Max-Planck-Institut für Innovation und Wettbewerb

Ausschließlichkeits- und Zugangsrechte an Daten

Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb vom 16. August 2016 zur aktuellen europäischen Debatte

Josef Drexl[*], Reto M. Hilty[*], Luc Desaunettes[**], Franziska Greiner[**], Daria Kim[**], Heiko Richter[**], Gintarė Surblytė[***] und Klaus Wiedemann[**]

I. Einleitende Bemerkungen

1. Der Wirtschaftsverkehr wird zunehmend von der Digitalisierung geprägt. Schlagworte wie „Industrie 4.0“ und „Internet der Dinge“ stehen sinnbildlich für die **datengetriebene Wirtschaft**. Dabei stellen datenbasierte Geschäftsmodelle keinen isoliert zu betrachtenden Industriezweig dar. Vielmehr durchdringt datengetriebenes Handeln heute nahezu alle Bereiche des modernen Wirtschaftslebens.

2. Die Europäische Kommission hat ihre Strategie für einen digitalen Binnenmarkt in Europa (COM(2015) 192 final) zu einem ihrer zehn prioritären Projekte erklärt. Einen der drei Pfeiler dieser Strategieerklärung stellt die „[b]estmögliche Ausschöpfung des Wachstumspotenzials der digitalen Wirtschaft“ dar. Diese soll unter anderem durch eine europäische **Initiative zum „freien Datenfluss“** (*free flow of data initiative*) verwirklicht werden, deren

[*] Prof. Dr., Direktor.
[**] Doktorand/in gefördert durch das MPI / Doktorand/in und wissenschaftl. Mitarbeterin/in am MPI.
[***] Dr. jur., Referentin am MPI.

Veröffentlichung für November 2016 geplant ist. Die Kommission hat angekündigt, dass sie in diesem Rahmen auch auf „die neuen Fragen des Eigentums an Daten, der Interoperabilität, ihrer Nutzbarkeit und des Zugangs zu den Daten in bestimmten Situationen“ eingehen wird. Allerdings verwendet die Kommission keine klar konturierte Definition des Begriffs „Datum“.

3. Das vorliegende Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb ist vor dem Hintergrund dieser Ankündigung und mit Blick auf die in Politik, Wirtschaft und Wissenschaft geführte Diskussion über die Frage nach der Schaffung von **Ausschließlichkeits- bzw. Zugangsrechten an digitalen Daten** entstanden. Es bezieht sich sowohl auf personenbezogene als auch auf nicht personenbezogene Daten. Der Schwerpunkt liegt auf Letzteren.

II. Keine Notwendigkeit für Ausschließlichkeitsrechte an Daten

4. Das Max-Planck-Institut für Innovation und Wettbewerb sieht momentan **weder eine Rechtfertigung noch eine Notwendigkeit, Ausschließlichkeitsrechte an Daten** zu schaffen.

5. Es gibt **keinen Grundsatz**, wonach Rechte an Daten von vornherein einem bestimmten Rechtssubjekt zuzuweisen wären. Weder legitimiert das personenbezogene Datenschutzrecht eine – letztlich ökonomisch motivierte – Kontrolle über die Nutzung der Daten als solche oder auf nachgelagerten Datenmärkten, noch sind Sacheigentümern von Gegenständen, die Daten über Sensoren generieren (z.B. Maschinen oder Alltagsgegenstände wie Fahrzeuge oder Heizkörper), ausschließliche Datennutzungsrechte zuzuweisen.

6. Für eine Zuweisung von Ausschließlichkeitsrechten an Daten sind nach aktuellem Kenntnisstand auch **keine ökonomischen Gründe ersichtlich**. Der damit verbundene Eingriff in die Berufs- und Wettbewerbsfreiheit implizierte vielmehr die Gefahr der Behinderung anderer, auf Daten angewiesener Marktteil-

nehmer sowie negativer Einflüsse auf die Entwicklung nachgelagerter Datenmärkte. Kritisch wären insbesondere die Verfestigung bestehender und die Schaffung neuer Datenmacht, was die Errichtung wettbewerbshemmender Marktzutrittsschranken begünstigen würde. Der drohenden Schaffung von „Informationsmonopolen" muss der Grundsatz der Gemeinfreiheit bloßer Informationen vorgehen. Im Lichte der zu beobachtenden dynamischen Entwicklung der Digitalwirtschaft ist kein generelles Marktversagen erkennbar oder absehbar. Damit bedarf es keiner gesetzgeberischen Anreize für die Datensammlung bzw. -erzeugung, da Daten ohnehin – häufig als Nebenprodukt – produziert werden.

7. Daten sind bereits heute – ohne bestehende Ausschließlichkeitsrechte – regelmäßig **Gegenstand von Transaktionen**. Die betroffenen Unternehmen haben in aller Regel die Möglichkeit, die in ihrem Geschäftsbetrieb angefallenen und aus ihrer Sicht schützenswerten Daten gegenüber Dritten mit technischen Mitteln wirksam abzuschirmen. Diese faktische Exklusivität reicht in der Praxis, um den Zugang zu Daten zum Gegenstand von Verträgen zu machen. Sie bewirkt *inter partes* einen weitreichenden Schutz und gewährleistet den Marktteilnehmern praktikable Handlungsoptionen. Namentlich behält das jeweilige Unternehmen die Kontrolle über „seine" Daten und den jeweiligen Kreis an Zugangsberechtigten. Die Einhaltung vertraglicher Vorgaben lässt sich zudem z.B. mittels Vereinbarung einer Vertragsstrafe für den Fall der unerlaubten Weitergabe von Daten absichern. Auf diese Weise entstehen Märkte auch ohne gesetzliche Ausschließlichkeitsrechte (vergleichbar den Märkten für Übertragungsrechte an Sportveranstaltungen). In dieses etablierte und funktionierende System mittels einer gesetzlichen Zuweisung von Rechten an Daten an Einzelne einzugreifen, verspricht aus ökonomischer Sicht keine Verbesserung der Marktbedingungen. Vielmehr wäre damit das Risiko verbunden, funktionierende Märkte zu stören.

8. Unabhängig von ökonomischen Argumenten würde die Normierung eines Ausschließlichkeitsrechts zahlreiche **praktische Probleme** aufwerfen, die kurzfristig kaum sinnvoll gelöst werden könnten. Zunächst müssten Schutzgegenstand und Schutzumfang eines Ausschließlichkeitsrechts bestimmt werden, womit u.a. die komplexe Frage nach der Definition des Begriffs „Datum“ zu beantworten wäre. Überdies müsste der Regelsetzer die Befugnisse des Schutzrechtsinhabers definieren und konkrete Rechte zuweisen. Letztere Herausforderung ist insbesondere bei mehreren Rechtsträgern schwer zu bewältigen. Aufgrund der vernetzten und arbeitsteiligen Wertschöpfung der datengetriebenen Wirtschaft bestünde damit die Gefahr, durch neue Schutzrechte an Daten Rechtsunsicherheit zu erzeugen. Problematisch wären schließlich die sachgerechte Abwägung der von dem Schutzrecht betroffenen Interessen und die Festlegung von Schutzgrenzen.

III. Keine Notwendigkeit für eine Anpassung des Rechtsschutzes sui-generis von Datenbanken

9. Da eine Zuordnung von Ausschließlichkeitsrechten an einzelnen Daten weder gerechtfertigt noch notwendig ist, sollte der in der Richtlinie 96/9/EG vom 11. März 1996 über den rechtlichen Schutz von Datenbanken verankerte Schutz **sui-generis von Datenbanken** (Art. 7 ff.) auch nicht in diese Richtung ausgeweitet oder uminterpretiert werden.

10. Der Schutz sui-generis von Datenbanken ist schon seiner Konzeption nach **ungeeignet** für einen Schutz einzelner Daten. Er knüpft an die Investitionen an, welche der Datenbankhersteller in die Beschaffung, Überprüfung oder die Darstellung des Datenbankinhalts tätigt. Der EuGH betont für die Auslegung der Datenbank-Richtlinie ihr Ziel, nämlich einen Anreiz für die Einrichtung von Datenbanken zu bereits verfügbaren Informationen zu geben, nicht hingegen für das Erzeugen von neuen Elementen, die später in einer Datenbank zusam-

mengestellt werden können (st. Rspr., erstmals EuGH, GRUR Int. 2005, 247, Rdnr. 31 ff. – *British Horseracing Board Ltd.*). Daher erstreckt sich der Schutz von Investitionen in die Beschaffung von Datenbankinhalten nicht auf die Mittel, die der Datenbankhersteller zur Erzeugung der einzelnen Datenbankelemente einsetzt.

11. Im Zuge der Richtlinienentstehung herrschte Einigkeit darüber, dass die einzelnen Datenbankinhalte keinen Schutz genießen sollen. Vielmehr sollte der Schutz der Datenbank als solcher unabhängig vom immaterialgüterrechtlichen Status ihrer einzelnen Inhalte bestehen (Art. 3 Abs. 2). Gleichwohl bestanden berechtigte Bedenken, ob – gerade im Fall von **Single-Source-Informationen** – sich nicht doch *de facto* ein Schutz der einzelnen Elemente ergeben könne, der in seiner Wirkung an ein Ausschließlichkeitsrecht an den Datenbankinhalten heranreicht. Um dieser Gefahr vorzubeugen, fügte der Richtliniengeber die Wesentlichkeitsschwelle für Entnahmen (Art. 7 Abs. 1) ebenso ein, wie die Evaluationspflicht der Kommission (Art. 16 Abs. 3) und einen mahnenden Verweis auf die Anwendbarkeit der Wettbewerbsvorschriften (vgl. Erwägungsgrund 47).

IV. Keine Notwendigkeit für einen besonderen Schutz von Algorithmen

12. Das Max-Planck-Institut für Innovation und Wettbewerb sieht keine Notwendigkeit dafür, einen eigenständigen Schutz der zur Datenverarbeitung eingesetzten **Algorithmen** zu schaffen (etwa im Rahmen von Big-Data-Analysen).

13. Ein Großteil der technologischen Herausforderungen in der digitalen Wirtschaft bezieht sich auf die Entwicklung von Werkzeugen zur Verarbeitung gesammelter Rohdaten, insbesondere ihrer Filterung und Analyse. Dabei sind die den Verarbeitungsprogrammen zugrunde liegenden Algorithmen *de lege lata* **nicht sonderrechtlich geschützt**.

14. Hingegen sind **konkrete Computerprogramme** für die Verarbeitung von Daten bereits heute durch das Urheberrecht der Mitgliedstaaten in Umsetzung der Richtlinie 2009/24/EG vom 23. April 2009 über den Rechtsschutz von Computerprogrammen geschützt. Dieser Schutz umfasst aber weder die Funktionalität eines Computerprogramms (EuGH, GRUR Int. 2012, 534, Rdnr. 39-41 – *SAS Institute Inc.*) noch den zugrunde liegenden, allgemeinen Algorithmus (hier verstanden als präzise Handlungsanweisung zur schrittweisen Lösung eines Problems, unabhängig von ihrer Ausdrucks- und Darstellungsform, also beispielsweise die Angabe der zur Datenanalyse oder -filterung vorzunehmenden Arbeitsschritte und der heranzuziehenden Kriterien). Dies geht bereits aus Erwägungsgrund 11 der Richtlinie hervor, der klarstellt, dass „die Ideen und Grundsätze, die irgendeinem Element des Programms [...] zugrunde liegen", vom urheberrechtlichen Schutz für Computerprogramme nicht erfasst sein sollen.

15. Ein Computerprogramm „als solches" kann auch **nicht Gegenstand patentrechtlichen Schutzes** sein (Art. 52 Abs. 2 lit. c, Abs. 3 EPÜ). Die dem Programm zugrunde liegende Aufgabe, nämlich die Veredelung von Daten mit Hilfe eines Algorithmus, wird als nichttechnischer Natur eingestuft.

16. **Ein pauschaler Schutz von Funktionalität, abstrakten Problemstellungen und zugrunde liegenden allgemeinen Algorithmen** eines Programms ist auch *de lege ferenda* **abzulehnen**. Ein solcher Schutz bedeutete, allgemeine Lösungsideen bzw. Geschäftsmodelle zu schützen. Ein derartiger Schutz würde die Voraussetzungen für Ausschließlichkeitsrechte auf ein Niveau absenken, das der gesetzgeberischen Grundentscheidung zum geltenden Immaterialgüterrecht widerspräche, wonach abstrakte Methoden, Ideen und Lehren gemeinfrei sein sollen.

17. Zudem drohte sich ein Schutz in zweierlei Hinsicht **negativ auszuwirken**: Erstens führte der Schutz abstrakter Gegenstände zu unnötigen – und im Falle von

Algorithmen zu unzumutbaren – Beeinträchtigungen des Wettbewerbs, ohne dass nach heutigem Kenntnisstand für einen solchen Schutz eine ökonomische Rechtfertigung ersichtlich wäre. Namentlich dürfte die damit einhergehende Monopolisierung von Ideen den technischen Fortschritt und die industrielle Entwicklung behindern (EuGH, GRUR Int. 2012, 534, Rdnr. 40 – *SAS Institute Inc.*). Zweitens ist kaum abzusehen, welche Märkte bzw. Sektoren durch eine solche wettbewerbsbeschränkende Wirkung betroffen wären. Das Aufstellen sachgerechter Regulierungsansätze erscheint dadurch unrealistisch.

V. Handlungsunrecht als Anknüpfungspunkt für Regulierung?

18. Bereits heute missbilligt die Rechtsordnung bestimmte Handlungen (**Handlungsunrecht)**, die für die datengetriebene Wirtschaft relevant sind. Entsprechende Normen sind etwa als „Fairness-Regulierung“ oder als Regulierung zur Bekämpfung von unlauterem Wettbewerb bekannt. Sie schaffen keine ausschließlichen Rechte *erga omnes*, untersagen aber gewisse Handlungen der Marktteilnehmer und ahnden ihre Nichteinhaltung delikts-, ordnungs- oder strafrechtlich.

19. Solche Regulierungsansätze bieten in der datengetriebenen Wirtschaft mehrere **Vorteile**. Insbesondere erlaubt ihre hohe Anwendungsflexibilität, rasche Veränderungen der Wirtschaft zu berücksichtigen. Außerdem unterbleibt die Schaffung von Ausschließlichkeitsrechten an bestimmten Schutzobjekten, wie z.B. Daten, womit der Zugang zu diesen grundsätzlich offen bleibt. Ferner ist eine als Handlungsunrecht ausgestaltete, typischerweise stark von der Rechtspraxis geprägte Regulierung einfacher anzupassen, soweit sie sich als dysfunktional erweisen sollte.

20. Allerdings greift auch eine an das Handlungsunrecht anknüpfende Regulierung in den Wettbewerbsprozess ein. Auch sie bedarf somit der **Rechtfertigung** und

einer entsprechend sorgsamen Analyse der Rahmenbedingungen. Ausgangspunkt bilden muss eine Bestandsaufnahme und eine Bewertung der bestehenden Regulierungen, sowohl auf Ebene der EU als auch der Mitgliedstaaten.

21. In diesem Zusammenhang ist insbesondere die Reichweite der neuen Richtlinie 2016/943/EU vom 8. Juni 2016 zum Schutz von Geschäftsgeheimnissen zu untersuchen. Wo technische Mittel eine faktische Exklusivität an Daten ermöglichen, erlangt der **Schutz von Geschäftsgeheimnissen** höchste praktische Relevanz für Unternehmer. Legt die Richtlinie die Voraussetzungen „für den Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb, rechtswidriger Nutzung und rechtswidriger Offenlegung fest“ (Art. 1 Abs. 1), so ist die entscheidende Frage, ob darunter auch die faktische Exklusivität an den Daten fällt. Im Lichte dieser Unsicherheiten wäre es im Hinblick auf die Umsetzung der Richtlinie durch die nationalen Gesetzgeber von zentraler Bedeutung, dass die EU-Kommission zu solchen Fragen zeitnah Stellung nimmt.

22. Art. 2 Abs. 1 der Richtlinie definiert **Geschäftsgeheimnisse** als „Informationen, die alle nachstehenden Kriterien erfüllen: a) Sie sind in dem Sinne geheim, dass sie 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; b) sie sind von kommerziellem Wert, weil sie geheim sind; c) sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt“.

23. **Einzelne Daten** als Geschäftsgeheimnisse zu werten, erschweren insbesondere die Merkmale des „geheimen Charakters“ sowie des „kommerziellen Werts“. Gesammelte oder abgegriffene Daten sind oftmals öffentlich zugänglich. Sollen etwa Schlaglöcher durch vorbeifahrende Fahrzeuge automatisch erfasst werden, so steht diese Möglichkeit jedem offen; generiert werden also von vornherein

nicht absolut „geheime“ Daten. Damit stellen sich auch Fragen zum kommerziellen Wert solcher Daten. Trotz fehlender Geheimhaltungsmöglichkeit eines Datums dürfte bezogen auf die dahinterstehenden Informationen dann von einem gewissen Wert auszugehen sein, wenn die Generierung des Datums mit spürbaren Kosten verbunden ist.

24. Allgemein zu berücksichtigen ist ferner, dass die Richtlinie **nicht** den Zweck verfolgt, **die datengetriebene Wirtschaft im Besonderen zu regeln**. Sie spricht zwar etwa im zweiten Erwägungsgrund von „Geschäftsdaten wie Informationen über Kunden und Lieferanten“. Es ist aber zweifelhaft, ob durch weite Auslegung solcher Formulierungen *sämtliche* Daten als Geschäftsgeheimnis im Sinne der Richtlinie aufgefasst werden können.

25. Eine Alternative bestünde darin, nicht auf das einzelne Datum abzustellen, sondern auf **Datensets**. Geschäftsgeheimnisse müssen nicht *ex nihilo* auftauchen, um als „geheim“ im Sinne der Richtlinie zu gelten. Eine frei zugängliche Information kann durchaus ebenfalls Bestandteil eines Geschäftsgeheimnisses sein. So können gewisse Informationen über Kunden zwar öffentlich zugänglich sein; gleichwohl können Kundendaten in ihrer Gesamtheit ein Geschäftsgeheimnis darstellen. Art. 2 Abs. 1 der Richtlinie sieht denn auch explizit vor, Informationen müssten „weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile“ geheim sein.

26. Auf den Datenkontext übertragen wäre daraus zu schließen, dass zwar das einzelne Datum kein Geschäftsgeheimnis darstellen mag, wohl aber die (als solche nicht öffentlich zugängliche) **Kombination von Daten bzw. Informationen**. Das gleiche Argument ist auch in Bezug auf den vorausgesetzten kommerziellen Wert einschlägig: Mögen öffentlich zugängliche Daten an sich auch keinen kommerziellen Wert haben, kann deren Kombination gleichwohl ein Wert zukommen und ihrem Inhaber damit einen wettbewerblichen Vorteil verschaffen.

27. Selbst wenn die Richtlinie nicht spezifisch auf eine Regulierung der datengetrieben Wirtschaft abzielen mag, wollte der Gesetzgeber jedenfalls einen **flexiblen Rechtsschutz** schaffen und sicherstellen, dass die Richtlinie an technische bzw. wirtschaftliche Entwicklungen anpassbar bleibt. Nach Erwägungsgrund 14 „ist es wichtig, eine homogene Definition des Begriffs ‚Geschäftsgeheimnis' festzulegen, ohne den vor widerrechtlicher Aneignung zu schützenden Bereich einzuengen".

28. Sollte die Richtlinie zum Schutz von Geschäftsgeheimnissen nicht greifen, wäre zu überlegen, ob gewisse spezifische Formen von „Handlungsunrecht" dahingehend bestehen sollten, dass Marktteilnehmer vor Eingriffen Dritter in ihre unternehmerische Sphäre geschützt werden. Unternehmen können letztlich nur wettbewerbsfähig sein und bleiben, wenn sie über eine gewisse Handlungsautonomie verfügen. Zwar lassen sich Eingriffe Dritter in die Geheimsphäre eines Unternehmens wohl schon nach geltendem Recht einzelner Mitgliedstaaten abwehren; ein vom europäischen Recht vorgegebenes **spezifisches Rechtsschutzregime** wäre aber dann erwägenswert, wenn eine einheitliche Rechtslage im Binnenmarkt anderweitig nicht zu erreichen sein sollte. Bei der Ausgestaltung eines solchen Schutzes müssten Negativanreize zulasten potentieller Investoren allerdings vermieden werden. Insbesondere dürfte ein solcher Sphärenschutz weder auf ein Schutzrecht an Daten als solchen hinauslaufen noch einen legitimen Zugang zu Daten erschweren.

VI. Notwendigkeit, den Zugang zu Daten sicherzustellen

a) Relevanz des Zugangs zu Daten

29. In der digitalen Wirtschaft dürften Konstellationen an Bedeutung gewinnen, in denen gewisse Marktakteure (etwa Startup-Unternehmen, Zulieferer etc.) **keinen Zugang zu Daten** haben, um neue Produkte oder Dienstleistungen zu ent-

wickeln oder zu verbessern, ihnen aber auch die Möglichkeit fehlt, die benötigten Daten selbst zu erzeugen oder zu sammeln. Auf der anderen Seite fehlen den die Daten erzeugenden oder sammelnden Unternehmen in aller Regel die Anreize, solchen (potentiellen) Wettbewerbern Zugang zu ihren Daten zu gewähren.

30. Aus ökonomischer Sicht ist eine **Regulierung von Zugangsmöglichkeiten** dann geboten, wenn ohne einen solchen Eingriff wettbewerbsgetriebene Märkte behindert werden bzw. die Entstehung neuer Märkte unterdrückt wird. Namentlich kann eine unter gewissen Bedingungen erzwungene Zugangsgewährung der Entstehung von Marktmacht entgegenwirken.

31. Das Kartellrecht ist allerdings schon grundsätzlich **kein geeignetes Instrument**, um Zugangsfragen zu Daten systematisch zu lösen (unter 2.). Sollten sich Zugangsprobleme in der Praxis häufen und Zugangsmöglichkeiten als wettbewerbs- bzw. innovationsrelevant erweisen, so wäre es verantwortungslos, die Notwendigkeit einer spezialrechtlichen Zugangsregulierung unter Verweis auf das Kartellrecht zu verneinen. Soweit eine spezielle Zugangsregulierung geboten sein sollte, wirft dies wiederum Folgefragen zur Interoperabilität und Standardisierung der Daten auf (unter 3.).

b) Unzulänglichkeit des Kartellrechts

32. Gestützt auf den **kartellrechtlichen Marktmachtmissbrauchstatbestand** (Art. 102 AEUV) lässt sich Zugang zu Daten nur in Ausnahmefällen erreichen. Vor allem vor dem Hintergrund des kartellrechtlichen Durchsetzungssystems handelt es sich um ein reaktives Instrumentarium *ex post*, dessen restriktiver – und nach wie vor nicht vollkommen klarer – Standard in Bezug auf Zugangsfragen keine systematische, Rechtssicherheit schaffende Vorwirkung entfaltet.

33. Gerade wenn es sich nicht um Wettbewerbsbeeinträchtigungen im Sinne von diskriminierendem Zugang oder der Gewährung von Exklusivität handelt, ist

ein kartellrechtlicher Zugangsanspruch nach Art. 102 AEUV an **sehr enge Voraussetzungen** geknüpft. Problematisch ist schon der Nachweis der marktbeherrschenden Stellung aufgrund der Kontrolle von Daten. Es ist noch keineswegs geklärt, wie Datenmärkte abzugrenzen sind, wenn nicht Zugang zu bestimmten Einzeldaten, sondern zu großen Datensätzen zu Zwecken des Data-Minings begehrt wird, und unter welchen Voraussetzungen verschiedene Datensätze als substituierbar betrachtet werden können. Schwierig ist auch die Feststellung eines Missbrauchs bei der Verweigerung des Datenzugangs.

34. In den Entscheidungen *Magill* (EuGH, GRUR Int. 1995, 490), *IMS Health* (EuGH, GRUR Int. 2004, 644) und *Microsoft* (Beck EuRS 2007, 455432) haben die europäischen Gerichte **fallspezifische Kriterien** aufgestellt: Der Zugangsinteressent muss insbesondere nachweisen, dass die begehrten Daten zur Erstellung eines neuen Produktes bzw. einer neuen Dienstleistung unerlässlich sind und keine anderen Möglichkeiten bestehen, sie selbst zu erzeugen oder anderweitig zu beschaffen. Ferner anerkannte der EuGH grundsätzlich die Möglichkeit einer objektiven Rechtfertigung, den Zugang zu verweigern. Über die Maßstäbe und über die Reichweite der einzelnen Voraussetzungen besteht aber nach wie vor Unklarheit. Zudem ergingen diese Entscheidungen unter der Annahme der Einschlägigkeit von Immaterialgüterrechten, so dass die Klärung ihrer Übertragbarkeit auf schutzfreie Rohdaten noch ausstünde. Vor diesem Hintergrund ist davon auszugehen, dass ein kartellrechtlicher Zugangsanspruch im Kontext der dynamischen, datengetriebenen Wirtschaft nur in Ausnahmekonstellationen durchsetzbar wäre.

35. Die hohe Vielfalt an Geschäftsmodellen und ihre Dynamik in der digitalen Wirtschaft steht denn auch in Kontrast zur notwendigen **Einzelfallbetrachtung** im Kartellrecht. Gerade in der schnelllebigen datengetriebenen Wirtschaft stößt die Anwendbarkeit des Kartellrechts an ihre Grenzen.

36. Daten können insbesondere dann eine Quelle von **Marktmacht** sein, wenn (potentielle) Marktakteure nicht dazu in der Lage sind, die Daten selbst zu sammeln oder anderweitig Zugang zu den Daten zu erhalten. Solche Marktmacht ist aber für sich genommen nicht hinreichend für die Feststellung eines Marktmachtmissbrauchs. Darüber hinaus lässt sich das Vorliegen von Marktmacht aufgrund der Schnelllebigkeit und Dynamik technologiegeprägter Märkte leicht bestreiten. In der Praxis übt die Kommission daher bislang große Zurückhaltung, wenn es darum geht, in solchen Märkten wettbewerbsrechtlich zu intervenieren. Das zeigen etwa die Zusammenschlussfälle *Microsoft/Skype* und *Facebook/Whatsapp*.

37. Zudem ging es bei den einschlägigen Entscheidungen (*Magill*, *IMS Health*, *Microsoft*) um den Zugang zu bestimmten, klar identifizier- und eingrenzbaren Informationen bzw. Daten. Bei Konstellationen im Zusammenhang mit „Big Data" dürfte es hingegen um den Zugang zu Datenmengen gehen, die **deutlich größer** und ihrem Inhalt nach **unbekannt bzw. unbestimmt** sind. Selbst die auf Grundlage der Daten entwickelten Produkte oder Dienstleistungen stehen im Zeitpunkt der Zugangsgewährung noch nicht zwingend fest. Eine Evaluierung der dynamischen Auswirkungen von verweigertem Zugang auf den Wettbewerb ist in solchen Fällen (noch) gar nicht möglich. Dies gilt umso mehr, wenn es um die zukunftsträchtige Bereitstellung von Echtzeitdaten über ein API (*application programming interface*) geht. Derartige Fälle hatte das Kartellrecht bislang noch nicht zu lösen.

38. Eine **effektive Durchsetzung** von Zugangsinteressen durch das Kartellrecht scheitert nicht zuletzt an langen Verfahrensdauern (das Verfahren *Magill* hat 10 Jahre, das Verfahren *Microsoft* hat über 14 Jahre gedauert). Darüber hinaus bringen kartellrechtliche Zugangsansprüche Folgeprobleme mit sich. Insbesondere Verfahrensbeendigungen durch Auflagen und Bedingungen greifen in das dynamische Marktgeschehen ein. Zudem muss ihre Einhaltung überwacht werden.

c) Grundlage und Modalitäten spezieller Zugangsregulierung

39. Eine **spezielle Regulierung des Zugangs zu Rohdaten** kann zum einen darauf abzielen, potentielles Marktversagen zu verhindern, indem sie die Funktionsfähigkeit des Wettbewerbs schützt und dadurch Innovation ermöglicht. Ein Beispiel hierfür bildet die Portabilitätsregelung in Art. 20 der Datenschutz-Grundverordnung (2016/679/EU). Ein entsprechender Regulierungsbedarf kann kontext- bzw. sektorspezifisch bestehen. Zum andern kann eine Zugangsregulierung an das Vorliegen eines öffentlichen Interesses anknüpfen. In jedem Fall besteht aber erheblicher Forschungsbedarf hinsichtlich der Rahmenbedingungen, Rechtfertigungen und Regulierungskonzepte, die ein effektives Zugangsregime zu bewirken vermögen.

40. Klärungsbedarf besteht auch hinsichtlich der **Zugangsmodalitäten** und insbesondere der Formate, in denen entsprechende Daten zugänglich zu machen sind. Es ist zu erwarten, dass sich der Wert von Daten durch Interoperabilität der Formate und Standardisierung steigern lässt. Hier ist auch eine Selbstregulierung durch die betroffenen Akteure denkbar. Die Kommission sollte solche Selbstregulierung durch das Setzen entsprechender Rahmenbedingungen fördern. Ausgangspunkt hierfür können u.a. die kartellrechtlichen Grundsätze zur Beurteilung von Standardisierungsvereinbarungen in den Leitlinien zu horizontalen Kooperationsvereinbarungen sein.