. Die vermeintliche Eindeutigkeit dieses Kriteriums löst sich allerdings schnell auf. Es herrscht weitgehende Einigkeit, dass mit hinreichendem Aufwand und durch Kombination mit geeigneten anderen Datensätzen die allermeisten vordergründig nicht mehr auf identifizierbare Personen bezogenen Daten in personenbezogene Daten (zurück) verwandelt werden können (sog. Deanonymisierung).[49] Der Anwendungsbereich des Datenschutzrechts hängt daher entscheidend davon ab, auf wessen Fähigkeiten, Mittel und Wissen bei der Beurteilung abgestellt wird, ob ein Personenbezug herstellbar ist.[50] Zum Teil wird ein relativer Ansatz vertreten. Danach kommt es nur darauf an, ob die verantwortliche Stelle selbst die Möglichkeit hat, den Betroffenen zu bestimmen. Dem steht eine absolute beziehungsweise objektive Interpretation des Begriffs der Personenbezogenheit gegenüber. Danach sind Daten bereits dann als personenbezogen zu behandeln, wenn irgendjemand die Möglichkeit, hat den Bezug des Datums zur betroffenen Person herzustellen.[51] Neben der Frage, auf wessen Horizont und Fähigkeiten es bei der Herstellung des Personenbezugs ankommt, ist zu klären, ob für die Personenbezogenheit von Daten bereits die theoretische Möglichkeit der Herstellung eines Personenbezugs genügt, oder ob erst dann von personenbezogenen Daten auszugehen ist, wenn die Herstellung eines Personenbezugs aufgrund der Umstände des Einzelfalls wahrscheinlich ist.

I. Interpretation der Personenbezogenheit

1. Personenbezogenheit in der Rechtsprechung des EuGH

Mit diesen Fragen war der EuGH in der Sache *Patrick Breyer vs Bundesrepublik Deutschland* befasst.[52] In Frage stand die Personenbeziehbarkeit von IP-Adressen. Das Vorabentscheidungsverfahren betraf die Auslegung des Begriffs „personenbezogene Daten“ nach Art. 2 lit. a der Richtlinie 95/46/EG.[53]

Der Kläger *Breyer* setzte sich im Ausgangsverfahren gegen die automatische Speicherung seiner dynamischen IP-Adresse beim Besuch offizieller Internetpräsenzen der Bundesrepublik Deutschland zur Wehr. Anders als statische IP-Adressen, die einem mit dem Internet verbundenen Endgerät unveränderlich zugewiesen werden und so eine dauerhafte Identifizierung des an das Netz angeschlossenen Gerätes ermöglichen, handelt es sich bei dynamischen IP-Adressen um vorübergehende Kennziffern, die bei jeder Internetverbindung neu zugewiesen und bei späteren

[49] Siehe *Herbst*, NVwZ 2016, 902, 904f; zum Begriff der „Deanonymisierung“, siehe *Kühling/Klar*, NJW 2013, 3611, 3613.
[50] Siehe *Schantz*, NJW 2016, 1841, 1842.
[51] Siehe *Herbst*, NVwZ 2016, 902, 903f; *Brink/Eckhardt,* ZD 2015, 205, 206 sprechen hier überzeichnend vom „gesamten Weltwissen“, das konsequenterweise in die Betrachtung einzustellen sei.
[52] EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland.
[53] Richtlinie 95/46/EG des Europäischen Parlaments und des Tates vom 24 . Oktober 1995
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Laut Art. 2 lit. a der Richtlinie 95/46/EG werden darunter alle Informationen über eine bestimmte oder bestimmbare natürliche Person verstanden. Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Verbindungen ersetzt werden.[54] Daten, die aus einer dynamischen IP-Adresse und dem Zeitpunkt des über sie vorgenommenen Zugriffs auf eine Website bestehen und von einem Anbieter von Online-Mediendiensten gespeichert werden, bieten für sich genommen also diesem Anbieter nicht die Möglichkeit, den Nutzer zu bestimmen, der die Website während dieses Zugriffs abgerufen hat. Allein der Internetzugangsanbieter verfügt über die notwendigen Zusatzinformationen, die – in Verbindung mit der IP-Adresse – eine Bestimmung des Nutzers ermöglichen.[55]

Der EuGH stellte zunächst fest, dass eine dynamische IP-Adresse für sich genommen keine Information darstellt, die sich auf eine „bestimmte natürliche Person" bezieht, da sich aus ihr unmittelbar weder die Identität der natürlichen Person ergibt, der der Computer gehört, von dem aus eine Website abgerufen wird, noch die Identität einer anderen Person, die diesen Computer benutzen könnte.[56]

Auch die indirekte Bestimmbarkeit der Person unter Hinzuziehung von Zusatzinformation kann allerdings zur Einstufung eines Datums als „personenbezogenes Datum" führen. Dabei ist es nicht erforderlich, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden.[57] Entscheidend für den Personenbezug ist, dass der Verarbeiter über rechtlich zulässige Mittel verfügt, die es ihm erlauben die betreffende Person – gegebenenfalls unter Zuhilfenahme Dritter oder der von diesen generierten Informationen – bestimmen zu können.[58] Dies ist nicht der Fall, wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar ist, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung *de facto* vernachlässigbar ist.[59]

2. Personenbezogenheit nach der DSGVO

Die Definition „personenbezogener Daten" nach Art. 4 Nr. 1 DSGVO ist nahezu deckungsgleich mit der Definition Art. 2 lit. a der Richtlinie 95/46/EG.[60] Das Begriffspaar „identifizierte oder identifizierbare Person" entspricht dabei dem in der Vorversion und im deutschen Recht bislang üblichen Dualismus „bestimmte oder bestimmbare Person".[61]

---

[54] Vgl. EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 36; zu den technischen Details anschaulich *Meyerdieks*, MMR 2009, 8f.

[55] Siehe EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 37.

[56] Siehe EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 38.

[57] Siehe EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 43.

[58] Siehe EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 49. Da das deutsche Recht es dem Anbieter erlaubt, sich insbesondere im Fall von Cyberattacken an die zuständige Behörde zu wenden, damit diese die nötigen Schritte unternimmt, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten, sei dies im vorliegenden Fall möglich. Kritisch hinsichtlich der Zuhilfenahme Dritter unter dem BDSG: *Meyerdieks*, MMR 2009, 8, 10ff.

[59] Siehe EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 46.

[60] Personenbezogene Daten sind demnach „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Personen beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."

[61] Siehe *Ernst* in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 4, Rz. 3; *Schreiber*, in: Plath, BDSG/DSGVO, Art. 4 DSGVO, Rz. 7; *Buchner*, DuD 2016, 155.

a) Welche Daten sind zur Identifikation sachlich geeignet?

Die DSGVO übernimmt die Rechtssprechung des EuGH, der zufolge natürlichen Personen zugeordnete Online-Kennungen wie IP-Adressen und Cookie-Kennungen als personenbezogene Daten zu gelten haben, wenn sie Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der Personen zu erstellen und sie zu identifizieren (Erwägungsgrund 30 DSGVO).[62] Dasselbe gilt für kleine Datenmengen oder Auszüge aus Dateisystemen, wenn sie – in größerer Zahl miteinander verknüpft – zur Identifikation von Personen genügen; oder für Einzelfotos, auf denen Personen zwar nicht erkennbar sind, die aber miteinander kombiniert eine Feststellung der Identität eines Abgebildeten ermöglichen, etwa durch Abgleich derselben Person aus unterschiedlichen Perspektiven.[63]

b) Objektive oder relative Personenbezogenheit

Auch unter der DSGVO bleibt jedoch umstritten, wie Fälle zu behandeln sind, bei denen es für einen Rückschluss auf ein personenbezogenes Datum einer Verknüpfung mit Informationen bedarf, die nicht in der Sphäre des nach der DSGVO Verantwortlichen liegen, oder die nicht direkt bei der in Rede stehenden Verarbeitung selbst anfallen. Entscheidend ist insoweit, ob von einer objektiven oder relativen Interpretation des Begriffs der Personenbezogenheit auszugehen ist. Hinsichtlich der zur Verknüpfung der verschiedenen Informationen und somit Identifizierung der Person nötigen Technologien und Daten ist zudem unklar, ob sie lediglich allgemein oder dem konkret Verantwortlichen zur Verfügung stehen müssen.[64]

Erwägungsgrund 26 der DSGVO legt auf den ersten Blick eine objektive Bestimmung der Personenbezogenheit nahe.[65] Dort heißt es zur Personenbeziehbarkeit von Daten: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle *objektiven Faktoren***,** wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind [...]“

Einige Autoren wollen die zur Identifizierung geeigneten Mittel auf ein „ohne weiteres erreichbares Zusatzwissen“ beschränken.[66] Hierzu gehören sicherlich frei zugängliche Angaben, auch wenn der Betroffene diese selbst z.B. online mitteilt.[67] Wäre das Zusatzwissen jedoch allein einer Behörde – z.B. mittels eines Gerichtsbeschlusses – zugänglich, soll es an der Erreichbarkeit des Zusatzwissens fehlen.[68] Eine derart enge Interpretation der Personenbezogenheit steht jedoch im Gegensatz zur Auffassung

[62] Siehe auch *Schreiber*, in: Plath, BDSG/DSGVO, Art. 4 DSGVO, Rz. 7: Auch *potentiell personenbezogene Daten* sind als Daten über bestimmbare Personen zu behandeln.
[63] Siehe *Ernst* in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 4, Rz. 12.
[64] Siehe *Ernst* in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 4, Rz. 11 diese Frage jedoch offenlassend.
[65] Siehe *Schreiber*, in: Plath, BDSG/DSGVO, Art. 4 DSGVO, Rz. 9; *Buchner*, DuD 2016, 155, 156.
[66] Siehe *Ernst* in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 4, Rz. 11.
[67] Siehe *Ernst* in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 4, Rz. 11.
[68] Siehe *Ernst* in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 4, Rz. 11.

des EuGH in der Sache *Breyer*, der zufolge grundsätzlich jede rechtlich zulässige Zugriffsmöglichkeit auf Zusatzinformation zu berücksichtigen ist, solange sie nicht mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften verbunden ist.[69]

Aus der Formulierung in Erwägungsgrund 26, dass alle Mittel zu berücksichtigen sind, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden, wird allerdings zum Teil gefolgert, dass für die Frage der Identifizierbarkeit auf die Möglichkeiten des konkret Verantwortlichen, d.h. auf die diesem zur Verfügung stehenden Mittel abzustellen ist.[70] Maßgeblich seien vor allem die Größe des verantwortlichen Unternehmens, dessen Datenbestand, Personalstärke und Sachkenntnis.[71] Der Kenntnisstand Dritter wird der verantwortlichen Stelle zugerechnet, wenn Daten und Zusatzwissen rechtmäßig zusammengeführt werden können und ein Zusammenführen auch hinreichend wahrscheinlich ist. Dies erfordert insbesondere das Wissen der verantwortlichen Stelle um den Dritten und den (anzunehmenden) beiderseitigen Willen zur Zusammenführung. Die allein theoretische Möglichkeit des Zusammenführens mit der Kenntnis eines Dritten genügt nicht.[72]

c) Berücksichtigung illegaler Mittel?

Umstritten ist zudem seit langem, ob illegale Mittel der Datenbeschaffung beziehungsweise Identifizierung (beispielsweise über hacking oder den sog. Datenschwarzmarkt) bei der Bewertung zu berücksichtigen sind.[73] Das Urteil des EuGH in der Sache *Breyer*, welches unter Verweis auf die Schlussanträge des Generalanwalts auf das Kriterium der Legalität der Datenbeschaffung abstellt,[74] spricht dagegen. Solange ein rechtswidriges Vorgehen nicht durch Tatsachen belegt ist, muss die verantwortliche Stelle es sich nicht unterstellen lassen. Nur wenn die verantwortliche Stelle nachweislich rechtswidrig auf Zusatzinformationen zugreift, werden die ihr vorliegenden Daten als personenbezogen bewertet.[75]

d) Dynamische Bestimmung

Noch mit Blick auf die Ermittlung der Personenbezogenheit von Daten nach Maßgabe der RL 95/46 EG hat die Artikel 29 Datenschutzgruppe[76] gefordert, auch die Aufbewahrungsdauer der Daten und die mit Zeitablauf zur Verfügung stehenden (ausgereifteren) technischen Möglichkeiten des

---

[69] Siehe EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 46.
[70] Siehe *Barlag* in: Roßnagel, Europäische Datenschutz-Grundverordnung, § 3, Rz. 9.
[71] Siehe *Barlag* in: Roßnagel, Europäische Datenschutz-Grundverordnung, § 3, Rz. 9; ebenso *Schreiber*, in: Plath, BDSG/DSGVO, Art. 4 DSGVO, Rz. 10ff. Auch *Gola* in: Gola, DS-GVO, Art. 4. Rz. 17.
[72] Siehe *Brink/Eckhardt*, ZD 2015, 205, 211.
[73] Dagegen: *Kühling/Klar*, NJW 2013, 3611, 3613; *Meyerdieks*, MMR 2009, 8, 11; dafür: *Ernst* in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 4, Rz. 13; *Bergt*, ZD 2015, 365, 370, der illegale Handlungen nicht pauschal als „unvernünftig" oder „unverhältnismäßig" ansehen will, ebenso *Herbst*, NVwZ 2016, 902, 905.
[74] Vgl. EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 46-49.
[75] Siehe *Brink/Eckhardt*, ZD 2015, 205, 211.
[76] Diese durch die RL 95/46/EG eingesetzte Gruppe ist ein unabhängiges Beratungsgremium der EU-Kommission in Fragen des Datenschutzrechts (siehe Art. 29 RL 95/46/EG). Ihre Aufgaben waren bislang in Art. 30 der RL 95/46/EG definiert und beinhalteten die Prüfung der Umsetzung der unionsrechtlichen Vorgaben in den Mitgliedstaaten, deren Mitwirkung an der Herstellung eines europaweit einheitlichen Schutzniveaus sowie Stellungnahmen zu auf Unionsebene erarbeiteten Verhaltensregeln. Mit Inkrafttreten der DSGVO wird die Art. 29-Datenschutzgruppe durch den neu zu errichtenden Europäischen Datenschutzausschuss ersetzt (siehe Art. 94 Abs. 2 DSGVO und Erwägungsgrund 139).

Verantwortlichen zu berücksichtigen.[77] Bei einer Aufbewahrungsdauer von zehn Jahren sollten beispielsweise die Möglichkeiten der Identifizierung berücksichtigt werden, die im neunten Jahr der Aufbewahrungsdauer der Daten entstehen könnten und die sie in diesem Moment zu personenbezogenen Daten machen würden.[78] Dies deckt sich mit Erwägungsgrund 26 zur DSGVO, dem zufolge bei den Mitteln zur Identifizierbarkeit auch zukünftige technologische Mittel berücksichtigt werden sollen. Um die präventiven Sicherungspflichten des Verarbeitenden nicht ausarten zu lassen, wollen Teile der Literatur demgegenüber auf den Jetzt-Zeitpunkt abstellen: Dass zunächst nicht personenbezogene Daten irgendwann mit dem Fortschreiten technischer Möglichkeiten einer Person zugeordnet werden könnten, könne kaum je ausgeschlossen werden.[79] Rechtsschutzlücken bestünden deswegen nicht, da das Datenschutzrecht ab dem Zeitpunkt wieder Anwendung findet, ab dem die vormals anonymen Daten einer Person zugeordnet werden können. Im Übrigen ist zu berücksichtigen, dass bei einer erst in der Zukunft liegenden, theoretisch möglichen Deanonymisierung die Datenbestände entsprechend an Aktualität und damit oftmals auch an persönlichkeitsrechtlicher Relevanz verloren haben.[80]

Um gleichwohl ein hohes Datenschutzniveau zu gewährleisten, erscheint es sachgerecht, bereits absehbare Entwicklungen, die eine Zuordnung bestimmter Informationen zu einer Person in naher Zukunft ermöglichen, in die Jetzt-Betrachtung einzubeziehen.[81]

II. Anonymisierung von Daten

Um den Beschränkungen zu entgehen, die das Datenschutzrecht einem Sekundärhandel mit personenbezogenen Daten auferlegt, kommt grundsätzlich eine Anonymisierung der Daten in Betracht. Hierzu heißt es in Erwägungsgrund 26 der DSGVO: „Die Grundsätze des Datenschutzes sollten [...] nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder [für] personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann."

Eine Anonymisierung ursprünglich personenbezogener Daten setzt voraus, dass diese nachträglich so verändert werden, dass die Identifizierbarkeit einzelner Personen nunmehr ausgeschlossen ist und auch nicht nachträglich wiederhergestellt werden kann. Eine absolute Anonymisierung, bei der eine nachträgliche Deanonymisierung der Person technisch unmöglich ist, ist nur schwer zu bewerkstelligen.[82] Allerdings wird es entsprechend dem allgemeinen Kriterium für die Personenbeziehbarkeit von Daten für die Anonymisierung auch nicht auf einen absoluten Maßstab ankommen können. Maßgeblich ist vielmehr, ob der Verarbeiter über rechtlich zulässige Mittel

[77] Siehe Artikel 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 20. Juni 2007, S. 18
[78] Siehe Artikel 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 20. Juni 2007, S. 18
[79] Vgl. *Kühling/Klar*, NJW 2013, 3611, 3614.
[80] Siehe *Kühling/Klar*, NJW 2013, 3611, 3614.
[81] Siehe *Schantz*, NJW 2016, 1841, 1843.
[82] Siehe *Kühling/Klar,* NJW 2013, 3611, 3613.

verfügt, unter Zugriff auf weitere Informationen – gegebenenfalls unter Zuhilfenahme Dritter – bestimmte Personen zu identifizieren,[83] oder ob dies einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung *de facto* vernachlässigbar ist.[84]

Nach dem bisherigen § 3 Abs. 6 BDSG sollte bei dieser Prüfung berücksichtigt werden, ob die verantwortliche Stelle ein Interesse an einer Deanonymisierung hat und inwiefern sich hieraus ein wirtschaftlicher Nutzen für sie ergeben kann, der gegebenenfalls auch hohe Kosten als gerechtfertigt erscheinen lässt.[85] Entsprechendes wird auch nach der DSGVO gelten.[86]

Die Trennlinie zwischen personenbezogenen und nicht personenbezogenen Daten bleibt allerdings gerade bei anonymisierten Daten häufig unscharf und kann nur im Einzelfall ermittelt werden.[87] So kann bei aggregierten statistischen Informationen trotz der vorgenommenen Anonymisierung ein Rückschluss auf einzelne Personen möglich sein, wenn die Originalstichprobe nicht ausreichend groß war und andere Informationen die Identifizierung von Personen ermöglichen.[88] Daten aus sozialen Netzwerken bis hin zu epidemologischen Daten werden häufig anonymisiert gespeichert, können aber Ziel von Deanonymisierungsattacken werden.[89]

III. Der Zugriff auf Datenderivate oder anonymisierte Daten als Substitut für den Handel mit personenbezogenen Daten

Der ökonomische Wert von Datensätzen mit ursprünglich personenbezogenen Daten kann von Dritten unter Umständen auch dann realisiert werden, wenn diese vollständig anonymisiert wurden – vorausgesetzt, die Granularität[90] der Ausgangsdaten ist erhalten geblieben.

Damit Dritte über ihre Anwendungen den ökonomischen Wert von personenbezogenen Daten erzielen können, bedarf es nicht notwendigerweise der Weitergabe in nicht-anonymisierter Form. Wie im Folgenden begründet, reicht es unter Umständen, wenn diese Daten anonymisiert „weitergegeben“

[83] Insoweit sehr kritisch hinsichtlich der Zuhilfenahme Dritter unter dem BDSG: *Meyerdieks*, MMR 2009, 8, 10ff.
[84] Siehe EuGH Urt. v. 19.10.2016, Rs. C-582/14 – Breyer ./. Deutschland, Rz. 46.
[85] Siehe *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 3, Rz. 44.
[86] Siehe Artikel 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20. Juni 2007, S. 24: Die Beurteilung, ob die Daten die Identifizierung einer Person ermöglichen und ob die Informationen als anonym betrachtet werden können hängt davon ab, inwieweit Mittel in vertretbarem Umfang eingesetzt werden könnten, um die betreffende Person zu bestimmen.
[87] Siehe Artikel 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20. Juni 2007, S. 24; ebenso *Kühling/Klar*, NJW 2013, 3611, 3613f mwN.
[88] Siehe Artikel 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20. Juni 2007, S. 24.
[89] Einen Überblick zu Deanonymisierungsattacken geben *Ji/Mittal/Beyah*, Graph Data Anonymization, De-Anonymization Attacks, and De-Anonymizability Quantification: A Survey, IEEE Communications Surveys & Tutorials 19(2), 2016, S. 1305-1326.
[90] Granularität beschreibt den Aggregationsgrad der Daten. Bei hoher Granularität stehen Daten stark disaggregiert zur Verfügung. Wenn beispielsweise bestimmte Daten für eine Wohnung mit einer bestimmten Adresse (Straße, Hausnummer, Postleitzahl, Stadt) bestehen, ist die Granularität des Datensatzes hoch, sofern Gebäude eine kleine Zahl von Haushalten beherbergen. Die Granularität reduziert sich Schritt für Schritt, wenn Hausnummer, Straßenname und Postleitzahl aus dem Datensatz entfernt werden.

werden, wobei eine Weitergabe auch darin bestehen kann, dass Dritten Zugang zu diesen Daten gewährt wird. In Schaubild 4 stellen wir bei datenbezogenen Angeboten von Dritten den Unterschied zwischen direktem Zugriff auf personenbezogene Daten und einem Zugriff auf anonymisierte Daten dar für den Fall, dass eine Person ihre eigenen personenbezogenen Daten diesem Dritten bereitgestellt hat. Der Dritte kennt dann relevante Charakteristika der Person und kann die anonymen Daten dazu verwenden, um beispielsweise sein Angebot zu personalisieren. Stellt eine konkrete Person eigene personenbezogene Daten bereit, so kann ihr mithilfe der Korrelationen, die auf der Grundlage des anonymisierten Datensatzes ermittelt wurden, gegebenenfalls das gleiche auf das Profil der Person zugeschnittene Angebot gemacht werden, als hätte das Unternehmen über einen nicht-anonymisierten Datensatz verfügt. Vorausgesetzt ist eine Einwilligung der Person in diese Art der Datenverarbeitung.

Nach einer erfolgreichen Anonymisierung kann kein Rückschluss von den Daten (im Schaubild dargestellt durch 1, 2, 3, 4, 5) auf konkrete Personen (A, B, C, D, E) gezogen werden (weil es viele Personen mit den gleichen erfassten Charakteristika gibt). Die Person, die ein datenbasiertes Angebot annimmt, (im Schaubild Person A) stellt personenbezogene Daten zur Verfügung. Beim Abgleich ihrer Charakteristika mit den bestehenden anonymen Daten, kann das Unternehmen dann ein gruppenspezifisches Angebot machen, das auf der Erfahrung mit anderen Konsumenten, insbesondere solchen mit Charakteristika 2 beruht. Wie spezifisch das Angebot sein kann, hängt von der Granularität der Daten ab. Bei geringer Granularität (die eventuell notwendig ist, um Anonymität zu gewährleisten) könnte es beispielsweise der Fall sein, dass Charakeristika A, B, C in einer Gruppe ABC zusammengefasst sind (und Charakeristika D und E in Gruppe DE). In einem solchen Fall kann zwar die Nutzung von anonymen Daten zusammen mit den personenbezogenen Daten eines Nutzers zu einem gruppenspezifischen Angebot führen (ein Angebot das auf Gruppe ABC zugeschnitten ist); ein solches Angebot ist aber weniger spezifisch als ein Angebot, das den gesamten Datensatz personenbezogener Daten verwenden könnte.

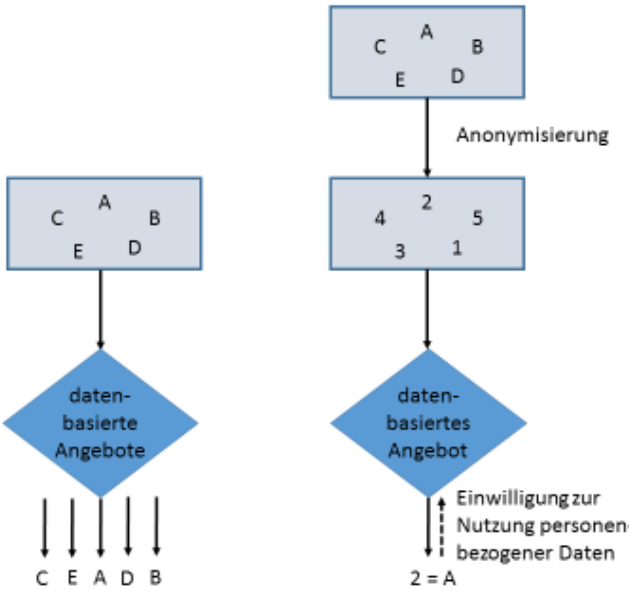

Schaubild 4: Nutzung personenbezogener vs. anonymisierter Daten

Es folgt daraus, dass ökonomische Wohlfahrtsgewinne (und eventuell Verluste der Konsumentenwohlfahrt[91]), die aufgrund der Weitergabe von personenbezogenen Daten entstehen würden, auch bei einer Weitergabe von anonymisierten Daten realisiert werden können, solange dies für die betroffene Person attraktiv ist (und die Granularität erhalten bleibt). Bei einer reduzierten Granularität verringert sich allerdings die Möglichkeit, maßgeschneiderte Angebote zu erstellen. In jedem Fall kann auch nach einer Anonymisierung die Konsumentenwohlfahrt aufgrund der Datenweitergabe leiden, weil zielgruppenorientierte Angebote dazu führen können, dass Konsumenten ausgebeutet werden. Hierzu ist es lediglich erforderlich, dass Datennutzer die Einwilligung der angesprochenen Konsumenten einholen und auf anonymisierte Datensätze zugreifen, um so ein zielgruppenspezifisches Angebot zu erstellen. Eine Reduktion der Konsumentenwohlfahrt kann selbst dann auftreten, wenn alle Konsumenten individuell rational handeln und sich bewusst sind, dass die Nutzung personenbezogener Daten nicht in ihrem Interesse ist.

Es ist a priori aber schwer zu sagen, ob Konsumenten in der Tat unter der Weitergabe anonymisierter Daten leiden. Zielgruppenorientierte Angebote können nämlich umgekehrt dazu führen, dass Konsumenten besser passende Angebote erhalten, ohne dass sie dafür hohe Suchkosten tragen müssen. Damit ersparen sie sich diese Kosten und profitieren von einem maßgeschneiderten Angebot. Es können eventuell auch Konsumenten erreicht werden, die sonst nicht am Marktgeschehen teilnehmen würden.

IV. Die Bedeutung des Datenschutzrechts beim Handel mit innerbetrieblich generierten Maschinendaten

Der Personenbezug von Daten ist stets zu prüfen, wenn es im B2C-Bereich um ursprünglich von den Nutzern erzeugte Daten geht. Auch Daten, die beim Betrieb von Maschinen im Unternehmen erzeugt werden, können aber einen Personenbezug aufweisen – namentlich einen Bezug auf diejenigen Arbeitnehmer, die mit dem jeweiligen Vorgang befasst waren.

Die DSGVO enthält keine Sonderregelungen zum Beschäftigtendatenschutz. In Art. 88 Abs. 1 DSGVO wird den Mitgliedstaaten das Recht eingeräumt, durch Rechtsvorschriften oder Kollektivvereinbarungen spezifische Vorschriften zum Beschäftigtendatenschutz zu schaffen. Der deutsche Gesetzgeber hat von dieser Ermächtigung mit § 26 DSAnpUG-EU[92] Gebrauch gemacht. Dort sind die Voraussetzungen geregelt, unter denen die Verarbeitung personenbezogener Daten von Beschäftigten zulässig ist.

Den Vorgaben des Beschäftigtendatenschutzes soll hier nicht weiter nachgegangen werden. Es ist davon auszugehen, dass innerbetrieblich erzeugte Maschinendaten nur anonymisiert weitergegeben werden dürfen. Externe Nutzer dieser Daten werden in aller Regel nicht über legale Mittel verfügen, um die Maschinendaten auf einzelne Arbeitnehmer zu beziehen – und sie werden hieran regelmäßig auch kein geschäftliches Interesse haben. Insoweit mit innerbetrieblich erzeugten Maschinendaten

[91] Die Konsumentenwohlfahrt leidet beispielsweise, wenn aufgrund von „unraveling“ viele Konsumenten ihre personenbezogenen Daten bereitstellen und es damit Dritten ermöglichen, die Konsumentenrente besser abzuschöpfen. Eine ausführlichere Beschreibung dieses Sachverhaltes befindet sich in E.II.5. weiter unten.
[92] Gesetz zur Anpassung des Datenschutzrechts an die DSGVO v. 30.6.2017, BGBl. I Nr. 44, S. 2097.

gehandelt wird, ist für die Zwecke dieses Berichts daher von nicht personenbezogenen Daten auszugehen.

E. Märkte für personenbezogene Daten

I. Bestandsaufnahme

Bislang gibt es keine zuverlässigen empirischen Befunde darüber, wie sich der Handel mit personenbezogenen Daten auf die von uns betrachteten Segmente des Datenhandels verteilt.

Es ist aber davon auszugehen, dass Unternehmen in ganz erheblichem Umfang über den Primärmarkt auf personenbezogene Daten zugreifen. Daten werden häufig im direkten Kontakt mit den Nutzern gesammelt. Insbesondere bei digitalen Plattformen im B2C-Segment ist das Geschäftsmodell „Dienste gegen Daten“ weit verbreitet.[93] Die Erlaubnis zur Verarbeitung der Daten für weitergehende, allerdings hinreichend spezifisch zu bezeichnende unternehmerische Zwecke folgt nach bisheriger Praxis und Ansicht ganz überwiegend aus der Einwilligung der Nutzer. Die Weiterverarbeitung zu damit zu vereinbarenden Zwecken ist nach Maßgabe der Art. 5 Abs. 1 lit. b in Verbindung mit Art. 6 Abs. 4 DSGVO zulässig.

Für den Bereich des kundengruppenspezifischen Marketing (Werbeansprache - „targeted advertising“; Rabatte) spielt überdies das Angebot von Datendiensten durch „datenreiche“ Unternehmen wie Google, Facebook, Amazon oder Apple, die ihrerseits in großem Umfang Nutzerdaten auf dem Primärmarkt „einsammeln“, eine wichtige Rolle. Auch hier ergibt sich die Zulässigkeit der Nutzung der personenbezogenen Daten für marketingbezogene Datendienste nach bisheriger Praxis und Ansicht aus der Einwilligung der Betroffenen. Datendienste von Auskunfteien werden ferner für die Prüfung der Bonität von Kunden in Anspruch genommen (z.B. Schufa).

Schließlich ist auch das Data Sharing bei personenbezogenen Daten von Bedeutung. Ein Beispiel für Data Sharing zwischen Systembetreiber und Händler sind Kundenbindungssysteme wie DeutschlandCard und Payback – zwei unternehmensübergreifende Bonusprogramme. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein beschreibt sie wie folgt:

„Diese Programme werden üblicherweise zentral durch einen Systembetreiber betrieben. Der Systembetreiber ist in der Regel Vertragspartner des Kunden im Hinblick auf dessen Teilnahme am Programm und die Verwaltung und Gutschrift seiner Rabattansprüche. Die Rabattansprüche werden in dieser Konstellation durch den Kunden bei teilnehmenden Partnerunternehmen erworben. Dies sind Händler oder Dienstleister, die sich zur Gewährung von Rabatten dem Systembetreiber angeschlossen haben. Üblicherweise sind an einem solchen Bonusprogramm mehrere Partnerunternehmen beteiligt; die Bonuskarte des Teilnehmers ist in allen Partnerunternehmen einsetzbar.“[94]

[93] Ausführlich dazu: *Schweitzer*, Neue Machtlagen in der digitalen Welt? Das Beispiel unentgeltlicher Leistungen, in: Kühling et. al. (Hrsg.), Regulierung – Wettbewerb – Innovation, 2017 [erscheint demnächst].

[94] Zitiert aus: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Erhöhung des Datenschutzniveaus zugunsten der Verbraucher, Studie im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft, 2006, S. 70.

Die vom Kundenbindungssystem erhobenen Daten werden allein dem Partner zur Verfügung gestellt, über den sich der Kunde angemeldet hat. Mit Zustimmung des Kunden können die Daten allerdings zusätzlich zu Marketingzwecken des Partners oder des Betreibers des Kundenbindungssystems verwendet werden.[95] Voraussetzung für eine wirksame Einwilligung ins Data Sharing ist, dass nicht nur der Zweck des „sharing" hinreichend konkret bezeichnet wird, sondern auch die Marktakteure, mit denen die Daten geteilt werden sollen.

Als eine spezifische, praktisch bedeutsame Form des Data Sharing können die sog. „social plugins" gelten. Bekannt ist insbesondere der Facebook „Like-Button", den Facebook nicht nur auf den eigenen Seiten benutzt, sondern den auch andere Webseitenbetreiber in ihre Seiten integrieren können. Wer auf Facebook eingeloggt ist, sieht dann auch auf der fremden Webseite eine Liste der Facebook-Freunde, die einen bestimmten Inhalt „geliked" haben. Klickt er/sie selbst auf den Button, so wird dies bei Facebook gespeichert und erscheint im Facebook-Profil des Nutzers. Facebook erlangt auf diese Weise Informationen über die Präferenzen, die Nutzer außerhalb des eigenen Netzwerks äußern. Die Betreiber der fremden Webseiten erhalten zwar keinen Zugriff auf den Datenfluss zwischen Facebook und den Nutzern. Sie profitieren aber von den auf Facebook bereitgestellten links und der Diskussion im sozialen Netzwerk. Die Einbindung solcher Social Plugins in Websites, die dem sozialen Netzwerk nicht zugehören, wirft zahlreiche bislang ungeklärte rechtliche Fragen auf. Sie sind gegenwärtig Gegenstand eines beim EuGH anhängigen Verfahrens. Das OLG Düsseldorf hat dem EuGH insbesondere die Frage vorgelegt, ob bei Einbindung von Social Plugins in eine Dritt-Webseite auch dieser Webseitenbetreiber für den Datenverarbeitungsvorgang beim sozialen Netzwerk im Sinne des Art. 2 lit. d der RL 95/46/EG verantwortlich ist, obwohl er diesen nicht selbst beeinflussen kann. Weiter möchte das OLG Düsseldorf wissen, wem gegenüber die Einwilligung nach Art. 7 lit. a und Art. 2 lit. h RL 95/46/EG vorliegen muss und ob den Betreiber der Website, der die Inhalte eines Dritten in seine Website eingebunden hat, auch die Informationspflichten nach Art. 10 RL 95/46 EG treffen.[96]

Ein über den Adresshandel hinausgehender sekundärer Datenhandel im engeren Sinn findet mit Blick auf personenbezogene Daten – soweit ersichtlich – nur in eingegrenztem Umfang statt.[97] Dies liegt mutmaßlich nicht an einer asymmetrischen Information zwischen potentiellen Datenverkäufern und potentiellen Datenkäufern betreffend die Datenqualität; dieses Informationsproblem lässt sich durch

[95] So heißt es bei den Nutzungsbedingungen von Payback: „Vor erstmaliger Nutzung leitet Sie der Partner auf eine PAYBACK Seite, auf der Sie sich bei PAYBACK einloggen und dort die zur Erbringung der Services nötige Einwilligung erteilen können: Mit dieser Einwilligung gestatten Sie uns und dem jeweiligen Partner, die jeweils zur Erbringung der Services erforderlichen Daten untereinander auszutauschen und zu nutzen (etwa den Punktestand bei einer Punktestandabfrage). Die im Rahmen der Services ausgetauschten Daten darf der Partner zur Erbringung der von Ihnen gewünschten PAYBACK Services verwenden. Darüber hinaus ermächtigen Sie mit Ihrer Einwilligung den Partner, diese Daten sowie die sonstigen beim Partner selbst anfallenden Rabatt- und Kommunikationsdaten in bestimmtem Umfang für Zwecke der Werbung und Marktforschung zu verwenden. Zusätzlich werden auch wir durch Ihre Einwilligung ermächtigt, Ihre bei PAYBACK selbst gespeicherten beziehungsweise anfallenden Daten in bestimmtem Umfang für Zwecke der Werbung und Marktforschung zu verwenden. Einzelheiten hierzu entnehmen Sie bitte dem Wortlaut Ihrer Einwilligung." (https://www.payback.de/pb/agb/id/32704/#A8, zuletzt aufgerufen am 30.7.2017)

[96] Siehe OLG Düsseldorf, Vorlagebeschl. v. 19.1.2017 – I-20 U 40/16. Siehe auch das erstinstanzliche Urteil des LG Düsseldorf, Urt. v. 9.3.2016 – 12 O 151/15.

[97] In der Vergangenheit spielte der sekundäre Handel mit Daten vor allem im Bereich Adresshandel (für Werbezwecke) eine Rolle.

Datenstichproben zumindest teilweise beheben. Für die tendenziell schwache Ausprägung des Handels personenbezogener Daten lassen sich vielmehr andere Gründe anführen:

(1) Eigeninteresse der Akteure

Ein zentraler Grund für das vergleichsweise geringe Ausmaß eines Handels mit personenbezogenen Daten ist das wirtschaftliche Eigeninteresse „datenreicher" Unternehmen: Für Unternehmen, die über einen breiten Zugriff auf Nutzerdaten verfügen – wie etwa Google, Facebook, Amazon oder auch Zalando – stellen diese Daten möglicherweise eine strategische Ressource dar und können einen Wettbewerbsvorteil begründen.[98] Sie haben dann kein Interesse an einer aktiven Vermarktung dieser Daten. Insbesondere sollen (potentielle) Wettbewerber keinen Zugriff auf diese Daten erlangen. Allenfalls werden sie – in begrenztem Umfang und unter Abschluss von „nondiclosure agreements" – mit Anbietern komplementärer Dienste geteilt.

(2) Rechtlicher Rahmen / Datenschutzrecht

Neben den Eigeninteressen „datenreicher" Unternehmen zieht das europäische Datenschutzrecht dem Handel mit personenbezogenen Daten auf „Sekundärmärkten" enge Grenzen – und deutlich engere Grenzen als in den USA.[99] In Übereinstimmung mit dem bisherigen Datenschutzrecht statuiert die DSGVO für die Verarbeitung personenbezogener Daten ein Verbot mit Erlaubnisvorbehalt. Erlaubnispflichtig ist dabei jeder einzelne Akt der Datenverarbeitung, von der Datenerhebung über die spezifische Datennutzung bis hin zur Übermittlung von Daten an Dritte – die für die Verarbeitung der Daten wiederum einer Erlaubnis bedürfen.[100] Das BDSG hat bislang besondere gesetzliche Erlaubnistatbestände für die geschäftsmäßige Verarbeitung von Daten zur Übermittlung zu Zwecken der Werbung, der Tätigkeit von Auskunfteien und des Adresshandels normiert.[101] Die DSGVO enthält keine entsprechende Regelung. Unklar ist, ob und gegebenenfalls unter welchen Voraussetzungen sich künftig aus der Generalklausel des Art. 6 Abs. 1 lit. f DSGVO, der die Befugnis zur Datenverarbeitung an eine Interessenabwägung knüpft, eine Erlaubnis zur Datenweitergabe im Rahmen eines sekundären Datenhandels ergeben kann. Die Bundesregierung hatte sich im Rahmen der Verhandlungen dafür eingesetzt, effektive Pseudonymisierungsmaßnahmen ausdrücklich als einen im Rahmen der Interessenabwägung relevanten Gesichtspunkt zu erwähnen. Ein solcher Passus ist nicht in Art. 6 Abs. 1 lit. f DSGVO übernommen worden. Dessen weit gefasster Wortlaut lässt aber auch ohne eine explizite Bezugnahme auf Maßnahmen der Pseudonymisierung deren Einbeziehung in die Abwägung zu.[102] Für

[98] Siehe beispielsweise Autorité de la Concurrence and Bundeskartellamt, Competition Law and Data, 10.05.2016.

[99] FTC, Data Brokers. A Call for Transparency and Accountability, 2014, S. 46 ff. mit folgendem Befund: Data brokers collect consumer data from numerous sources, largely without consumers' knowledge; the data broker industry is complex, with multiple layers of data brokers providing data to each other; data brokers collect and store billions of data elements covering nearly every U.S. consumer; data brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences; data brokers combine online and offline data to market to consumers online.

[100] Art. 6 Abs. 1 DSGVO ordnet ein Verbot mit Erlaubnisvorbehalt für sämtliche Verarbeitungsvorgänge an. Bereits die Datenerhebung durch Dritte stellt gem. Art. 4 lit. 2 DSGVO eine eigene Verarbeitung dar.

[101] Siehe § 29 BDSG. Entscheidend für die Zulässigkeit ist eine Abwägung der Interessen des von der Datenverarbeitung Betroffenen an einem Ausschluss der Datenübermittlung mit den Interessen des Dritten, dem die Daten übermittelt werden, an einer Kenntnis dieser Daten. Nur wenn der Dritte ein berechtigtes Informationsinteresse geltend machen kann und seitens des Betroffenen kein schutzwürdiges Vertraulichkeitsinteresse besteht, dürfen die entsprechenden Daten übermittelt werden.

[102] Siehe *Buchner/Petri*, in: Kühling/Buchner, DSGVO, Art. 6 Rn. 154.

die Entscheidung, ob eine Datenübermittlung zu Zwecken des sekundären Datenhandels auf Basis des Art. 6 Abs. 1 lit. f. DSGVO zulässig ist, wird aber stets eine umfassende Abwägung aller Umstände notwendig sein. Der Pseudonymisierung wird dabei umso mehr Gewicht zukommen, je höher der zu erwartende Aufwand ist, den der Datenempfänger zur Identifizierung der betroffenen Personen betreiben müsste, und je gravierender hierdurch die Interessen der Betroffenen beeinträchtigt wären. Ist eine Identifizierung der Betroffenen durch den Datenempfänger ausgeschlossen, so handelt es sich im konkreten Kontext um anonymisierte Daten, die dem Anwendungsbereich der DSGVO nicht mehr unterfallen (vgl. Erwägungsgrund 26 der DSGVO).

Greift keine gesetzliche Erlaubnis, so hängt die Zulässigkeit der Datenübermittlung im Rahmen eines sekundären Datenhandels auch künftig von einer wirksamen Einwilligung ab. Der Wirksamkeit einer Einwilligung in den sekundären Datenhandel werden durch das Bestimmtheitserfordernis bezüglich der beabsichtigten Zwecke der Datenverarbeitung allerdings Grenzen gezogen. Blankoeinwilligungen und pauschal gehaltene Einwilligungserklärungen sind unwirksam.[103] Das Bestimmtheitserfordernis steht in engem Zusammenhang mit dem Grundsatz der Zweckbindung, also dem Grundsatz, dass sich die Einwilligung in die Datenerhebung stets auf die konkrete Verwendung bestimmter Daten für einen vorher genau festgelegten Zweck beziehen muss (Art. 5 Abs. 1 lit. b DSGVO). Ist eine Weitergabe der Daten beabsichtigt, so folgt aus der Kombination von Bestimmtheits- und Zweckbindungsgrundsatz bislang, dass der Personenkreis, an den die Daten gegebenenfalls weitergegeben werden, hinreichend bestimmt bezeichnet sein muss – jedenfalls der Kategorie nach. Eine Einwilligung in die Weitergabe der Daten an einen nicht näher bestimmten Kreis von potentiellen „Datenerwerbern" wäre danach unzulässig, ebenso eine Einwilligung, welche die Zwecke der Verwendung durch den „Datenerwerber" offenhält. Ein Kennzeichen eines echten Sekundärmarktes für Daten wäre jedoch, dass die Nachfrager nach Daten mit dem Datenzugriff ihre eigenen Ziele verfolgen können. Gerade in der Suche nach neuen Anwendungsideen liegt das Innovationspotential der neuen Datenwirtschaft.

Die Lockerung des Zweckbindungsgrundsatzes durch die DSGVO kann hier in Teilbereichen einen Ausweg bieten. Nach Art. 5 Abs. 1 lit. b DSGVO ist künftig nur noch die Datenweiterverarbeitung für mit der ursprünglichen Zweckbindung inkompatible Zwecke verboten. Die Datenweiterverarbeitung zu anderen, mit dem ursprünglichen Zweck zu vereinbarenden Zwecken bleibt unter den Voraussetzungen des Art. 6 Abs. 4 DSGVO möglich. Die Vereinbarkeit soll anhand einer umfangreichen Interessenabwägung bestimmt werden, welche die Verbindung mit dem ursprünglichen Zweck, die Art der beabsichtigten Weiterverarbeitung sowie das Vorhandensein geeigneter Schutzvorkehrungen berücksichtigt.[104] Neben Verschlüsselungen kann auch hier eine etwaige Pseudonymisierung berücksichtigt werden. Ein weiteres Kriterium für eine Vereinbarkeit kann laut einer Stellungnahme des European Data Protection Supervisor sein, ob die Dienstleistung, für die die jeweiligen Nutzerdaten ursprünglich erhoben und verwendet wurde, und die Dienstleistung, für welche die Daten hernach als Input weitergeleitet werden, zu unterschiedlichen Märkten gehören. Ist dies der Fall, so soll die Datenübermittlung über die ursprüngliche

[103] Siehe *Schild*, in: BeckOK-Datenschutzrecht, DSGVO Art. 4 Rn. 125; *Ernst*, in: Paal/Pauly, DSGVO, Art. 4 Rn. 78
[104] Siehe *Plath*, in: Plath, BDSG/DSGVO, Art. 6 DSGVO, Rz. 38.

Zweckbindung hinausreichen.[105] Rechtssicherheit existiert in dieser Frage bislang nicht.[106] Eindeutig ist, dass auch der gelockerte Zweckbindungsgrundsatz dem sekundären Handel mit personenbezogenen Daten beachtliche Grenzen zieht. Ein Handel mit standardisierten Datenprodukten und standardisierten Zugriffsmöglichkeiten allein wird daher die Innovationspotentiale personenbezogener Daten nicht realisieren können.

II. Marktversagen auf Märkten für personenbezogene Daten?

Die EU-Kommission hat sich in ihrem Bericht zum Aufbau einer europäischen Datenwirtschaft auf nicht personenbezogene Daten konzentriert. Auch personenbezogene Daten sind aber in der neuen Datenökonomie ein wesentlicher Treiber von Innovation. Die weite Erstreckung des Anwendungsbereichs des Datenschutzrechts auf alle „personenbeziehbaren" Daten ist ein weiterer Faktor, der für eine nähere Befassung gerade auch mit Märkten für personenbezogene Daten spricht. Sollte Europa, um in der digitalen Ökonomie innovations- und wettbewerbsfähig zu bleiben, den sekundären Handel mit personenbezogenen Daten stärken? Falls ja: was wäre zu tun?

Ein zentraler Grund für die bisherige Schwäche von Sekundärmärkten für personenbezogene Daten in Europa ist – neben dem fehlenden Eigeninteresse vieler Dateninhaber – die Strenge des europäischen Datenschutzrechts. Politisch zu klären ist daher, ob ein Handel mit personenbezogenen Daten überhaupt wünschenswert ist. Der Europäische Datenschutzbeauftragte hat jüngst klar gegen einen solchen Handel Stellung bezogen: Personenbezogene Daten dürften nicht einfach als Wirtschaftsgut behandelt, ein Grundrecht dürfe nicht im Rahmen einer wirtschaftlichen Transaktion monetarisiert werden.[107]

Zwar ist eine Kommerzialisierung personenbezogener Daten im Rahmen des Geschäftsmodells „Dienste gegen Daten" und auf der Grundlage breit gefasster vorformulierter Einwilligungserklärungen bereits Realität. Eine Ausdehnung des sekundären Handels mit personenbezogenen Daten wäre datenschutzrechtlich aber wohl nur denkbar, wenn die jeweils Betroffenen selbst in zuvor nicht hinreichend konkretisierte Transaktionen einbezogen würden oder neuen Verwendungszwecken ausdrücklich zustimmen würden. Es bedürfte damit einer besonderen institutionellen Ausgestaltung der Sekundärmärkte für Daten (näher siehe unten).

Bemühungen um einen Ausbau des sekundären Datenhandels sind aber – auch vor dem Hintergrund der Bedenken gegen den Handel mit personenbezogenen Daten – nur opportun, wenn tatsächlich ein Marktversagen zu beobachten ist.

1. Schwäche des sekundären Datenhandels als Marktversagen?

[105] Siehe Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, March 2014, S. 27.
[106] Vgl. *Albers*, in: Beck-OK, Datenschutzrecht, Art. 6 DSGVO, Rz. 69.
[107] European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14.3.2017, S. 7-8.

Die geringe Verbreitung eines sekundären Handels mit personenbezogenen Daten könnte das Innovationspotential europäischer Unternehmen schwächen, wenn (noch) nicht „datenreiche“ Unternehmen hierdurch vom Zugang zu innovationsrelevanten Daten abgeschnitten wären, der Markteintritt von jungen Unternehmen mit innovativen, datengetriebenen Geschäftsideen mithin verhindert würde, oder wenn sie an einer Marktexpansion gehindert wären. Dies wäre vor allem dann zu befürchten, wenn keine angemessenen anderen Möglichkeiten bestünden, Zugang zu den relevanten Daten zu finden.

Gerade bei personenbezogenen Daten haben allerdings die Primärmärkte große Relevanz erlangt. Unternehmen – auch neu in den Markt eintretende Unternehmen – erlangen die für die Ausgestaltung der Dienste relevanten Daten regelmäßig unmittelbar von ihren Nutzern.

Unternehmen mit guten Geschäftsideen, die Dienste anbieten, die komplementär zu den Diensten anderer, häufig größerer Anbieter sind, können unter Umständen über ein Data Sharing Zugang zu den relevanten, gegebenenfalls anonymisierten Daten des vorgelagerten Anbieters erlangen.

Zwar profitieren kleine, neu in den Markt eintretende Unternehmen (noch) nicht in demselben Maße wie ihre größeren Wettbewerber von den positiven Netzwerkeffekten der eigenen Datensammlung, die eine kontinuierliche Produktverbesserung und Individualisierung auf der Grundlage der aggregierten Nutzererfahrung ermöglichen. Im Wettbewerb kann dies aber häufig durch eine überzeugende neue Geschäftsidee wettgemacht werden – die dann durch eine kluge Verarbeitung der eigenen Daten kontinuierlich verfeinert werden kann. Mit der Überzeugungskraft des Produkts wächst auch der Datenpool. Für das Marketing eines neuen Produkts kann wiederum auf Daten-Diensteanbieter zurückgegriffen werden.

Der zu Beginn geringe Zugriff auf personenbezogene Daten kann daher für junge Unternehmen zwar sehr wohl ein Marktzutrittshindernis sein; insoweit nicht – etwa wegen der Komplementarität der beabsichtigten Dienstleistung – eine Abhängigkeit von einem vorgelagerten Diensteanbieter besteht, ist das Marktzutrittshindernis aber typischerweise nicht prohibitiv.

Zwar bleibt es damit bei dem Befund, dass schwach entwickelte dezentrale sekundäre Datenmärkte den Marktzutritt oder die Expansion erschweren können. Insoweit die schwache Entwicklung solcher Märkte aber durch das Datenschutzrecht bedingt ist, ist sie nicht Ausdruck einer Fehlfunktion von Märkten, sondern einer politischen Wertentscheidung.

2. Stärkung des Primärmarktes für personenbezogene Daten?

Ganz erhebliches Gewicht liegt damit auf der Funktionsfähigkeit der primären Datenmärkte, auf denen Unternehmen in unmittelbarem Kontakt zu Betroffenen Zugang zu deren Daten und die Erlaubnis zu Datenverarbeitung erlangen. Ein im digitalen Umfeld verbreitetes Geschäftsmodell zur Erlangung des Zugriffs auf die relevanten Daten ist das Geschäftsmodell „Dienste gegen Daten“: Im Gegenzug für die (häufig unentgeltliche) Bereitstellung eines digitalen Dienstes verlangt der Anbieter von den Nutzern

die Einwilligung in die Datenverarbeitung zu bestimmten, näher gekennzeichneten Zwecken.[108] Auf der Grundlage des geltenden Rechts ist dieses Geschäftsmodell trotz erheblicher Rechtsunsicherheiten, die aus dem Spannungsverhältnis zwischen den neuen Möglichkeiten der Datenverarbeitung einerseits, den Grundprinzipien des Datenschutzrechts (Datensparsamkeit, Zweckbindungsgrundsatz) andererseits folgen, aus Sicht der Diensteanbieter eine taugliche Grundlage, um Zugriff auf Nutzerdaten zu erlangen.

Zwar stellt das Zweckbindungsprinzip erhöhte Anforderungen an die Konkretisierung der Verarbeitungszwecke in der Einwilligungserklärung. Auch muss diese den datenschutzrechtlichen Anforderungen an Transparenz und Klarheit genügen. Sind diese Voraussetzungen gewahrt, so steht die Freiwilligkeit und damit Wirksamkeit der Einwilligungserklärung nach geltendem Recht hingegen regelmäßig nicht in Frage. Dies gilt ungeachtet der in § 28 Abs. 3b BDSG und § 95 Abs. 5 TKG niedergelegten Kopplungverbote: Gemäß § 28 Abs. 3b BDSG darf der Abschluss eines Vertrags nicht von der Einwilligung in die Verarbeitung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung abhängig gemacht werden, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Gemäß § 95 Abs. 5 TKG gilt ein entsprechendes Kopplungsverbot auch für die Erbringung von Telekommunikationsdiensten: Sie dürfen vorbehaltlich eines zumutbaren Alternativangebots nicht von einer Einwilligung in eine über die in § 95 TKG ausdrücklich normierten Zwecke hinausgehende Datenverarbeitung abhängig gemacht werden. Insbesondere der Zugang zu monopolisierten Diensten musst danach gegenwärtig ohne eine Einwilligung in die Datennutzung für Werbung und Adresshandel (§ 28 Abs. 3b BDSG) beziehungsweise in gesetzlich nicht normierte Zwecke (§ 95 Abs. 5 TKG) möglich bleiben. Die Verfügbarkeit einer – gegebenenfalls entgeltlichen – Alternative reicht demgegenüber aus, um die Freiwilligkeit der Einwilligung wieder herzustellen.[109]

Die Anforderungen an die Wirksamkeit der Einwilligung im Geschäftsmodell „Dienste gegen Daten“ ändern sich allerdings mit Inkrafttreten der DSGVO zum Mai 2018. Gemäß Art. 7 Abs. 4 DSGVO soll künftig bei der „Beurteilung, ob die Einwilligung freiwillig erteilt wurde, [...] dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind“. Eine Einwilligung gilt, so die Begründungserwägung 43, „nicht als freiwillig erteilt, [...] wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist“.

Nimmt man die Begründungserwägung 43 ernst,[110] so sind die Anforderungen an die Freiwilligkeit der Einwilligung künftig deutlich erhöht. Allerdings weist der unscharfe Wortlaut des Art. 7 Abs. 4 DSGVO zugleich auf einen Formelkompromiss hin: Welche Bedeutung Art. 7 Abs. 4 DSGVO künftig für das Geschäftsmodell „Dienste gegen Daten“ hat, wird abschließend der EuGH klären müssen. Ein nicht

[108] Ausführlich zu diesem Geschäftsmodell und zu den mit diesem verbundenen Fragen: *Schweitzer*, Neue Machtlagen in der digitalen Welt? Das Beispiel unentgeltlicher Leistungen, in: Kühling et. al. (Hrsg.), Regulierung – Wettbewerb – Innovation, 2017, 269 ff. [erscheint demnächst].

[109] Siehe in diesem Sinne auch Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, April 2014, S. 47.

[110] Zur Entstehungsgeschichte der DSGVO und den wiederholten Widersprüchen zwischen Begründungserwägungen und Normteil siehe Gola, K&R 2017, 145.

unerheblicher Teil des Schrifttums will Art. 7 Abs. 4 DSGVO in Anlehnung an das bisherige Kopplungsverbot des § 28 Abs. 3b BDSG auslegen.[111] Die Begründung eines Gegenseitigkeitsverhältnisses zwischen Leistungsbereitstellung und datenschutzrechtlicher Einwilligung kann nach dieser Vorstellung für sich genommen die Freiwilligkeit nicht in Frage stellen.[112] Ins Gespräch gebracht wird gelegentlich auch eine Lesart, der zufolge das für die Vertragserfüllung Erforderliche mittels einer wirtschaftlichen Betrachtungsweise, und mithin unter Einbeziehung des Geschäftsmodells beurteilt werden soll.[113] Eine solche Interpretation würde sich von einem an den Funktionserfordernissen des jeweiligen Dienste anknüpfenden Verständnis der „Erforderlichkeit der Datenverarbeitung für die Vertragserfüllung" lösen, wie es im Richtlinienvorschlag zu digitalen Inhalten zugrunde gelegt wird. Gerichte müssten dann bei der Prüfung der Wirksamkeit der datenschutzrechtlichen Einwilligung inzident die Angemessenheit des Austauschverhältnisses „Dienste gegen Daten" ermitteln – wobei der mit der „Erforderlichkeit" in Bezug genommene Maßstab offenbleibt. Beide vorgenannten Ansichten beruhen auf der Annahme, dass man die Begründungserwägung 43 nicht beim Wort nehmen kann, ohne ein aus Anbieter- wie aus Nutzersicht in vielen Fällen attraktives Geschäftsmodell zu zerstören.

Eben diese Annahme ist allerdings voreilig. Die individuelle Einwilligung in die Datenverarbeitung ist im Datenschutzrecht nur einer von mehreren möglichen Erlaubnistatbeständen. Alternativ kann sich die Zulässigkeit der Datenverarbeitung aus einer gesetzlichen Erlaubnis ergeben. Als Erlaubnistatbestand kommt vor allem Art. 6 Abs. 1 lit. f DSGVO in Betracht. Demzufolge ist eine Datenverarbeitung rechtmäßig, wenn sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen [...]". Zu den berechtigten Interessen eines Diensteanbieters zählt auch das Interesse, den angebotenen Dienst mittels einer wirtschaftlichen Verwertung personenbezogener Nutzungsdaten zu finanzieren.[114] Diese Interessen sind gegen die Interessen der Nutzer am Schutz ihrer Privatheit und effektiven Selbstbestimmung abzuwägen.[115]

Die weitreichende „Materialisierung" der Freiwilligkeit,[116] die Art. 7 Abs. 4 DSGVO und insbesondere der Wortlaut der Begründungserwägung 43 nahelegt, wäre also nicht das Ende des Geschäftsmodells „Dienste gegen Daten". Sie würde aber den empirischen Befunden der faktischen Ineffektivität des Einwilligungsmodells als Modus der datenschutzrechtlichen Selbstbestimmung bei der Inanspruchnahme von digitalen Diensten Rechnung tragen.[117] In einem datenschutzrechtlichen

[111] Siehe z.B. *Metzger*, AcP 216 (2016), 817, 824: Auch nach der DSGVO sei darauf abzustellen, „ob eine Zwangslage für den Betroffenen besteht oder ob es die Möglichkeit des Ausweichens auf kostenpflichtige Angebote des selben Anbieters oder vergleichbare Dienste anderer Anbieter gibt". Siehe ferner *Gola*, K&R 2017, 145, 147.

[112] So auch – allerdings noch zum alten Recht – dezidiert *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 267 ff.

[113] In diese Richtung *Buchner*, DuD 2016, 155, 159.

[114] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, S. 25-26.

[115] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, S. 30.

[116] Verstanden als der Versuch, die tatsächlichen Voraussetzungen wirksamer Freiheitsausübung sicherzustellen.

[117] Dazu *Schweitzer*, Neue Machtlagen in der digitalen Welt? Das Beispiel unentgeltlicher Leistungen, in: Kühling et. al. (Hrsg.), Regulierung – Wettbewerb - Innovation, 2017, S. 269 ff. [erscheint demnächst].

Regime, das den Schutz des Allgemeinen Persönlichkeitsrechts in einen Bereich vorverlagert hat, der weit vor der Identifizierbarkeit konkreter Risiken liegt, erleichtert die gesetzliche Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO eine sinnvolle Begrenzung der Erlaubnis zur Datenverarbeitung und ihre Verknüpfung mit besonderen Sicherungsauflagen, die kein einzelner Nutzer aushandeln könnte.[118] Die Interessenabwägung ermöglicht es überdies, neben den Interessen der Vertragsparteien auch die externen Effekte zu berücksichtigen, welche die datenschutzrechtliche Einwilligung jedes Einzelnen auf Dritte haben kann:[119] Bei einem hinreichend großen Datenpool erlauben moderne Techniken der Datenanalyse Rückschlüsse auf das Verhalten auch solcher Personen, über die nur sehr wenige detaillierte Informationen bereitstehen. Auch diese kollektiven Wirkungen des Datenzugriffs von Unternehmen sprechen dafür, dessen Grenzen nicht ausschließlich bilateral zu verhandeln. Das scheinbar radikale Kopplungsverbot der neuen Datenschutzgrundverordnung gewinnt vor diesem Hintergrund an Plausibilität.

Für Unternehmen ist mit der allgemeinen Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO allerdings zunächst ein hohes Maß an Rechtsunsicherheit verbunden. Auf die Erteilung weitreichender Einwilligungen konnten sie sich in der Vergangenheit verlassen.[120] Gravierende Fehleinschätzungen in der Reichweite des gesetzlichen Erlaubnistatbestandes können in Zukunft beachtliche Geldbußen nach sich ziehen.[121] Ist gerade der Primärmarkt für Daten von grundlegender Bedeutung für datengetriebene Innovation, so ist diese Rechtsunsicherheit nur schwer hinzunehmen.

Die Rechtsunsicherheit lässt sich reduzieren, wenn von der in der DSGVO vorgesehenen Möglichkeit zur Zertifizierung von Verhaltensregeln Gebrauch gemacht wird.[122] Eine wesentliche Aufgabe besteht daher nach der hier vertretenen Ansicht darin, bis 2018 praktikable Kategorien für die Zulässigkeit der Datenverarbeitung im Modell „Dienste gegen Daten“ zu entwickeln. Hierbei werden die möglichen Zwecke der Datenverarbeitung (z.B. Big Data-Analyseverfahren zur besseren Identifizierung von Kundengruppen mit spezifischen Interessen im Marketing, Targeted Advertising,[123] Bonitätsprüfungen etc.) ebenso eine Rolle spielen wie technische Vorkehrungen gegen Fehler[124] und Missbräuche sowie Möglichkeiten und Ausgestaltung eines „opt out“ für Nutzer. Leitbilder für eine solche Interessenabwägung finden sich im (noch geltenden) deutschen Recht in den §§ 28-29 BDSG (v.a. mit Blick auf Adresshandel und Auskunfteien[125]). Die Interessenabwägung ist aber mit Blick auf die teilweise veränderte Situation des Geschäftsmodells „Dienste gegen Daten“ und die damit verbundenen Datenverarbeitungszwecke neu auszutarieren. Ungeachtet der weitreichenden Unterschiede zwischen dem europäischen und dem US-amerikanischen Datenschutzrecht liegt es

[118] Kritisch gegenüber einem solchen Ansatz allerdings *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 110 f.

[119] Mögliche externe Effekte aufgrund von „unraveling“ werden in der ökonomischen Literatur diskutiert; siehe unsere Ausführungen hierzu in E.II.5 weiter unten. Die Auswirkungen von „unraveling“ werden auch in der juristischen Literatur erkannt, siehe Hermstrüwer, Informationelle Selbstgefährdung, 2016, S. 193 ff.

[120] Zu diesem Vorteil des Einwilligungsmodells auch Buchner, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 253 ff.

[121] Siehe Art. 83 DSGVO.

[122] Siehe Art. 40 ff. DSGVO. Näher Bergt, CR 2016, 670 ff.

[123] Zu den insoweit bestehenden Widerspruchsrechten Betroffener siehe Art. 21 Abs. 2 und 3 DSGVO.

[124] Siehe hierzu insb. Art. 22 DSGVO zum Recht betroffener Personen, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Datenverarbeitung beruht.

[125] Z.B. Sonderregelung zu Auskunfteien: Detaillierte Interessenabwägung unter Berücksichtigung des legitimen, wir das Funktionieren von Wirtschaftsabläufen wichtige Interesses, Kenntnisse über die Bonität des Vertragspartners zu erlangen, aber auch des Interesses der Betroffenen an der Richtigkeit der Daten.

nahe, hierbei auch den „Data Broker"-Bericht der FTC zu berücksichtigen, der zwischen dem Handel mit personenbezogenen Daten zu Zwecken des Marketing, zu Zwecken der Risikominimierung und zu Zwecken der Personensuche („peoples search") unterscheidet[126] und versucht, Vorteile[127] und Risiken[128] eines Handels mit personenbezogenen Daten zu diesen Zwecken zu systematisieren. Ferner ist die Art und Sensibilität der konkreten Daten zu berücksichtigen – hierzu finden sich bereits wichtige Anknüpfungspunkte in der DSGVO.[129] Grundsätzlich denkbar sind auch sektorspezifische Lösungen.

Nicht nur die Einbeziehung von Möglichkeiten zum „opt out" zeigt, dass das Konzept der datenschutzrechtlichen Selbstbestimmung mit dem hier skizzierten Regimewechsel nicht aufgegeben ist. Grundlage der Verarbeitung personenbezogener Daten bleibt bei dem Geschäftsmodell „Dienste gegen Daten" die Entscheidung des Einzelnen für die Inanspruchnahme der Dienste. Nur die Höhe des „Datenpreises" wird künftig nicht mehr einseitig in vorformulierten Einwilligungserklärungen festgelegt, sondern durch eine Interessenabwägung begrenzt. Im Rahmen der Interessenabwägung können wiederum die Transparenz und Verständlichkeit eine Rolle spielen, mit welcher dem einzelnen Nutzer die Reichweite der geplanten Datenverarbeitung zur Kenntnis gebracht wird. Bei der Entwicklung allgemeiner datenrechtlicher Marktverhaltensregeln sollte Raum für Selbstbestimmung der Nutzer dort gewährleistet werden, wo diese auch faktisch wirksam werden kann. Unabhängig von dem Gebrauch, den einzelne Nutzer von dieser Möglichkeit machen, sorgen die Verhaltensregeln aber für eine Balance zwischen den Vorteilen von „Big Data" und deren Risiken in breiterer gesellschaftlicher Perspektive, die bei der Ausgestaltung des Ordnungsrahmens einer neuen Datenökonomie nicht außer Betracht bleiben kann. Das Einwilligungsmodell führt demgegenüber faktisch zu einer einseitigen Bestimmung des „Datenpreises" durch datensammelnde Unternehmen.[130] Es fehlt möglicherweise eine effektive Kontrolle durch den Wettbewerb, und es fehlt ein anderweitiger Kontrollmechanismus, der dieses Fehlen ersetzen könnte.

---

[126] FTC Report, Data Broker, S. 50 ff.

[127] Siehe dazu unter anderem FTC Report, Data Broker, S. 47-48: "Data broker products help to prevent fraud, improve product offerings, and deliver tailored advertisements to consumers. Risk mitigation products provide significant benefits to consumers by, for example, helping prevent fraudsters from impersonating unsuspecting consumers. Marketing products benefit consumers by allowing them to more easily find and enjoy the goods and services they need and prefer. In addition, consumers benefit from increased and innovative product offerings fueled by increased competition from small businesses that are able to connect with consumers they may not have otherwise been able to reach. Similarly, people search products allow individuals to connect with old classmates, neighbors, and friends."

[128] FTC Report, Data Broker, S. 48: "For example, if a consumer is denied the ability to conclude a transaction based on an error in a risk mitigation product, the consumer can be harmed without knowing why. In such cases, the consumer is not only denied the immediate benefit, but also cannot take steps to prevent the problem from recurring. Similarly, the scoring processes used in some marketing products are not transparent to consumers. This means that consumers are unable to take actions that might mitigate the negative effects of lower scores, such as being limited to ads for subprime credit or receiving different levels of service from companies. As to other marketing products, they may facilitate the sending of advertisements about health, ethnicity, or financial products, which some consumers may find troubling and which could undermine their trust in the marketplace. Moreover, marketers could even use the seemingly innocuous inferences about consumers in ways that raise concerns."

[129] Siehe etwa Art. 9 und Art. 10 DSGVO.

[130] Über das Einwilligungsmodell bestimmt das datensammelnde Unternehmen, welche Daten es zu welchem Zweck sammelt. Der Datenpreis entspricht den Opportunitätskosten der Datenüberlassung, die die Nachteile beinhalten, die der Einwilligende durch die Datenverarbeitung erleidet. Der Datenpreis kann aus Sicht des Konsumenten in einigen Fällen auch negativ sein, dann nämlich, wenn die Datenüberlassung im Interesse des Konsumenten ist.

3. Stärkung von Datenportabilität als Alternative zur Stärkung des Datenhandels?

Ein weiterer Mechanismus, der Unternehmen Zugang zu geschäftsrelevanten personenbezogenen Daten – insb. auch zu über die Zeit entstandenen Nutzungsprofilen – verschaffen kann, ist die Portierung solcher Daten durch den Nutzer eines Dienstes vom bisherigen Diensteanbieter zu einem Wettbewerber oder zu einem Mehrwertdiensteanbieter.

a) Recht auf Datenübertragbarkeit, Art. 20 DSGVO

aa) Funktion des Rechts auf Datenportabilität in Art. 20 DSGVO

Ein allgemeines Recht auf eine solche Datenübertragung ist nunmehr in Art. 20 DSGVO festgeschrieben. Die Vorschrift räumt jeder Person einen Anspruch gegen jeden Datenverarbeiter ein,

„[...] die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und [...]diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln“, sofern die Datenverarbeitung auf einer Einwilligung beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Art. 20 DSGVO ergänzt und erweitert das in Art. 15 Abs. 3 DSGVO festgeschriebene Recht auf eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, in entscheidender Weise: Den Betroffenen wird die Möglichkeit gegeben, sich durch Mitnahme der Daten zu einem anderen Anbieter aus einem „lock-in“ zu befreien oder aber die auf sie bezogenen Daten für sich selbst nutzbar zu machen, indem sie diese Anbietern von Zusatzdiensten zur Verfügung stellen. Das in der Begründungserwägung 68 genannte Ziel, den Betroffenen eine „bessere Kontrolle über die eigenen Daten“ zu ermöglichen, erhält damit in Art. 20 DSGVO eine spezifisch verbraucherschützende und zugleich wettbewerbsfördernde Ausprägung: Datenportabilität erleichtert den Anbieterwechsel der Betroffenen – oder auch die Parallelnutzung mehrerer Dienste („Multi-Homing“). Die beim bisherigen Anbieter akkumulierten personenbezogenen Daten und der damit verbundene Personalisierungsvorteil wirken so nicht als Marktzutrittsschranke. Innovative Anbieter erlangen die Chance, Zugriff nicht nur auf Echtzeit-Nutzerdaten zu erhalten, sondern auf die Nutzerprofile, wie sie sich über die Zeit der bisherigen Dienstenutzung herausgebildet haben. Der Marktzutritt neuer, innovativer Unternehmen in datengetriebene Dienstemärkte wird so erleichtert.[131]

bb) Inhalt und Grenzen des Rechts auf Datenportabilität

Art. 20 DSGVO beinhaltet im Kern ein Recht des Betroffenen gegen einen Datenverarbeiter zur Herausgabe der auf ihn bezogenen „Roh“-Daten an ihn selbst oder einen Dritten in einem gängigen, maschinenlesbaren Format. Von dem Herausgabeanspruch umfasst sind allerdings nur solche Daten, die der Betroffene dem Verantwortlichen auf der Grundlage einer Einwilligung in die Datenverarbeitung „bereitgestellt“ hat. Vom Anspruch auf Datenübertragung ausgenommen sind damit Daten, welche der Datenverarbeiter aufgrund eines anderen Erlaubnistatbestands (Wahrnehmung einer Aufgabe im öffentlichen Interesse, Wahrnehmung berechtigter Interessen Dritter, siehe Art. 6 Abs. 1 c) – f)) verarbeitet. Insoweit eine Einwilligung zur Datenverarbeitung

[131] Siehe in diesem Sinne auch die Guidelines on the right to data portability der Article 29 Data Protection Working Party v. 13.12.2016, WP 242, S. 3.

vorliegt, gelten als vom Betroffenen „bereitgestellt“ dann allerdings nicht nur Daten welche der Nutzer selbst aktiv eingibt (Name, Kontaktdaten, weitere personenbezogene Information), sondern auch Inhalte (z.B. E-mails, Sprachnachrichten, Bilder) sowie Daten, die der Betroffene bei der Nutzung von Diensten generiert (z.B. Bewegungsdaten, medizinische Daten, Suchverlauf sowie Daten von sog. Smartmetern).[132] Nicht vom Recht auf Datenportierung umfasst sind demgegenüber die „abgeleiteten Daten“, d.h. die Daten, welche der Datenverarbeiter auf der Grundlage der „Roh“-Daten selbst erzeugt – obgleich auch diese Daten auf die Person des Betroffenen bezogen sein können. Berechnet etwa ein Finanzdienstleister aus den vom Nutzer selbst bereitgestellten Daten über Einkommen und Sparvermögen auf der Grundlage eines gewichteten Alogrithmus eine Kreditausfallwahrscheinlichkeit, so unterliegt dieser abgeleitete Wert nicht dem Herausgabeanspruch aus Art. 20 DSGVO. Der Anspruch auf Datenportierung soll den Betroffenen beziehungsweise Drittdienstleister nicht zur Aneignung fremder Leistungen ermächtigen, sondern nur zur Portierung der unmittelbar durch den Betroffenen erzeugten Daten.

Schwierige Fragen sind aufgeworfen, wenn diese Daten zugleich Rechte Dritter berühren. Wenn der Nutzer eines sozialen Netzwerks sein Konto zu einem anderen Netzwerk transferieren möchte, so gehören zu diesem Konto neben Daten die nur ihn betreffen (Name, Profilbild, Hobbies, Ausbildung, etc.) auch Daten welche sowohl mit ihm, als auch mit anderen Nutzern verbunden sind (z.B. Chat-Verläufe, Bilder mit mehreren Personen, die Kontaktliste, usw.). Zu fragen ist daher, ob der Anspruch auf Datenportierung auch diese Daten umfasst, und falls ja, wie die Rechte der betroffenen Dritten geschützt werden können. Wären Daten mit Bezug auf Dritte grundsätzlich vom Recht auf Datenportabilität ausgeschlossen, so könnten sie in vielen Fällen ein erhebliches Wechselhindernis darstellen. Bei Online-Bezahldiensten etwa ist die Möglichkeit, alte Zahlungsinformationen zu überprüfen, für den Nutzer häufig unerlässlich, um zu kontrollieren oder nachzuweisen, welche Zahlungen getätigt wurden. Bei Foto-basierten sozialen Netzwerken sind häufig auf vielen Bildern auch andere Nutzer (oder sogar Dritte welche keine Nutzer des Netzwerks sind) zu erkennen, so dass ein Ausschluss dieser Bilder eine Portierung unattraktiv werden ließe. Soll das Recht auf Datenportierung in solchen Fällen den ihm zugedachten Zweck erfüllen, so muss daher auch eine Portierung von Daten mit Drittbezug möglich sein.

Für den Altanbieter bedeutet dies allerdings, dass er persönliche Daten von Betroffenen mit dem Neuanbieter teilen muss, ohne dass diese eingewilligt haben. Der Neuanbieter muss personenbezogene Daten verarbeiten, ohne mit den betroffenen Dritten in einem Vertragsverhältnis zu stehen oder deren Einwilligung hierfür zu haben. Die Art. 29 Datenschutz-Arbeitsgruppe hat vorschlagen, in diesen Fällen ein berechtigtes Interesse an der Datenverarbeitung gemäß Art. 6 Abs. 1 (f) DSGVO anzunehmen. Dies soll sich jedoch nur auf diejenige Datenverarbeitung erstrecken, die zur Ermöglichung der Portabilität notwendig ist. Der neue Dienstleister darf also etwa eine Kontaktliste nicht dazu nutzen, um an die dort aufgeführten Personen Werbung zu verschicken oder über diese Nutzungsprofile anzulegen.[133]

Weitere Fragen betreffen die effektive praktische Umsetzung des Rechts auf Datenportierung. Der Anbieter muss bei der Übermittlung der Daten die Identität des Kunden ermitteln, um Missbräuchen

[132] Siehe die Guidelines on the right to data portability der Article 29 Data Protection Working Party v. 13.12.2016, WP 242, S. 8-9.
[133] Siehe die Guidelines on the right to data portability der Article 29 Data Protection Working Party v. 13.12.2016, WP 242, S. 9-10.

vorzubeugen. Auf welche Weise dies zu geschehen hat, ist bislang nicht geklärt. Offen ist bislang auch der genaue Inhalt der Verpflichtung des Datenverarbeiter, die Daten dem Betroffenen oder einem anderen Verantwortlichen in einem „strukturierten, gängigen und maschinenlesbaren Format […]“ und ohne Behinderung“ zur Verfügung stellen. Art. 20 DSGVO zielt auf den größtmöglichen Erhalt der Nutzungsmöglichkeiten der Daten ab, verlangt jedoch nur Datenportabilität, nicht volle Interoperabilität. Die Nutzung der Daten durch vom Betroffenen ermächtigte Dritte soll realistisch möglich sein. Gleichzeitig soll das Recht auf Datenportierung aber den Datenverarbeitern keine unangemessenen Kosten auferlegen. Erwägungsgrund 68 verlangt vor diesem Hintergrund einen „gewissen Grad an Interoperabilität“. Gemäß Erwägungsgrund 21 der Richtlinie 2013/37/EU ist ein Format maschinenlesbar, wenn es „so strukturiert ist, dass Softwareanwendungen die konkreten Daten einfach identifizieren, erkennen und extrahieren können“. Andere Datenverarbeiter müssen also die enthaltenen Daten automatisiert verarbeiten können. Auszugehen ist dabei von einem Datenverarbeiter, der industrieübliche Möglichkeiten verfügt. Welche Formate „gängig“ sind, kann nur bereichsabhängig bestimmt werden. Für einige Bereiche gibt es bereits etablierte Formate, für andere nicht. Die Artikel 29 Datenschutz-Arbeitsgruppe hat die Industrieakteure zur Kooperation in der Schaffung geeigneter Standards aufgerufen und zugleich festgestellt, dass Formate, die teuren Lizenzen unterliegen, ungeeignet sind.[134] Soll der Zweck des Art. 20 DSGVO nicht verfehlt werden, dürfen die Lizenzen für die verwendeten Datenformate für andere Diensteanbieter keine unangemessenen Hindernisse schaffen.

Art. 20 Abs. 4 DSGVO stellt klar, dass durch die Datenportierung die „Rechte Dritter“ nicht beeinträchtigt werden dürfen. Zu diesen zählen gemäß Erwägungsgrund 63 Rechte des geistigen Eigentums, insbesondere auch das Urheberrecht an der Software, welche zur Datenverarbeitung verwendet wird.[135] Das Recht auf Datenportabilität soll nicht missbraucht werden, um an (urheberrechtlich oder als Geschäftsgeheimnis) geschützte Informationen zu gelangen.[136] Zugleich darf der Schutz des geistigen Eigentums und von Geschäftsgeheimnissen einer effektiven Durchsetzung der Datenportabilität nicht im Wege stehen. Die Vorstellung des Centre for Information Policy (CIPL), dass Portabilitätsanfragen Konkurrenten keinen „unfairen Vorteil“ in Form des Zugriffs auf wertvollen und mühsam zusammengetragene Daten verschaffen dürften,[137] geht daher deutlich zu weit. Die Datenportierung darf, wie die Artikel 29 Arbeitsgruppe zu Recht festgestellt hat, selbst dann nicht verweigert werden, wenn hieraus geschäftliche Risiken für den verpflichteten Datenverarbeiter

[134] Siehe die Guidelines on the right to data portability der Article 29 Data Protection Working Party v. 13.12.2016, WP 242, S. 14.

[135] Erwägungsgrund 63 Satz 5 Datenschutzgrundverordnung: „Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen.“

[136] Stellungnahme der Art 29 Datenschutz Arbeitsgruppe, S. 10.

[137] So lassen sich die Kommentare des CIPL verstehen: "However, the data provided in data fields, for example, may aggregate to a specific analysis and competitive advantage that a business has carefully constructed; thus parting with the data could be seen as giving an unfair advantage to a competing business. With data driving new products, services and economic growth, the guidelines should confirm that the interests and rights of controllers are taken into account when dealing with a request to data portability. Indeed, the implementation of the data portability right should take place in a balanced manner, doing full justice to these other competing rights and interests“.
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf

entstehen.[138] Der Datenverarbeiter darf jedoch der Anfrage in einer Art und Weise nachkommen, die seine geistigen Eigentumsrechte wahrt.[139]

b) Spezialgesetzliche Vorschriften zur Datenportabilität

Das Recht auf Datenportabilität ist keine Erfindung der DSGVO. Funktional verwandte Vorschriften zur Portabilität personenbezogener Daten finden sich in verschiedenen spezialgesetzlichen Regelungskontexten.

aa) Smart Metering

Für den Energiesektor hat die Elektrizitätsbinnenmarkt-RL 2009/72/EG in Art. 3 Abs. 5 die Verpflichtung der Mitgliedstaaten festgeschrieben, den Energiekunden einen kurzfristigen Lieferantenwechsel zu ermöglichen und dabei den Kunden das Recht einzuräumen, sämtliche sie betreffende Verbrauchsdaten zu erhalten. Die Kunden sollen in der Lage sein, auf der Grundlage ihres konkreten Verbrauchsprofils attraktivere Angebote ausfindig zu machen.[140]

In ganz ähnlicher Weise verpflichtet Art. 9 Abs. 2 lit. d der Energie-Effizienz-RL 2012/27/EU die Mitgliedstaaten, zu „gewährleisten, dass, falls die Endkunden dies wünschen, ihnen oder einem im Auftrag des Endkunden handelnden Dritten Messdaten über ihre Stromeinspeisung und Stromentnahme in einem leicht verständlichen Format zur Verfügung gestellt werden, dass es ermöglicht, Angebote unter gleichen Voraussetzungen zu vergleichen“.

In Deutschland wurden diese Vorgaben in den §§ 10 Abs. 3, 52 Abs. 1, 61 und 69 Abs. 1 Nr. 2 Messstellenbetriebsgesetz (MsbG) umgesetzt. § 52 Abs. 1 MsbG lautet:

„Die nach § 49 Absatz 2 berechtigten Stellen haben eine verschlüsselte elektronische Kommunikation von personenbezogenen Daten, von Mess-, Netzzustands- und Stammdaten in einem einheitlichen Format zu ermöglichen, die den Bestimmungen dieses Gesetzes genügt. Soweit Messwerte oder Stammdaten betroffen sind, muss das Format die vollautomatische Weiterverarbeitung im Rahmen der Prozesse für den Datenaustausch zwischen den Beteiligten ermöglichen, insbesondere auch für den Wechsel des Lieferanten.“

Zweck der Vorschriften ist es, die Vergleichbarkeit von Angeboten und damit zugleich den Marktzutritt anderer Anbieter zu erleichtern und dadurch den Wettbewerb zu stärken[141].

---

[138] Siehe die Guidelines on the right to data portability der Article 29 Data Protection Working Party v. 13.12.2016, WP 242, S. 10.

[139] Stellungnahme der Art 29 Datenschutz Arbeitsgruppe, S. 10.

[140] Erwägungsgrund 50 der Elektrizitätsbinnenmarkt-RL.

[141] Siehe Erwägungsgrund 45 der Elektrizitätsbinnenmarkt-RL 2009/72/EG: „Die Mitgliedstaaten sollten dafür Sorge tragen, dass Haushalts-Kunden und, soweit die Mitgliedstaaten dies für angezeigt halten, Kleinunternehmen das Recht auf Versorgung mit Elektrizität einer bestimmten Qualität zu leicht vergleichbaren, transparenten und angemessenen Preisen haben.“ sowie Erwägungsgrund 8 der Elektrizitätsbinnenmarkt-RL 2009/72/EG: „Um den Wettbewerb zu gewährleisten und die Stromversorgung zu den wettbewerbsfähigsten Preisen sicherzustellen, sollten die Mitgliedstaaten und die nationalen Regulierungsbehörden den grenzüberschreitenden Zugang sowohl für neue Stromversorger aus unterschiedlichen Energiequellen als auch für Stromversorger, die innovative Erzeugungstechnologien anwenden, begünstigen.“

Mit Inkrafttreten der DSGVO ergibt sich künftig das Recht auf Portabilität von Energie-Verbrauchsdaten bereits aus Art. 20 DSGVO. Die sektorspezifischen Regeln sind allerdings mit der Verpflichtung der Mitgliedstaaten verbunden, Vorgaben zur Standardisierung des Datenformats zu machen (s. Anhang I Abs. 1 lit. h RL 2009/72/EG).

bb) Zahlungsdienste-RL 2015/2366 (PSD-2)

Auch die Zahlungsdienste-RL 2015/2366 hat ein neues Recht auf Datenportabilität eingeführt. Gem. Art. 67 der RL haben die Mitgliedstaaten sicherzustellen, „dass ein Zahlungsdienstenutzer das Recht hat, Dienste, die den Zugang zu Zahlungskontoinformationen … ermöglichen, zu nutzen." Die kontoführende Einrichtung muss zu diesem Zweck gegebenenfalls die Kontoinformation an den vom Zahlungsdienstenutzer benannten Kontoinformationsdienstleister herausgeben. Der Kontoinformationsdienstleister braucht für die Geltendmachung des Herausgabeanspruchs die ausdrückliche Zustimmung des Zahlungsdienstenutzers und muss eine Datenübermittlung über sichere und effiziente Kanäle gewährleisten. Er darf die Daten nur für den ausdrücklich angeforderten Kontoinformationsdienst nutzen. Die Bundesregierung plant, diese Pflichten in § 50 eines Gesetzes zur Umsetzung der Zweiten Zahlungsdiensterichtlinie in deutsches Recht umzusetzen.[142] Die Pflichten sollen aufsichtsrechtlich durchgesetzt werden.

cc) Datenportabilität im RL-Entwurf der EU-Kommission zu bestimmten vertragsrechtlichen Aspekten der Bereitstellung digitaler Inhalte

Ein Recht auf Datenportabilität ist schließlich auch im Vorschlag der Europäischen Kommission für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 09.12.2015[143] vorgesehen.[144] Das Recht auf Datenportierung nach der DSGVO und nach dem Richtlinienvorschlag unterscheiden sich jedoch in Zweck, Anwendungsbereich und Voraussetzungen.

Das im Richtlinienvorschlag zu digitalen Gütern verankerte Recht auf Datenportierung zielt darauf ab, Verbrauchern eine effektive Durchsetzung ihres Kündigungsrechts zu ermöglichen. Während das Recht aus Art. 20 DSGVO jederzeit in Anspruch genommen werden kann, ist Voraussetzung für die Datenportierung nach dem Richtlinienvorschlag daher eine wirksame Kündigung eines bestehenden Vertrages, entweder wegen des nicht-vertragsgemäßen Zustandes digitaler Güter (Art. 13 Abs. 2 lit. c), oder bei langfristigen Verträgen mit einer Laufzeit von mehr als 12 Monaten oder bei unbefristeten Verträgen nach Ablauf einer Zeit von 12 Monaten (Art. 16 Abs. 4 lit. b). Der Vertragspartner darf dem Richtlinienvorschlag für digitale Güter zufolge für die Datenportierung eine angemessene Gebühr erheben (Art. 16 Abs. 4). Der Anspruch auf Datenportierung erstreckt sich dann auf alle Inhalte und

[142] Siehe § 50 des Referentenentwurfs vom 28.02.2017: „(1) Der kontoführende Zahlungsdienstleister ist verpflichtet,
1. mit dem Kontoinformationsdienstleister auf sichere Weise zu kommunizieren und
2. Anfragen nach der Übermittlung von Daten, die von einem Kontoinformationsdienstleister übermittelt werden, ohne Benachteiligung zu behandeln, es sei denn, es bestehen objektive Gründe für eine abweichende Behandlung.
(2) Das Erbringen von Kontoinformationsdiensten ist nicht davon abhängig, ob der Kontoinformationsdienstleister und der kontoführende Zahlungsdienstleister zu diesem Zweck einen Vertrag abgeschlossen haben."

[143] [2015/0287 (COD)]

[144] Siehe Art. 13 Abs. 2 (c) als auch in Art. 16 Abs. 4 (b).

Daten, welche durch die Nutzung der Dienstleistung generiert wurden.[145] Anders als die DSGVO verpflichtet der Richtlinienvorschlag die Datenverarbeiter nicht, die Daten gebündelt bereitzustellen, sondern nur „ohne erhebliche Unannehmlichkeiten“ (Art. 12 Abs. 2) und in einem „allgemein gebräuchlichen Datenformat“ (Art. 13 Abs. 2 (c)). Datenverarbeiter können ihrer Pflicht daher gegebenenfalls auch durch Einräumung des Zugriffs auf die Einzeldaten nachkommen. Der Transfer der Daten zu einem neuen Anbieter würde dadurch erschwert.

Unumstritten ist, dass das Recht auf Datenportierung nach der DSGVO neben dem Richtlinienvorschlag für digitale Dienste anwendbar bliebe. Insoweit das Recht auf Datenportierung nach dem Richtlinienvorschlag also hinter Art. 20 DSGVO zurückbleibt, könnte sich der Dienstenutzer in dem dort vorgesehenen Umfang auf die DSGVO stützen.

c) Schlussfolgerungen zur Portabilität personenbezogener Daten

Die sektorspezifischen Vorschriften zur Datenportierung verdeutlichen die Zielrichtung und Wirkweise des Rechts, wie es nunmehr in allgemeiner Form in Art. 20 DSGVO verankert ist: Die Ermächtigung der durch personenbezogene Daten in Bezug genommenen Person zur Datenportierung dient weniger dem Schutz des allgemeinen Persönlichkeitsrechts. Es kompensiert vielmehr ein durch das Datenschutzrecht induziertes Marktversagen: Bei Diensten, deren Funktionalität oder Wettbewerbsfähigkeit vom Zugriff auf personenbezogene Daten abhängt, verhindert oder erschwert das Datenschutzrecht den Erwerb dieser Daten über den Markt. Das Recht auf Datenportierung ermöglicht es dem Betroffenen, sich gleichwohl aus einem dateninduzierten „lock-in“ zu befreien und vom Wettbewerb der Anbieter zu profitieren.[146] Die Wechselkosten werden erheblich reduziert. Das Recht auf Datenportierung macht die Person, auf die sich die Daten beziehen, zur Schaltstelle für den Datenzugriff, und wird damit zu einem wesentlichen Bestandteil der Funktionsweise von Märkten für datengetriebene Dienste.

Das Recht auf Datenportierung hat zugleich einen Preis. Für diejenigen, welche die Portierung gewährleisten müssen, bedeutet es zusätzliche Kosten. Weil die Verweildauer einer Person bei einem Datenverarbeiter möglicherweise kurz ist, mindert es die Anreize der Datenverarbeiter, in eine langfristige Beziehung zu den Betroffenen zu investieren.

Bemerkenswert ist, dass Art. 20 DSGVO wie auch die sektorspezifischen Ausformungen des Rechts auf Datenportierung weder eine Marktmachtstellung des jeweiligen Anbieters noch ein festgestelltes Problem des „lock-in“ voraussetzen. Das Recht wird unabhängig von einem festgestellten *marktmachtbedingten* Marktversagen gewährt. Es ist in dieser Hinsicht Teil einer Wendung fort vom Datenschutz hin zur „Datensouveränität“, d.h. zu einer Ermächtigung des Einzelnen zur wirtschaftlichen Nutzung seiner Daten.

[145] Z.B. Fotobücher, welche nicht den Nutzer sondern Dritte zeigen – siehe *Janal*, Data Portability – A tale of two concepts, JIPITEC Vol. 8, S. 8.

[146] Art. 29 Data Protection Working Party: Guidelines on the right to data portability, 13 December 2016: Datenportabilität ist “an important tool that will support the free flow of personal data in the EU and foster competition between data controllers”.

4. Stärkung sekundärer Datenmärkte für personenbezogene Daten durch Schaffung eines „Eigentumsrechts“ an personenbezogenen Daten?

Die Diskussion über ein neues Eigentum- bzw. Immaterialgüterrecht, also ein subjektives Ausschließlichkeitsrecht an Daten mit Abwehrwirkung gegenüber jedermann und einem positiven Zuweisungsgehalt,[147] wurde ganz überwiegend mit Blick auf nicht personenbezogene Daten geführt (näher dazu unten, F.). Auch für personenbezogene Daten lässt sich aber fragen, ob ein neues Eigentumsrecht sinnvoll ist.

Überzeugende Gründe hierfür sind bislang allerdings nicht vorgebracht worden. Das Datenschutzrecht weist den Betroffenen bereits viele Rechte zu, die – wenn man das Eigentumsrecht als „bundle of rights“ versteht – Facetten eines typischen Eigentumsrechts sind, insb. das Recht des Ausschlusses Dritter von der Verarbeitung der auf sie bezogenen Daten. Ein Besitzrecht an den Daten ist dem Betroffenen demgegenüber nicht zugewiesen (wohl aber ein Löschungsrecht). Die Möglichkeit der/des Betroffenen, die auf sie/ihn bezogenen Daten wirtschaftlich zu verwerten, ist faktisch ein Annex des Ausschlussrechts, wird durch die Rechtsordnung bislang aber als solches nicht näher ausgestaltet. Die „Kommerzialisierung“ von Daten ist – gerade unter Datenschutzrechtlern – vielmehr weiterhin umstritten. Ungeachtet der Einschränkungen, die aus verschiedenen gesetzlichen Erlaubnistatbeständen folgen, kann man daher die Rechte, die das Datenschutzrecht den Betroffenen zuweist, als „ausgedünntes Eigentumsrecht“ verstehen. Eine noch stärkere Ausformung der Rechte der Betroffenen würde nicht nur die wirtschaftliche, sondern auch die gesellschaftliche Interaktion erheblich erschweren.

Man muss die den Betroffenen durch das Datenschutzrecht zugewiesenen Rechte allerdings nicht als „ausgedünntes Eigentumsrecht“ verstehen. Alternativ kann man in ihnen eine Art „dingliche Last“ sehen, die den fraglichen Daten anhaftet und beim Handel mit personenbezogenen Daten zu berücksichtigen ist. Grundsätzlich bliebe dann die Schaffung eines (beschränkten) Dateneigentumsrechts zugunsten desjenigen möglich, der für die Erhebung und Verarbeitung personenbezogener Daten sorgt. Die Frage, nach welchen Kriterien das Eigentumsrecht zugeordnet werden sollte, ist damit noch nicht beantwortet. Auch die Spannung zwischen einem auf die Erleichterung der Verkehrsfähigkeit angelegten Eigentumsrecht und den unverzichtbaren Rechten der Daten-Betroffenen würde durch ein solches Eigentumsrecht nicht aufgelöst.

Die Frage, ob es gute Gründe für die Schaffung eines solchen Dateneigentumsrechts gibt, ist für personenbezogene wie nicht personenbezogene Daten grundsätzlich nach den denselben Kriterien zu beurteilen und wird im Abschnitt F ausführlich behandelt. Entscheidend ist, ob es der Schaffung zusätzlicher Anreize zur Investition in die Erhebung und Verarbeitung personenbezogener Daten bedarf, und/oder ob durch Eigentumsrechte die Transaktionskosten erheblich abgesenkt werden könnten. Die gegenwärtige datenschutzrechtliche Debatte spricht dafür, dass zusätzliche Anreize zur Sammlung und Verarbeitung personenbezogener Daten nicht erforderlich und gesellschaftspolitisch auch nicht erwünscht sind. Transaktionskosten im Handel mit personenbezogenen Daten werden vor allem durch das Datenschutzrecht selbst geschaffen. Ungeachtet der Debatte über ein Eigentumsrecht an nicht personenbezogenen Daten lassen sich daher gute Argumente für ein Eigentumsrecht

[147] *Zech,* Information als Schutzgegenstand, 2012, S. 64 mit Verweis auf *Peukert,* Güterzuordnung als Rechtsprinzip, 2008, S. 56 ff.

desjenigen, der für die Erhebung und Verarbeitung personenbezogener Daten sorgt, gegenwärtig nicht finden.

5. Stärkung sekundärer Datenmärkte durch eine veränderte institutionelle Ausgestaltung – Einführung von „Personal Information Management Systemen" (PIMS)

Wie bereits dargestellt, muss die Schwäche des sekundären Handels mit personenbezogenen Daten kein Marktversagen bedeuten, solange ein anderweitiger Zugriff auf personenbezogene Daten oder die hiermit verbundenen Erkenntnisse gewährleistet ist.

Will man den sekundären Handel mit personenbezogenen Daten gleichwohl stärken, so ist dies datenschutzrechtlich nur möglich, wenn die Betroffenen in Transaktionen, die mit Blick auf Zweck und/oder den Kreis der Handelspartner nicht von der ursprünglichen Einwilligung gedeckt sind, unmittelbar einbezogen werden. Konkret bedarf es in solchen Fällen einer transaktionsspezifischen Einwilligung des Betroffenen in die Weitergabe der Daten und in die beabsichtigte Datenverarbeitung. Tatsächlich gibt es verschiedene Initiativen, die einen solchen sekundären Datenhandel „unter Einwilligungsvorbehalt" mithilfe von neuartigem Einwilligungsdesign, das den Betroffenen ein einfaches Management der auf sie bezogenen Daten ermöglichen, praktikabel machen wollen. Sie werden unter dem Begriff der „Personal Information Management Systeme" (PIMS) zusammengefasst.[148] Beispiele hierfür sind die Initiative „Industrial Data Space" der Fraunhofer-Gesellschaft; die finnische Initiative „MyData"; wie auch private Initiativen wie „Citizenme"[149] oder „Datacoup".[150]

Beispielhaft vorgestellt werden soll hier die Initiative „Industrial Data Space" (IDS). Auch wenn deren Fokus eher auf nicht-personenbezogenen Daten im industriellen Kontext liegt, führt sie doch die Governance-Strukturen eines PIMS beispielhaft vor.[151] Ziel des IDS ist die Schaffung eines virtuellen Datenraums, der den sicheren Austausch und die einfache Verknüpfung von Daten auf Basis von Standards und mit Hilfe gemeinschaftlicher Governance-Modelle unterstützt soll.[152] Es handelt sich bei IDS nicht um einen Datenspeicher, sondern um eine „Geschäftsarchitektur" beziehungsweise ein „data governance"-System. Ausgegangen wird dabei von einer „Eigentümerstellung" der Betroffenen an den auf sie bezogenen Daten. Den Betroffenen soll das System zur digitalen Souveränität verhelfen. Auf dieser Grundlage werden allgemeine Rechte und Pflichten der System-Teilnehmer festgelegt. Die System-Teilnehmer – insb. die „Datenbroker" – werden nach Maßgabe bestimmter Kriterien zertifiziert; IDS stellt eine Infrastruktur für einen sicheren Austausch und zur einfachen Verknüpfung von Daten bereit (Verifizierung der Identität der Teilnehmer; Dienste zur Transformation von Daten von einem Quellschema in ein Zielschema, Nachverfolgbarkeit der Daten, Dienste zur Datenanonymisierung, Unterstützung der Entwicklung und Pflege von gemeinschaftlichen Vokabularen). Möglich sind ferner Datenqualitätsdienste und Datenanalysedienste. Auf dieser institutionellen Grundlage erhält der „Dateneigentümer" die Möglichkeit, über die

[148] Näher dazu z.B. *Poikola et. al.*, 2015. Siehe auch *Koutroumpis et. al.* 2016a. Siehe auch EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 19.
[149] Siehe citizenme.com.
[150] Siehe datacoup.com.
[151] Siehe näher: Fraunhofer Gesellschaft, Industrial Data Space – Digitale Souveränität über Daten, White Paper, 2016
[152] Fraunhofer Gesellschaft, Industrial Data Space – Digitale Souveränität über Daten, White Paper, 2016, S. 4

Nutzungsbedingungen „seiner“ Daten zu entscheiden (z.B. sachliche oder zeitliche Nutzungsbeschränkungen; Beschränkung des Kreises möglicher Partner von Austauschgeschäften). IDS gewährleistet, dass ein Zugriff auf die Daten nur unter Wahrung dieser Bedingungen möglich ist. Zugleich soll der IDS dazu beitragen, dass innovative Unternehmen Zugriff auf diejenigen Daten erhalten, die sie für innovative Geschäftsideen benötigen. Insbesondere die Entwicklung von „smart services“ soll durch den IDS erleichtert werden.

Andere PIMS verfolgen – mit Variationen in der konkreten Ausgestaltung – einen ähnlichen Grundansatz. Einige PIMS sind primär als Einwilligungs-Management-Systeme konzipiert – wobei es denkbar ist, dass die Betroffenen das konkrete Einwilligungsmanagement an „Trusted Third Parties“ abgeben können. Bei anderen dient das PIMS zugleich als zentraler Speicherplatz für Daten. PIMS können durch Vorgabe bestimmter Datenformate die Interoperabilität zwischen verschiedenen Datensätzen erleichtern; sie können die Nachverfolgbarkeit der Datennutzung sichern und damit eine Kontrolle darüber ermöglichen, ob der Grundsatz der Zweckbindung bei der Datennutzung eingehalten wird; und Betroffene können grundsätzlich verbindliche Beschränkungen der Datennutzung – etwa eine zeitliche Begrenzung – vorgeben.[153]

PIMS können unterschiedliche Geschäftsmodelle verfolgen. Denkbar ist etwa ein Provisionsmodell. Möglich ist, dass sich PIMS für bestimmte Anwendungsbereiche herausbilden (beispielsweise für den Umgang mit Gesundheits- oder Finanzdaten). Ebenso können PIMS aber auch die Kontrolle über Daten aus verschiedenen Lebensbereichen ermöglichen. Schließlich ist denkbar, dass PIMS künftig vertikal integriert angeboten werden. So ist vorstellbar, dass in Zukunft Personal Digital Assistants (beispielsweise Alexa von Amazon, Cortana von Microsoft, Siri von Apple oder der Google Assistant) die Rolle von PIMS übernehmen.

Wird künftig ein sekundärer Handel personenbezogener Daten durch Bereitstellung eines gut handhabbaren Einwilligungsmanagements leicht gemacht, ist dies zugleich ein Schritt in eine weitergehende Kommerzialisierung personenbezogener Daten: Die Betroffenen können „ihre“ Daten dann nicht mehr nur im Rahmen des Geschäftsmodells „Dienste gegen Daten“ als alternatives Entgelt nutzen; sie können ihre Einwilligung in eine von der Bereitstellung bestimmter Dienste unabhängige Datenverarbeitung gegebenenfalls auch gegen ein monetäres Entgelt verkaufen. PIMS können hierfür einen ökonomischen Bewertungsmechanismus für Daten bereitstellen.[154]

Gegenwärtig ist ein Markterfolg der PIMS als Instrument zum Management personenbezogener Daten durch die Betroffenen noch nicht absehbar.

Zu fragen ist aber, ob eine Durchsetzung von PIMS am Markt zur Stärkung des sekundären Handels mit personenbezogenen Daten wünschenswert ist. Die damit potentiell verbundene aktive Kommerzialisierung personenbezogener Daten durch Verbraucher ist nicht vollständig neu: Eine aktive Kommerzialisierung von personenbezogenen Daten findet gegenwärtig bereits bei den z.B. im Einzelhandel verbreiteten Kundenkarten statt. Im Gegenzug für die Bereitstellung ihrer Daten erlangen die Kunden zwar kein monetäres Entgelt, aber Rabatte.

[153] Zur Bedeutung einer Begrenzung der Speicherdauer für Handelszwecke siehe etwa auch FTC Report, Data Broker, S. 48-49.
[154] Fraunhofer Gesellschaft, Industrial Data Space – Digitale Souveränität über Daten, White Paper, 2016, S. 11

Eine solche Kommerzialisierung von personenbezogenen Daten kann allerdings aus einer ökonomischen Perspektive nachteilig sein. Dies gilt insbesondere, wenn man Konsumentenwohlfahrt als das relevante Wohlfahrtskriterium erachtet.

Da Nutzer von PIMS in der Regel Zugangsoptionen langfristig festlegen, ist davon auszugehen, dass es sich hierbei um bewusste Entscheidungen handelt, nicht um rein spontane Entscheidungen beim Besuch einer Webseite. Somit ist zu erwarten, dass bei der Nutzung von PIMS psychologische Einflussfaktoren eine geringere Rolle spielen als bei spontanen Entscheidungen zum Transfer personenbezogener Daten. Insbesondere können Konsumenten mit Selbstkontrollproblemen PIMS als Mittel zur Selbstbindung verwenden.

Die Kommerzialisierung von personenbezogenen Daten über PIMS kann aber zu einer Reduktion der Konsumentenwohlfahrt selbst dann führen, wenn jeder Nutzer vollkommen rational handelt und seinen Erwartungsnutzen maximiert; und zwar dann, wenn die Zustimmung zur Datenverarbeitung negative externe Effekte auslöst. Dies gilt beispielsweise, wenn aufgrund der Zustimmung zur Datenverarbeitung ein Unternehmen mit Monopolmacht personenbezogene Rabatte anbietet. Individuelle Rabatte stellen ceteris paribus die betroffene Person besser. Im Extremfall, wenn ein Unternehmen aufgrund der personenbezogenen Daten die Zahlungsbereitschaft der Konsumenten perfekt erfassen kann, wird es personenbezogene Rabatte so setzen, dass die Konsumenten das Angebot gerade annehmen. In diesem Fall werden alle Konsumenten Zugang zu ihren Daten gewähren, denn wer das nicht tut, müsste einen überhöhten Listenpreis zahlen. Das Unternehmen ist dadurch in die Lage versetzt, die gesamtem Wohlfahrtsgewinne selbst einzubehalten. Bei PIMS wird im Vergleich zum direkten Datentransfer von Konsumenten zu Unternehmen das Problem der verringerten Konsumentenwohlfahrt evtl. sogar verschärft, da Transaktionskosten der Informationsoffenlegung drastisch verringert werden. Eine solche Wohlfahrtsreduktion wäre selbst dann denkbar, wenn personenbezogene Rabatte (oder allgemeiner personenbezogene Preise) verboten wären. Hier könnte durch Targeted Advertising einem Konsumenten eine Variante eines Produktes zu einem Preis so angeboten werden, dass gerade seine Zahlungsbereitschaft abgeschöpft wird.[155] Im Ergebnis hängt die

[155] In der ökonomischen Literatur ist das Phänomen der Offenlegung privater Information bekannt und auch im Kontext des Datenschutzes diskutiert worden. So schreiben Acquisti und Koautoren (auf Seite 455): „Granting consumers the right to sell their personal data may undermine consumer welfare. Sellers in a monopolistic market try to improve their capacity to price-discriminate collecting personal information on consumers. Marginal consumers in a monopolistically priced market make no surplus on their consumption and will be willing to sell their personal information for any marginal price. That enables the seller to collect more data and improve price discrimination and will reveal their preferences. The monopolistic seller ends up with perfect price discrimination information across the entire market and acquires all the surplus." (*Acquisti/Taylor/ Wagman*, The Economics of Privacy, Journal of Economic Literature, vol. 54(2), 2016, S. 442-492.)
Das Offenlegen personenbezogener Daten muss nicht perfekt sein, um zu einer verringerten Konsumentenwohlfahrt zu führen. Es reicht, wenn ein Unternehmen aufgrund des Zugangs zu personenbezogenen Daten ein besseres Verständnis über die individuellen Zahlungsbereitschaften erhält.
Wir illustrieren dies anhand eines Zahlenbeispiels. Ein digitales Gut werde von einem Unternehmen verkauft; dabei entstehen für zusätzliche Einheiten keine Kosten. Unterstellen wir, dass Konsumenten für dieses Gut zwischen 10 Euro und 90 Euro bereit sind zu zahlen und dass alle Zahlungsbereitschaften in diesem Intervall die gleiche Wahrscheinlichkeit haben. Ein Unternehmen, das nur Information über die Verteilung hat, wird zum Preis von 50 Euro verkaufen. Im Schnitt wird jeder zweite Konsument das Produkt zu diesem Preis kaufen, so dass ein erwarteter Gewinn von 25 Euro pro Konsument entsteht. Die erwartete Konsumentenrente beträgt 10 Euro.
Konsumenten können ihre personenbezogenen Daten dem Unternehmen mitteilen. Wir nehmen an, dass Konsumentendaten Aufschluss über das 10er-Intervall gibt, in dem die Zahlungsbereitschaft liegt. Wenn beispielsweise ein Konsument mit Zahlungsbereitschaft 13 dem Unternehmen Zugang zu seinen persönlichen

Wirkung von PIMS auf die Konsumentenwohlfahrt entscheidend von der Marktstruktur im nachgelagerten Produktmarkt ab. Wenn Konsumenten über PIMS Unternehmen ohne Aufwand Daten kontrolliert zur Verfügung stellen können, wird der Wettbewerb zwischen Unternehmen tendenziell gefördert. Dann ist die individuelle Offenlegung personenbezogener Daten weniger problematisch, weil Unternehmen aufgrund der erhöhten Wettbewerbsintensität daraus keinen Vorteil ziehen können.[156] Je schwächer der Wettbewerb ist, desto eher können Unternehmen hingegen ökonomische Renten abschöpfen

Unser Fazit zu PIMS lautet, dass unklar ist, ob sich diese in der Praxis durchsetzen. Sie bergen Chancen und Risiken, so dass sich Fragen nach Regulierung und insbesondere Zertifizierung stellen.

F. Der Handel mit nicht personenbezogenen Daten

I. Bestandsaufnahme

Auf der Webseite der Europäischen Kommission heißt es zum Digital Single Market: „Building a European data economy is part of the Digital Single Market strategy. The initiative aims at fostering

Daten gibt, so lernt das Unternehmen, dass der Konsument eine Zahlungsbereitschaft zwischen 10 und 20 hat. Das Unternehmen kann nun einen Listenpreis festsetzen und nicht übertragbare Coupons abhängig von den persönlichen Daten Konsumenten anbieten. Folgende Strategie ist für das Unternehmen optimal: Es setzt einen Listenpreis von 80 Euro. Wenn es persönliche Daten von einem Konsumenten erhält, bietet es einen Coupon an. Dieser beträgt 20 Euro, wenn beispielsweise ein Konsument eine Zahlungsbereitschaft von 67 Euro hat; er liegt bei 70 Euro im Fall einer Zahlungsbereitschaft von 13 Euro. Der resultierende Preis, den ein Konsument gefragt wird zu zahlen, ist damit so gewählt, dass der Konsument mit der kleinsten Zahlungsbereitschaft in der Gruppe gerade noch bereit ist, das Produkt zu kaufen. Bei einer solchen Strategie wird jeder Konsument das Produkt kaufen. Der durchschnittliche Preis (nach Einlösen der Coupons), den Konsumenten zahlen, ist 45 Euro. Damit ist der erwartete Gewinn pro Konsument 45 Euro, fast das Doppelte dessen, was ohne das Verwerten der persönlichen Daten möglich wäre. Wie hoch ist nun die erwartete Konsumentenrente? Jeder Konsument erwartet, das Produkt zu kaufen. Im Schnitt kostet das Produkt 5 Euro weniger als die Zahlungsbereitschaft. Somit ist die erwartete Konsumentenrente 5 Euro, die Hälfte dessen, was Konsumenten im Schnitt erhielten, wenn dem Unternehmen die persönlichen Daten nicht zur Verfügung stünden.
Es mag überraschend klingen, dass rationale Konsumenten, die eine hohe Zahlungsbereitschaft haben, ihre persönlichen Daten zugänglich machen. Bei einem Preis von 80 Euro erhält aber jeder Konsument mit einer niedrigeren Zahlungsbereitschaft einen Coupon, von dem das Unternehmen die persönlichen Daten hat. Also werden alle Konsumenten mit einer Zahlungsbereitschaft kleiner als 80 Euro Zugang zu ihren persönlichen Daten gewähren. Die verbleibenden Konsumenten haben keinen strikten Anreiz dies zu tun und zahlen den Listenpreis. Gegeben das beschriebene rationale Konsumentenverhalten, ist es in der Tat gewinnmaximierend für das Unternehmen, einen Listenpreis von 80 Euro zu verlangen und Coupons in Abhängigkeit der erfassten persönlichen Daten zu verschicken. Aufgrund der stark reduzierten erwarteten Konsumentenrente haben Konsumenten also guten Grund das Bereitstellen persönlicher Daten als nicht in ihrem Interesse anzusehen, obwohl sie einen individuellen Anreiz haben (und es somit individuell rational ist), Zugang zu ihren Daten zu gewähren.

[156] Siehe beispielsweise *Capozza/van Order*, A generalized model of spatial competition. American Economic Review 68, 1978, S. 896-908 im Fall von personalisierten Preisen und *Liu/Serfes*, Quality of information and oligopolistic price discrimination, Journal of Economics and Management Strategy 13, 2004, S. 671-702, im Fall von gruppenspezifischen Discounts. Eine vereinfachte formale Analyse findet sich in *Belleflamme/Peitz*, Industrial Organization: Markets and Strategies, 2. Aufl., 2015, S. 204-209.

the best possible use of the potential of digital data to benefit the economy and society. It addresses the barriers that impede the free flow of data to achieve a European single market."[157] Die Stärkung des Handels mit nicht personenbezogenen Daten ist dabei ein erklärtes Ziel der EU-Kommission.[158]

Bei nicht personenbezogenen Daten handelt es sich teilweise um offene Daten und andernteils um nicht offene Industriedaten. Offene Daten sind häufig Daten der öffentlichen Verwaltung. Offene Daten können aber auch von Nichtregierungsorganisationen und Unternehmen bereitgestellt werden.

Im Folgenden betrachten wir in erster Linie nicht offene Industriedaten, die im Unternehmen entstehen und eventuell auch für andere Unternehmen relevant sind.

Gegenwärtig findet ausweislich der Mitteilung der EU-Kommission zum Aufbau einer Datenwirtschaft ein Handel mit nicht personenbezogenen Daten sektorspezifisch in unterschiedlicher Weise und in unterschiedlichem Umfang statt.[159] Anders als bei personenbezogenen Daten spielen „Primärmärkte" für die Datenbeschaffung eine geringere Rolle: Während Unternehmen sich substituierbare personenbezogene Daten oft mit unterschiedlichen Angeboten auch mehrfach von den Endkunden beschaffen können, ist dies bei Industriedaten in vielen Fällen nicht möglich. Die Herrschaft über produktive Ressourcen und geschäftliche Information geht häufig mit der Möglichkeit des Ausschlusses Dritter von diesen Informationen einher. Nicht selten wird von dieser Möglichkeit Gebrauch gemacht, und die Daten werden ausschließlich unternehmensintern genutzt.

In bestimmten Bereichen spielt Data Sharing eine große Rolle: Maschinenhersteller teilen die durch Sensoren erzeugten Maschinendaten unter Umständen in der ein oder anderen Weise mit dem Maschineneigentümer. Bei Anwendungen im Bereich des autonomen Fahrens wird Data Sharing vermutlich ebenfalls eine große Rolle spielen.[160] Einige Unternehmen stellen eigene Informationen über Schnittstellen (Application Programming Interfaces – APIs) für Drittunternehmen zur Verfügung, die auf dieser Grundlage Mehrwertdienste anbieten und so die Kerndienste des Unternehmens attraktiver machen können – so etwa im Bereich „mobility" oder „banking" und Informationsdienste (z.B. Reuters, Elsevier, Twitter)[161]. Denkbar ist aber auch, dass sich Unternehmen bewusst gegen ein Data Sharing entscheiden, weil sie mithilfe der Daten ihre Wettbewerbsposition auf dem Kernmarkt und/oder Wettbewerbsvorteile auf angrenzenden Märkten absichern wollen. In bestimmten Fällen können daraus „Aftermarket"-Probleme entstehen.[162]

Die Trennlinie zwischen Data Sharing und einem bilateralen Datenhandel ist unscharf. Ein bilateraler Datenhandel mit individuell ausgehandelten Verträgen kann komplementär oder alternativ zum Data Sharing eingesetzt werden. Beispielsweise können die durch Sensoren erzeugten Maschinendaten

[157] Siehe https://ec.europa.eu/digital-single-market/en/building-european-data-economy, zuletzt aufgerufen am 30.7.2017.
[158] Siehe EC Communication on Building a European Data Economy, 10.01.2017 COM(2017) 9 fin.
[159] Siehe 2.2 in Teil 3 von EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin.
[160] Zur Nutzung von Mobilitätsdaten hat beispielsweise der VDA ein Positionspapier vorgelegt, siehe https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html
[161] Für konkrete Beispiele siehe EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 13. Twitter bietet seine Daten auf seiner Plattform "Gnip" an. Siehe https://gnip.com/.
[162] Siehe zur Aftermarket-Problematik allgemein *Gundlach*, Antitrust Bulletin 52, 2007, 17 ff.; *Coppi*, Antitrust Bulletin 52, 2007, S. 53 ff. Siehe auch G.I. weiter unten.

auch an Dritte „verkauft“ werden, die auf der Grundlage dieser Daten zusätzliche Mehrwertleistungen entwickeln. In den meisten Fällen ist dabei aber nicht von einem „Verkauf“ der Daten im rechtlichen Sinne, sondern von einer Lizensierung des Datenzugriffs auf der Grundlage von Digital Rights Management-Systemen auszugehen. Die Daten verbleiben auf dem Server des ursprünglichen Dateninhabers, der den Lizenznehmern technisch eine – gegebenenfalls auf bestimmte Nutzungen beschränkte – Zugriffsmöglichkeit einräumt. Der Datenzugriff wird dabei präzise protokolliert.

In etwas größerem Umfang als bei personenbezogenen Daten findet auch ein Datenhandel über Plattformen statt – also eine stärker standardisierte Form des Datenhandels als Massengeschäft. Allerdings gilt dies vor allem für öffentliche Daten. Auf der Grundlage der PSI-Richtlinie 2003/98/EG (ergänzt durch RL 2013/37/EU) hat sich ein Handel von Daten auf der Basis von öffentlicher Information und insbesondere öffentlicher Sektorinformation entwickelt.[163] Ein Beispiel ist der Handel mit Wetterdaten für Landwirte, verbunden mit Analysemethoden.[164] Weit entwickelt ist auch der Handel mit nicht personenbezogenen Finanzmarktdaten.[165] Ein Beispiel für eine Plattform, die offene Daten aus der öffentlichen Verwaltung anbietet, ist Enigma.[166] Die Plattform hält zusätzlich auch eigene Analyseinstrumente bereit.

Bei nicht personenbezogenen Daten, die im einzelunternehmerischen Umfeld erzeugt werden, nimmt der Plattformhandel gegenwärtig hingegen einen geringen Raum ein. Sehr wohl gibt es Versuche, in bestimmten Sektoren Datenaustausch über eine Plattform zu organisieren, gefolgt von konkreten Transaktionen. Ein Beispiel im Logistikbereich ist das Pooling und die Beförderung von Lademitteln.[167] In diesem Beispiel dienen die Daten allerdings direkt der Erbringung einer Dienstleistung, die über die Plattform vermittelt wird.

Die Gründe dafür, dass der Datenhandel über Plattformen keine größere Rolle spielt, sind vielfältig. Ein als Massengeschäft konzipierter Plattformhandel mit Daten setzt regelmäßig voraus, dass bestimmte Datensätze als mehr oder weniger standardisiertes Produkt gehandelt werden. Welche Daten ein Kunde benötigt, kann aber in vielen Fällen von der genauen Zwecksetzung oder Anwendungsidee abhängen. Auch der Wert, den Datensätze für einen Kunden haben, hängt entscheidend von dem konkreten Verwendungszweck ab. Will der Dateninhaber die Zahlungsbereitschaft des Kunden abschöpfen, so kann dies – sofern überhaupt eine Bereitschaft zur Datenübermittlung besteht – für individuelle bilaterale Verhandlungen sprechen. Für letztere spricht auch, dass sich der Dateninhaber dann der Vertrauenswürdigkeit und Zuverlässigkeit seines Geschäftspartners versichern kann; denn mit der Datenübermittlung riskiert er u.U. den Verlust der Kontrolle über die Daten.

[163] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 13

[164] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 13. Ein Anbieter von Daten und Auswertung ist Weather Analytics (https://www.weatheranalytics.com/).

[165] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 13.

[166] Siehe https://public.enigma.com/. Enigma bietet auch Daten aus Organisationen und Firmen kostenlos zum Download an. Beispielsweise steht Information von Nike zu allen Zulieferbetrieben zur Verfügung.

[167] Siehe https://www.swoplo.com/de.

Zwar kann es gerade eine zentrale Funktionalität von Handelsplattformen sein, eigene Mechanismen zur Gewährleistung der Zuverlässigkeit der Geschäftspartner anzubieten.[168] Es ist sehr wohl denkbar, dass in Zukunft für bestimmte relativ standardisierte Datensätze neue Plattformmärkte entstehen und ein Matching von Datenanbietern und Datensuchenden erleichtern. Zu erwarten ist dies allerdings nur für wenig sensible Datensätze mit typisierbarem Verwendungszweck, nicht aber für diejenigen Daten, die Unternehmen bislang ausschließlich der Eigennutzung und gegebenenfalls dem Data Sharing vorbehalten.

Die Kommission erwartet für die Zukunft gleichwohl ein deutliches Wachstum im Datenhandel[169] und ist bestrebt, diesen aktiv zu fördern. Ein gewisser Schwerpunkt scheint dabei auf der Förderung eines dezentralen Plattformhandels zu liegen. Zwar identifiziert die Kommission kein allgemeines Marktversagen auf Märkten für nicht personenbezogene Daten. Sie geht aber davon aus, dass mögliche Hindernisse für eine Ausweitung des Datenhandels in potentiell (zu) hohen Transaktionskosten und einer fehlenden Standardisierung der Lizenzbedingungen bestehen. Die Kommission sieht ferner die Möglichkeit von Ungleichgewichtslagen im Zugang zu Daten, die einer Regelung bedürfen, damit sich die Möglichkeiten von datenbasierter Innovation voll entfalten können. Als mögliches Mittel zur Bewältigung der genannten Probleme erörtert die EU-Kommission unter anderem die Einführung eines neuen „Eigentumsrechts an Daten“ oder eines neuen „Datenherstellerrechts“ (dazu II.). Die Kommission schlägt ferner Modell-Verträge für Datennutzungsverträge vor (III.).

II. Eigentumsrechte für nicht personenbezogene Daten?

1. Eigentumsrechte an Daten – Grundlagen

Die Theorie der „property rights“ untersucht aus einer ökonomischen Perspektive die Funktion und Zuweisung von Verfügungsrechten in einer Marktwirtschaft. Verfügungsrechte beinhalten individuelle Entscheidungsrechte über den Einsatz von Ressourcen. Das Sacheigentum ist der Prototyp eines umfassenden Verfügungsrechts über knappe Ressourcen: Es umfasst eine Gesamtheit von Rechten („bundle of rights“), namentlich das Recht, „mit der Sache nach Belieben zu verfahren und andere von jeder Einwirkung auszuschließen“ (§ 903 BGB). Bei Sachen, deren Nutzung von vornherein rivalisierend ist, sind klar definierte Verfügungsrechte geboten, um Nutzungskonflikte betreffend den Einsatz knapper Ressourcen zu bewältigen.

Bei Daten verhält sich dies anders. Sie sind nicht rivalisierend im Konsum[170] – eine Eigenschaft, die sie mit den sogenannten öffentlichen Gütern wie Hochwasserschutz und Sicherheit aufgrund nationaler

[168] Systeme wie Industrial Data Space ermöglichen über eine Zertifizierung die Kontrolle der Handelspartner

[169] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 13 unter Hinweis auf IDC, Europe’s Data Marketplaces – Current Status and Future Perspectives, 2016

[170] Häufig können dieselben Daten auch von mehreren Unternehmen gesammelt werden: “*Big data is non-rivalrous. In other words, collecting a particular piece of data does not prevent other companies from collecting identical data by similar or other means*” (*Tucker/Wellford*, Big Mistakes Regarding Big Data, Antitrust Source, American Bar Association, December 2014, S. 3). Hierbei handelt es sich aber nicht um die Eigenschaft der Nicht-Rivalität. So können auch andere private Güter von mehreren Unternehmen produziert werden.

Verteidigung teilen. Während sich öffentliche Güter aber gleichzeitig durch die Nicht-Ausschließbarkeit der Nutzung durch Dritte kennzeichnen, besteht bei Daten die Möglichkeit, Fremdzugriffe durch technische Maßnahmen zu unterbinden. Die Eigenschaften der Nicht-Rivalität im Konsum bei gleichzeitiger faktischer Ausschließbarkeit der Nutzung durch Dritte teilen Daten mit (anderen) immateriellen Gegenständen, etwa mit technischen Innovationen, Akten kreativer Schöpfung oder auch bloßen Ideen.[171] Für Erfindungen und persönlich-geistige Schöpfungen der Literatur, Wissenschaft und Kunst hat der Gesetzgeber mit Patenten und Urheberrechten Immaterialgüterrechte geschaffen, die den Ausschluss Dritter durch absolute Abwehrrechte absichern und damit die Offenlegung zu ermöglichen, ohne dass damit ein Verlust der Kontrolle über das Gut einhergeht. Könnte der Erfinder oder Werkurheber seine Schöpfung nur durch Geheimhaltung seiner ausschließlichen Kontrolle unterwerfen, wäre eine Teilhabe der Gesellschaft an kreativen Schöpfungen und technischen Innovationen beeinträchtigt; die deutlich schwierigere Kommerzialisierung derartiger Immaterialgüter würde zugleich Investitionen in deren Schöpfung unrentabel werden lassen. Die Schaffung von Immaterialgüterrechten schützt die Anreize zur Investition.[172]

Die klare Definition und exklusive Zuweisung von „property rights“ ex ante kann außerdem dazu beitragen, Transaktionskosten abzusenken und damit einen Austausch von Ressourcen über den Markt zu erleichtern.[173] Fehlt es an klar definierten Verfügungsrechten an einer Ressource, so entscheidet über die wirtschaftliche Nutzungsmöglichkeit im Zweifel der faktische Zugriff, verbunden mit der Möglichkeit zum Ausschluss Dritter. Will der Inhaber der Verfügungsmacht Dritten Zugriff gewähren, so müssen Rechte und Pflichten im Einzelnen vertraglich geregelt werden. Verträge sind aber typischerweise unvollständig: Die Vertragsparteien sind nicht in der Lage, sämtliche Eventualitäten vorauszudenken. Ohne klare ex ante-Definition der Verfügungsrechte kann es an einer Zuweisung der residualen Entscheidungsrechte fehlen.[174]

Ferner gelten Verträge nur im Verhältnis zwischen den Vertragsparteien. Gelangt die Ressource in den Zugriff Dritter, mit denen kein Vertragsverhältnis besteht, so genießt der ursprüngliche Kontrollinhaber ohne ein Verfügungsrecht unter Umständen keinen rechtlichen Schutz. Das kann den Inhaber der nur faktischen Kontrolle über eine Ressource zu besonderer Vorsicht in der Einräumung von Zugriffsrechten oder zu besonderen – womöglich teuren – Schutzmaßnahmen verleiten.

---

[171] Anders ein nicht unerheblicher Teil der immaterialgüterrechtlichen Literatur, der Immaterialgüter als nicht-exklusiv und damit im Ergebnis als öffentliche Güter einordnet, vgl. statt vieler *Bechtold,* GRUR Int. 2008, 484, 485. Für den Bereich technischer Innovationen muss dieser Befund ganz grundsätzlichen Bedenken begegnen, stellt dort die Geheimhaltung, insbesondere für Innovationen im Umfeld der eigenen Produktionsprozesse des Erfinders, oft eine praktikable und gegenüber dem Patentschutz vorteilhafte Option dar; vgl. zu alternativen Schutzmechanismen und deren Bedeutung gegenüber einem Patentschutz *Rammer,* Patente und Marken als Schutzmechanismen für Innovation, 2003. Im Bereich des Urheberrechts ermöglichen neue Wege des digitalen Vertriebs – über Digital Rights Management (DRM) oder andere technische Absicherungen – ebenfalls (grundsätzlich) eine faktische Exklusivität, vgl. *Hilty,* in: Ohly/Klippel (Hrsg.), Geistiges Eigentum und Gemeinfreiheit, 2007, S. 109 f.

[172] Zu dieser „Anspornungstheorie“ und weiteren Begründungsansätzen für ein Patentrecht grundlegend *Machlup,* GRUR Int. 1961, 373, 376 f.; ferner *Kerber,* GRUR Int. 2016, 989, 992 ff.

[173] *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 5: “Economists are generally inclined to think that well-specified property rights reduce transaction costs and uncertainty and thereby increase the efficiency of markets.”

[174] Hierzu allgemein *Grossman/Hart,* Journal of Political Economy 94, 1986, S. 691 ff.

Trotzdem begründet das Recht „property rights“ an Immaterialgütern nur selektiv. Die Gewährung eines Ausschließlichkeitsrechts erlaubt die Monopolisierung des geschützten Immaterialgutes. Diese Einschränkung des statischen (Imitations-)Wettbewerbs führt zu Wohlfahrtsverlusten; ebenso kann die Einschränkung von technischen Folgeentwicklungen oder von „Weiterentwicklungen“ eines urheberrechtlich geschützten Werkes (sog. „downstream developments“) den dynamischen Wettbewerb beschränken.[175] Der Gesetzgeber wägt diese ökonomischen Nachteile (beziehungsweise die Vorteile der Gemeinfreiheit) mit den soeben beschriebenen Vorteilen der Gewährleistung eines Immaterialgüterrechts ab: die Innovations- und Investitionsanreize können den dynamischen Wettbewerb fördern, der Handel mit Immaterialgütern kann durch die Absenkung von Transaktionskosten vereinfacht werden. Um ein möglichst optimales Gleichgewicht zu schaffen, werden Immaterialgüterrechte gewährt, aber zugleich wieder begrenzt – etwa durch eine enge Definition des Schutzgegenstandes, eine zeitlich begrenzte Dauer oder Schrankenbestimmungen.

Bestehen auch in einem System der Gemeinfreiheit ausreichende Innovations- und Investitionsanreize[176] und tragen Immaterialgüterrechte auch nicht zur Absenkung von Transaktionskosten bei, stehen der durch das Immaterialgüterrecht begründeten Einschränkung des Wettbewerbs keine Vorteile gegenüber. Sofern keine klaren ex ante-Erkenntnisse über die effiziente Allokation residualer Entscheidungsrechte existieren,[177] kann die Schaffung von Eigentumsrechten sogar eine Fehlallokation begründen, deren dann erforderliche vertragliche Korrektur mit ebenso hohen oder sogar höheren Transaktionskosten verbunden wäre wie in einem System der de facto-Ausschließbarkeit der Fremdnutzung und einer vertraglichen Zuweisung von Entscheidungsrechten.

Im Folgenden ist deshalb zu klären, ob unter Berücksichtigung des bestehenden Rechtsrahmens (2.) ein Anreizdefizit hinsichtlich der Erzeugung von Daten besteht und ob eine ex ante-Allokation der Verfügungsrechte an Daten Transaktionskosten senken kann (3.). Ist das nicht der Fall, dominieren die ökonomischen Vorteile der Gemeinfreiheit.

2. Rechte an Daten nach geltendem Recht

Das geltende Recht kennt kein eigenständiges Eigentumsrecht an Daten (a)). Auch das Sacheigentum an den Speichermedien ist kein funktionaler Ersatz für ein Schutzrecht an den Daten selbst (b)). Es existieren jedoch verschiedene datenbezogene Schutzrechte, die bestimmte absolute Abwehrrechte gegen eine Vielzahl an möglichen Eingriffshandlungen begründen, funktional aber nicht mit einem voll entwickelten Verfügungsrecht über Daten vergleichbar sind (c)). An die Stelle eines solchen voll entwickelten Verfügungsrechts tritt derzeit eine vertragliche und technische Absicherung durch den (faktischen) Dateninhaber (d)).

[175] Der Grund liegt darin, dass die Folgeentwicklung auf die Nutzung der ursprünglichen Literatur angewiesen ist. Die ökonomische Literatur zu kumulativer Innovation beschäftigt sich mit dieser Problematik; vgl. *Scotchmer*, Innovation and Incentives, 2004, S. 127 ff. und *Belleflamme/Peitz*, Industrial Organization: Markets and Strategies, 2. Aufl., 2015, S. 548 ff. Das Grundproblem wurde bereits von *Cournot*, Recherches sur les Principes Mathematique de la Theorie des Richesses, 1838, als Preistheorie bei Komplementärgütern beschrieben und hat insbesondere in der juristischen Literatur als „Tragedy of the Anti-Commons“ große Aufmerksamkeit gefunden, vgl. beispielsweise *Heller/Eisenberg,* Science 1998, S. 698.

[176] Für den Bereich des Patentschutzes gibt es einige Autoren im ökonomischen Schrifttum, die die Anreiztheorie kritisch hinterfragen; vgl. etwa *Boldrin/Levine,* Against Intellectual Monopoly, 2008.

[177] Einige Schwierigkeiten hierbei zeigen *Duch-Brown/Martens/Müller-Langer,* The economics of ownership, access and trade in digital data, 2017, S. 29 ff. auf.

a) Kein eigenständiges Eigentumsrecht an Daten

Bislang kennt keine der europäischen Rechtsordnungen ein eigenständiges, voll ausgeprägtes Eigentums- beziehungsweise Immaterialgüterrecht an Daten,[178] also an *maschinenlesbar codierter Information*.[179] Der Begriff der Information ist mit terminologischen Unklarheiten behaftet; Informationen können auf einer semantischen, syntaktischen oder strukturellen Ebene voneinander abgegrenzt werden.[180] Da ein Eigentums- beziehungsweise Immaterialgüterrecht an Daten – unabhängig davon, auf welcher dieser Informationsebenen man sie abgegrenzt – nicht besteht, kann diese Differenzierung vorerst noch dahinstehen. Auf sie wird jedoch später (unter 3.) noch zurückzukommen sein.

b) Daten- und Sacheigentum

Das Sacheigentum an den Speichermedien, auf denen Daten verkörpert sind, ist kein funktionaler Ersatz für ein Schutzrecht an den Daten selbst.

Zwar stehen dem Sacheigentümer Abwehr- und Beseitigungsansprüche (§ 1004 BGB) sowie ein (verschuldensabhängiger) deliktischer Schadensersatzanspruch (§ 823 Abs. 1 BGB) bei jeglichen Formen der Datenveränderung zu – das Überschreiben oder Löschen von Daten stellt stets eine Modifikation der Struktur des Datenträgers dar und greift dadurch in die Sachsubstanz ein.[181] Bei bloßen unbefugten Lesezugriffen auf das Speichermedium ist ein Eingriff in das Eigentum jedoch deutlich schwieriger zu konstruieren. Die Kenntnisnahme, Vervielfältigung und Nutzung der Daten *an sich* stellt keinen Eingriff in vom Sacheigentum umfasste Rechtspositionen dar – das Sacheigentum und ein in der Sache verkörpertes Immaterialgut sind strikt zu trennen.[182] Sofern ein Lesezugriff auf das Speichermedium das Anlegen elektrischer Spannungen voraussetzt oder sogar – wie bei Festplattenspeichern – mechanische Komponenten in Bewegung setzt, die dem Verschleiß unterliegen, kann dem Eigentümer gegen die darin liegende unbefugte (Ab-)Nutzung seiner Sache ein Unterlassungsanspruch (§ 1004 BGB) zustehen.[183] Ein Abwehrrecht gegen die Nutzung oder Weitergabe der auf diesem Weg erlangten Daten folgt hieraus aber nicht.

[178] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 19 m.w.N.
[179] *Zech,* Information als Schutzgegenstand, S. 39.
[180] *Zech,* a.a.O., S. 35 ff.
[181] Vgl. *Spindler,* NJW 2004, 3145, 3146; *ders.,* in: BeckOGK, Stand 1.5.17, § 823 BGB Rn. 135.
[182] Für das Urheberrecht grundlegend BGH, Urt. v. 13.10.1965 – Ib ZR 111/63, GRUR 1966, 503 („Apfel-Madonna"). Diesen Grundsatz durchbrechend BGH, Urt. v. 20.9.1974 – I ZR 99/73, NJW 1975, 778 („Schloss Tegel") und Urt. v. 17.12.2010 – V ZR 45/10, NJW 2011, 749: das Grundstückseigentum vermittele ein Abwehrrecht gegenüber der Anfertigung von Fotografien von auf dem Grundstück belegenen Gebäuden oder beweglichen Sachen, sofern das Grundstück hierfür betreten werden muss und die Aufnahmen kommerziell verwertet werden sollen. Diese Rechtsprechungslinie begegnet starker Kritik aus dem Schrifttum, vgl. die Nachweise bei *Spohnheimer,* in: BeckOGK, Stand 1.5.17, § 1004 BGB Rn. 134.1. Da der BGH diese Rechtsprechung auf die soeben beschriebenen, engen Sachverhaltskonstellationen beschränkt, ist ihnen kein verallgemeinerungsfähiges Prinzip dahingehend zu entnehmen, das Sacheigentum schütze vor der Kenntnisnahme oder Vervielfältigung der in der Sache verkörperten Informationen.
[183] Auch ein deliktischer Schadensersatzanspruch aus § 823 Abs. 1 BGB ist denkbar – hinsichtlich des Schadens, der aufgrund der Kenntnisnahme, Vervielfältigung oder Nutzung der Daten entsteht, dürfte es allerdings an der haftungsausfüllenden Kausalität zur Rechtsgutsverletzung (Abnutzung der Sache!) fehlen.

Ferner versagt das Sacheigentum am Datenträger bei der Erfassung von Daten während eines Übermittlungsvorgangs.[184] Es kann Daten nicht mehr erfassen, sobald diese (mit Einwilligung des Eigentümers) auf ein fremdes Speichermedium kopiert wurden. Und schließlich liegt mit Blick auf die verbreiteten Phänomene Hardware-Leasing und Cloud-Computing das Sacheigentum häufig auch gar nicht bei der Person, „deren" Daten auf dem Speichermedium abgelegt sind.[185]

c) Sachlich begrenzte Schutzrechte an Daten

Im geltenden Recht fest verankerte datenbezogene Schutzrechte sind der Datenbankschutz (aa)) und der Schutz von Geschäftsgeheimnissen (bb)). Daneben bestehen strafrechtliche Schutzgesetze gegen bestimmte datenbezogene Handlungen, deren Verletzung über § 823 Abs. 2 BGB i.V.m. § 1004 BGB analog zivilrechtliche Ansprüche auslösen kann (cc)). Auch diese Schutzrechte sind aber funktional nicht mit einem voll entwickelten Verfügungsrecht an maschinengenerierten Rohdaten vergleichbar.

aa) Datenbankenschutz – Datenbank-Richtlinie 96/9/EG, §§ 87a ff. UrhG

Mit der Verabschiedung der Datenbank-Richtlinie 96/6/EG[186] wollte der europäische Gesetzgeber einen Anreiz für europäische Unternehmen schaffen, mehr in den Aufbau elektronischer Datenbanken zu investieren und damit im Wettbewerb zu amerikanischen Unternehmen aufzuholen.[187] Die Richtlinie wurde mit den §§ 87a ff. UrhG in nationales Recht umgesetzt. Sie schafft zwei Schutzrechte:

(1) Die Struktur von Datenbanken (nicht aber ihr Inhalt, Art. 3 Abs. 2 Datenbank-RL[188]) genießt vollen urheberrechtlichen Schutz, wenn sie Ausdruck einer kreativen menschlichen Schöpfung oberhalb einer gewissen (allerdings nicht näher definierten) Originalitätsschwelle ist. Ein Schutz für maschinengenerierte Daten, wie sie hier im Vordergrund stehen, folgt daraus nicht: Zwar fließt substantielle schöpferische Leistung in die Hard- und Software, mit der diese Daten generiert werden. Die Datensätze selbst werden aber automatisch erzeugt und sind für sich genommen keine schöpferische Leistung.

(2) Die Datenbank-Richtlinie will Investitionen in den Aufbau von Datenbanken, namentlich in die Beschaffung, Überprüfung oder Darstellung des Inhalts, aber auch dann schützen, wenn die Struktur der Datenbank unterhalb der urheberrechtlichen Originalitätsschwelle liegt. Unter der Voraussetzung, dass erhebliche Investitionen in diesem Sinne geflossen sind, wird dem Hersteller einer Datenbank auf 15 Jahre beschränkt das Recht eingeräumt, die Entnahme und/oder Wiederverwendung der Gesamtheit oder eines qualitativ oder quantitativ wesentlichen Teils des Inhalts der Datenbank zu

[184] Ebenso *Faustmann,* VuR 2006, 260, 263.
[185] Ebenso *Spindler,* in: BeckOGK, Stand 1.5.17, § 823 BGB Rn. 136
[186] Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABl. L 77/20.
[187] In diesem Sinne: *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 13. Allerdings hat die Datenbank-Richtlinie auch nach der eigenen Einschätzung der Kommission ihr industriepolitisches Ziel nicht erfüllt: Siehe die Evaluierung der Datenbank-Richtlinie durch die EU-Kommission aus dem Jahr 2005. Danach gibt es keinen Hinweis darauf, dass die Datenbank-Richtlinie die Investitionen in Datenbanken wesentlich beeinflusst hat.
[188] EuGH, Urt. v. 1.3.2012, Rs. C-604/10, ECLI:EU:C:2012:115 – Football Dataco, Rn. 30.

unterbinden (Art. 7 Abs. 1, 2 Datenbank-RL; siehe auch Art. 7 Abs. 5 Datenbank-RL; §§ 87b Abs. 1, 87d UrhG).

Auch aus diesem Recht folgt kein genuines „Recht an Daten“.[189] Die Entnahme oder Wiederverwendung einzelner Daten(sätze) kann durch das *sui generis*-Recht nur in (kaum vorstellbaren) Fällen unterbunden werden, in denen das einzelne Datum bereits ein wesentlicher Teil des Inhalts der Datenbank darstellt. Der Investitionsaufwand für die Erzeugung oder Beschaffung des Datums sowie dessen wirtschaftlicher Wert ist bei der Beurteilung dieses Wesentlichkeitskriteriums nicht von Belang.[190]

Aber auch der Schutz größerer Datensätze, die einen wesentlichen Teil einer Datenbank bilden, ist durch die Datenbank-RL aufgrund der restriktiven Auslegung durch den EuGH nur sehr eingeschränkt gewährleistet.

Erstens hat der EuGH in seinem Urteil „British Horseracing“ (2004)[191] den Anwendungsbereich des „sui-generis“-Rechts auf Datenbanken begrenzt, in deren Zusammenstellung und Struktur erhebliche Investitionen geflossen sind.[192] Investitionen in die Erzeugung der in der Datenbank organisierten Daten sollen durch die Datenbank-RL nicht geschützt werden.[193] Bei maschinengenerierten Daten wird jedoch ganz regelmäßig der Schwerpunkt der Investition in der Herstellung von Hard- und Software zur Erzeugung der Daten fließen, nicht in deren Zusammenfassung innerhalb eines Datensatzes.[194] Die Datenbank-RL erfasst somit die hier erörterten Sachverhalte nicht, wie sie aus der neuen wirtschaftlichen Bedeutung maschinengenerierter Daten folgen.[195]

Zweitens gewährt das „sui-generis“-Recht nur Abwehrrechte gegenüber solchen Handlungen, die geeignet sind, dem Datenbankhersteller „Einkünfte zu entziehen, die es [ihm] ermöglichen sollen, die Kosten [der] Investition zu amortisieren.“[196] Umfasst sind also nur solche Handlungen, die das Geschäftsmodell des Datenbankherstellers unterlaufen.[197]

bb) Schutz von Geschäftsgeheimnissen – Richtlinie 2016/943

---

[189] Der „sui generis“-Schutz von Datenbanken entfaltet keinen Schutz hinsichtlich der einzelnen Datenbankelemente: EuGH, Urt. v. 9.11.2004, Rs. C-203/02, ECLI:EU:C:2004:695 – British Horseracing Board, Rn. 72.

[190] EuGH, Urt. v. 9.11.2004, Rs. C-203/02, ECLI:EU:C:2004:695 – British Horseracing Board, Rn. 71 f., 78.

[191] EuGH, Urt. v. 9.11.2004, Rs. C-203/02, ECLI:EU:C:2004:695 – British Horseracing Board.

[192] EuGH, a.a.O., Rn. 30 ff.

[193] EuGH, a.a.O., Rn. 31.

[194] *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 13 f.: „The investment has to refer to resources used to make databases and seek out existing materials, not to resources used for the creation of data. That would rule out protection of data collected through sensors – essentially all electronic digital data.“

[195] Siehe auch *Drexl*, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, S. 22,: „It is quite obvious that the Database Directive is based on database technology that no longer corresponds to the use of data in an era of the Internet of Things. In particular, by protecting a collection of materials for a given period of time […], the concept of a database is much to static to adequately respond to the features of [...] real-time data services”.

[196] EuGH, Urt. v. 9.11.2004, Rs. C-203/02, ECLI:EU:C:2004:695 – British Horseracing Board, Rn. 51.

[197] Ähnlich *Thum/Hermes,* in: Wandtke/Bullinger, Praxiskommentar zum Urheberrecht, 4. Aufl. 2014, § 87b Rn. 26 f.

Automatisiert erzeugte Daten oder Datensätze können außerdem als Geschäftsgeheimnisse geschützt sein. Auf europäischer Ebene ist der Schutz von Geschäftsgeheimnissen durch die Richtlinie (EU) 2016/943[198] neu gefasst worden. Eine Umsetzung in nationales Recht steht derzeit noch aus, auch ein Gesetzesentwurf lag bei Fertigstellung dieser Studie noch nicht vor.[199] Die Umsetzungsfrist endet am 9.6.2018.[200]

Als Geschäftsgeheimnis geschützt ist jede Information, die geheim ist, gerade deshalb einen kommerziellem Wert besitzt und angemessenen Geheimhaltungsmaßnahmen unterworfen wird (Art. 2 Nr. 1 Geschäftsgeheimnis-RL). Als „geheim" erachtet die Richtlinie hierbei alle Informationen, die „weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich sind" (Art. 2 Nr. 1 lit. a) Geschäftsgeheimnis-RL). Art. 4 Geschäftsgeheimnis-RL gewährt dem Geheimnisinhaber Abwehrrechte gegen den rechtswidrigen Erwerb, die rechtswidrige Nutzung sowie die rechtswidrige Offenlegung eines Geschäftsgeheimnisses.

Einer Vielzahl maschinengenerierter Daten dürfte bereits die Eigenschaft als Geheimnis im Sinne der Richtlinie fehlen; das betrifft insbesondere Sensordaten über Umwelteigenschaften, die ohne Weiteres von Dritten durch eigene Messungen reproduziert werden könnten. Die Geschäftsgeheimnis-Richtlinie definiert ihren Schutzgegenstand (das Geschäftsgeheimnis) auf einer semantischen Ebene (hierzu siehe unten) – geschützt wird die Information selbst, nicht deren konkrete Verkörperung. Erhebt ein Unternehmen bspw. Daten über die Beschaffenheit öffentlicher Straßen, so können diese mangels Geheimheit keinen Geschäftsgeheimnisschutz genießen: die in diesen Daten codierte semantische Information – etwa das Vorhandensein eines Schlaglochs – ist für jedermann ohne weiteres zugänglich.[201]

Den Charakter eines Geschäftsgeheimnisses können jedoch – etwa im Kontext von Industrie 4.0 oder des Internet of Things (IoT) – solche maschinengenerierten Daten haben, die sich unmittelbar auf den Produktionsprozess und dessen Steuerung beziehen.

Hinsichtlich maschinengenerierter Daten, in denen geheime Informationen codiert wurden, kann unklar sein, ob diese für sich genommen einen kommerziellen Wert haben und ob der kommerzielle Wert kausal auf der Geheimhaltung beruht. Einzelnen Daten wird für sich genommen häufig ein relevanter wirtschaftlicher Wert fehlen.[202] An dem wirtschaftlichen Wert größerer Datensätze allerdings kann demgegenüber kein Zweifel bestehen. Werden vom Inhaber der faktischen

[198] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157/1.

[199] Der Entwurf eines Umsetzungsgesetzes befindet sich nach Angaben der Bundesregierung in Erarbeitung, vgl. BT-Drs. 18/13079, S. 6f.

[200] Art. 19 Geschäftsgeheimnis-RL; zu etwaigen Vorwirkungen der Richtlinie auf das nationale Recht, insb. §§ 17–19 UWG, *Harte-Bavendamm,* in: Harte-Bavendamm/Henning-Bodewig, 4. Aufl. 2016, Vorb. §§ 17-19 UWG, Rn. 10a.

[201] Ebenso *Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblytė/Wiedemann*, GRUR Int. 2016, 914, 916.

[202] *Drexl*, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, S. 22.

Verfügungsmacht über die Daten die von der Richtlinie geforderten Schutzmaßnahmen getroffen, so liegt danach ein Geschäftsgeheimnis vor.[203]

Eine erhebliche Schwierigkeit des rechtlichen Schutzes von Geschäftsgeheimnissen liegt in der Praxis allerdings in dem Umstand begründet, dass der Geheimnisinhaber im Rahmen eines Rechtsstreits mit der Offenlegung des Geschäftsgeheimnisses und damit mit dessen Verlust rechnen muss.[204]

cc) Strafrechtlicher Schutz

Strafrechtliche Regelungen begründen einen umfangreichen Schutz des Dateninhabers gegenüber vorsätzlichen Schädigungshandlungen.[205] Die §§ 202a – 202c StGB stellen das vorsätzliche Ausspähen und Abfangen von Daten sowie verschiedene Vorbereitungshandlungen unter Strafe. Diesen Tatbeständen ist gemein, dass sie ein gewisses Maß an Geheimheit und/oder technischer Sicherung der Daten voraussetzen: § 202a StGB erfordert die Überwindung einer Sicherung gegen unberechtigten Zugang,[206] § 202b StGB eine „nichtöffentliche Datenübermittlung". § 303a StGB stellt das vorsätzliche, rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern unter Strafe; auf eine Geheimheit oder besondere Sicherung der Daten kommt es nicht an.

Alle soeben bezeichneten Straftatbestände stellen Schutzgesetze im Rahmen von § 823 Abs. 2 BGB dar;[207] ihre Verletzung löst einen deliktischen Schadensersatzanspruch aus. Anspruchsinhaber ist diejenige Person, deren Schutz das Schutzgesetz intendiert. Sowohl §§ 202a ff. StGB[208] als auch § 303a StGB[209] schützen denjenigen, der die „Verfügungsmacht" an den Daten innehält. Regelmäßig ist das der Speichernde oder, bei einer Datenverarbeitung in fremdem Auftrag, der Auftraggeber dieser Datenverarbeitung.[210]

Dieser deliktische Schutz löst daneben einen quasinegatorischen Unterlassungs- und Beseitigungsanspruch gemäß §§ 823 Abs. 2, 1004 analog BGB aus.[211]

Der faktische „Datenbesitz" wird über diesen Weg nahezu umfassend zivilrechtlich geschützt: der „Datenbesitzer" verfügt über Unterlassungs- und Beseitigungsansprüche gegen das vorsätzliche Ausspähen, Abfangen und Verändern von Daten sowie über deliktische Schadensersatzansprüche

[203] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 20.
[204] Siehe z.B. *Lejeune*, CR 2016, 330, 341 f.
[205] *Zech*, C&R 2015, 137, 143: „echte Pionierfunktion" des Strafrechts beim Schutz von Daten.
[206] Eine solche Sicherung "muss den Zweck haben, den Zugang Unbefugter zu den geschützten Daten zu verhindern oder zumindest erheblich zu erschweren."; ausreichende Sicherungen stellen neben physischer Maßnahmen (Aufbewahrung in verschlossenen Behältnissen) auch Software-Sicherungen wie Passwörter, Firewalls, selektive Lese- und Schreibberechtigungen oder eine Verschlüsselung der Daten dar: *Graf*, in: MüKo-StGB, 2. Aufl. 2012, § 202a StGB Rn. 35 ff. m.w.N.
[207] *Spindler,* in: BeckOGK, Stand 1.5.17, § 823 BGB Rn. 283, 284.
[208] *Weidemann,* in: BeckOK StGB, 34. Ed., § 202a StGB Rn. 7; § 202b StGB Rn. 4.
[209] *Wieck-Noodt,* in: MüKo-StGB, 2. Aufl. 2014, § 303a StGB Rn. 9.
[210] Str., wie hier *Lenckner/Eisele,* in: Schönke/Schröder, 29. Aufl. 2014, § 202a StGB Rn. 9. Vgl. ferner *Hoeren,* MMR 2013, 486.
[211] Hierzu allgemein *Spohnheimer,* in: BeckOGK, Stand 1.5.17, § 1004 BGB Rn. 13, 13.1.

gegen den Täter. Die Pflicht zur Beseitigung der Beeinträchtigung analog § 1004 BGB dürfte dabei auch die Pflicht umfassen, die erlangten Daten herauszugeben oder zu vernichten.[212]

Die Rechte, die dem „Datenbesitzer" hiernach zugewiesen werden, begründen eine dem possessorischen Besitzschutz nicht unähnliche Rechtsmacht – trotz der offenkundigen Unterschiede.[213] Mit einem vollwertigen Dateneigentumsrecht sind sie damit zwar ebenfalls nicht vergleichbar; indem sie eine rechtliche Handhabe bieten, Datenzugriffe und -nutzungen außerhalb von Transaktionen zu unterbinden, erfüllen sie jedoch eine zentrale Rolle in der Absicherung eines auf vertraglichen Abreden basierenden Systems des „Private Ordering" (hierzu siehe unten).

d) Vertraglicher und technischer Schutz von Datensätzen

In Ermangelung eines vollwertigen „Rechts an Daten" ist der Ausgangspunkt des Handels mit Daten der faktische Besitz beziehungsweise die faktische Verfügungsmacht über Daten, verbunden mit einer Zugangsgewährung unter bilateral ausgehandelten, vertraglich vereinbarten Konditionen.[214] Der Inhaber der faktischen Kontrolle über die Daten – im Verhältnis eines Maschinenherstellers zu einem Eigentümer der Maschine kann dies z.B. der Maschinenhersteller sein[215] – handelt mit seinen Vertragspartnern vertraglich deren Zugriffsrechte aus und sichert sie nach Möglichkeit über ein digitales Zugriffsmanagement technisch ab.

3. Eigentumsrechte an Daten de lege ferenda: Brauchen wir ein neues „Recht an Daten"?

Fraglich ist, ob vor dem Hintergrund dieser Rechtslage zur Verbesserung der Funktionsfähigkeit von Datenmärkten die Einführung eines neuen „Eigentumsrechts an Daten" rechtspolitisch opportun ist.[216] Einleitend (siehe oben, unter 1.) wurden bereits die potentiellen ökonomischen Vor- und Nachteile aus der Schaffung von Immaterialgüterrechten skizziert: der möglichen Schaffung von Innovations-, Investitions- und Offenbarungsanreizen sowie der potenziellen Senkung von Transaktionskosten stehen die Vorteile der Gemeinfreiheit, namentlich die ungehinderte Möglichkeit zur Nutzung der Daten als innovationstreibende Ressource und die darin liegende Förderung von Datenanalyseprozessen, gegenüber.

Es ist also zu fragen, ob die gegenwärtige Rechtslage, die von einem rein faktischen Datenbesitz ausgeht, unzulängliche Anreize zur Sammlung, Nutzung und Weitergabe von Daten schafft oder gar die Sammlung, Nutzung und Weitergabe von Daten behindert (a); oder ob durch die Schaffung von

[212] *Hoeren,* MMR 2013, 486, 491.

[213] Insbesondere richten sich possessorische Besitzschutzansprüche nicht nur gegen vorsätzliche Besitzstörungen!

[214] So auch die Bilanz von *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 5.: „De facto ownership seems to dominate the data economy."

[215] Mitteilung der EU-Kommission „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 11 f.

[216] Tendenziell für die Schaffung eines neuen Datenrechts: *Wiebe*, GRUR Int. 2016, 877; dagegen: *Kerber*, GRUR Int. 2016, 989; *Drexl*, Designing Competitive Markets for Industrial Data - Between Propertisation and Access; *ders.*, NZKart, 2017, 339; *Drexl/Hilty/Desaunettes* u.a., GRUR Int. 2016, 914. Zu alledem: *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 18 f.

Eigentumsrechten an Daten jedenfalls die Transaktionskosten im Datenhandel deutlich gesenkt werden könnten (b).

Unter den Juristen, die ein Eigentumsrecht im Grundsatz begrüßen, ist wiederum umstritten, wie ein solches Verfügungsrecht im Detail ausgestaltet werden sollte.[217] Bereits über ganz grundlegende Fragen wie die Definition des Schutzgegenstands eines solchen Rechts herrscht Unklarheit – insbesondere hinsichtlich der Frage, ob der Schutzgegenstand „Datum" auf einer semantischen oder syntaktischen Informationsebene abgegrenzt werden soll (siehe oben, 1.).

Diese Weichenstellung beeinflusst den Schutzumfangs eines (zu schaffenden) Eigentumsrechts substantiell: Ein Eigentumsrecht an Daten, dessen Gegenstand anhand des semantischen Informationsgehalts der Daten abgegrenzt wird, würde es erlauben, Dritte von der Nutzung sämtlicher Daten auszuschließen, die ebenfalls diese semantische Information enthalten; das Recht erlaubte hierdurch eine Monopolisierung von Wissen,[218] die – vor allem bei öffentlich zugänglichen semantischen Informationen – eine erhebliche Einschränkung der Informationsfreiheit (Art. 5 Abs. 1 S. 1 Var. 2 GG) darstellte. Dennoch ist unserer Rechtsordnung ein solcher Schutz semantischer Information nicht fremd: sowohl das Datenschutzrecht als auch der Schutz von Geschäftsgeheimnissen (s.o.) begründet absolute Abwehrrechte in Bezug auf bestimmte semantische Informationen, nicht nur hinsichtlich deren konkreter syntaktischer Codierung.[219] Ein Eigentumsrecht an Daten, dessen Gegenstand anhand der syntaktischen Information abgegrenzt wird, hätte demgegenüber einen begrenzteren Schutzumfang. Es würde dem Eigentümer insbesondere keinen Abwehranspruch dagegen einräumen, dass Dritte, die durch die Kenntnisnahme und anschließende Interpretation der Daten deren semantische Information extrahieren konnten, diese durch neuerliche Codierung („aus dem Gedächtnis heraus") reproduzieren oder sich das angeeignete Wissen anderweitig zu Nutze machen.

In der rechtspolitischen Debatte werden beide Abgrenzungsarten vorgeschlagen, oft ohne eindeutige Klarstellung oder präzise Bezeichnung, welcher Ansatz präferiert wird.[220]

Die Mehrzahl der Begründungsansätze für ein Dateneigentums- beziehungsweise -Immaterialgüterrecht können gleichermaßen hinsichtlich beider Arten von Dateneigentumsrechten untersucht werden. Wo dies im Folgenden nicht der Fall ist, wird differenziert.

a) Eigentumsrechte an Daten zur Stärkung der Anreize, Daten zu erzeugen?

Eine zentrale Funktion von Immaterialgüterrechten aus ökonomischer Sicht ist die Stärkung von Investitionsanreizen durch Einräumung eines – nach Umfang und Dauer begrenzten – ausschließlichen Nutzungs- und Verwertungsrechts, um einer Unterversorgung mit dem geschützten immateriellen Gut vorzubeugen (aa)).[221] Neben diesem Anreiz für die *Schaffung* eines Immaterialguts können

[217] Für eine Übersicht verschiedener Ausgestaltungsvorschläge m.w.N. vgl. *Kerber*, GRUR Int. 2016, 989, 991.
[218] Ähnlich *Kerber,* GRUR Int. 2016, 989, 992.
[219] Ebenso *Drexl*, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, S. 13; für das Datenschutzrecht *Zech*, C&R 2015, 137, 138.
[220] Zur Schwierigkeit dieser Abgrenzung *Drexl,* Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, S. 12 ff.; *Kerber,* GRUR Int. 2016, 989, 991 f.
[221] Vgl. beispielsweise *Belleflamme/Peitz*, Industrial Organization: Markets and Strategies, 2. Aufl., 2015, S. 532 ff. oder, auf Deutsch, *Müller-Langer/Scheufen,* WiSt 2011, 137, 137 f.

Immaterialgüter auch gezielt Anreize zur *Offenlegung* geheim gehaltener Informationen schaffen (bb)).[222]

aa) Erfordernis von Investitionsanreizen für die Datenerzeugung

Gibt es ein Defizit an Investitionen in die Erzeugung von Daten?

Daten sind der „Rohstoff" der Digitalisierung; ihre Analyse in Big Data- und sonstigen Data Analytics-Anwendungen verspricht Effizienzgewinne in vielen Wirtschaftsbereichen und trägt zur Schaffung von Produkt- und Prozessinnovationen bei. Zur Erzeugung von Daten sind Investitionen erforderlich; könnten die aus diesen Investitionen gewonnen Daten von jedem ungehindert genutzt werden, käme dem Datenerzeuger kein Wettbewerbsvorsprung zuteil, aus dem er seine Investition refinanzieren könnte. Nach der „Public Goods"-Theorie, die die Nichtexklusivität von immateriellen Gütern voraussetzt, bestünde daher kein Anreiz für private Investitionen in die Erzeugung von Daten. Die Konsequenz wäre eine Unterversorgung mit Daten, eine suboptimale Realisierung der Effizienzgewinne durch Data Analytics-Anwendungen und ein daraus folgender Wohlfahrtsverlust.

Eine solche Unterversorgung mit Daten ist jedoch bislang nicht festgestellt.[223] Zwar fehlen wissenschaftliche Erkenntnisse über das Wohlfahrtsoptimum an Datenerzeugung. Es existieren jedoch keine belastbaren Hinweise, die auf eine Unterproduktion an Daten hinweisen.

Das augenscheinliche Fehlen eines Anreizdefizits mag zum einen daran liegen, dass Daten ohnehin in großer Menge als kostenloses „Nebenprodukt" bestehender Produktionsprozesse abfallen.[224] Zum anderen stehen Datenerzeugern technische und vertragliche Instrumente zur Verfügung, um sich die faktische Zugriffshoheit auf ihre Daten zu erhalten und hierdurch ein Trittbrettfahrerverhalten („free riding") durch Dritte auszuschließen. Die Prämisse der „Public Goods"-Theorie – Nichtexklusivität in der Nutzung – wird hierdurch eingeschränkt, wenn nicht gar aufgehoben.

Das gilt nicht nur dann, wenn der Datenerzeuger die Daten ausschließlich selbst nutzen will. Bei Einsatz technischer Schutzmaßnahmen („Digital Rights Management", DRM) ist auch ein Data Sharing oder Datenhandel unter vertraglicher Einräumung begrenzter Zugriffsrechte auf die auf dem Server des Datenerzeugers verbleibenden Daten möglich.[225] Ein rechtlicher Schutz vor Free Riding wird damit entbehrlich.

Der vertragliche Schutz der Interessen des Datenerzeugers weist allerdings konzeptionell eine Schwäche gegenüber einem „Dateneigentumsrecht" auf: die vertraglichen Vereinbarungen entfalten Wirkungen nur zwischen den Vertragsparteien; gelangen Dritte an die Daten, können sich insofern Schutzlücken auftun. Derartige Fälle sind denkbar, wenn der Vertragspartner des „Datenüberlassers" (der „Datenerwerber") die Daten vertragswidrig – unter Umständen unter Umgehung technischer

[222] Für das Patentrecht: *Kraßer/Ann*, Patentrecht, 7. Aufl. 2016, § 3 Rn. 11. Dies wird auch in der ökonomischen Literatur betont.
[223] So dargestellt in der juristischen Literatur von *Kerber*, GRUR Int. 2016, 989, 992 f.; *Drexl* Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, S. 30 ff. Siehe auch *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 14 f.
[224] *Kerber,* GRUR Int. 2016, 989, 993.
[225] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 16.

Schutzmaßnahmen – an Dritte weitergibt (1) oder Dritte sich unbefugt Zugriff zu den beim Datenerwerber gespeicherten Daten verschaffen (2):

(1) Eine Weitergabe von Daten an Dritte wird – ebenso wie sonstige vertraglich nicht eingeräumte Nutzungshandlungen – regelmäßig schuldrechtliche (§§ 280 Abs. 1, 241 Abs. 2 BGB) Schadensersatzansprüche gegen den Datenerwerber auslösen, die neben dem Wertverlust der Daten wegen ihrer (unter Umständen) nunmehr freien Verfügbarkeit auch den entgangenen Gewinn des Datenüberlassers umfassen (§ 252 BGB). Rechtliche Mittel, dem Dritten die Nutzung oder Weitergabe der Daten zu untersagen, stehen dem Datenüberlasser aus dem Schuldverhältnis jedoch nicht zur Verfügung. Hierin besteht eine potentiell nicht unerhebliche Schutzlücke.

(2) Verschaffen sich Dritte unerlaubt Zugriff zu den Daten durch ein Eindringen in die IT-Infrastruktur des Datenerwerbers, stehen dem Datenerwerber deliktische Schadensersatz- (§§ 823 Abs. 2 BGB i.V.m. § 202a StGB) und quasinegatorische Unterlassungsansprüche (§§ 823 Abs. 2, 1004 analog BGB i.V.m. § 202a StGB) gegen den Dritten zu, deren Abtretung der Datenüberlasser bei entsprechender Vertragsgestaltung verlangen kann. Sofern der Datenerwerber seiner Sorgfaltspflicht bei der IT-Sicherheit nicht nachgekommen ist, können auch hieraus schuldrechtliche Schadensersatzansprüche des Datenüberlassers gegen den Datenerwerber folgen.

All diese Ansprüche sind praktisch jedoch nur durchsetzbar, sofern der Datenüberlasser nicht nur das „Datenleck“ feststellt, sondern auch ermitteln kann, von welchem seiner Vertragspartner der Dritte die Daten erlangt hat.

Die wirtschaftlichen Anreize zur Datengenerierung werden durch die soeben skizzierten Schutzlücken nicht nachhaltig beeinträchtigt. Verbleibende Schutzlücken können zudem durch punktuelle Schutzgesetze geschlossen werden, ohne dass hierfür die Schaffung eines neuen Immaterialgüterrechts erforderlich wäre. Die unter (1) skizzierte Schutzlücke fehlender Abwehrrechte gegenüber Dritterwerbern ist für solche Datensätze, die zugleich ein Geschäftsgeheimnis darstellen, beispielsweise durch die Geschäftsgeheimnis-RL geschlossen:

Die Geschäftsgeheimnis-RL gewährt dem Geheimnisinhaber einen Abwehranspruch, mit dem Dritten die Nutzung oder Offenlegung (also Weitergabe) der Daten untersagt werden kann, sofern diese die Daten auf rechtswidrige Weise erworben haben.[226] Ein rechtswidriger Erwerb liegt nicht nur vor bei Formen des unbefugten Zugriffs,[227] sondern auch bei jedem „sonstigen Verhalten, das unter den jeweiligen Umständen als mit einer seriösen Geschäftspraxis nicht vereinbar gilt“[228]. Welche Verhaltensweisen von dieser Generalklausel erfasst sein werden, ist noch unklar. Größere Relevanz dürfte in diesem Kontext aber Art. 4 Abs. 4 Geschäftsgeheimnis-RL zukommen: der Geheimnisinhaber kann Dritten die Nutzung und Offenlegung auch dann untersagen, wenn sie im Zeitpunkt des Erwerbs, der Nutzung oder Offenlegung wussten oder fahrlässig nicht wussten („hätte[n] wissen müssen“), dass sie die Daten von einer Person erlangt haben, für die die Offenlegung rechtswidrig war. Der Datenerwerber, von dem der Dritterwerber die Daten erlangt hat, dürfte ganz regelmäßig aufgrund eines Vertragsverstoßes gemäß Art. 4 Abs. 3 lit. b)–c) Geschäftsgeheimnis-RL das Geheimnis rechtswidrig offenbart haben. Wird dem Dritten dieser Umstand durch den Datenerzeuger

[226] Art. 4 Abs. 3 lit. a) Geschäftsgeheimnis-RL
[227] Art. 4 Abs. 2 lit. a) Geschäftsgeheimnis-RL
[228] Art. 4 Abs. 2 lit. b) Geschäftsgeheimnis-RL

beziehungsweise -überlasser mitgeteilt, ist er bei künftigen Nutzungs- und Offenbarungshandlungen bösgläubig und damit tauglicher Anspruchsgegner eines Unterlassungs- oder Schadensersatzanspruchs.

Durch die Kombination von vertraglichen Lösungen mit punktuell eingreifenden Schutzgesetzen könnte der Vorteil größerer Flexibilität, der vertragliche Lösungen gegenüber gesetzlichen definierten Immaterialgüterrechten auszeichnet, erhalten werden. Diese Flexibilität fällt insbesondere ins Gewicht bei der Zuordnung von Zugriffs- und Nutzungsrechten im Verhältnis zwischen mehreren an der Datengenerierung beteiligten Parteien, von denen in Abwesenheit eines Immaterialgüterrechts niemand eine rechtlich abgesicherte Hold-Up-Position innehat. Die Interessenlage innerhalb komplexer Wertschöpfungsketten[229], wie sie für die Datenökonomie charakteristisch sind,[230] kann von den beteiligten Unternehmen oftmals besser abgeschätzt beziehungsweise ausgehandelt werden.[231]

Gibt es ein Defizit an Investitionen in Datenanalyse?

Auch für Investitionen in Data-Analytics-Anwendungen kann kein grundlegendes Anreizdefizit festgestellt werden. Die zur Datenanalyse eingesetzten Techniken sind bereits jetzt regelmäßig Gegenstand von Immaterialgüterrechten, insbesondere eines Patents oder eines Urheberrechts an Software. Die durch Data Analytics-Anwendungen gewonnenen *Erkenntnisse* genießen als solche keinen Immaterialgüterschutz. Sie könnten allerdings, da auch sie in maschinengenerierten Daten codiert werden, dem Schutz eines Dateneigentumsrechts unterstellt werden.[232] Diesbezüglich gelten dieselben Ausführungen wie zur Anreizbildung der Datenerzeugung, nämlich dass die Ergebnisse von Datenanalysen durch vertragliche und technische Absicherungen vor Trittbrettfahrern geschützt werden können, sodass ein Anreizdefizit verhindert wird. Die Schaffung eines Dateneigentumsrechts, das Daten auf einer semantischen Ebene schützt, könnte sich hier sogar als kontraproduktiv erweisen: Da Big Data-Analysen im Wesentlichen Korrelationen in großen Datenmengen aufspüren, also letztlich semantische Informationen aufzeigen, die aus den Datensätzen ableitbar sind, müsste der eigentumsrechtliche Schutz an den Ausgangsdaten auf das Analyseergebnis erstreckt werden – zu dessen „Entdeckung“ der Datenerzeuger einen eher untergeordneten Beitrag geleistet hat.[233]

bb) Erfordernis von Offenbarungsanreizen

Eine ökonomische Begründung von Immaterialgüterrechten, die als Registerrecht ausgestaltet sind – insbesondere das Patentrecht – ist daneben die Schaffung von Offenbarungsanreizen. Der Patentschutz wird als „Gegenleistung“ dafür gewährt, dass der Erfinder seine technische Innovation in einem Patentregister veröffentlicht und somit die entsprechende Information der Öffentlichkeit zugänglich macht.[234]

[229] Es wird hier auch von Wertschöpfungsnetzwerken gesprochen.
[230] Hierzu *Drexl,* Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, S. 16 ff.
[231] Ebenso *Drexl,* Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, S. 41.
[232] *Kerber,* GRUR Int. 2016, 989, 991.
[233] *Drexl,* Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 2016, S. 16.
[234] Vgl. *Kraßer/Ann,* Patentrecht, 7. Aufl. 2016, § 3 Rn. 11. Die Einführung eines Eigentums(ähnlichen)rechts an Daten in der Form eines Registerrechts schlägt u.a. *Zech,* C&R 2015, 137, 146, vor.

Dieser Zweck ist auf Daten allerdings nicht oder nur eingeschränkt übertragbar. Insbesondere liegt der Wert von Daten in der digitalen Ökonomie häufig in ihrer unmittelbaren Echtzeit-Verfügbarkeit,[235] die eine technische Schnittstelle zum Datenüberlasser voraussetzt und durch ein öffentliches Register nicht hergestellt werden kann.

b) Eigentumsrechte an Daten zur Absenkung der Transaktionskosten im Datenhandel?

Denkbar bleibt, dass die Schaffung eines „Dateneigentumsrechts" den Handel mit Daten erleichtert, damit die Zugänglichkeit der Daten für Dritte erhöht und so die Innovations- und Wettbewerbsfähigkeit von Unternehmen steigert. Klar definierte Dateneigentumsrechte können die Transaktionskosten reduzieren und die Effizienz des Handels erhöhen.[236] Dieser Gesichtspunkt wird auch von der EU-Kommission in ihrem die Mitteilung zum Aufbau einer europäischen Datenwirtschaft begleitenden „Staff Working Paper" ausdrücklich angeführt.[237]

Das Ausmaß der Transaktionskostenabsenkung wird allerdings davon abhängen, inwieweit es gelingt, die „Eigentumsrechte" an Daten gesetzlich so zuzuordnen, dass diese Zuordnung der typischen Interessenlage entspricht. Andernfalls muss die Zuordnung später durch Parteivereinbarung korrigiert werden; hierfür fallen erneut Transaktionskosten an. Selbst diejenigen, die für ein neues Datenrecht eintreten, halten die konkrete Ausgestaltung eines solchen Rechts einschließlich seiner Zuordnung aber für eine offene Frage.[238] Die Autoren dieser Studie vermuten, dass die effiziente Zuweisung sektorspezifisch ist.

Die Transaktionskosten in der vertraglichen Reallokation ursprünglich zugewiesener Immaterialgüterrechte können besonders hoch ausfallen, wenn Immaterialgüterrechte an Daten nach Maßgabe einer Beteiligung an der Datengenerierung zugewiesen werden, und damit häufig Konstellationen eines (unter Umständen vielfachen) Miteigentums entstehen.[239] Nicht nur werden die Beiträge der verschiedenen Beteiligten zueinander mitunter schwer in ein eindeutiges Verhältnis zu setzen sein – dieses Problem lässt sich mit einer Vermutung gleicher Miteigentumsanteile überwinden. Schwerwiegender ist, dass die Fragmentierung des „Dateneigentums" zu einem Hold-up einzelner

[235] *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 15.
[236] *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 15.
[237] Siehe EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 33: Eine Möglichkeit sei die Schaffung eines neuen Datenherstellerrechts "with the objective of enhancing the tradability of non-personal or anonymised machine-generated data as an economic good."
[238] Dazu *Wiebe,* GRUR Int. 2016, 877, 881.
[239] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 34 f.: „One of the criteria for allocating the right could be to take into account the investments done and the resources put into the creation of the data. Such investments are made most often by two sides: The manufacturer of sensor-equipped machines, tools or devices (generating the data) who has invested in to the development and market commercialisation of the machine, tool or device and the economic operators using such machines, tools or devices paying a purchase price or lease and have to amortise the machine, tool or device. When several persons or entities jointly make investments into to data collection through a machine, tool or device, this could result in joint rights on the data generated. Freedom to contract should allow departing from that rule."

Rechteinhaber und damit zu dem bekannten Problem der „anti-commons“ führen kann.[240] Eine effiziente vertragliche Lösung wird hierdurch möglicherweise verhindert.[241] Verschärft wird die Lage durch die fehlende Publizität des Dateneigentums.[242] Die Zahl der Akteure, die zu einem Hold-up in der Lage sind, ist in einem Regime, in dem die Möglichkeit zu strategischem Verhalten allein von der faktischen Verfügungsmacht über Daten abhängt, unter Umständen geringer.[243]

c) Zwischenergebnis

Im Ergebnis lassen sich gegenwärtig damit weder aus der Anreizwirkung noch aus den Vorteilen, die mit einer klaren und rechtssicheren Zuweisung von Immaterialgüterrechten für den Handel verbunden sein können, überzeugende Argumente für die Schaffung eines neuen „Dateneigentumsrechts“ entnehmen. Der Umstand, dass Verträge über die Nutzung nicht personenbezogenen Daten bislang vor allem dezentral abgeschlossen und individuell ausgehandelt werden, Plattformen für den Datenhandel hingegen nur eine geringe Rolle spielen, liegt wahrscheinlich nicht in den hohen Transaktionskosten begründet, sondern im wirtschaftlichen Eigeninteresse der datenbesitzenden Unternehmen.

Für die Schaffung eines neuen Immaterialgüterrechts an (nicht personenbezogenen) Daten gibt es bislang keine hinreichend belastbare Rechtfertigung.

d) Alternative: „Private Ordering“ unter rechtlicher Absicherung technischer Schutzmaßnahmen

Aus ökonomischen Gesichtspunkten ist die Schaffung eines Eigentums- beziehungsweise Immaterialgüterrechts an Daten entbehrlich. Die derzeitige Kombination aus faktischem, technisch abgesichertem „Datenbesitz“ und dessen punktueller Aufhebung im Rahmen von bilateralen Verträgen schafft ein nahezu lückenloses Schutzregime, bewahrt aber die Vorteile vertraglicher Flexibilität im Gegensatz zu einer starren, gesetzlichen Allokation von Entscheidungsrechten.

Schutzlücken bestehen im Wesentlichen nur in zwei Fällen:

(1) Der „Datenbesitz“ wird rechtlich nur gegen vorsätzliche Verletzungshandlungen geschützt (§§ 823 Abs. 2, 1004 analog BGB i.V.m. §§ 202a–c, 303a StGB). Obgleich fahrlässige Umgehungen technischer Sicherungen eher die Ausnahme bilden dürften, sind sie doch vorstellbar – beispielsweise, sofern der Täter über das Vorliegen einer Einwilligung irrte.[244] Ferner ist Inhaber dieser Ansprüche der

[240] *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 29 ff. Ein ähnlich gelagertes Problem besteht allerdings auch bei Patenten und wird dort durch Patent-Pools adressiert.

[241] *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 29 ff.

[242] Zur kaum praktikablen Ausgestaltung als Registerrecht siehe oben.

[243] Für eine größere Flexibilität in einem vertraglichen Regime siehe auch *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 32, mit Verweis auf IDC and Open Evidence, European data market, SMART 2013/0063, D6, First Interim Report, European Commission, DG CONNECT, und auf *Merges*, IP Rights and technological platforms, 2008, sowie *West*, in: Greenstein/Stango (Hrsg.), Standards and public policy, 2007, S. 87.

[244] Irrtümer über die Rechtswidrigkeit lassen nach der im Zivilrecht herrschenden Vorsatztheorie den Vorsatz entfallen: *Schaub,* in: BeckOGK, Stand 1.5.17, § 276 Rn. 47; kritisch *Wagner,* in: MüKo-BGB, 7. Aufl. 2017, § 823 Rn. 48 f.

„Datenbesitzer“ (beziehungsweise der „Verfügungsbefugte“ im strafrechtlichen Sinn), nicht der Datenerzeuger. Zwar kann der Datenerzeuger sich bei der Veräußerung seiner Daten vertraglich die Abtretung derartiger Ansprüche einräumen lassen; sofern ihm lediglich bekannt ist, dass ein Dritter rechtswidrig Zugang zu den Daten erlangt hat, die Quelle aber unbekannt bleibt, sind derartige Ansprüche jedoch faktisch undurchsetzbar.

(2) Sofern Datenerwerber die Daten vertragswidrig an Dritte weiterleiten, liegt keine Verletzung des „Datenbesitzes“ vor. Der Datenerzeuger kann gegen den Dritten nur dann Abwehrrechte geltend machen, sofern die Daten ein Geschäftsgeheimnis darstellen und damit der Geschäftsgeheimnis-RL unterfallen.

Beide Schutzlücken ließen sich durch die Schaffung eines reinen Abwehrrechts vergleichbar dem Schutz von Geschäftsgeheimnissen schließen. Ein solches Recht müsste dem Datenhersteller ermöglichen, all diejenigen, die sich die Daten unrechtmäßig angeeignet haben, auf Unterlassung zu verklagen, eine Vermarktung zu verhindern und gegebenenfalls Schadensersatz zu verlangen. Die EU-Kommission erwägt in ihrem Staff Working Document die Einführung eines solchen Schutzrechts.[245]

III. Schaffung eines „Datenherstellerrechts“ zur Bekämpfung von Ungleichgewichtslagen in der neuen Datenwirtschaft?

Die EU-Kommission erwägt in ihrer Mitteilung zum Aufbau einer europäischen Datenwirtschaft ferner die Schaffung eines neuen „Datenherstellerrechts“.[246] Dies könne, so die Kommission, zu einem „fairen Vorteilsausgleich für alle an der Wertschöpfungskette Beteiligten (Dateninhaber, Auftragsverarbeiter und Anbieter von Anwendungen)“ beitragen.[247]

Der rechtliche Zuschnitt dieses Rechts ist unklar. Die Kommission hat bei der Schaffung dieses Rechts vor allem die Interessenlage im Verhältnis von Maschinenherstellern und den Maschinennutzern (und möglichen Maschineneigentümer) vor Augen. Sowohl der Maschinenhersteller als auch der Maschinennutzer tragen auf je eigene Weise zur Datengenerierung bei. Der Maschinenhersteller investiert in die Ausrüstung der Maschinen mit datengenierenden Sensoren.[248] Die Maschinenbetreiber nutzen die Maschinen entsprechend ihrer eigenen Unternehmensplanung, um einen Gewinn zu erzielen. Ihr Einsatz der Maschine löst den Datenstrom aus. Die Kommission nimmt an, dass trotz des beiderseitigen Beitrags zur Datengenerierung im Verhältnis von Maschinenhersteller

[245] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S. 33 ff.
[246] Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 14; näher EU Commission Staff Working Paper 2017, S. 33 ff. Siehe dazu *Wiebe*, CR 2017, 87, 93: es sei „überraschend, dass die Frage des „Ob“ eines neuen Datenproduzentenrechts“ nicht mehr ausdrücklich aufgeworfen werde.
[247] EU-Kommission, Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 12 f.
[248] Dies ist nicht notwendigerweise der Fall. So können manche Maschinen mit externen Sensoren ausgestattet werden. Damit erfolgt eine Primärdatenerhebung durch den Maschinennutzer ohne Beteiligung des Maschinenherstellers. Ein Beispiel ist die nachträgliche Ausrüstung von Aufzügen mit Sensoren zur Überwachung der Funktionstüchtigkeit.

und Maschinenbetreiber häufig ein Machtungleichgewicht besteht. Hierzu heißt es in der Mitteilung zum Aufbau einer europäischen Datenwirtschaft: [249]

„Für die Hersteller kann die faktische Kontrolle über diese Daten ein Differenzierungsmerkmal sein und ihnen einen Wettbewerbsvorteil verschaffen. Dies kann jedoch dann zum Problem werden, wenn der Nutzer, wie so häufig, vom Hersteller daran gehindert wird, die Nutzung der Daten durch Dritte zuzulassen. Die verschiedenen Marktteilnehmer, die die Kontrolle über die Daten haben, können abhängig von den jeweiligen Besonderheiten der Märkte Lücken in der Rechtslage oder die vorstehend erläuterten rechtlichen Unklarheiten ausnutzen, und den Nutzern unfaire Standardvertragsbedingungen aufzwingen oder zu technischen Mitteln wie proprietären Formaten oder Verschlüsselung greifen."

Wo diese Standardbedingungen im B2B-Bereich nicht der AGB-Kontrolle unterfielen, könne es vorkommen,

„dass Nutzer und Unternehmen in Vereinbarungen über ausschließliche Verwertungsrechte feststecken. Möglicherweise kommt es dazu, dass Daten freiwillig geteilt werden, doch die Aushandlung entsprechender Verträge könnte bei ungleichen Verhandlungspositionen erhebliche Transaktionskosten für die schwächeren Parteien nach sich ziehen, die Rechtsberatung in Anspruch nehmen müssen."

Um diesem Problem abzuhelfen, erwägt die EU-Kommission, dem „Erzeuger der Daten", d. h. dem Eigentümer oder langfristigen Nutzer der Maschinen, ein Recht zu gewähren,

„nicht personenbezogene Daten zu nutzen oder anderen deren Nutzung zu gestatten. Dieser Ansatz zielt darauf ab, für eine klare Rechtslage zu sorgen und den Datenerzeugern mehr Entscheidungsfreiheit zu geben, indem sie Nutzern die Möglichkeit eröffnen können, mit ihren Daten zu arbeiten, wodurch ein Beitrag dazu geleistet würde, den ausschließlichen Zugang zu von Maschinen erzeugten Daten aufzuheben. Allerdings müsste genau festgelegt werden, welche Ausnahmen insbesondere für den nicht ausschließlichen Zugang zu den Daten durch den Hersteller oder durch Behörden gelten, etwa für das Verkehrsmanagement oder aus Umweltgründen."[250]

Die EU-Kommission geht bei ihren Erwägungen zu einem „Datenerzeugerrecht" gegenwärtig, soweit ersichtlich, von einem quasi-dinglichen Exklusivitätsrecht und damit von einem neuen IP-Recht aus. Um dem von der Kommission skizzierten Problem abzuhelfen, ist eine Konzeption des „Datenerzeugerrechts" als quasi-dingliches Recht aber gar nicht erforderlich. Die angenommene Ungleichgewichtslage hat ihre Wurzel im Verhältnis von Maschinenhersteller und Maschinennutzer. Ein Recht des Maschinenbetreibers zur Eigennutzung und Weitergabe der bei der Nutzung anfallenden Daten kann daher alternativ auch als ein Annexrecht zu dem Rechtsverhältnis verstanden werden, mit welchem der Maschinenhersteller dem Maschinenbetreiber die Nutzung der Maschine gestattet – sei es ein Kauf- oder ein Leasingvertrag. Häufig wird die volle Realisierung des wirtschaftlichen Wertes der Maschine durch den Maschinenbetreiber von der Befugnis zur Datennutzung abhängen, so dass die Einräumung dieser Befugnis im Regelfall ein wesentlicher Bestandteil der vertraglichen Verpflichtung des Maschinenherstellers gegenüber dem Maschinennutzer ist. Denkbar wäre also eine

[249] EU-Kommission, Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 11 f.
[250] EU-Kommission, Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 14.

Auslegungsregel funktional vergleichbar dem § 311c BGB, der zufolge die Veräußerung oder Vermietung der Maschine im Zweifel auch das Recht des Käufers oder Mieters umfasst, die beim Betreiben der Maschine anfallenden Daten zu nutzen beziehungsweise an Dritte weiterzugeben.

Die Auslegungsregel hätte damit die Gestalt einer widerleglichen Vermutung. Sie griffe nicht ein, wenn ein abweichender Parteiwillen feststünde. Besteht allerdings das von der Kommission vermuteten Machtungleichgewicht zwischen Maschinenhersteller und Maschinenbetreiber, so müsste dieses Annexrecht zur Datennutzung, um der unterlegenen Vertragspartei effektiven Schutz zu gewähren, als nicht dispositives Recht ausgestaltet sein, dürfte also vertraglich nicht abbedungen werden.[251]

Die Problematik, die der EU-Kommission vor Augen steht, wird in der Literatur unter dem Schlagwort „end of ownership" diskutiert:[252] Mit dem Fortschreiten der Digitalisierung verliert das Sacheigentum im Verhältnis zu dessen digitalen Funktionalitäten – die rechtlich häufig als Dienstleistung ausgestaltet sind – an Bedeutung. Auch die Möglichkeit zur Eigennutzung und gegebenenfalls Weitergabe der bei der Nutzung von Sacheigentum erzeugten Daten (z.B. an potentielle Anbieter von Mehrwertleistungen) kann ein wesentlicher Bestandteil des Nutzens von Sacheigentum sein. Wird aber nur noch das Sacheigentum übertragen und behält sich der Verkäufer im Übrigen sämtliche Rechte an digitalen Inhalten und Daten vor, so kann dies zu einer Ausdünnung von Eigentumsrechten und damit verbunden zu einer gesellschaftlich relevanten Umverteilung von Kontrollbefugnissen führen. Denkbar ist auch, dass sich aus einer solchen Umverteilung von Kontrollbefugnissen neue wettbewerbsrechtliche Fragen ergeben. So ist etwa denkbar, dass die Kontrolle eines Maschinenherstellern über die Daten, die bei der Nutzung „seiner" Maschinen in verschiedenen Unternehmen erzeugt werden, die miteinander im Wettbewerb stehen, implizit zu einem wettbewerbsrechtlich problematischen Informationsaustausch und insbesondere zum Ausgangspunkt eines „hub and spoke"-Kartells[253] führen kann.

Während eine Umverteilung von Kontrollmöglichkeiten auf der Grundlage der fortlaufenden Datenkontrolle auf Endverbrauchermärkten naheliegt (da die Rechte an digitalen Inhalten und Daten hier nicht individuell ausgehandelt werden)[254], ist die Situation im B2B-Verkehr weniger offenkundig. Für unternehmerisch tätige Maschinenkäufer und -nutzer ist der Wert der Verfügungsmöglichkeiten über Daten grundsätzlich absehbar. Bei funktionierendem Wettbewerb auf dem Markt für die fraglichen Maschinen liegt ein Machtungleichgewicht zum Nachteil der Maschinenbetreiber nicht von vornherein auf der Hand. Wo es an einem Machtungleichgewicht fehlt, wäre ein Datennutzungs- und (eingegrenztes) Weitergaberecht des Maschinenbetreibers allenfalls als dispositives Recht vorzusehen. Es kann für den Maschinenhersteller legitime geschäftliche Gründe geben, sich die

[251] Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 11: EU-Kommission, Mitteilung zum Aufbau einer europäischen Datenwirtschaft: „Verfügen die verschiedenen Marktteilnehmer ... nicht über die gleiche Verhandlungsposition, könnten marktgestützte Lösungen allein sich als nicht ausreichend erweisen, um für Fairness und Innovationsfreundlichkeit zu sorgen, den Zugang für Marktneulinge zu erleichtern und Lock-in-Effekte zu vermeiden".

[252] *Perzanowski/Schultz*, The End of Ownership. Personal Property in the Digital Economy, 2016.

[253] In einem „hub-and-spoke"-Kartell werden Handlungen der Kartellmitglieder über ein Unternehmen koordiniert, das auf vorgelagerter oder nachgelagerter Stufe tätig ist.

[254] Zu dieser Problematik siehe *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge. Wissenschaftliches Rechtsgutachten für den Sachverständigenrat für Verbraucherfragen, Bundesministerium der Justiz und für Verbraucherschutz (BMJV), 2016.

Datennutzung vorzubehalten, und für den Maschinenbetreiber kann es Gründe geben, sich auf eine solche Regelung einzulassen. Wird das dispositive Datennutzungsrechts des Maschinenbetreibers abbedungen, wäre dies daher nur im Falle von festgestellter Marktmacht (nach deutschem Recht: auch von relativer Marktmacht, § 20 GWB) am Missbrauchsverbot zu messen. Daneben steht die AGB-Kontrolle, die nach deutschem Recht[255] auch den B2B-Bereich erfasst (§ 310 Abs. 4 BGB).

Auch wenn es nach alledem also Gründe für die Schaffung einer (widerleglichen) Vermutung geben kann, dass ein Vertrag, mit dem einem Dritten ein – irgendwie geartetes – Recht zum Betreiben einer Maschine eingeräumt wird, auch das Recht umfasst, die hierbei generierten Daten für eigene Zwecke zu nutzen und (gegebenenfalls in einem näher zu definierenden Umgang / zu näher zu definierenden Zwecken) an Dritte – z.B. Mehrwertdienstleister – weiterzugeben – so ist bislang doch unklar, warum dieses Recht im B2B-Bereich marktmachtunabhängig ausgestaltet werden sollte.

IV. Modellverträge für die Lizensierung von Daten?

Unabhängig von der Schaffung neuer Rechte an Daten kann die Funktionsfähigkeit des Datenhandels von der Stärkung des institutionellen Rahmens des Datenhandels (z.B. Mechanismen zur Zertifizierung der Teilnehmer zur Schaffung von Vertrauen, besondere Sicherheitsarchitektur etc.) profitieren. Hierzu kann unter Umständen auch die Schaffung eines dispositiven Rechtsrahmens für den Datenhandel beitragen.

Die EU-Kommission erwägt insbesondere die Veröffentlichung von ausgewogenen Standardvertragsklauseln für Datennutzungslizenzen. Weitergehend denkt die Kommission darüber nach, die Richtlinie über missbräuchliche Vertragsklauseln auf B2B-Verträge zu erstrecken sowie einen Leitfaden zu erstellen, wie Kontrollrechte über nicht personenbezogene Daten unter Berücksichtigung einschlägiger Transparenz- und Fairnessanforderungen vertraglich geregelt werden sollen.[256] Standardvertragsklauseln und Leitfaden würden dann zu einem Maßstab in der AGB-Kontrolle B2B.

Rechtspolitisch ist ein solches Vorgehen allerdings fraglich. Die allgemeine Erstreckung der AGB-Kontrolle auf die Verwendung von AGB zwischen Unternehmen, wie sie im deutschen Recht seit langem geltendes Recht ist, ist ein deutlich weiterreichender Eingriff als die Einführung eines dispositiven Datenherstellerrechts. In der deutschen Diskussion wird die von Marktmacht unabhängige Erstreckung der AGB-Kontrolle auf den B2B-Verkehr zunehmend als rechtspolitisch verfehlt abgelehnt.[257] Fraglich ist ferner, ob es bereits genug Erfahrung mit Daten-Lizenzverträgen in verschiedenen Kontexten gibt, um interessengerechte Modellverträge zu erstellen. Die Märkte befinden sich noch immer am Anfang ihrer Entwicklung. Mit geeigneten Vertragsklauseln wird erst experimentiert.

Gerade in dieser Phase ist es wichtig, dass – vorbehaltlich einer besonderen, durch Wettbewerb nicht kontrollierten Machtposition – die Vertragsfreiheit der Marktakteure nicht eingeschränkt wird. Die

[255] Die Unfair Contract Terms Directive 93/13/EEG ist hingegen im B2B-Bereich nicht anwendbar.
[256] Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 13 f.
[257] Siehe z.B. *Basedow*, in MüKo, BGB, 6. Aufl. 2012, § 310 Rn. 16; *Leuschner*, ZIP 2015, 1045 ff.; *Drygala*, JZ 2012, 983 ff. u.a.

Zuordnung von Nutzungsbefugnissen an Daten sowie die konkrete Ausgestaltung der Zugriffsrechte muss an die konkreten Bedürfnisse der Vertragsparteien angepasst werden können. Staatlich verordnete Modellverträge und eine hierauf bezogene AGB-Kontrolle laufen Gefahr, frühzeitig ein den Interessenlagen nicht entsprechendes Korsett einzuziehen. Sie sollten daher nicht am Anfang einer solchen Entwicklung stehen.

V. Schlussfolgerungen zum Handel mit nicht personenbezogenen Daten

Der Handel mit nicht personenbezogenen Daten erfolgt, soweit er stattfindet, bislang vor allem auf der Grundlage bilateral oder multilateral ausgehandelter Verträge. Die Einführung von „Eigentumsrechten“ an Daten würde daran voraussichtlich nichts ändern. Auch der Umstand, dass es bislang relativ wenige Marktplätze für nicht personenbezogene Datensätze gibt, ist nicht auf das Fehlen von „Eigentumsrechten“ an Daten zurückzuführen.

Das „private ordering“ auf Datenmärkten, wie es derzeit in weitgehender Abwesenheit von dispositivem Gesetzesrecht zu beobachten ist, funktioniert nicht perfekt. Die Transaktionskosten sind vergleichsweise hoch. Verhandlungsungleichgewichte zwischen den Vertragspartnern können sich in einen ungleichen Zugriff der Vertragspartner auf Daten übersetzen.

Hieran würden „Eigentumsrechte“ an Daten aber nichts ändern. Die eigentliche rechtspolitische Herausforderungen im Umgang mit maschinengenerierten, nicht personenbezogenen Daten liegt ferner nicht im rechtlichen Schutz einer faktisch ohnehin gewährleisteten Ausschließlichkeit, sondern in den Grenzen dieser Ausschließungsmöglichkeit (näher dazu unten, G.).

Zur Erleichterung des Handels mit Daten schlägt die EU-Kommission im Übrigen verschiedene Initiativen vor: Zu fördern sei die Entwicklung technischer Lösungen für verlässliche Identifikation, der Austausch von und differenzierter Zugang zu Daten, Watermarking, die technische Verankerung von Nutzungsbedingungen in Datensätzen sowie die Nutzung offener, standardisierter und dokumentierter APIs. Soweit diese Initiativen nicht mit der Einführung zwingenden Rechts einhergehen, bestehen keine grundsätzlichen Bedenken. Allerdings ist im Einzelfall zu prüfen, wo ein Marktversagen und in der Folge ein politischer Handlungsbedarf identifiziert werden kann. Ist dies nicht der Fall, ist abzuwarten, welche Initiativen von den Marktteilnehmern entwickelt werden.

G. Neue Zugangsrechte zu Daten?

Die breit geführte Debatte über „Eigentumsrechte an Daten“ stellt die Möglichkeit des Ausschlusses Dritter von der Datennutzung in den Mittelpunkt. Die rechtliche Ausgestaltung von Eigentumsrechten, und in besonderem Maße die Ausgestaltung von Immaterialgüterrechten, hat jedoch stets *auch* die Funktion, Ausschließungsbefugnisse mit Nutzungs- und Zugangsrechten Dritter in einen Ausgleich zu bringen. In einer Datenwirtschaft, die auf der faktischen, technisch getriebenen Möglichkeit zum Ausschluss Dritter vom Zugriff zu Daten basiert, können diese Schranken der Ausschließungsbefugnis

fehlen. In einem solchen Fall kann es notwendig sein, positive Zugangsrechte zu schaffen.[258] Tatsächlich sind es auch nicht die Ausschließungsbefugnisse von „Datenbesitzern“, sondern mögliche Nutzungs- und Zugangsrechte, die in der Mitteilung der EU-Kommission über den Aufbau einer europäischen Datenwirtschaft im Mittelpunkt stehen.

Das Ziel einer besseren Nutzung vorhandener Daten hat bereits die Initiativen der EU-Kommission zur Öffnung von Informationen des öffentlichen Sektors für die kommerzielle Weiterverwendung angetrieben. Die Richtlinie 2013/37/EU[259] soll dafür sorgen, dass öffentliche Stellen vorbehaltlich besonderer Ausnahmen ihre vielfältigen Informationen für eine private beziehungsweise gewerbliche Weiterverwendung öffnen und damit die Entwicklung neuer Dienste und Anwendungen ermöglichen. Die Mitteilung über den Aufbau einer europäischen Datenwirtschaft stößt diese Diskussion nunmehr für die unternehmerisch erzeugten Daten an.

Allerdings gibt es bereits nach geltendem Recht Begrenzungen der mit dem faktischen Datenbesitz einhergehenden Ausschließungsmöglichkeiten. Sie können insbesondere aus spezialgesetzlichen, typischerweise sektorspezifischen Regeln oder aber dem allgemeinen Wettbewerbsrecht folgen. Zu prüfen ist, ob jenseits der so erfassten Fallkonstellationen ein regulierungsbedürftiges Marktversagen hinsichtlich des Zugangs zu Daten verbleibt. Angesichts der Bedeutung des Rechts, die aus eigener unternehmerischer Initiative folgenden Wettbewerbspotentiale eigennützig zu verwerten, sollten neue Datenzugangsrechte nur dann in Betracht kommen, wenn sie tatsächlich erforderlich sind, um (neue) Märkte offenzuhalten. Dies kann insbesondere dann der Fall sein, wenn im Kontext des Angebots bestimmter Produkte oder Dienste für spezifische, nicht zugängliche Daten keine angemessenen Substitute existieren.

Schließlich ist bei der Erörterung von Zugangsrechten die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten relevant. Zugangsrechte von Drittunternehmen zu personenbezogenen Daten in der Hand eines anderen Unternehmens kommen schon aus datenschutzrechtlichen Gründen häufig nicht in Betracht. Sollen Drittunternehmen Zugang zu solchen Daten erlangen, so muss vielmehr eine Portabilität dieser Daten durch den Betroffenen angeordnet werden (siehe dazu bereits oben, Teil E).

I. Spezialgesetzliche Regelungen eines Datenzugangs

Sonderregelungen betreffend Datenzugang existieren bislang vor allem mit Blick auf personenbezogene Daten, und sie begünstigen regelmäßig die Person, auf welche sich die Daten beziehen. Das wichtigste Beispiel ist die bereits erörterte Regelung zur Datenportabilität in Art. 20 DSGVO. Bereits erörtert wurden ferner auch die spezialgesetzlichen Sonderregelungen im Bereich Energie und Zahlungsdienste. Das – marktmachtunabhängige – Recht auf Portabilität

[258] Siehe für einen entsprechenden Gedanken: *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 15: „From an economic policy perspective, the maximization of social welfare from data requires maintaining a balance between data ownership protection and access rights. When the importance of investment incentives for data owners diminishes, access rights can be widened”.
[259] Richtlinie 2013/37/EU v. 26.6.2013 zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. 2013 Nr. L 175/1.

personenbezogener Daten dient der Vermeidung eines „lock-in“ und der Öffnung angrenzender Märkte für neue Mehrwertdienste, und es schafft ein Substitut für sekundäre Märkte für personenbezogene Daten, deren Entwicklung durch das Datenschutzrecht nachhaltig behindert wird.

Im B2B-Sektor gibt es bislang, soweit ersichtlich, keine spezialgesetzlichen, sektorspezifischen Vorschriften zur Gewährleistung eines (wettbewerblich motivierten) Datenzugangs. Die gelegentlich als Ausnahme von diesem Befund genannte Verordnung (EG) Nr. 715/2007[260] (Euro-VO 5/6) verpflichtet die Kfz-Hersteller, unabhängigen Marktteilnehmern[261] über das Internet mithilfe eines standardisierten Formats uneingeschränkten, standardisierten und im Verhältnis zu autorisierten Händlern und Betrieben diskriminierungsfreien Zugang zu Reparatur- und Wartungsinformation zu geben (Art. 6).[262] Hier geht es allerdings um die Zugänglichmachung von Servicehandbüchern, technischen Anleitungen, Informationen über Bauteile und Diagnose, Schaltplänen, Fehlercodes des Diagnosesystems, Kennnummern der Softwarekalibrierung und Informationen über Spezialwerkzeuge und –geräte[263] in einer spezifischen „Aftermarket“-Konstellation, nicht um die Zugänglichmachung von automatisiert erzeugten Daten in dem hier behandelten Sinne. Erörtert wird eine Verpflichtung zum Austausch solcher Daten gegenwärtig im Kontext der von der Kommission angestoßenen europäischen Strategie für Kooperative Intelligente Verkehrssysteme (C-ITS – „cooperative, connected and automated mobility“).[264] Eine eng begrenzte Regelung zur diskriminierungsfreien Zugänglichkeit des mittlerweile verpflichtenden, auf dem 112-Notruf basierenden E-Call-System für Kfz enthält die VO 2015/758.[265]

II. Wettbewerbsrechtlich begründete Ansprüche auf Datenzugang

Jenseits dieser vereinzelten sektorspezifischen Regeln greift mit Blick auf nicht personenbezogene Daten und im B2B-Bereich allein das allgemeine Wettbewerbsrecht. Der ausschließliche Zugriff eines Unternehmens auf Daten kann Grundlage von Marktmacht sein. Die Weigerung, anderen Unternehmen Zugriff auf die Daten einzuräumen, kann unter engen Voraussetzungen ein Missbrauch von Marktmacht sein, ebenso die Diskriminierung zwischen Nachfragern in der Ermöglichung des

[260] Verordnung (EG) Nr. 715/2007 v. 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge, Abl. 2007 Nr. L 171/1; zuletzt geändert durch VO No. 459/2012 v. 29.5.2012.

[261] Für eine Definition siehe Art. 3 Nr. 15 Euro-VO 5/6.

[262] Die Regelungen zum Zugang zu Reparatur- und Wartungsinformationen werden derzeit auf der Grundlage eines Vorschlags der EU-Kommission für eine VO über die Genehmigung und Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern überarbeitet – siehe Abschnitt XIV des Vorschlags der EU-Kommission v. 27.1.2016, COM(2016)31 fin., Art. 65 ff.

[263] Siehe im Einzelnen Art. 6 Abs. 2 Euro-VO 5/6.

[264] Siehe dazu EU-Kommission, Mitteilung: Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme – ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität, Brüssel, 30.11.2016, COM(2016)766 fin.

[265] Art. 5 Abs. 7 VO (EU) 2015/758 v. 29. April 2015, ABl. Nr. L 123/77. Gem. Art. 12 Abs. 2 der VO soll die Kommission im Anschluss an eine Konsultation die Notwendigkeit prüfen, Anforderungen für eine interoperable, standardisierte, sichere und frei zugängliche Plattform festzulegen.

Datenzugriffs. Die Pflicht, anderen Unternehmen Zugriff auf bestimmte Daten zu ermöglichen, kann ferner als Abhilfe für einen Missbrauch in Betracht kommen.

1. Marktmacht durch Daten

Dass der exklusive Zugriff auf Daten ein relevanter Faktor bei der Ermittlung einer marktbeherrschenden Stellung sein kann, ist mit Blick auf mehrseitige Märkte und Netzwerke[266] nunmehr ausdrücklich in § 18 Abs. 3a GWB anerkannt.[267] Auch außerhalb mehrseitiger Märkte kann aber der exklusive Zugriff auf große, nicht anderweitig verfügbare Datensätze Marktmacht begründen oder verstärken. In der modernen Datenökonomie kann der Zugriff auf große Datenmengen aus vielfältigen Datenquellen etwa erhebliche Vorteile in der Entwicklung neuer Produkte oder in der Verbesserung bestehender Produkte oder in der Optimierung von Produktions- und Vertriebssystemen sein. Insbesondere Selbstlernprozesse („deep learning“) von Algorithmen sind auf große Datenmengen angewiesen. Auf der Grundlage derart generierter Lernprozesse kann sich ein Marktvorsprung verfestigen.[268]

Der Umstand, dass der Zugriff auf große Datensätze, verbunden mit dem Einsatz von Deep Learning ein Wettbewerbsvorteil sein kann, begründet für sich allein allerdings noch keine marktbeherrschende Stellung. Ob der Zugriff auf Daten – gegebenenfalls verbunden mit anderen Faktoren – Marktmacht begründet, ist stets mit Blick auf einen spezifischen relevanten Markt hin zu prüfen. Mit Blick auf die Tätigkeit in diesem Markt können die konkreten Datensätze durch andere Daten oder der unmittelbare Zugriff auf Daten durch am Markt verfügbare Erkenntnisse aus Data Analytics substituierbar sein.[269] Wer neue Dienste entwickelt, kann Nutzungsdaten unter Umständen selbst ansammeln. Insoweit der Zugriff auf personenbezogene Daten erheblich ist, ist bei der Ermittlung von Marktmacht das Recht auf Datenportabilität nach § 20 DSGVO zu berücksichtigen. Auch ist davon auszugehen, dass Größen- und Skalenvorteile bei Daten ab einem bestimmten Punkt häufig einen abnehmenden Grenznutzen haben werden[270] und der Wert von Daten kurzlebig sein kann. Ob ein exklusiver Datenzugriff Marktmacht vermittelt, ist daher im Einzelfall unter genauer Ermittlung der Marktgegebenheiten zu ermitteln.

Besondere Aufmerksamkeit ist der Bedeutung von Daten für die Markstellung der neuen unternehmerischen Einheit auch im Rahmen der Fusionskontrolle zu widmen, etwa beim Aufkauf von „datenreichen“ potentiellen Wettbewerbern durch bereits marktstarke Unternehmen.[271] Bei einer absehbaren wesentlichen Behinderung wirksamen Wettbewerbs kann die Fusionskontrolle dazu

[266] Die Bezeichnung „mehrseitige Märkte und Netzwerke“ ist unglücklich gewählt. *Schweitzer/Fetzer/Peitz*, Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen, ZEW Discussion Paper 16-042, 2016, S. 4 ff. wählen stattdessen eine breite Definition von Plattformen. Eine systematische Darstellung hierzu geben *Belleflamme/Peitz*, Platforms and Network Effects, University of Mannheim Discussion Paper 16-14, September 2016.

[267] Siehe BKartA, B6-113/15, Working Paper – Market Power of Platforms and Networks, Juni 2016.

[268] Auf Marktzutrittschranken aufgrund fehlender Daten weisen beispielsweise Autorité de la Concurrence and Bundeskartellamt, Competition Law and Data, 10.05.2016, hin.

[269] Für die Bedeutung der Prüfung von Substitutionsbeziehungen für die Feststellung einer marktbeherrschenden Stellung auch *Körber*, NZKart 2016, 303, 305; *Grave/Nyberg*, WuW 2017, 363, 364.

[270] *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 5.

[271] Hierzu, unter Bezugnahme auf die bislang einschlägige Fallpraxis der EU-Kommission: *Grave/Nyberg*, WuW 2017, 363, 366 f.

dienen, mit geeigneten Abhilfen Marktzutrittsschranken, die aus einer besonderen „Datenmacht“ resultieren, frühzeitig vorzubeugen.

2. Verweigerung des Zugriffs auf Daten als Missbrauch einer marktbeherrschenden Stellung? Zur Anwendung der „essential facilities“-Doktrin im Kontext von Daten

Breit diskutiert worden ist in jüngerer Zeit, ob beziehungsweise unter welchen Voraussetzungen die Weigerung eines marktbeherrschenden Unternehmens, Wettbewerbern Zugang zu automatisiert erstellten Datensätzen zu gewähren, einen Missbrauch einer marktbeherrschenden Stellung darstellen kann.[272]

Die Voraussetzungen, unter denen die Weigerung, Wettbewerbern den Zugriff auf eigene unternehmerische Ressourcen einzuräumen, einen Missbrauch von Marktmacht darstellen kann, sind im europäischen Wettbewerbsrecht in der „essential facilities“-Doktrin (EFD) zusammengefasst. Das marktbeherrschende Unternehmen muss den Zugang zu einer wesentlichen, nicht duplizierbaren Ressource kontrollieren, deren Nutzung für die Tätigkeit auf einem angrenzenden Markt erforderlich ist; die Weigerung, Zugang zu gewähren, muss geeignet sein, den Wettbewerb auf dem angrenzenden Markt auszuschließen; und sie darf nicht durch sachliche Gründe – etwa durch den Schutz von Geschäftsgeheimnissen – gerechtfertigt sein.[273]

Ob diese Voraussetzungen vorliegen, ist mit Blick auf den jeweiligen Datensatz und den geplanten Zweck der Verwendung unter Berücksichtigung der in diesem Bericht ermittelten Substitutionsbeziehungen sorgfältig zu prüfen. Zu ermitteln ist die Art von Wettbewerb, wie sie sich mit und ohne die Anordnung solcher Zugriffsrechte ergeben würde. Im Schrifttum wird zu Recht ein vorsichtiger Umgang mit der Essential Facilities-Doktrin (EFD) angemahnt.[274] Zwar wird bei der Anordnung eines Zugangs zu Daten – anders als in den bisher diskutierten Anwendungsfällen der EFD – regelmäßig nicht in rechtlich geschützte Eigentumsrechte eingegriffen.[275] Eingegriffen wird aber in die Ausschließungsmöglichkeit, die aus dem faktischen Besitz folgt, sowie in die unternehmerische Freiheit, von dieser eigennützig Gebrauch zu machen. Auch mit dieser faktischen Ausschließungsmöglichkeit sind wichtige Anreize für Investitionen und Innovation verbunden. In viele Märkte kann mit einer guten Geschäftsidee auch ohne Zugriff auf größere Datenmengen eingetreten werden. Zwar kann der Zugriff auf Daten Vorteile im Wettbewerb begründen. Sie führen aber regelmäßig nicht zu einem Marktverschluss. Dann aber ist den mit der Ausschließungsmöglichkeit verbundenen Investitions- und Innovationsanreizen Vorrang zu geben. Gerade bei Sammlungen (ursprünglich) personenbezogener Nutzungsdaten, für welche die EFD bislang primär diskutiert worden ist, wird sie angesichts der alternativen Zugriffsmöglichkeiten auf vergleichbare Daten nur sehr selten in Betracht gezogen werden können. Bislang ist die EDF mit Blick auf die hier interessierenden automatisiert erzeugten Datensätze nicht angewandt worden. Ungeklärt ist daher bislang auch, ob auf der Grundlage der EFD eine Verpflichtung zur Gewährung von Zugang zu ursprünglich personenbezogenen Nutzungsdaten in Betracht kommen kann, wenn diese aus

[272] Dazu *Körber*, NZKart 2016, 303, 308 f.; *Grave/Nyberg*, WuW 2017, 363, 365 f.

[273] Zur Essential Facilities-Doktrin allgemein: *Mestmäcker/Schweitzer*, Europäisches Wettbewerbsrecht, 3. Aufl. 2014, § 19 VI, S. 490 ff.

[274] Siehe z.B. *Körber*, NZKart 2016, 303, 309; Grave/Nyberg, WuW 2017, 363, 365 f.; *Duch-Brown/Martens/Müller-Langer*, The economics of ownership, access and trade in digital data, 2017, S. 20 f.

[275] Differenzierend insoweit: *Grave/Nyberg*, WuW 2017, 363, 366.

datenschutzrechtlichen Gründen vor der Weitergabe erst anonymisiert werden müssten, und dies eine zusätzliche Investition des Datenbesitzers erfordern würde.

Anders kann sich die Situation darstellen, wenn ein Unternehmen über den exklusiven Zugang zu Spezialdaten verfügt, hinsichtlich derer eine Substitution von vornherein ausgeschlossen ist. Ein Beispiel können etwa die Fahrplandaten des öffentlichen Nah- und Fernverkehrs sein. Wer auf der Grundlage solcher Daten Mehrwertdienste anbieten will, kommt ohne den Zugriff auf Fahrplandaten nicht aus. Die durch eine Verweigerung des Datenzugriffs bedingte Verhinderung neuer Mehrwertdienste hat der EuGH im Urteil Magill[276] als einen Missbrauch durch „Einschränkung der Erzeugung, des Absatzes oder der technischen Entwicklung zum Schaden des Verbrauchers“ (Art. 102 lit. b) AEUV) qualifiziert.

3. Andere Formen eines datenbezogenen Missbrauchs einer marktbeherrschenden Stellung

Eine gegenüber der „essential facilities“-Doktrin praktisch bedeutsamere datenbezogene Form des Missbrauchs kommen Ausschließlichkeitsbindungen eines marktbeherrschenden Unternehmens mit Blick auf den Zugang zu wettbewerbsrelevanten Daten in Betracht, mit denen Wettbewerbern der Zugriff auf relevante Daten beziehungsweise die hieraus folgenden wettbewerbserheblichen Erkenntnisse verbaut oder jedenfalls erschwert wird. Derartige Vereinbarungen eines marktbeherrschenden Unternehmens sind stets kritisch zu prüfen.[277]

Auch darf ein marktbeherrschendes Unternehmen in der Gewährung des Datenzugriffs zwischen Handelspartnern nicht diskriminieren, wenn aus der Diskriminierung eine Benachteiligung im Wettbewerb und damit eine Wettbewerbsverfälschung auf dem nachgelagerten Markt folgen würde (Art. 102 lit. d) AEUV).

4. Verweigerung des Zugriffs auf Maschinennutzungsdaten im Verhältnis Maschinenhersteller – Maschinennutzer

Die Kommission sieht eine innovationsfreundliche, wettbewerbsfähige Datenwirtschaft gegenwärtig offenbar vor allem durch ungleiche Verhandlungspositionen der Marktteilnehmer gefährdet.[278] Im Fokus steht dabei zum einen das Verhältnis zwischen Maschinenhersteller und Maschinennutzer,[279] zum anderen Vertragsverhältnisse mit digitalen Dienstleistern. Die Kommission sieht die Gefahr, dass sich etwa der Maschinenhersteller im Verhältnis zum Maschinennutzer, um die Wertschöpfungskette nachhaltig zu kontrollieren, die Nutzung und Verwertung der im Maschinenbetrieb durch Sensoren erzeugten Daten vorbehalten und eine Nutzung durch den Maschinennutzer beziehungsweise eine Weitergabe der Daten durch den Maschinennutzer an Dritte ausschließen kann. Durch eine solche Praxis kann ein volkswirtschaftlich sinnvoller Gebrauch der Daten – etwa durch ihren Einsatz zur Entwicklung innovativer Mehrwertdienste – verhindert werden. Dasselbe Problem kann im Verhältnis

[276] EuGH 4.6.1995, Rs. C-241/91 P und C-242/91 P, Slg. 1995 I 743 – Magill.
[277] Siehe auch *Körber*, NZKart 2016, 303, 309; *Grave/Nyberg*, WuW 2017, 363, 366.
[278] Kommission, Mitteilung zum Aufbau einer europäischen Datenwirtschaft, 2017, S. 12: „Jede künftige Lösung sollte den wirksamen Datenzugang fördern und hierbei beispielsweise etwaige Unterschiede in der Verhandlungsposition der Marktteilnehmer berücksichtigen.“
[279] Der Maschinennutzer kann Eigentümer der Maschine sein, Leasingnehmer oder auch eine andere Rechtsposition an der Maschine haben.

von Anbietern digitaler Dienste zu Dienstenutzern entstehen.[280] So können digitale Plattformen wie Amazon ein Interesse haben, sich den ausschließlichen Zugriff auf die auf der Plattform erzeugten (anonymisierten) Daten zu sichern, während die Unternehmen, die ihre Dienste über die Plattform anbieten, keinen Zugriff erhalten.

Derartige Konstellationen können im deutschen Recht gegebenenfalls über das Verbot des Missbrauchs relativer Marktmacht erfasst werden, insoweit die Maschinennutzer als kleine oder mittlere Unternehmen von einem Maschinenhersteller abhängig sind (§ 20 Abs. 1 GWB). Eine Abhängigkeitslage ist im Einzelfall festzustellen. Im Verhältnis Maschinenhersteller – Maschinennutzer kommt sie insbesondere bei einem längerfristigen Lock-in des Nutzers in Betracht. Für die hier interessierende Fallgruppe haben sich konkrete Grundsätze zur Handhabung des § 20 Abs. 1 GWB noch nicht herausgebildet. Das europäische Wettbewerbsrecht kennt keine Vorschriften zur relativen Marktmacht.

III. Handlungsbedarf zur Gewährleistung eines Zugangs zu Daten?

Es stellt sich die Frage, ob rechtspolitischer Handlungsbedarf zu einer Gewährleistung von Datenzugang besteht, der über die Grenzen des aktuellen Wettbewerbsrechts hinausreicht.

Das Wettbewerbsrecht adressiert Formen des Marktversagens, die aus der Existenz von Marktmacht folgen. Denkbar ist, dass erhebliche öffentliche Interessen einen weitergehenden Datenzugang gebieten (1.). Denkbar ist auch, dass die Marktmachtschwelle, wie sie für das Verbot des Missbrauchs von Marktmacht nach EU-Wettbewerbsrecht maßgeblich ist, im Kontext der neuen Datenwirtschaft zu hoch ist und eine Absenkung opportun ist – etwa durch Erfassung von Konstellationen relativer Marktmacht, aber unter Umständen auch darüber hinaus (2.). Die EU-Kommission denkt ferner über die Erstreckung des – marktmachtunabhängigen – Rechts auf Datenportabilität, wie Art. 20 DSGVO es für personenbezogene Daten statuiert, auf nicht personenbezogene Daten nach (3.). Schließlich werden auch rein sektorspezifische Zugangsgebote erwogen (4.).

1. Verpflichtung zur Gewährung von Datenzugang mit Blick auf öffentliche Interessen

In bestimmten Fällen kann ein öffentliches Interesse daran bestehen, die allgemeine Zugänglichkeit bestimmter Datenkategorien zu gewährleisten. Ein Beispiel können Daten sein, die autonom fahrende Kfz generieren und die der Steigerung der Straßenverkehrssicherheit dienen.[281] Das Pooling aller einschlägiger Daten kann hier einen hohen gesellschaftlichen Nutzen generieren. Der Datenzugang sollte in diesem Fall marktmachtunabhängig gewährleistet werden. Auf europäischer Ebene wird im Rahmen der C-ITS-Initiative über die Notwendigkeit eines allgemeinen Datenzugangs im Kontext automatisierten Fahrens nachgedacht.[282]

[280] Sofern es sich um nicht personenbezogene Daten handelt. Bei personenbezogenen Daten greift künftig das Recht auf Datenportabilität, Art. 20 DSGVO.
[281] Siehe hierzu auch VDA, Positionspapier „Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten“, S. 2.
[282] https://ec.europa.eu/transport/themes/its/c-its_en.

Die OECD hat in einem weiteren Kontext über die Opportunität von Datenzugangsrechten und „data commons“ im öffentlichen Interesse nachgedacht.[283]

Ein öffentliches Interesse an der Allgemeinzugänglichkeit automatisiert erzeugter Daten, welches die legitimen unternehmerischen Interessen an der Möglichkeit der Ausschließung überwiegen, wird aber schon wegen der aus der Ausschließung folgenden Anreize zur Datengenerierung nur in eingegrenzten Kontexten zu bejahen sein.

2. Verbot des Missbrauchs relativer Marktmacht – Absenkung der Marktmachtschwelle für den Missbrauch datenbezogener Machtpositionen auf europäischer Ebene?

Fraglich ist, ob angesichts der großen wirtschaftlichen Bedeutung von Daten für die Entwicklung einer Datenwirtschaft die Machtschwelle, ab der ein Unternehmen zur Gewährung von Datenzugang verpflichtet werden kann, im Verhältnis zu der im europäischen Wettbewerbsrecht im Übrigen geltenden Schwelle der Marktbeherrschung abgesenkt werden sollte. Denkbar wäre etwa die Einführung eines Verbots des Missbrauchs relativer Marktmacht auf europäischer Ebene, vergleichbar der Regelung des § 20 GWB. Hierdurch würden auch wettbewerbsrelevante bilaterale Machtlagen erfasst.

Allerdings ist im Kontext des § 20 GWB bislang ungeklärt, unter welchen Voraussetzungen die Kontrolle über den Datenzugang eine Abhängigkeit kleiner oder mittlerer Anbieter oder Nachfrager begründet. Zu erfassen wären Situationen eines „lock-in“, in denen etwa ein Maschinennutzer den AGB eines Maschinenherstellers nicht durch Wechsel zu einem anderen Hersteller oder durch Verhandlungen über die AGB ausweichen kann und hierdurch dazu veranlasst wird, ungünstige Datennutzungsbedingungen zu akzeptieren. Ähnliche Situationen können im Verhältnis von Diensteanbieter und Dienstenutzer im B2B-Bereich entstehen. Da auf europäischer Ebene aber keine allgemeine Übernahme des Verbots des Missbrauchs relativer Marktmacht angestrebt wird – und eine solche Absenkung der Interventionsschwelle auch wettbewerbspolitisch seit jeher umstritten ist – scheint es sinnvoll, stattdessen über die Einführung von spezifisch auf den Datenzugang zugeschnittenen Tatbeständen nachzudenken.

3. Datenportabilität für nicht personenbezogene Daten – Datenherstellerrecht als Datennutzungsrecht

Die Kommission sieht einen Bedarf nach der Gewährleistung von Datenzugangsansprüchen jenseits des europäischen Wettbewerbsrechts vor allem im Verhältnis zwischen Maschineneigentümer und Maschinennutzer beziehungsweise im Vertragsverhältnis mit digitalen Dienstleistern. Grund hierfür ist die Sorge um eine ungleiche Verhandlungsmacht in diesen Beziehungen und um ein naheliegendes „lock-in“ des Maschinen- oder Dienstenutzers. Die Kommission erwägt vor diesem Hintergrund die Schaffung eines auf Grundsätze wie Fairness, Angemessenheit und Nichtdiskriminierung gestützten

[283] OECD, Maximising the Economic and Social Value of Data, 2017: “The OECD ... refers to a "data commons" as a way to describe non-discriminatory access to certain data for at least a wider group of players, specifying that this should neither be confused with an "open data" or "open access" approach (access for the public at large), nor should it mean that access is given at no costs. The defining element of a "commons" is that non-discriminatory access is to be given, i.e. any member of a certain group (e.g. users of an industrial data platform […]) can use the data for purposes defined by the party making the data accessible.”

Regelrahmens, der die Zugänglichmachung von Daten – gegebenenfalls gegen Entgelt – gewährleistet.[284] Dem Schutz von Geschäftsgeheimnissen soll Rechnung getragen werden.

Das Zugangsrecht des Maschinen- oder Dienstenutzers kann die Form eines „Datenherstellerrechts“ (in Form eines Datennutzungsrechts, nicht eines vollumfänglichen Dateneigentumsrechts) oder die Form eines Rechts auf Datenportabilität auch für nicht personenbezogene Daten annehmen. Die Übergänge zwischen beiden sind fließend: Ein Recht auf Datenportabilität könnte auf die Datenportabilität bei Vertragsende begrenzt werden – muss es aber nicht. Art. 20 DSGVO zeigt für personenbezogene Daten, dass Datenportabilität auch als ständiges Nutzungsrecht denkbar ist. Hauptziel der Datenportabilität nach Art. 20 DSGVO ist die Möglichkeit der Nutzer, die Daten konkurrierenden Diensteanbietern zur Verfügung stellen zu können und so einem „lock-in“ entgegenzuwirken. Das potentielle Interesse von Maschinen- oder Dienstenutzer reicht hierüber hinaus und erfasst auch die eigene wirtschaftliche Verwertung von Daten. Dieses Interesse kann unter den Begriff der „Datenportabilität“ oder unter das Konzept eines „Datenherstellerrechts“ subsumiert werden. Wichtig ist, dass es an dieser Stelle nicht um die Begründung einer Ausschließungsbefugnis des Maschinen- oder Dienstenutzers im Verhältnis zum Maschinenhersteller oder Diensteanbieter geht, sondern „nur“ um ein eigenes – gegebenenfalls zusätzliches – Nutzungsrecht, das gegenüber dem Maschinenhersteller oder Diensteanbieter geltend gemacht werden kann. Es handelt sich also um eine Begrenzung der faktischen Ausschließungsbefugnis des Maschinenherstellers oder Diensteanbieters. Durch diese Begrenzung soll gewährleistet werden, dass Maschinen- und Dienstenutzer mit den durch ihre Nutzungshandlungen erzeugten Daten eigene Zwecke verfolgen oder die Entwicklung neuer Mehrwertdienste in Auftrag geben können. Maschinenhersteller und Diensteanbieter verlieren so die Möglichkeit, sich die Realisierung des wirtschaftlichen Werts der Daten, der ganz verschiedene Dimensionen haben kann, alleine vorzubehalten.

Die Schaffung eines solchen Rechts des Maschinen- oder Dienstenutzers auf Datennutzung scheint in jedem Fall gerechtfertigt, wenn ein „lock-in“ entstanden ist oder wenn die aus der eigenen Machtposition beziehungsweise aus der Wettbewerbslage folgende Verhandlungsmacht von vornherein so beschränkt ist, dass der Maschinen- oder Dienstenutzer die eigenen wirtschaftlichen Interessen nicht effektiv durchsetzen kann.

Zweifelhaft ist, ob ein solches Recht von diesen Voraussetzungen gelöst und somit verallgemeinert werden sollte.

Ein wichtiger Grund für die marktmachtunabhängige Ausgestaltung des Rechts auf Portabilität personenbezogener Daten gemäß Art. 20 DSGVO ist nach hier vertretener Ansicht, dass dadurch den Beschränkungen des Handels mit personenbezogenen Daten, wie sie aus dem Datenschutzrecht folgen, entgegengewirkt wird. Diese Begründung für eine marktmachtunabhängige Ausgestaltung eines Rechts auf Datenportabilität entfällt bei nicht personenbezogenen Daten.

In Situationen, in denen keine bilaterale Machtlage des Maschinenherstellers oder Diensteanbieters im Verhältnis zum Maschinen- beziehungsweise Dienstenutzer besteht, kann ein Verzicht des

[284] Kommission, Mitteilung zum Aufbau einer europäischen Datenwirtschaft, 2017, S. 15. Siehe auch EU-Commission, Staff Working Paper, 2017, S. 48: Einführung eines allgemeinen Recht auf Portabilität nicht personenbezogener Daten als mögliches Mittel, Wettbewerb zu fördern, Data Sharing zu stimulieren und einen Lock-in von Nutzern digitaler Dienste zu vermeiden.

Maschinen- oder Dienstenutzers auf den Datenzugriff im beiderseitigen Interesse sein. Der Maschinenhersteller oder Diensteanbieter erlangt so besonders hohe Anreize zur Investition in eine langfristige Beziehung. Die Anreize zu Investitionen in die Datengenerierung sinken, wenn Maschinenhersteller und Diensteanbieter jederzeit mit einem Wechsel unter Mitnahme der Daten beziehungsweise in eine eigene wirtschaftliche Verwertung der Daten durch die Maschinen- und Dienstenutzer rechnen müssen.

Die Kommission selbst weist ferner auf die erheblichen Kosten und Nachteile eines verallgemeinerten Rechts auf Datenportierung im B2B-Bereich hin: Die Anforderungen an die Datenübertragbarkeit seien technisch anspruchsvoll und kostenaufwendig, da Daten von verschiedenen Anbietern derselben Dienste möglicherweise auf unterschiedliche Art und Weise gespeichert werden könnten. Eine sinnvolle Übertragbarkeitsregelung für nicht personenbezogene Daten müsse gegebenenfalls auch weiter gefasste Überlegungen zur Datenverwaltung berücksichtigen, wie beispielsweise die Transparenz für Nutzer, die Verwaltung des Zugangs und die Interoperabilität, damit verschiedene Plattformen so verknüpft werden könnten, dass Innovationsanreize entstehen.[285] Ein Recht auf Datenportabilität ist mithin regulierungsintensiv: Unternehmen müssen weitreichende technische Vorgaben gemacht werden. Sie können für kleine Unternehmen zu einer Marktzutrittsschranke werden. Die Möglichkeit, dass einzelne Wettbewerber eigene Lösungen zur Datenportierung entwickeln und hiermit im Wettbewerb stehen, wird ausgeschlossen.

Nur wenn eine Machtlage im Verhältnis Maschinenhersteller-Maschinennutzer beziehungsweise Diensteanbieter-Dienstenutzer allgemein unterstellt werden könnte, erscheint daher ein Verzicht auf eine entsprechende Eingrenzung des Rechts auf Datenportabilität beziehungsweise eines Datenherstellerrechts naheliegend. Dass eine solche Machtlage generell angenommen werden kann, hat die Kommission allerdings nicht aufgezeigt. Ungleichgewichte in der Verhandlungsmacht sind im B2B-Bereich deutlich weniger naheliegend als im B2C-Bereich. Gerade im B2B-Bereich liegt es nicht fern, dass unternehmerisch tätige Nachfrager bei grundsätzlich funktionsfähigem Wettbewerb zwischen verschiedenen Leistungsanbietern künftige dateninduzierte Lock-in-Gefahren antizipieren und vertraglich bewältigen. Die Einräumung von Datenportabilität würde dann zum Bestandteil des Wettbewerbs zwischen Unternehmen.

Womöglich als Korrektiv für den Verzicht auf ein irgendwie geartetes Machtkriterium geht die Kommission davon aus, dass Maschinenhersteller und Diensteanbieter für die Datenportierung oder –nutzung (anders als bei der Datenportabilität nach Art. 20 DSGVO) ein Entgelt verlangen können. Besteht aber die von der Kommission unterstellte Machtlage in einem konkreten Fall tatsächlich, so ist zu befürchten, dass Maschinenhersteller und Diensteanbieter abschreckende und somit deutlich überhöhte Entgelte wählen werden. Der Verzicht auf ein eingrenzendes Kriterium bei der Begründung des Nutzungsrechts geht damit potentiell mit der Notwendigkeit einher, eine Preishöhenkontrolle einzuführen.

4. Sektorspezifische Datenzugangsregelungen

Die Kommission sieht in ihrer Mitteilung die Probleme und Nachteile allgemeiner Zugangsrechte zu Daten im B2B-Bereich. Sie erwägt daher die Möglichkeit, Datenzugangsrechte sektorspezifisch nur dort

[285] Mitteilung „Aufbau einer europäischen Datenwirtschaft, 10.1.2017, COM(2017)9 fin., S. 17

zu schaffen, wo ein Zugang erforderlich ist, um (potentiellen) Akteuren auf einem Sekundärmarkt den Marktzugang zu eröffnen.[286]

Angesichts der skizzierten Probleme der Schaffung allgemeiner Datenzugangsrechte im B2B-Bereich hat aus Sicht der Autoren dieser Studie – jedenfalls in der näheren Zukunft – ein sektorspezifischer Ansatz tatsächlich erhebliche Vorteile. Ein solcher Ansatz ermöglicht den Akteuren vor allem, die Marktentwicklung und die Wirkungen von Datenzugangsrechten anhand konkreter Beispiele besser zu verstehen und mit verschiedenen Regelungsmodellen zu experimentieren.

H. Zusammenfassende Thesen

1. Maschinendaten wie auch von Nutzern erzeugte Daten sind in der datengetriebenen Ökonomie ein wichtiger Rohstoff. Haben Unternehmen Zugang zu diesem Rohstoff, können diese Daten maßgeblich zu verbesserten Produktions- und Vertriebsabläufen, zur Produktentwicklung und –innovation und zu einem erfolgreicheren Marketing beitragen. Zum gegenwärtigen Stand der Entwicklung ist häufig allerdings nicht der Zugang zu Daten der beschränkende Faktor, sondern die Fähigkeit der Unternehmen, die Daten für die eigenen Zwecke mit einer eigenen Anwendungsidee zu verwerten.

2. Unternehmen, die selbst keinen oder keinen hinreichenden Zugang zu den Daten haben, können versuchen, sich Zugang zu Daten auf „Datenmärkten“ zu beschaffen. Eine Untersuchung von Datenmärkten sollte sich aber nicht von vornherein auf bestimmte Erscheinungsformen von Märkten (z.B. „Sekundärmärkte“ für Daten) verengen. Ein *Zugriff auf Daten* ist entweder über den Primärmarkt möglich – d.h. über eine Erhebung von Daten unmittelbar beim Datenerzeuger, oder über sekundäre Datenmärkte im engeren Sinne, wobei hierbei zwischen durch bilaterale Verhandlungen geprägte Marktbeziehungen und stärker standardisierte Marktbeziehungen (einschließlich solcher, die über Plattformen zustande kommen) unterschieden werden kann. Ferner kommt ein Zugriff über Data Sharing in Betracht. Eine Alternative zum Zugriff auf Daten kann die *Nutzung von Datendienstleistungen* sein (Märkte für Datenderivate). Je nach dem verfolgten Zweck können diese verschiedenen Formen des Datenzugriffs aus Nachfragersicht Substitute sein.

3. In der Analyse der Funktionsweise und möglicher Funktionsdefizite von Datenmärkten ist zwischen Märkten für personenbezogene Daten und Märkten für nicht personenbezogene Daten zu unterscheiden. Die Funktionsweise von Märkten für personenbezogene Daten wird maßgeblich durch das Datenschutzrecht beeinflusst. Wie die DSGVO die Funktionsweise von Primärmärkten beeinflussen wird, auf denen Daten direkt bei den Konsumenten erhoben werden, gilt es dringend zu klären. Es hängt von den Anforderungen ab, welche die DSGVO an die Wirksamkeit der Einwilligung stellt – gerade auch dort, wo Daten als „Entgelt“ fungieren.

[286] EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Brussels, 10.1.2017, SWD(2017)2 fin., S.37: “for certain services, a convincing product and the capacity to create network effects may be more critical than access to data.”

Das Datenschutzrecht schließt im Übrigen auch einen Datenhandel auf Sekundärmärkten nicht gänzlich aus. Ein solcher Datenhandel – wie auch ein Data Sharing – kann aber nur in engen rechtlichen Grenzen stattfinden.

4. Der Zugriff auf *personenbezogene Daten* erfolgt derzeit vor allem über den Primärmarkt – Daten werden im direkten Kontakt mit den Konsumenten gesammelt. Mittelbar profitieren Unternehmen von der Existenz personenbezogener Daten bei der Inanspruchnahme von Datendienstleistungen (z.B. Targeted Advertising), die von besonders „datenreichen" Unternehmen angeboten werden. Schließlich ist auch Data Sharing bei personenbezogenen Daten von Bedeutung. Eine sehr begrenzte Bedeutung hat demgegenüber der Datenhandel im engeren Sinne. Ein Grund hierfür ist das oftmals begrenzte Eigeninteresse „datenreicher" Marktakteure am Handel mit personenbezogenen Daten: Die Daten werden dann als zentraler Wettbewerbsvorteil begriffen. Aber auch das Datenschutzrecht zieht dem Datenhandel im engeren Sinne enge Grenzen (siehe These 3). Die Fortentwicklung eines Datenhandels im engeren Sinne für personenbezogene Daten ist nur unter Einbeziehung der Betroffenen möglich. Betroffene müssten konkret in die Weitergabe an bestimmte Marktakteure einwilligen. Diese kann über Personal Information Management Systeme (PIMS) erfolgen (zum Beispiel Industrial Data Space; MyData) – allerdings ist deren Markterfolg bislang nicht absehbar.

5. Eine praktisch größere Bedeutung für die Gewährleistung des Zugriffs von Unternehmen auf personenbezogene Daten hat die Einführung eines Rechts auf *Datenportabilität* (Art. 20 DSGVO). Es beinhaltet eine Ermächtigung der Betroffenen zur wirtschaftlichen Nutzung der auf sie bezogenen Daten, und erleichtert so den Anbieterwechsel. Spezialgesetzliche Ausformungen der Datenportabilität zum Beispiel im Bereich „Smart Metering" und bei Zahlungsdiensten, zeigen, dass hierin – und nicht im Schutz des Allgemeinen Persönlichkeitsrechts – die eigentliche Funktion der Datenportabilität liegt. Funktional ist das Recht auf Portabilität personenbezogener Daten zugleich als Kompensation für die Schwächung der Sekundärmärkte für personenbezogene Daten durch das Datenschutzrecht zu sehen.

6. Die derzeitige Struktur des Handels mit personenbezogenen Daten (im weiteren Sinne) gewährleistet zwar keine positive Chancengleichheit von Unternehmen im Zugriff auf Daten: Die große Bedeutung des Primärmarktes für den Datenzugriff kann zu einem Wettbewerbsvorteil großer und erfolgreicher Marktakteure führen. Netzwerkeffekte, welche die Konzentration in Plattformmärkten begünstigen, können zugleich zu einer gewissen Konzentration des Datenzugriffs führen. Dieser Wettbewerbsvorteil verhindert aber nach derzeitigem Erkenntnisstand neue Marktzutritte nicht systematisch beziehungsweise führt nicht systematisch zu Marktabschottung. Kleineren Unternehmen sind andere Formen des (unmittelbaren oder mittelbaren) Datenzugriffs möglich.

7. Ein gesetzgeberischer Handlungsbedarf zur allgemeinen Förderung des Handels mit personenbezogenen Daten über den geltenden Rechtsrahmen hinaus ist zurzeit nicht ersichtlich. Sinnvoll wäre allerdings eine Klärung der Voraussetzungen und Grenzen des Datenzugriffs am Primärmarkt. Auch kann in bestimmten Konstellationen eine Anwendung des

Wettbewerbsrechts zu prüfen sein: Im B2B-Bereich gibt es Beschwerden, dass große Plattformen wie Apple und Google den Zugriff von App-Anbietern auf Nutzerdaten behindern beziehungsweise sich den Datenzugriff selbst vorbehalten.[287] Auch Ausschließlichkeitsvereinbarungen bzgl. eines Datenzugriffs unter Beteiligung marktbeherrschender Unternehmen sind kritisch zu prüfen.

8. Auch bei *nicht personenbezogenen Daten* spielt Eigennutzung und vertikale Integration eine große Rolle. Data Sharing spielt dort eine Rolle, wo Unternehmen ein Eigeninteresse an der Zusammenarbeit haben (zum Beispiel autonomes Fahren; Mobility Data; denkbar auch: paralleler Datenzugriff durch Maschinenhersteller und Maschinennutzer). In eingegrenztem Umfang findet ein bilateraler Datenhandel im engeren Sinne statt. Grundlage dieses Handels sind Verträge, die bilateral ausgehandelt werden. Ein Datenhandel über Plattformen findet vor allem mit öffentlichen Daten statt. Wenige Beispiele finden sich dagegen für einen Plattformhandel mit privaten Daten. Dem stehen zwar keine rechtlichen Vorgaben entgegen. Auch ist nicht davon auszugehen, dass fehlende Dateneigentumsrechte einen solchen „Handel" verhindern – denn der Zugriff von „Datenkäufern" auf die Daten, die typischerweise auf dem Server des „Datenverkäufers" verbleiben, kann technisch wirksam verhindert beziehungsweise begrenzt werden. Wie schon bei personenbezogenen Daten, so besteht aber auch bei nicht personenbezogenen Daten ein erhebliches Eigeninteresse der Unternehmen an der Nicht-Weitergabe der Daten und an der Nutzung des exklusiven Datenzugriffs als Wettbewerbsvorteil.

9. Einige wenige Plattformen bieten einen zentralisierten Zugang zu Datensätzen an. Mehrere Faktoren sind für einen Plattformhandel mit Daten förderlich: (a) Bei den Daten handelt es sich um standardisierte Produkte / die Kompatibilität der Daten ist gewährleistet; (b) es bestehen zuverlässige technische Möglichkeiten zur effektiven Begrenzung von Zugriffsmöglichkeiten und zur Sicherung der Daten; und (c) es besteht Vertrauen in die Zuverlässigkeit der Geschäftspartner. Plattformen können zwar diese Faktoren beeinflussen, es ist aber nicht eindeutig, ob eine etwaige Standardisierung von Datenzugängen der Vielfalt der Verwendungsinteressen der Nachfrager entspricht. Es ist auch nicht klar, ob die technischen Sicherungsmöglichkeiten derzeit einem de facto stärker anonymisierten Handel ermöglichen. Jenseits des begrenzten Eigeninteresses vieler datenreicher Unternehmen an einem offenen Handel mit Datensätzen über Plattformen folgen aus diesen spezifischen Anforderungen weitergehende Grenzen für die Bereitstellung von Daten auf Plattformen.

10. In Märkten für nicht personenbezogene Daten lässt sich auf der Grundlage der den Autoren dieser Studie zur Verfügung stehenden Information sektorübergreifend kein systematisches Marktversagen feststellen. Der Fokus auf Eigennutzung und bilateralen Handel beziehungsweise Data Sharing, der derzeit zu beobachten ist, führt nicht zu perfekten Lösungen. Die Transaktionskosten im Datenhandel sind tendenziell hoch. Ein fehlender Datenzugang kann – je nach Kontext – zu Marktzutrittshindernisse führen. Ebenso sind Konstellationen denkbar, in denen neue „Aftermarket"-Probleme entstehen. Diese Probleme sind aber grundsätzlich mit Mitteln des Wettbewerbsrechts zu bewältigen – wobei in

[287] European Innovators Open Letter to the EU Commission on DSM and Platforms, 4 May 2017.

Deutschland neben dem Verbot des Missbrauchs marktbeherrschender Stellungen (Art. 102 AEUV; § 19 GWB) auch das Verbot des Missbrauchs relativer Marktmacht zur Verfügung steht (§ 20 GWB).

11. Neue Eigentumsrechte werden die Funktionsweise der Märkte für nicht personenbezogene Daten voraussichtlich nicht verbessern. Angesichts der Unsicherheiten hinsichtlich des richtigen Zuschnitts und hinsichtlich der richtigen Allokation dieser Rechte sind sie nicht geeignet, die Transaktionskosten in Datenmärkten zu senken. Eigentumsrechte sind ferner von vornherein ungeeignet, Machtungleichgewichten im Markt zu begegnen.

12. Die EU-Kommission erwägt die Schaffung eines neuen *Datenerzeugerrechts*. Dieses Recht muss nicht als Eigentumsrecht gedacht werden. Seine Funktion soll vor allem in der Gewährleistung des Zugangs der Maschinen- beziehungsweise Dienstenutzer zu den Nutzungsdaten liegen. Zwar besteht Grund zur Annahme, dass Maschinenhersteller beziehungsweise Diensteanbieter im Ausgangspunkt regelmäßig eine de facto-Kontrolle über die bei der Maschinen- oder Dienstenutzung anfallenden Nutzungsdaten haben. Das von der Kommission marktmachtunabhängig angenommene Marktversagen in der Gewährleistung eines Datenzugangs der Maschinen- oder Dienstenutzer ist aber bislang nicht hinreichend validiert. Zwar kann ein Interesse an der Offenhaltung etwa von Wartungs- und Mehrwertdienstemärkten und damit auch ein Interesse an Datenzugangs- und Weitergaberechten der Maschinen- oder Dienstenutzer bestehen. Umgekehrt sind aber auch legitime Interessen von Maschinenherstellern und Diensteanbietern an einem exklusiven Datenzugriff denkbar – etwa mit Blick auf Produktsicherheitsbedenken beim Datenzugriff oder mit Blick auf legitime Geheimhaltungsinteressen. Ein allgemeines „Datenerzeugerrecht“ im Sinne eines marktmachtunabhängigen Datenzugangsrechts der Nutzer ist daher nicht opportun. Ausgangspunkt muss die Feststellung einer regelungsbedürftigen Machtlage sein – wobei auch relative Marktmacht zu berücksichtigen ist. Im Übrigen kann es sinnvoll sein, nach der Art der Daten und Verwendungszwecke zu differenzieren. Das Recht auf Datenportabilität bei personenbezogenen Daten (Art. 20 DSGVO) lässt sich schon deswegen nicht pauschal auf nicht personenbezogene Daten übertragen, weil ersteres – jenseits der Bekämpfung von lock-in-Effekten – gerade auch die Schwächung des Datenhandels durch das Datenschutzrecht kompensiert.

13. Ein Data Sharing zwischen Wettbewerbern – ob in Märkten für personenbezogene Daten oder für nicht personenbezogene Daten – darf das *Kartellverbot* nicht verletzen. Die Grenzen des Art. 101 Abs. 1 AEUV / § 1 GWB sind daher im Blick zu halten.