D. Rechtliche Lösungen für erweiterten Zugang

Der Gesetzgeber kann eine Erweiterung des Zugangs auf verschiedenen Ebenen und mit verschiedenen Instrumenten fördern. Im Folgenden werden dazu unterschiedliche Optionen vorgestellt, die auch untereinander kombiniert werden können.

Es bedarf kaum der Erwähnung, dass für neue Regeln grundsätzlich zu verlangen ist, dass diese klar und handhabbar sind. Rechtliche Konflikte um die Auslegung sollten von Anfang an minimiert werden. Das bedeutet auch, dass die Regeln praktisch umsetzbar sein müssen und technische Lösungen stets mitzudenken sind. Die Regeln sollten auch schnell durchsetzbar sein: In der digitalen Welt ist niemandem mit einem Zugangsanspruch nach einem mehrjährigen Gerichtsverfahren gedient. Die Regeln sind darauf ausgerichtet, Handlungsmöglichkeiten zu erweitern. Innovationen sollen incentiviert, nicht erschwert werden.

Auch den Gesetzgebern ist längst offenbar, dass die europäische Datenwirtschaft nicht durch Abschottung oder das Einziehen monopolistischer Zugangsentgelte geschwächt werden darf. Das wäre ein Standortnachteil und würde gerade KMU sowie Verbraucherinnen und Verbraucher in der EU schädigen. Die Europäische Kommission hat 2017 in einer Mitteilung über den „Aufbau einer europäischen Datenwirtschaft“[255] und 2020 in der „Europäischen Datenstrategie“[256] mehrere Maßnahmen vorgeschlagen, um dieser Gefahr vorzubeugen. Genannt wurden 2017 Leitlinien für die gemeinsame Nutzung von Daten, technologische Verbesserungen und Musterverträge. Als gesetzgeberische Maßnahmen wurden Änderungen des Vertragsrechts, Zugangsverpflichtungen im öffentlichen Interesse, das Recht eines Datenerzeugers auf nicht-personenbezogene oder anonymisierte Daten sowie Zugangsverpflichtungen gegen Entgelt angeregt. In der europäischen Datenstrategie wird drei Jahre später der Fokus auf gemeinsame europäische Datenräume in strategisch besonders wichtigen Sektoren gelegt. Die Umsetzung ist bislang defizitär. Allerdings scheinen die struk-

255 Europäische Kommission, Kommunikation „Building a European Data Economy”, 10.1.2017, COM(2017) 9 final.

256 Europäische Kommission, Mitteilung „Eine europäische Datenstrategie“, 19.2.2020, COM(2020) 66 final.

turellen und flächendeckenden Probleme, die hier thematisiert werden, weniger im Blick zu sein als bestimmte Leuchtturmprojekte.

I. Abbau technischer Barrieren

Das Zugangsproblem stellt sich schon gar nicht, wenn es keine technischen Einschränkungen beim Zugang gibt. Es ist daher eine Option, offene Schnittstellen, frei zugängliche Formate oder Standardisierungen zu fördern, sodass das Ausschließungspotenzial geringer wird. Würden beispielsweise alle Smart Homes mit einer gleichartigen, standardisierten Software gesteuert, würde dies allen Handwerkern den Zugang zu diesem Smart Home erleichtern, ohne dass sie zunächst Lizenzverträge mit dem Operator schließen müssten. Eine abgeschwächte, aber weiterhin radikale Lösung wäre eine Verpflichtung für Gatekeeper, bei größeren Anlagen oder Projekten offene Schnittstellen zu gewährleisten, sodass zumindest alle anderen Unternehmen mit eigenen „Werkzeugen" andocken könnten, ohne zuvor einen Lizenzvertrag abschließen zu müssen.

Die Vorstellung ist nicht abwegig: Auch die Werkzeuge mit denen Handwerker klassisch arbeiten, sind zum Teil genormt oder standardisiert, etwa wenn die Schraubwerkzeuge zu Steckschlüsseleinsätzen passen sollen. Normung und Standardisierung schließen nicht aus, dass Einzelne mit abweichenden Anfertigungen spezielle Aufgaben lösen. Volkswirtschaftlich und in der Alltagspraxis erleichtert die Standardisierung aber das Vorgehen. Für den Finanzsektor wurde mit der PSD2-Richtlinie eine offene Schnittstelle verpflichtend eingerichtet, die die Arbeit von FinTech-Unternehmen ermöglicht.

Gerade im Bereich Smart Home zeigt eine Initiative der relevantesten Plattformbetreiber, dass Standardisierung im Grundsatz möglich ist. Apple, Amazon, Google und andere Unternehmen entwickeln einen gemeinsamen quelloffenen Kommunikationsstandard für Smart Home-Geräte. So soll es den Herstellern von Smart Home-Geräten vereinfacht werden, sich in die Systeme der Plattformen einzugliedern.[257] Nach Vorbild dieser Vereinheitlichung ist gleichermaßen denkbar, eine derartige Schnittstelle auch für den Zugriff auf relevante Wartungsinformationen und Protokoll-

257 Apple, Pressemitteilung vom 18.12.2019, abrufbar unter https://www.apple.com/de/newsroom/2019/12/amazon-apple-google-and-the-zigbee-alliance-to-develop-connectivity-standard/.

daten zu gewähren, welche auf den Geräten oder den Plattformen gespeichert sind.

1. Interoperabilität, Portabilität, Standardisierung und Normung

Der Abbau technischer Barrieren bedeutet, dass Interoperabilität, Portabilität und Standardisierung in den relevanten Praxisfeldern gestärkt werden müssen.[258]

- Interoperabilität bedeutet, dass verschiedene Dienste oder Formate bruchlos miteinander verknüpft werden können, also auf technischer Ebene miteinander kommunizieren können, obwohl sie verschiedenen Systemen entspringen.[259]
- Portabilität bedeutet, dass Informationen ohne Schwierigkeiten von einem Gerät oder einer Plattform zu einem/einer anderen mitgenommen werden können.[260]
- Standardisierung bedeutet, dass sich ein bestimmtes technisches Format in einer Branche durchsetzt (ggf. auch auf rein faktischer Basis).[261]
- Normung bedeutet, dass der Standard zur Norm erhoben wird, also im Wege eines offiziellen Vorgangs durch Einigung in einem Normungsgremium durchgesetzt wird.[262]

Allen vier Verfahren ist gemein, dass technische Barrieren reduziert werden. Die Gatekeeping-Problematik wird also technisch gelöst. Das könnte für ein Smart Home beispielsweise funktionieren: Warum sollen nicht Anbieter verschiedener Lösungen sich auf einen Standard einigen, sodass auch Wettbewerb um die besten Anwendungen im Smart Home entstehen kann? Interoperabilität oder gemeinsame Standards sind in der Datenökonomie durchaus bekannt: E-Mails können von einem Anbieter zum anderen zugestellt werden (anders als Messenger-Nachrichten von WhatsApp

258 Europäische Kommission, Kommunikation „Building a European Data Economy", 10.1.2017, COM(2017) 9 final.
259 Vgl. *Wegner*, 28(1) ACM Computing Surveys 1996, S. 285.
260 Vgl. *Engels*, 5(2) Internet Policy Review 2016, S. 3. Siehe auch *Busch*, Der Mittelstand in der Plattformökonomie, WISO Diskurs 8/2019, S. 14; *Gill/Kerber*, Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data, 2020.
261 Vgl. *Blind*, The impact of standardisation and standards on innovation, Nesta Working Paper No. 13/15, S. 6 ff.
262 ZDH, Positionspapier Handwerk und Normung, 2020, S. 2.

zu Signal). Eine Einigung auf solche Standards würde den Zugang erheblich vereinfachen.

Dem entgegengesetzt ist proprietäre, nicht offen zugängliche Software, die nur bei Preisgabe von Schnittstelleninformationen zugänglich ist. Die geschützte Schnittstelle wird dadurch zur Zollstelle für die Zugangsgewährung. Solche Systeme sind durchaus bekannt – und sogar rechtlich sanktioniert: Im Urheberrecht sind abschottende Schutzmaßnahmen anerkannt worden. Das ist für die Entwicklung einer freien Zugangskultur kontraproduktiv. In § 95a UrhG werden technische Schutzmaßnahmen definiert, deren Verletzung verboten ist. Es dürfen auch keine Geräte vertrieben werden, um solche Schutzmaßnahmen zu durchbrechen. Die Regelung, die aus dem Jahr 2003 stammt, sollte etwa den Kopierschutz von CDs sichern. Für die entstehenden IoT-Netzwerke wäre eine entsprechende Regelung, die technische Schutzmaßnahmen positiv sanktioniert, allerdings eine hohe Belastung. Es besteht allerdings auch kein Anlass, für Daten oder Plattformen eine vergleichbare Regel zu schaffen, da sie keine Schöpfungshöhe aufweisen, wie es bei künstlerischen Schutzgütern der Fall sein mag.[263]

2. Rechtliche Einflussmöglichkeiten

Mit den Mitteln des Rechts kann der Abbau technischer Schranken incentiviert werden. In der Europäischen Union wurde beispielsweise mit der INSPIRE-Richtlinie 2007/2/EG versucht, Geodaten dadurch zu standardisieren, dass für Geodaten des öffentlichen Sektors Konformitätsregeln erlassen wurden.[264]

Hoheitsträger können sich auch an privaten Normungsinitiativen beteiligen, diese fördern oder ihre Vorgaben in Rechtsakten verwenden. Die private Non-profit-Initiative OASIS Open beispielsweise setzt sich unter Beteiligung führender IT-Unternehmen, aber auch von Regierungsstellen dafür ein, offene Standards zu definieren und nicht-proprietären Code zu entwickeln, sodass technische Barrieren gering sind.[265] Beispiele für OASIS-Entwicklungen sind der freie Dokumentenstandard OpenDocument,

263 Software könnte ggf. urheberrechtlich geschützt sein, siehe Kap. B.I.2. Ggf. wäre eine Schranke vorzusehen, um Beeinträchtigungen des freien Zugangs durch urheberrechtliche Abschottungsmechanismen aufzubrechen.

264 Vgl. die Liste der Rechtsakte bezüglich der INSPIRE-Rahmenbedingungen unter: https://inspire.ec.europa.eu/inspire-directive/2.

265 OASIS steht für Organization for the Advancement of Structured Information Standards, vgl. https://www.oasis-open.org/.

der Standard TOSCA für Cloud-Operationen oder das Kommunikationsprotokoll MQTT, das als Standard für die Kommunikation zwischen IoT-Geräten genutzt wird und als ISO-Standard registriert ist.[266] Für derartige Standards ist der Code frei lesbar. Soweit Lizenzierungen erforderlich sind, haben sich die Unternehmen dazu verpflichtet, zu RAND-Bedingungen (reasonable and non-discriminatory) zu lizenzieren. Die Standards, die von OASIS gesetzt werden, können durch Normung in das hoheitliche Regelungsvokabular überführt werden. Dies kann auch dadurch geschehen, dass bestimmte Standards als Sorgfaltspflichten im Rahmen von Haftungstatbeständen anerkannt werden.[267]

Hoheitliche Interventionen können auch vorsehen, dass gerade keine Zugangsschranken errichtet werden dürfen, sondern dass Schnittstellen offen sein müssen. Damit wäre ein regulatorischer Ansatz geschaffen, wie er in einigen Sektoren bereits verwirklicht wurde, z.B. bei der PSD2-Richtlinie im Finanzsektor. Dies führt mittelfristig zu programmiertem Zugang: So lässt es sich bezeichnen, wenn bereits in der Programmierung zu Beginn des Prozesses eine Zugangslösung eingebaut wird, die offen zugänglich ist. Eine Zulassung wichtiger smarter Hubs könnte dann davon abhängig gemacht werden, dass die Schnittstellen offen sind oder wenigstens Zugangsmöglichkeiten hinterlegt sind.

Die Entwicklung interoperabler Formate und Standards liegt typischerweise nicht in den Händen eines hoheitlichen Gesetzgebers, sondern wird weitgehend der Selbstregulierung der Industrie überlassen und vom Gesetzgeber sodann nur für verbindlich erklärt. Finden derartige Aushandlungsprozesse statt, ist es essentiell, dass Vertreter aller Gruppen beteiligt werden, die in der Zukunft ggf. betroffen sind. Initiativen, in denen allein Gatekeeper vertreten sind oder die unter Ausschluss des Handwerks beraten, werden keine Lösungen finden, die die spezifischen Interessen des Handwerks berücksichtigen. Hier kann es z.B. für Handwerksunternehmen darauf ankommen, dass die Lösungen auch für KMU einfach zugänglich sind, dass Reparatur- und Wartungsfragen von vornherein berücksichtigt werden, dass kein hoher bürokratischer Aufwand durch Registrierung, Dokumentation oder ähnliches entsteht, den sich kleinere Unternehmen nicht erlauben können, oder dass individuelle Materiallösungen berücksichtigt werden können.

266 Siehe https://www.iso.org/standard/69466.html.
267 Vgl. *Wagner* in MüKo-BGB, Band 7, 8. Auflage 2020, § 823 BGB Rn. 489.

3. Vor- und Nachteile des Abbaus technischer Schranken

Die Vorteile technischer Lösungen liegen nicht nur darin, dass Handwerksbetriebe vereinfachten Zugang erhalten. Eine Standardisierung ermöglicht, dass die Kosten für unterschiedliche technische Lösungen, die sonst ggf. erforderlich sind, um Daten bei verschiedenen Anbietern auszulesen, gesenkt werden. Das Spektrum potentieller Arbeitsfelder wird ausgeweitet, weil Hürden wegfallen. Dadurch kann effizienter angeboten werden. Auch der Wettbewerb zwischen Anbietern wird hierdurch verbessert: Wenn alle Unternehmen die Leistung erbringen können, ohne von der Zugriffsgewährung abhängig zu sein, entsteht damit auf ihrer Ebene wieder ein Leistungs- und Qualitätswettbewerb, der sich auf andere Aspekte fokussieren kann und damit die Leistung steigern wird.

Mit einer Öffnung der Schnittstellen können freilich auch Gefahren einhergehen. Standardisierung birgt immer die Gefahr, dass überlegene technische Lösungen sich nicht mehr am Markt durchsetzen können, weil die Wechselkosten von einem Standard weg zu einem neuen Format zu hoch sind. Standardisierung kann so zur Zementierung eines minderwertigen oder überkommenen Zustands führen.[268] Zudem ist nicht ausgeschlossen, dass die Standardsetzung einzelnen Unternehmen in die Hände spielt und andere erheblich benachteiligt, die zuvor möglicherweise in ein anderes System investiert haben.

Offene Schnittstellen und Interoperabilität können auch zum Auslesen von Daten führen, die nicht offengelegt werden sollten. Schließlich kann Portabilität dazu führen, dass opportunistisches Verhalten von Marktteilnehmern so stark wird, dass negative Wirkungen entstehen. Investitionen sind schwieriger zu kalkulieren, wenn es keine Möglichkeit gibt, Kunden langfristig technisch zu binden.

Der Standard muss weiterentwickelt und abgesichert werden, auch das verursacht Kosten, für die im Zweifel mangels Gewinnaussichten kein Unternehmen aufkommen mag.

Trotz dieser Nachteile überwiegen in der spezifischen Situation des Handwerks 4.0 die Vorteile: Offene Schnittstellen und Interoperabilität würden den Einflussbereich der digitalen Gatekeeper zurückdrängen. Voraussetzung für das Funktionieren derartiger Systeme ist aber, dass eine Governance-Architektur geschaffen wird, die sicherstellt, dass die offenen Schnittstellen nicht einseitig zugunsten bestimmter Marktteilnehmer ausgestaltet und die technischen Lösungen weiterentwickelt werden.

---

268 Vgl. TT-GVO-Leitlinien, EU-Kommission, 2014/C 89/03, Rn. 180.

II. Konsensuale Lösungen

Immer wieder wird es zu Verträgen zwischen verschiedenen Parteien kommen müssen, z.B. Gatekeepern und Handwerkern. Wenn diese eine für beide Seiten zufriedenstellende vertragliche Lösung finden, ohne dass es eines hoheitlichen Eingriffs bedarf, ist das eine vorzugswürdige Lösung. Solche konsensualen Vorgehensweisen können durch die Rechtsordnung incentiviert werden. Als „Marktlösungen" sind sie häufig effizient.[269] Demgegenüber besteht bei zu harten hoheitlichen Eingriffen die Gefahr, dass Innovationen gehemmt werden.

1. Selbstregulierung

Anreize zum Vertragsschluss können sich aus einer (staatlich geförderten oder geforderten) Selbstregulierung der Marktakteure ergeben. Dass eine Selbstregulierung des Marktes gegenüber staatlicher Regulierung alleine schon aus grundrechtlicher Sicht grundsätzlich zu befürworten ist, liegt auf der Hand. Einige Stimmen in der Wissenschaft bevorzugen die Erleichterung von freiwilligem Datentausch gegenüber gesetzlichen Zugangsansprüchen, zumindest zum jetzigen Zeitpunkt.[270] Eine Selbstregulierung der Industrie kann durch freiwillige Maßnahmen wie Selbstverpflichtungen oder Codes of Conduct realisiert werden. Dadurch können Anreize zum Datenteilen geschaffen und Transaktionskosten gesenkt werden.[271] Damit kann zudem größere Transparenz geschaffen werden, was insbesondere neuen Marktteilnehmern zugutekommt, denen die Branchenstandards bisher nicht bekannt sind.[272]

a) Beispiel Automobilwirtschaft

Die Entwicklungen in der Automobilwirtschaft stehen dafür beispielhaft. Das Problem, dass Daten in vernetzten Fahrzeugen vielfach erhoben wer-

269 *Schweitzer/Welker*, A legal framework for access to data – a competition policy perspective, 2020, S. 6.
270 Siehe etwa *Schlinkert*, ZRP 2017, 222, 224; *Richter/Slowinski*, IIC 2019, 4, 17; *Staudenmayer*, IWRZ 2020, 147, 154.
271 *Richter/Slowinski*, IIC 2019, 4, 18.
272 *Richter/Slowinski*, IIC 2019, 4, 18.

den und Zugang dazu für zahlreiche wirtschaftliche Tätigkeiten unerlässlich ist, ist bereits bekannt. In Verhandlungen, die im Wesentlichen in Brüssel geführt werden, werden Data-Governance-Modelle entwickelt und durchgesetzt, durch welche Zugriffsrechte verteilt werden.[273] Modellhaft stehen diese Prozesse für die Themen, die eine IoT-Wirtschaft lösen muss. In die Verhandlungen schalten sich auch Verbände ein, die beispielsweise Autowerkstätten repräsentieren, also die sog. Aftermarkets im Blick haben.[274]

Die erste Erkenntnis aus diesem Prozess der geförderten Selbstregulierung ist, dass sehr frühzeitig die Weichen für den zukünftigen geschäftlichen Erfolg gestellt werden. Es sind schon die ersten Programmierungen, an denen sich das Schicksal ganzer Branchen entscheiden kann. Die Pfadabhängigkeit, die durch technische Vorfragen ausgelöst werden kann, ist enorm.

In den Verhandlungen zeigt sich auch, wie wichtig eine Beteiligung der relevanten Kreise ist, damit nicht einzelne Stakeholder ihre Interessen absprechen und durchsetzen können. In den Diskussionen um connected cars sind es zunächst die Automobilhersteller, die die Agenda setzen können. Kleinere und mittlere Unternehmen, zudem wenn sie auf nachgelagerten Märkten tätig sind, die zunächst nicht im Blickpunkt stehen, haben häufig geringere Verhandlungsmacht, sodass die Organisatoren und Vermittler entsprechender Gespräche, z.B. aus dem politischen Raum, ihre Belange besonders stützen müssen.

Die Lösung für die Zuordnungsprobleme im vernetzten Auto wird überwiegend in Datenplattformen gesucht. Entscheidend wird die technische Ausgestaltung solcher zentraler Daten-Hubs.

Leitprinzipien für die rechtliche Gestaltung werden nur selten explizit formuliert. Es muss aber darum gehen, einen freien und fairen Leistungswettbewerb zu ermöglichen und die Konsumentensouveränität zu wahren. Das bedeutet: Alle Unternehmen müssen in der Lage sein, ihre Leistungen am Markt anzubieten. Marktzutrittsschranken dürfen nicht entstehen, Abhängigkeiten dürfen nicht in unfairer Weise ausgenutzt werden. Am Ende sollen es die Verbraucher sein, die über Erfolg oder Misserfolg der Unter-

273 Siehe *Specht/Kerber*, Datenrechte, 2017, S. 163 ff.; *Kerber/Gill*, JIPITEC 10 (2019), 244 ff.; *Kerber*, JCLE 15(4) 2019, 381 ff., *Falkhofen*, CRi 2018, 165 ff.

274 Siehe beispielhaft das Papier der Verbände ADPA, AIRC, CECRA, EGEA, ETRma, FIA, FIGIEFA und Leaseurope, Secure On-board Telematics Platform Approach, Feb. 2021.

nehmen entscheiden, nicht digitale Gatekeeper, die sich zu Beginn des Verteilungsprozesses geschickt die „Pole Position" gesichert haben.

Eine Vorbedingung dafür ist, dass die Plattform zur Sammlung der Daten, zu ihrem Austausch und zu ihrer Bereitstellung technisch neutral und für alle zugänglich gestaltet wird. Ein unabhängiger Betreiber würde dies am ehesten garantieren können. Die Pläne der Autohersteller würden diesen hingegen eine Gatekeeper-Position bescheren – Kritiker sprechen von „control by technical design".[275]

Gerade für kleinere Unternehmen muss dann aber auch faktisch ein einfacher Zugang gewährleistet werden. Die Möglichkeit, Rohdaten abzufragen, ist im Zweifel nicht zielführend. Hier sind eigene Anstrengungen des Handwerks notwendig. Unabhängige Dienstleister, die ggf. Anwendungen entwickeln, die an offene Schnittstellen angeschlossen werden können, können unterstützen.

Die datenschutzrechtliche Einwilligung, die ggf. einzuholen ist (typischerweise wohl vom Autohersteller/-verkäufer), muss die Interessen der übrigen Unternehmen wahren und darf nicht zum Marktausschluss missbraucht werden. In der Folge stellen sich Haftungs- und Vergütungsfragen. Das Ausarbeiten sämtlicher Details wird im Vorfeld kaum gelingen. Wichtig ist daher die Bereitstellung eines Governance Boards und Streitschlichtungsmechanismus. Der Fortgang der Diskussionen im Automobilsektor wird weitere Elemente, die einer (Selbst-)Regulierung bedürfen, erkennen lassen.

b) Vorbild FRAND-Lizenz?

Ein etabliertes Beispiel für Selbstregulierung sind die Selbstverpflichtungen von Patentinhabern, die im Rahmen von Standardisierungsverfahren typischerweise angeben, ihre standardessentiellen Patente zu FRAND-Bedingungen zu lizenzieren.[276] Standardisierungs- oder Normierungsvorhaben sind im Hinblick auf das Kartellverbot aus Art. 101 Abs. 1 AEUV grds. unproblematisch.[277] Die Bedingungen dieses Zugangs müssen „fair, rea-

275 ADPA/AIRC u.a., Secure On-board Telematics Platform Approach, Feb. 2021, S. 3.

276 Vgl. für den Telekommunikationssektor ETSI, Rules of Procedure Annex 6: ETSI Intellectual Property Rights Policy, 2020, abrufbar unter: https://www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf, Rn. 6.1. ff.

277 Vgl. Kommission, Leitlinien zur Anwendbarkeit von Artikel 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über hori-

sonable and non-discriminatory" (FRAND) sein.[278] Im Streitfall stellt sich die Frage, welche Bedingungen denn im Einzelfall „FRAND" sind. Dies müssen die Parteien selbst aushandeln.[279] Ob ein Vertragsangebot FRAND-gemäß ist, ist von den Gerichten vollumfänglich überprüfbar.[280]

Könnte sich ein ähnliches Verfahren, wie es sich etwa für die Telekommunikationsbranche ergeben hat, für die Zusammenarbeit in datengetriebenen Wertschöpfungsnetzwerken unter Beteiligung des Handwerks ergeben?

Der Vergleichbarkeit könnte zunächst entgegenstehen, dass an Daten, anders als an Patenten, keine (unmittelbaren) Ausschließlichkeitsrechte bestehen (siehe dazu oben B.I). In den Grenzen bestehender sonstiger Gesetze (etwa des GeschGehG) können Daten also von jedem verwendet werden. Problematisch ist die Erlangung der Daten. Bei Patenten ist es umgekehrt gerade so, dass diese allgemein zugänglich sind, aber aufgrund von Ausschließlichkeitsrechten nicht frei genutzt werden können. Dass bei Daten kein rechtliches Monopol besteht, ändert aber nichts daran, dass tatsächlich dennoch eine Lizenzierung erfolgen muss. Der Inhaber von Daten hat nämlich in der Regel aufgrund technischer Schutzmaßnahmen als einziger Zugriff auf diese und damit ein faktisches Monopol.[281] Dritte bedürfen hier also in vergleichbarer Weise einer Lizenzierung. Das Fehlen von Ausschließlichkeitsrechten steht der Vergleichbarkeit folglich nicht entgegen.

Dennoch bleibt zweifelhaft, dass es ohne Eingriffe des Gesetzgebers branchenübergreifend zu einer Einigung auf bestimmte Vergütungskonzepte kommen würde. Dabei ist die FRAND-Vergütung hier nur ein Beispiel für eine mögliche Regelung. Derartige Modelle wie FRAND könnten sich auch für die Art der Datenbereitstellung, ihren Umfang, die Sicherheitsmaßnahmen und andere typische Regelungsfragen ergeben.

Das FRAND-Konzept wurde allerdings im spezifischen Governance-Kontext von Standardisierungsorganisationen geschaffen, an denen alle beteiligten Unternehmen ein Eigeninteresse hatten, da sie in der Regel eben-

---

zontale Zusammenarbeit, 2011, abrufbar unter: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:011:0001:0072:DE:PDF, Rn. 277 ff.

278 Vgl. für den Telekommunikationssektor ETSI, Rules of Procedure Annex 6: ETSI Intellectual Property Rights Policy, 2020, abrufbar unter: https://www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf, Rn. 6.1.

279 BGH, 5.5.2020, Az. KZR 36/17, GRUR 2020, 961, 969.

280 Vgl. OLG Karlsruhe, 8.9.2016, Az. 6 U 58/16, BeckRS 2016, 17467, Rz. 36; OLG Düsseldorf, 17.11.2016, Az. I-15 U 66/15, BeckRS 2016, 21067, Rz. 14 ff.

281 *Schur*, Die Lizenzierung von Daten, 2020, S. 139.

so abhängig waren von Patenten anderer wie diese von ihnen.[282] Für Daten gilt das nicht in vergleichbarer Weise. Weder gibt es Standardisierungsorganisationen, die sich sektorenübergreifend um derartige Themen kümmern würde, noch besteht bei Gatekeepern ein vergleichbares Interesse am Austausch wie bei der Marktgegenseite. FRAND-Selbstverpflichtungen werden von den Patentinhabern abgegeben, weil andernfalls ihre Produkte nicht zum Standard werden und sie im Zweifel keinen Zugriff auf die von anderen geschützten Standards haben. Die Selbstregulierung bei standardessenziellen Patenten beruht also nicht auf dem guten Willen der Patentinhaber, sondern auf ihren wirtschaftlichen Überlegungen. Bei Patenten werden die Inhaber für die Freigabe einer gesicherten Rechtsposition entlohnt. Die Entlohnung für Daten, an denen kein „Dateneigentum" o.ä. besteht, würde geringer ausfallen können. Abgegolten werden muss nur der Aufwand der Datensammlung, nicht der Wert der Information an sich.

Eine vergleichbare Situation, sowohl materiell (wirtschaftlicher Zwang der Gatekeeper) als auch institutionell (Selbstregulierungsorganisationen), müsste zunächst künstlich herbeigeführt werden, indem den Gatekeepern Pflichten auferlegt werden und eine institutionelle Data Governance-Struktur geschaffen wird.[283]

c) Sonstige Selbstverpflichtungen

Selbstregulatorische Ansätze sind dennoch denkbar. Ein Anfang würde bereits gemacht, wenn Handwerksunternehmen untereinander und mit wichtigen Industriepartnern, also horizontal und vertikal, bestimmte Standards setzen oder Selbstverpflichtungen abgeben. Denn auch das Handwerk kann, mit seiner gebündelten Macht, durchaus ein wichtiger Impulsgeber für Selbstverpflichtungen werden. Codes of Conduct könnten diejenigen, die sich an solche Kodizes binden, gegenseitig berechtigen und verpflichten, bestimmte Zugangsoptionen einander offenzuhalten und keine Abschottungsstrategien zu betreiben. Ein Einschreiten des Gesetzgebers zur Incentivierung solcher Selbstverpflichtungen ist allerdings nicht angezeigt. Der entsprechende Impuls müsste ggf. aus den Branchen selbst kommen.

---

282 *Richter/Slowinski*, IIC 2019, 4, 22.
283 Zu beiden Aspekten siehe unten.

d) Aufbau kollektiver Gegenmacht

Die Zusammenarbeit ist nicht nur wichtig für die Setzung von Standards. Sie kann auch dem Aufbau einer gewissen Verhandlungsmacht gegenüber Gatekeepern dienen. Einzelne Handwerksunternehmen werden in der Verhandlungssituation mit mächtigen Digitalunternehmen stets überfordert sein und lediglich die vorgelegten AGB akzeptieren. Das wird für viele Handwerker sogar im Zusammenspiel mit wichtigen Herstellern gelten. In diesen Situationen sollte eine Bündelung von Verhandlungsmacht ermöglicht werden. Das „collective bargaining", wie bei Arbeitnehmern, die kollektiv Tarifabschlüsse treffen, würde den Plattformbetreibern die Möglichkeit nehmen, ihre Macht einseitig auszuspielen. Hierfür ist eine Anpassung des Kartellrechts erforderlich, die derzeit auch erwogen wird.[284]

2. Datenschuldrecht

Aushandlungsmodelle für Zugang bleiben dominant – immer wird es zu Vereinbarungen zwischen Plattformbetreibern und Gatekeepern kommen.[285] Der Gesetzgeber könnte dabei den breiteren Austausch von Daten durch die Anpassung privatrechtlicher Regelungen und die Unterstützung bestimmter Regeln fördern. Es geht dabei darum, wie die Freigabe von Daten vertraglich ausgestaltet sein soll. Bei der Schaffung eines „Datenschuldrechts" handelt es sich um eine grundrechtsschonende Regulierungsoption, da damit keine zwangsweisen Eingriffe geschaffen werden. Vielmehr kann das freiwillige Teilen von Daten erleichtert und damit gefördert werden. Bislang gibt es jedoch kaum Märkte für den freiwilligen Austausch von Maschinendaten.[286] Solche Märkte kann der Gesetzgeber schaffen oder jedenfalls fördern.

---

284 Europäische Kommission, Initiative „Collective bargaining agreements for self-employed", Inception Impact Assessment, 6.1.2021. Vgl. schon die Diskussionen in Giesen/Junker/Reichold/Rieble (Hrsg.), Kartellrecht und Arbeitsmarkt, 2010; *Bayreuther*, Sicherung der Leistungsbedingungen von (Solo-)Selbständigen, Crowdworkern und anderen Plattformbeschäftigten, 2018; Authority for Consumers and Markets [ACM, Niederlande], Guidelines: Price arrangements between self-employed workers, 2020.

285 *Fries/Scheufen*, MMR 2019, 721.

286 *Schweitzer/Welker*, A legal framework for access to data – a competition policy perspective, 2020, S. 6.

Ein Datenaustausch auf freiwilliger Basis ist insbesondere dann attraktiv, wenn nur geringe Transaktionskosten bestehen. Die Veränderung der vertragsrechtlichen Regelungen kann den Aufwand für den Datenaustausch reduzieren.[287] Auf europäischer Ebene ist in der Verordnung (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union ein erster Ansatz zur Förderung des freiwilligen Datenaustauschs zu finden.

Viele der hier zu behandelnden Fragen sind aber nicht nur im Rahmen freiwilliger Datenfreigabe, sondern auch bei Existenz eines gesetzlichen Zugangsanspruchs relevant.[288] Es ist davon auszugehen, dass auch ein gesetzlicher Zugangsanspruch nicht sämtliche Modalitäten des Datenaustauschs abschließend regeln wird, sondern lediglich der erste Schritt in einem Prozess ist, in dem weitere Fragen zu klären sind, die dann der Aushandlung bedürfen. Beim Kontrahierungszwang wird der Dateninhaber in der Regel zum Abschluss eines Vertrags zu angemessenen Bedingungen verpflichtet, die aber im Einzelnen nicht vorgegeben werden, so dass sich auch dann die Frage stellt, wie das Vertragsverhältnis konkret auszugestalten ist.[289] Nach dem Grundsatz der Privatautonomie sind Unternehmen bereits jetzt in der Lage, Verträge über Daten völlig frei auszugestalten. Mit dieser Gestaltungsmöglichkeit geht aber Rechtsunsicherheit einher.[290] Eines der größten Hindernisse für den vertraglichen Austausch von Daten sind hohe Kosten für die notwendige Rechtsberatung.[291]

Die Grenzen dieser Vertragsfreiheit ergeben sich aus zwingendem Recht, wobei in der Praxis vor allem bei Verwendung von Allgemeinen Geschäftsbedingungen (AGB) die Regeln der §§ 305 ff. BGB zu beachten sein dürften.

---

287 *Staudenmayer*, IWRZ 2020, 147; *Schur*, Die Lizenzierung von Daten, 2020, S. 293.

288 Vgl. *Schweitzer/Welker*, A legal framework for access to data – a competition policy perspective, 2020, S. 7.

289 So auch im Falle eines kartellrechtlich begründeten Kontrahierungszwangs im Rahmen der sog. essential-facilities-Doktrin, vgl. *Fuchs* in: Immenga/Mestmäcker, Wettbewerbsrecht, Band 1, 6. Auflage 2019, Art. 102 AEUV, Rn. 333.

290 *Fries/Scheufen*, MMR 2019, 721.

291 Europäische Kommission/Deloitte, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, 2018, S. 72 f.

a) Regelungsgegenstand

In Verträgen wird – nach der grundsätzlichen Einigung auf das Ob – vor allem das Wie des Zugangs ausgestaltet. Dabei geht es insbesondere um folgende Fragen: Vergütung/Entgelt, wie Zugang gewährt wird, wie Daten zu sichern sind, ob die Daten zu anderen Zwecken weiterverarbeitet oder ob sie weiterverkauft werden dürfen, ob das Nutzungsrecht zeitlich befristet ist sowie Gewährleistungs- und Haftungsfragen.[292]

Der Nutzungszweck der Daten wird typischerweise möglichst stark beschränkt. Dies führt dazu, dass jedes Mal, wenn die Daten für noch einen anderen Zweck genutzt werden sollen, neue Vertragsverhandlungen erforderlich sind.[293]

Vertragsverletzungen werden in der Regel über Vertragsstrafen sanktioniert, da die hohen Nachweisanforderungen des Schadensrechts für den Datenhandel ungeeignet sind.[294]

b) Derzeit maßgebliche Vorschriften und deren Probleme

Es gibt derzeit nur lückenhaft Vorschriften, die auf Verträge über Daten anwendbar sind.[295] Die für sämtliche Verträge geltenden Vorschriften des allgemeinen Schuldrechts lassen sich teilweise nur mit großer Transferleistung auf die auftretenden Sachverhalte anwenden. Dies führt zu Rechtsunsicherheit.

aa) Rechtliche Einordnung von Datenverträgen

Drei Konstellationen von Datenverträgen lassen sich unterscheiden:

In der ersten gewährt der Dateninhaber einem Dritten Zugang zu einem bereits vorhandenen Datensatz oder fortlaufend Zugang zu Daten, die in diesem Moment generiert werden. Dies können z.B. Rohdaten eines Sen-

292 Vgl. *Fries/Scheufen*, MMR 2019, 721, 724; vgl. auch Europäische Kommission/Deloitte, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, 2018, S. 73.

293 Europäische Kommission/Deloitte, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, 2018, S. 80.

294 *Fries/Scheufen*, MMR 2019, 721, 724.

295 *Fries/Scheufen*, MMR 2019, 721. Vgl. *Metzger* in: BMJV/MPI, Data Access, Consumer Interests and Public Welfare, 2021, S. 287 ff.

sors an einer Maschine sein. Der Dritte kann diese Daten dann dauerhaft frei und zu jedem Zweck verwenden. Dieses Vertragsverhältnis soll als Datenzugangsvertrag bezeichnet werden.

In der zweiten Konstellation gewährt der Dateninhaber die Daten lediglich zu einem vorher bestimmten Zweck oder zeitlich befristet. Der Dateninhaber behält damit die Kontrolle über die Daten und kann ihren Wert erhalten.[296] Dies wird nachfolgend als Datenlizenzvertrag bezeichnet.[297]

Die Abgrenzung zwischen diesen beiden Verträgen erfolgt maßgeblich danach, ob der Erwerber dauerhaften Zugriff auf die Daten erhält, oder ob die Nutzungsmöglichkeit nur vorübergehender Natur ist.[298]

In der dritten Konstellation geht es um die Fälle, in denen Unternehmen eine bestimmte Software benötigen, um auf einem nachgelagerten Markt tätig werden zu können. Diese Verträge sollen hier als Softwareverträge bezeichnet werden.

(1) Einordnung des Datenzugangsvertrags

Der Datenzugangsvertrag kann in der Regel als (Rechts-)Kaufvertrag i.S.d. §§ 453, 433 BGB qualifiziert werden.[299]

Kaufverträge zeichnen sich durch die Übergabe und Übereignung körperlicher Gegenstände i.S.d. § 90 BGB oder, beim Rechtskaufvertrag nach § 453 BGB, durch die Übertragung von Rechten oder sonstigen Gegenständen aus. Sonstige Gegenstände i.S.d. § 453 Abs. 1 BGB können auch unkörperliche Objekte wie Know-How, Ideen, nicht geschützte Erfindungen oder eben Daten sein.[300] Der Einordnung als Kaufvertrag steht nicht entgegen, dass der Verkäufer ebenfalls weiterhin Zugriff auf die Daten hat.[301] Unbeachtlich ist auch, ob der Verkäufer die Daten an den Käufer übermit-

296 *Schur*, GRUR 2020, 1142, 1143.
297 So auch *Schur*, GRUR 2020, 1142, 1143.
298 *Schur*, Die Lizenzierung von Daten, 2020, S. 169.
299 Vgl. *Hilbig*, ITRB 2007, 170; *Hauck*, NJW 2014, 3616; *Hoeren/Pinelli*, JZ 2020, 879, 880; *Schur*, Die Lizenzierung von Daten, 2020, S. 169 f.
300 Vgl. OLG Düsseldorf, 17.2.2010, Az. I-17 U 167/09, BeckRS 2010, 9514; *Beckmann* in: Staudinger-BGB, Neubearbeitung 2013, § 453 BGB Rn. 37. Vgl. auch OLG Brandenburg, 10.1.2013, Az. 5 U 54/11, BeckRS 2013, 1597; *Westermann* in: MüKo-BGB, Band 4, 8. Auflage 2019, § 453 BGB Rn. 6; *Faust* in: BeckOK-BGB, 56. Edition 2020, § 453 BGB Rn. 24.
301 Vgl. *Hilbig*, ITRB 2007, 170.

telt, oder ob dieser die Daten über eine technische Schnittstelle (sog. API) selbst abruft.[302] Entscheidend ist die Zugangsmöglichkeit.

Die Einordnung als Kaufvertrag hat zur Folge, dass die kaufrechtlichen Gewährleistungsvorschriften aus §§ 434 ff. BGB Anwendung finden. Die Gewährleistungsrechte der Nacherfüllung (§§ 437 Nr. 1, 439 Abs. 1 BGB), Rücktritt (§§ 437 Nr. 2 Alt. 1, 323, 326 Abs. 5, 346 ff. BGB), Minderung (§§ 437 Nr. 2 Alt. 2, 441, 323, 326 Abs. 5, 346 ff. BGB) und Schadensersatz (§§ 437 Nr. 3, 280 ff.) scheinen auf Datenzugangsverträge insgesamt sachgerecht anwendbar zu sein.

(2) Einordnung des Datenlizenzvertrags

Im Unterschied zum Datenzugangsvertrag ist der Datenlizenzvertrag nicht auf die dauerhafte Überlassung eines Datensatzes gerichtet, sondern auf die inhaltlich oder zeitlich begrenzte Nutzungsmöglichkeit eines solchen. Bei Verträgen über Daten ist es üblich, den zulässigen Nutzungszweck und insbesondere die Weitergabe der Daten einzuschränken. Darin besteht der wesentliche Unterschied zum Datenzugangsvertrag, bei dem der Erwerber mit dem Datensatz frei verfahren darf.

Zur Einordnung der Datenlizenz existiert soweit ersichtlich bislang keine höchstrichterliche Rechtsprechung. Es kann aber auf die Grundsätze zur Lizenzerteilung aus dem Immaterialgüterrecht zurückgegriffen werden.

Bei der Datenlizenz handelt es sich nicht um eine „echte" Lizenz im immaterialgüterrechtlichen Sinne, da dies ein subjektives Ausschließlichkeitsrecht des Dateninhabers voraussetzt.[303] Mit anderen Worten muss der Rechteinhaber die Nutzung des Rechts durch Dritte untersagen können, so dass er mit einer Lizenzerteilung sein Monopol aufgibt.[304] Der Inhaber eines Datensatzes kann die Nutzung der Daten selbst jedoch gerade nicht untersagen, weil Daten nicht an sich Schutz genießen, sondern allenfalls reflexartig geschützt sind.[305] Der Dateninhaber hat daher ein rein faktisches Monopol.[306]

302 *Hoeren/Pinelli*, JZ 2020, 879, 880.
303 *Schur*, Die Lizenzierung von Daten, 2020, S. 132 f.
304 *Schur*, Die Lizenzierung von Daten, 2020, S. 133.
305 *Schur*, Die Lizenzierung von Daten, 2020, S. 108.
306 *Schur*, Die Lizenzierung von Daten, 2020, S. 139.

Dennoch gewährt der Dateninhaber auch bei der hier vorliegenden Datenlizenz ein positives Benutzungsrecht,[307] so dass die Fälle hinreichend vergleichbar sind und die Grundsätze zur Lizenzerteilung aus dem Immaterialgüterrecht herangezogen werden können. Das allerdings löst die Probleme nur teilweise – wie ein Gericht den Vertrag rechtlich einordnet, lässt sich aktuell schwer prognostizieren, da eine klare Regel fehlt und die entwickelten Lösungen allesamt als „Krücken" gelten müssen:

- Der Datenlizenzvertrag kann eher nicht als Kaufvertrag angesehen werden, da der Zugang nur zeitlich und inhaltlich beschränkt gewährt wird. Das ist mit dem dauerhaften Austausch des Kaufs nicht vergleichbar.[308]
- Immaterialgüterrechtliche Lizenzverträge werden teilweise als (Rechts-)Pacht i.S.d. §§ 581, 535 BGB angesehen.[309] Das ist freilich schon im immaterialgüterrechtlichen Lizenzvertrag mit zahlreichen Anpassungen verbunden; die Einordnung hängt letztlich vom Einzelfall ab.[310] Die Gebrauchsüberlassung von Daten weist noch einmal nicht unerhebliche Unterschiede zur Lizenzierung von IP-Rechten auf.[311] Insbesondere behält der Dateninhaber Zugriff auf Daten und zieht auch Früchte aus diesen, was für eine Rechtspacht unüblich ist.[312] Daher passt der Pachtvertrag nur schwerlich auf die Lizenzierung von Daten.[313]
- Aufgrund der Probleme mit der Einordnung als Pachtvertrag wird von Rechtsprechung und Literatur überwiegend wohl eine Behandlung des Lizenzvertrags als Vertrag sui generis befürwortet.[314] Bei der Bestimmung des Pflichtenprogramms dieses Vertrags wird jedoch teilweise

307 *Schur*, Die Lizenzierung von Daten, 2020, S. 153.

308 Vgl. *Schur*, Die Lizenzierung von Daten, 2020, S. 139. Vgl. zum Lizenzvertrag im Patentrecht BGH, 23.3.1982, Az. X ZR 76/80, NJW 1982, 2861, 2863.

309 *Cebulla*, Die Pacht nichtsächlicher Gegenstände, 1999, S. 132; *Schaub* in: Staudinger-BGB, Neubearbeitung 2018, § 581 BGB Rn. 83 f.; *Harke* in: MüKo-BGB, Band 5, 8. Auflage 2020, § 581 BGB Rn. 27; *Teichmann* in: Jauernig, BGB, 18. Auflage 2021, § 581 BGB Rn. 2.

310 Vgl. *Fehrenbacher*, JR 2001, 309, 312; *Patzak/Beyerlein*, MMR 2007, 687, 690; *C. Wagner* in: BeckOK-BGB, 56. Edition 2020, § 581 BGB Rn. 9; *Weidenkaff* in: Palandt, 80. Auflage 2021, Einf v § 581 BGB Rn. 7.

311 *Schaub* in: Staudinger-BGB, Neubearbeitung 2018, § 581 BGB Rn. 58; *Bartenbach*, Die Patentlizenz als negative Lizenz, 2002, S. 88 f.

312 *Schaub* in: Staudinger-BGB, Neubearbeitung 2018, § 581 BGB Rn. 58.

313 *Schaub* in: Staudinger-BGB, Neubearbeitung 2018, § 581 BGB Rn. 58.

314 BGH, 15.6.1951, Az. I ZR 121/50, NJW 1951, 705, 706; BGH, 28.6.1979, Az. X ZR 13/78, GRUR 1979, 768, 769; *Fezer*, Markenrecht, 4. Auflage 2009, § 30

wieder auf pachtrechtliche oder kaufrechtliche Vorschriften rekurriert.[315] Die Rechte und Pflichten der Vertragsparteien sind also nicht klar am Gesetz ablesbar, sondern werden von den Gerichten jeweils im Einzelfall danach bestimmt, was wohl sachgerecht wäre. Es ist davon auszugehen, dass die Rechtsprechung so auch bei Datenlizenzverträgen verfahren würde.

Es zeigt sich: Die Rechtslage bei Datenlizenzverträgen ist unklar. Es ist bei Vertragsschluss kaum vorhersehbar, wie ein Gericht den Vertrag einordnen wird, welche Pflichten bestehen und welches Leistungsstörungsrecht Anwendung findet. Dies führt zu erheblichen Rechtsunsicherheiten und veranlasst die Parteien im Zweifel dazu, sämtliche Aspekte selbst vertraglich zu regeln. Dies führt aber zu erhöhten Transaktionskosten und zu Asymmetrien; der freie Austausch von Daten und die Gewährung von Zugang werden unattraktiver.

(3) Einordnung des Softwarevertrags

Beim hier sog. „Softwarevertrag" geht es darum, über Software Zugang zu erhalten. Alle Geräte, die mit einem „Bordcomputer" ausgestattet sind, ob Fahrzeuge, Maschinen oder Energieanlagen setzen in der Regel die Nutzung einer Software voraus, mit der auf das System zugegriffen werden kann. Dem Handwerker kommt es auf die Nutzungsmöglichkeit an. Nicht entscheidend ist, wie die Software zur Verfügung gestellt wird. Besonders interessant ist die Möglichkeit, über eine technische Schnittstelle auf das System zugreifen zu können. Das ermöglicht es beispielsweise einfach, das Betriebssystem zu aktualisieren, neue Funktionen freizuschalten oder Fehler (sog. „Bugs") zu beheben. Möglich ist so aber auch das Auslesen von Daten, die von Sensoren erfasst wurden. So können etwa Werkstätten mögliche Fehlerquellen und defekte Teile identifizieren. All das setzt aber Zugriff auf die Software voraus, die ggf. gegen Entgelt zur Verfügung gestellt wird.

MarkenG Rn. 1; *Ingerl/Rohnke*, MarkenG, 3. Auflage 2010, § 30 MarkenG Rn. 52; *Schulze* in: Dreier/Schulze, UrhG, 6. Auflage 2018, Vor § 31 UrhG Rn. 6; *Schur*, Die Lizenzierung von Daten, 2020, S. 181; *Taxhet* in: BeckOK-MarkenR, 23. Edition 2020, § 30 MarkenG Rn. 9; *Loth/Hauck* in: BeckOK-PatentR, 18. Edition 2020, § 15 PatG Rn. 40.

315 *Ingerl/Rohnke*, MarkenG, 3. Auflage 2010, § 30 MarkenG Rn. 52.

Für eine derartige Konstellation im Kfz-Gewerbe hat der europäische Gesetzgeber bereits den oben dargestellten sektorspezifischen Zugangsanspruch geschaffen (siehe dazu C.III.2). Aus diesem ergibt sich ein Anspruch von Werkstätten gegen die Fahrzeughersteller auf Zugang zur notwendigen Wartungssoftware zu angemessenen Bedingungen. Allerdings besteht auch in vergleichbaren Fällen für das Handwerk die Gefahr entsprechender Abschottungskonstellationen – etwa wenn der „Betreiber" eines Smart Homes sich die Instandhaltungsmaßnahmen exklusiv selbst vorbehalten will.

Softwareverträge sind als (Rechts-)Kaufverträge i.S.d. §§ 453, 433 BGB einzuordnen, sofern die Software auf Dauer überlassen wird und sie auch dauerhaft verwendet werden kann.[316] In der Praxis wird die Software häufig gegen monatliches Entgelt lizenziert und laufend aktualisiert, etwa um neue Modelle einzupflegen. Bei fortlaufender Aktualisierung und Nutzung nur auf Zeit ist in der Tendenz eher ein Rechtspachtvertrag i.S.d. § 581 BGB anzunehmen.[317]

bb) Vertragsgemäßheit der Daten

Neben der Einordnung zu einem bestimmten Vertragstypen stellt sich im Kaufrecht, im Pachtrecht und auch im allgemeinen Schuldrecht die Frage, wann ein überlassener Datensatz vertragsgemäß bzw. mangelfrei ist.

Im Rahmen eines als Rechtskaufvertrag zu behandelnden Datenzugangsvertrags (s.o.) stellt sich nach § 434 Abs. 1 BGB im Zweifel die Frage nach der „gewöhnlichen Beschaffenheit" der gekauften Daten. Dieser gemischt subjektive-objektive Mangelbegriff, wonach es vorrangig auf eine vertragliche Beschaffenheitsvereinbarung, hilfsweise auf die gewöhnlich zu erwartende Beschaffenheit ankommt, ist auch im Mietrecht[318] und damit nach § 581 Abs. 2 BGB auch im Pachtrecht maßgeblich.

Im Hinblick auf die Qualität der Daten wird in der Regel zwischen fünf Qualitätsebenen differenziert: „availability, usability, reliability, relevance, and presentation quality".[319] Es kommt nämlich gerade nicht nur auf die

316 Vgl. BGH, 22.12.1999, Az. VIII ZR 299/98, NJW 2000, 1415; *Heydn*, CR 2010, 765, 772; *Czychowski/Siesmayer* in: Kilian/Heussen, Computerrechts-Handbuch, 35. EL Juni 2020, 20.4 Urheberrecht Rn. 121.

317 Vgl. *Heydn*, CR 2010, 765, 773; *Czychowski/Siesmayer,* in: Kilian/Heussen, Computerrechts-Handbuch, 35. EL Juni 2020, 20.4 Urheberrecht Rn. 121.

318 Vgl. *Schüller,* in BeckOK-MietR, 22. Edition 2020, § 536 BGB Rn. 2.

319 *Hoeren/Pinelli*, JZ 2020, 879, 883.

Korrektheit der Daten an, sondern für eine wertschöpfende Verwendung müssen diese auch richtig dargestellt und lesbar sein.[320] Diskussionen zur Festlegung von Standards sind allerdings bisher im Sande verlaufen.[321] Hier könnte der Gesetzgeber gemeinsam mit Vertretern der Unternehmen beraten, wie der Mangelbegriff für Daten gesetzlich oder in Branchenvereinbarungen definiert werden sollte.[322] Allerdings ist fraglich, ob eine Konkretisierung die genaue Analyse im Einzelfall ersetzen kann.[323]

cc) Rückabwicklung

Klärungsbedarf besteht hinsichtlich der Frage, wie Verträge über Daten rückabgewickelt werden können, etwa wegen eines Rücktritts oder im Rahmen des Bereicherungsrechts. Die Rückgewähr, d.h. Rückübertragung der erhaltenen Datensätze dürfte häufig nicht erforderlich sein, da der Verkäufer oder Lizenzgeber diese regelmäßig noch in seinem Bestand haben sollte. Damit der Erwerber oder Lizenznehmer auf diese keinen Zugriff mehr hat, ist er stattdessen zur Löschung verpflichtet.[324] Auf einem anderen Blatt steht, wie das vollständige Löschen sämtlicher Kopien sicherzustellen ist.[325] Allerdings wird der Erwerber die Daten regelmäßig bereits ausgewertet oder in anderer Form verwertet haben. Dann ist es mit der bloßen Löschung der Daten beim Erwerber nicht getan, um eine Rückabwicklung des Vertrags, also die Herstellung des vorherigen Zustandes, zu verwirklichen. In Betracht kommt hier ein Anspruch auf Wertersatz für die gezogenen Nutzungen gem. § 346 Abs. 1, Abs. 2 Nr. 1 BGB.[326] Zu beachten ist aber, dass der Gesetzgeber bei § 346 BGB keine nichtgegenständlichen Leistungen vor Augen hatte und der hier nach dem Wortlaut anfallende Nutzungsersatz sehr weitgehend ist.[327] Der Wertersatz wäre nach § 346 Abs. 2 S. 2 BGB wohl auf die Höhe der vertraglich vereinbarten Ge-

320 *Hoeren/Pinelli*, JZ 2020, 879, 883.
321 *Hoeren/Pinelli*, JZ 2020, 879, 882.
322 *Hoeren/Pinelli*, JZ 2020, 879, 883.
323 Vgl. dazu im Kontext der Digitale Inhalte-Richtlinie (EU) 2019/770 *Faust*, Gutachten zum 71. Deutschen Juristentag, 2016, S. 27.
324 Vgl. zur Rückgewähr von Software schon *von Gravenreuther*, BB 1989, 1925, 1926 und *Redeker*, IT-Recht, 7. Auflage 2020, B. Der Erwerb von Soft- und Hardware, Rn. 392.
325 *Hoeren/Pinelli*, JZ 2020, 879, 881.
326 Vgl. *Hoeren/Pinelli*, JZ 2020, 879, 881.
327 *Hoeren/Pinelli*, JZ 2020, 879, 881 f.

genleistung begrenzt, da sämtliche Nutzungen, die gezogen werden können, im Kaufpreis eingepreist sein werden.[328] Damit kann das Problem umgangen werden, den Wert der Daten bzw. der Nutzungsmöglichkeit der Daten berechnen zu müssen, was schwer fallen dürfte.

Auch bei einer bereicherungsrechtlichen Rückabwicklung würden sich Probleme der Herausgabe und des Wertersatzes stellen.[329]

c) Legislative Möglichkeiten

Durch den Gesetzgeber könnte der Abschluss von Zugangsverträgen erleichtert werden.

aa) Neue Vertragstypen

Denkbar ist die Ergänzung neuer Vertragstypen in BGB oder HGB, bei denen, vergleichbar mit dem Kauf-/oder Werkvertragsrecht, vertragstypische Pflichten für Zugangs- und Datenverträge niedergelegt werden. Ebenso wäre es sinnvoll, mehrseitige Plattformverträge als Regelungsthema im Privatrecht zu verankern.[330]

Durch eigene Vertragstypen würden die neuartigen Erscheinungen einen rechtlichen Ankerpunkt erhalten. Einige rechtliche Ungewissheiten würden beseitigt, gesetzliche Leitbilder würden etabliert. Von diesen könnte zwar abgewichen werden, das würde aber zumindest Transaktionskosten senken und eine Orientierung bei der Überprüfung – etwa im Rahmen einer AGB-Kontrolle nach § 307 Abs. 2 Nr. 1 BGB – bieten.[331] Eine solche Regelung wäre auch ein starkes Signal an die Wirtschaft pro Zugang und Datenteilung.

Die gesetzliche Regelung müsste klarstellen, dass die erforderliche Leistungshandlung des Dateninhabers in der Verschaffung einer Zugangsmöglichkeit besteht, denn nur dies ist für den Zugangspetenten relevant. Aufgenommen werden sollten vor allem Regelungen zu den Modalitäten der

---

328 *Hoeren/Pinelli*, JZ 2020, 879, 881 f; vgl. auch *Gaier* in: MüKo-BGB, Band 3, 8. Auflage 2019, § 346 BGB Rn. 27.
329 Vgl. *Sprau* in: Palandt, BGB, 80. Auflage 2021, § 818 BGB Rn. 23.
330 Vgl. *Podszun*, Gutachten F zum 73. Deutschen Juristentag, 2020, S. F20 f.
331 Vgl. *Fries/Scheufen*, MMR 2019, 721, 725 f.; *Schur*, GRUR 2020, 1142, 1149; *Richter/Slowinski*, IIC 2019, 4, 25.

Bereitstellung, zum Mangelbegriff, zu den Gewährleistungsrechten, zur Rückabwicklung bei Rücktritt und zur Datensicherheit.

Darüber hinaus könnten bestimmte inhaltliche Vorgaben, Klauselverbote oder Optionen im Gesetz vorgesehen werden. So wäre etwa denkbar, dass ein gesetzliches Rahmenwerk die Anforderung enthält, dass Zugang technisch so ermöglicht wird, dass keine erheblichen Zusatzkosten anfallen oder exotische Dateiformate verwendet werden müssen. Solche Verpflichtungen enthalten beispielsweise die Regeln für den Kfz-Sektor oder die DS-GVO. Untersagt werden könnte beispielsweise, die Zugangseröffnung an Exklusivität oder an Beschränkungen im Kundenkontakt zu knüpfen. Optionen könnten etwa für die Vergütung vorgesehen werden, indem der Gesetzgeber drei verschiedene Wege der Kompensation zur Wahl stellt. Der Gestaltungsspielraum ist hier – in Abstimmung mit dem europäischen Recht – groß, setzt aber voraus, dass Gesetzgeber und betroffene Parteien sich überhaupt dazu durchringen, die Zugangseröffnung und den Datenaustausch zu einer politischen Priorität zu machen.

bb) Erleichterung der AGB-Kontrolle

Mit der Einführung eines gesetzlichen Vertragstypus würde die AGB-Kontrolle in rechtssicherer Weise ermöglicht. Es läge ein normatives Leitbild vor, an dem sich Gerichte orientieren könnten, um die Auswüchse von Machtasymmetrien bei der Vertragsverhandlung auszugleichen. Bislang sind für Zugangsverträge zwischen gewerblichen Nutzern keine Standards etabliert, an denen sich Justiz und Vertragspraxis orientieren könnten.

Zwar ist umstritten, ob der deutsche Weg, AGB-Kontrolle auch im unternehmerischen Rechtsverkehr durchzuführen, nicht zu weit führt.[332] Dies ist jedoch nicht der Ort, um diese Diskussion zu führen. Es mag der Hinweis genügen, dass gerade das Ungleichgewicht zwischen Big Tech-

332 Vgl. *Staudenmayer,* IWRZ 2020, 147, 154, *Schlinkert*, ZRP 2017, 222, Europäische Kommission, Mitteilung zum Aufbau einer europäischen Datenwirtschaft, 2017, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017DC0009&from=DE, S. 14; *Schweitzer/Welker*, A legal framework for access to data – a competition policy perspective, 2020, abrufbar unter: https://ssrn.com/abstract=3693874, S. 7; Bitkom, Stellungnahme Rechtliche Rahmenbedingungen von Industrie 4.0, 2016, S. 14; *Berger*, NJW 2010, 465, 466; *Schlinkert*, ZRP 2017, 222; *Leuschner*, NJW 2016, 1222; *Maier-Reimer*, NJW 2017, 1, 3 f.; *Pfeiffer*, NJW 2017, 913, 917, *Wurmnest* in: MüKo-BGB, Band 2, 8. Auflage 2019, § 307 BGB Rn. 80 f.

Konzernen einerseits und kleinen Handwerksbetrieben andererseits ein gutes Beispiel dafür sein kann, dass auch Unternehmen sich öfter in einer „Friss-oder-stirb"-Situation wiederfinden können, in der eine gewisse Kontrolle doch angemessen scheint. Fatal wäre es, mangels normativer Leitbilder für Datenverträge schlicht die bisherige Praxis zum Leitbild zu erheben. Die Interessengerechtigkeit bei dem, was aktuell branchenüblich sein mag, muss mit Fug und Recht bezweifelt werden.[333]

cc) Musterverträge und Standardklauseln

Anstelle oder zumindest komplementär zur Einführung dispositiver gesetzlicher Vorschriften könnten einige der zuvor skizzierten Probleme auch durch die Etablierung von Musterverträgen oder zumindest einzelner Standardklauseln abgefangen werden.[334] Musterverträge können die Transaktionskosten erheblich senken und Hold-up-Probleme, also das Zurückhalten von Innovationen wegen rechtlicher Unsicherheiten, auflösen. Rechtsberatungs- und damit Transaktionskosten fallen in geringerem Umfang an, wenn die Parteien auf Musterverträge für sämtliche Aspekte oder zumindest auf Standardklauseln für einzelne Fragestellungen zurückgreifen können. Solche Vertragsmuster könnten durch Branchenvertreter ausgehandelt und zur Verfügung gestellt werden. Das Bundeskartellamt (etwa im Rahmen einer Kontrolle nach §§ 24 ff. oder § 32c GWB) oder andere staatliche Stellen könnten entsprechenden Musterverträgen durch eine Kontrolle oder Zertifizierung einen gewissen offiziellen Status verleihen. Wie gut das in der Praxis funktioniert, zeigt das Mietrecht, wo Standardverträge den Vertragsschluss erheblich vereinfachen. Solche Standardverträge sind auch im Handelsverkehr mit Daten oder beim Zugang zu Plattformen denkbar. Wesentlich ist aber, dass das in der Konstellation angelegte Ungleichgewicht bei der Aushandlung nicht perpetuiert wird. Hier müssten also die Verbände des Handwerk (und anderer Zugangspetenten) auf Augenhöhe am Tisch mit denjenigen sitzen, die Zugang gewähren sol-

333 *Graf von Westphalen* in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, S. 255; *ders.*, IWRZ 2018, 9, 16.

334 Befürwortend auch Europäische Kommission, Mitteilung zum Aufbau einer europäischen Datenwirtschaft, 2017, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017DC0009&from=DE, S. 14. Siehe auch *Schur*, Die Lizenzierung von Daten, 2020, S. 294.

len. Erste Versuche zur Formulierung von Standardverträgen für Daten sind bereits in der Literatur zu finden.[335]

Anreize dafür könnten durch die finanzielle Förderung von Modellprojekten gesetzt werden. Der Staat selbst könnte für seine Bereiche sein eigenes Verhandlungsgewicht in die Waagschale werfen, um entsprechend faire Musterverträge zu entwickeln.

Noch weitergehend könnte eine gesetzliche Verpflichtung für bestimmte Anbieter vorgesehen werden, solche Vertragsmuster zur Verfügung zu stellen. So könnten Gatekeeper etwa verpflichtet werden, Vertragsmuster für den Zugang bereitzustellen, die einer Vorab-Kontrolle unterliegen. Hier wären, unter Zuhilfenahme ökonomischer Modelle, verschiedene Anreize denkbar, um die Fairness solcher Vertragsmuster zu steigern.

Eine derartige Verpflichtung würde freilich nur für besonders mächtige Anbieter in Betracht kommen. Sie wären als große Gatekeeper damit verpflichtet, qualifizierten Zugangspetenten zu einheitlichen Bedingungen, die öffentlich bekannt sind, Zugang zu gewähren.

In den Mustervereinbarungen sollten dann auch die Modalitäten der Bereitstellung geklärt werden, etwa hinsichtlich der Aktualität und des Formats von Daten, der technischen Modalitäten des Zugangs, der Vergütung, der einzuhaltenden Sicherheitsstandards und der Haftung. Wenn über diese neuralgischen Punkte Klarheit besteht und sich auch kleinere Unternehmen darauf verlassen können, dass ihre schwache Position nicht ausgenutzt wird, lassen sich zahlreiche Probleme lösen. Allerdings basiert das Modell, das ist der Haken, auf der freiwilligen Teilnahme der Parteien.

3. Zusammenfassung

Die Förderung vertraglicher Lösungen des Zugangsproblems ist als eine relativ wenig invasive Regulierungsoption zu befürworten. Die derzeitige Rechtslage insbesondere zu Datenlizenzverträgen ist mit erheblichen Unsicherheiten verbunden und stellt ein Handelshemmnis dar. In neuen Regelwerken oder in Musterverträgen sollten die Modalitäten des Zugangs geklärt werden.

Eine Option ist es, dies ganz der Selbstregulierung zu überlassen. Die Erfahrungen damit, etwa im Patentbereich, sind allerdings gemischt.

---

335 *Apel* in: Beck´sche Online-Formulare IT- und Datenrecht, 4. Edition 2020, 3.5 Vertrag über die Nutzung von bereitgestellten Daten ("Datenlizenzvertrag"), 3.6. Datenkaufvertrag.

Der Gesetzgeber sollte für die neueren Phänomene (mehrseitige Plattformverträge, Zugang, Datennutzung) Verträge gesetzlich typisieren. Das würde abweichende Vereinbarungen nicht ausschließen, gäbe aber einen normativen Ankerpunkt und würde das Zivilrecht an die Wirtschaft des 21. Jahrhunderts anpassen. Durch Verpflichtungen, Optionen und Verbote könnten entsprechende Verträge in vom Gesetzgeber vorgesehene Bahnen gelenkt werden und extreme Auswüchse bekämpft werden. Das würde auch mit der AGB-Kontrolle besser gelingen, wenn ein Vertragstypus normiert ist.

Eine Erleichterung fände die Praxis bereits, wenn für die entsprechenden Vereinbarungen faire Muster vorlägen. Bei deren Aushandlung ist auf eine Beteiligung der unterschiedlichen Gruppen zu achten. Auch hierfür kann der Staat Anreize setzen.

III. Zugangsansprüche

Wenn technische Barrieren fortbestehen und vertragliche Lösungen nicht funktionieren, ist den Petenten ggf. mit einem rechtlich verankerten Anspruch Zugang zu gewähren. Ein Zugangsanspruch, der ggf. zwangsweise durchgesetzt werden kann, kann technische und vertragliche Lösungen auch anreizen. In der öffentlichen Diskussion wurde bislang der Fokus auf den Zugangsanspruch als solchen gelegt. In der Reform des Kartellrechts, die 2021 mit der 10. GWB-Novelle abgeschlossen wurde, sind Datenzugangsansprüche – wie gesehen – verstärkt worden. Es stellen sich aber viele Folgefragen, die der Klärung zugeführt werden müssen. An deren Ausgestaltung entscheidet sich erst der Erfolg eines Zugangsanspruchs, der aus der Wettbewerbslogik heraus gewährt wird. Ein allgemeiner, branchenübergreifender Zugangsanspruch ist nicht undenkbar, müsste aber klare Begrenzungen haben, um genügend Investitions- und Innovationsanreize zu belassen. Eine realistische und sinnvolle Möglichkeit sind sektorspezifische Zugangsansprüche.

1. Kartellrechtliche Ansprüche

Im Kartellrecht sind inzwischen explizit verschiedene Zugangsansprüche vorgesehen: In § 20 Abs. 1a GWB geht es um den Zugang zu Daten, aus § 19 Abs. 2 Nr. 4 GWB kann sich ein Zugangsanspruch zu „Infrastrukturen“ ergebe, womit auch Plattformen erfasst sind. Auch aus § 20 Abs. 3a

GWB und aus § 19a GWB können sich branchenübergreifende Zugangsansprüche ergeben. Allerdings wurde bereits betont, dass der kartellrechtliche Zugangsanspruch kein Selbstläufer ist, sondern regelmäßig eine aufwändige Einzelfallprüfung unter Abwägung verschiedener wettbewerblicher Interessen voraussetzt.

Zentral bleibt im Kartellrecht die Abhängigkeit des Zugangspetenten von einem anderen Unternehmen. Das mag auf den ersten Blick einleuchtend erscheinen, ist doch sonst auch gar keine Notwendigkeit gegeben, einen Anspruch vorzusehen. Allerdings meint Abhängigkeit das Fehlen ausreichender und zumutbarer Ausweichmöglichkeiten.[336] Das bedeutet, dass zum einen der Nachweis zu erbringen ist, dass es keine derartigen Ausweichmöglichkeiten gibt. Es wird mit Blick auf die bisherige Rechtsprechung zur Abhängigkeit (die sich freilich noch nicht mit § 20 Abs. 1a GWB auseinandersetzen musste) nicht genügen, wenn in einem einzelnen Fall der Auftrag nicht erfüllt werden kann. Es dürfte vielmehr erforderlich sein, dass keine gleichwertigen Möglichkeiten bestehen, andere Aufträge auszuführen. Wenn die Rechtsprechung sich in eine solche Richtung entwickelt, kommt § 20 Abs. 1a GWB (ebenso wie die anderen Missbrauchstatbestände) vor allem in Betracht, wenn eine starke Abhängigkeit von einem einzelnen Anbieter vorliegt (z.B. Abhängigkeit eines Handwerkers von einem führenden Industriehersteller) oder wenn ein Bündel gleichartiger Verweigerungshaltungen letztlich den gesamten Markt sperrt.

In den übrigen Fällen würde es hingenommen, dass sich ein Plattformbetreiber zwischen den Kunden und den Handwerker drängt. Damit schafft der kartellrechtliche Zugangsanspruch in vielen Fällen keine Abhilfe; die konkrete Kundenbeziehung würde auseinandergerissen. Der verdrängte Handwerker muss sich, wie ein vom Hof geprügelter Hund, ein neues Revier suchen. Das mag eine Folge von aggressivem Verdrängungswettbewerb sein. Ob es aber ein fairer Leistungswettbewerb ist, mag bezweifelt werden.

Eine Auslegung der Norm, wie sie hier skizziert wird, ist nicht zwingend. Die bisherige Rechtsprechung aber und die vorsichtigen Worte in der Gesetzesbegründung zu den neu geschaffenen Datenzugangsansprüchen lassen nicht erwarten, dass im Rahmen der kartellrechtlichen Würdigung ohne weitergehenden gesetzgeberischen Eingriff eine erhebliche Ausdehnung der Zugangsrechte erfolgt. Das Grundproblem des kartellrechtlichen Anspruchs, seine hohen Voraussetzungen und der hohe Aufwand des

336 Vgl. *Loewenheim* in: Loewenheim/Meessen/Riesenkampff/Kersting/Meyer-Lindemann, Kartellrecht 4. Auflage 2020, § 20 Rn. 13.

Nachweises jeweils im Einzelfall, kann innerhalb dieses Rechtsgebiets nicht gelöst werden. Der Gesetzgeber hat mit der 10. GWB-Novelle schon einen – im Rahmen dieser Regelungsrationalitäten – sehr weitgehenden Schritt gemacht.

2. Alternativer Zugangsanspruch

Ein noch weitergehender Zugangsanspruch müsste einen Anspruch auf Zugang zu digitalen Systemen vorsehen, wenn dieser Zugang erforderlich ist, um auf nachgelagerten Märkten tätig zu werden oder den Kontakt zu aktuellen und potentiellen Kunden zu halten.

Weitergehend wäre dieser Anspruch gegenüber dem Kartellrecht nur dann, wenn er unterschiedslos, ohne aufwändige Analyse im Einzelfall, gegebenenfalls gestützt auf Vermutungen gewährt würde.

Allerdings sind auch die Schattenseiten eines solchen Anspruchs zu sehen: Für diejenigen, die Daten sammeln oder Plattformen aufbauen, wäre der Investitionsanreiz erheblich gemindert, wenn in der Folge jedermann Zugang beanspruchen könnte. Das würde digitale Innovationen in Deutschland oder Europa gefährden. Wird der Zugangsanspruch weit geöffnet, müssten deshalb an anderen Stellen die Stellschrauben so justiert werden, dass dennoch ein Investitions- und Innovationsanreiz erhalten bleibt. Das ließe sich zum Beispiel über die Anspruchsberechtigung oder eine gesetzliche Einschränkung der Voraussetzungen erreichen.

a) Anspruchsberechtigte Personen

Der Anspruch wird im Verhältnis von Leistungserbringer (Handwerksunternehmen) und Inhaber des digitalen Schlüssels geltend zu machen sein. Der ebenfalls beteiligte Kunde sollte aus diesem Verhältnis herausgehalten werden, auch wenn der Kunde erst die beiden Seiten miteinander verbindet. Die Einbeziehung des Kunden (die einem mehrseitigen Markt ja grundsätzlich entsprechen würde) ist aus Servicesicht abzulehnen – die Kunden sollen mit der Organisation der Leistung nicht behelligt werden.

Mit Blick auf die Anspruchsberechtigung ist festzuhalten, wer Zugang erhalten soll. In der vorliegenden Untersuchung wird insbesondere das Handwerk in den Blick genommen. Es ist aber keineswegs gesagt, dass alle Handwerksunternehmen in gleicher Form eine Zugangsberechtigung erhalten sollen, und es ist auch nicht gesagt, dass der Kreis auf Handwerks-

unternehmen beschränkt sein soll. Die Zugangsprobleme stellen sich für sehr viele verschiedene Unternehmen, auch solche, die nicht dem Handwerk zugehörig sind. Eine eigene Regelung für das Handwerk scheint derzeit weder geboten, noch durchsetzbar.

Mit Blick auf eine nötige Eingrenzung des Anspruchs könnte an Größenkriterien auf beiden Seiten angeknüpft werden. Bei besonders hoher Marktmacht oder besonders hohen Umsätzen des Inhabers des digitalen Schlüssels ist eine Pflicht zur Zugangseröffnung leichter zu bejahen als bei anderen Unternehmen. Kleine Unternehmen könnten eher Zugang erhalten als größere.

b) Identifikation des Zugangsziels

Der Zugangsanspruch muss auf ein Zugangsziel gerichtet sein. Es muss also klar zu erkennen sein, worauf sich der Zugang richtet. Wie gesehen ist dies nur in einer Minderheit der Fälle ein „Zugang zu Daten" im Sinne von Rohdaten. Die Rohdaten, die nicht verarbeitet, nicht veredelt oder sortiert sind, dürften im Regelfall wertlos für den Handwerker sein, insbesondere wenn sein Unternehmen nicht auf die Datenanalyse spezialisiert ist. Vielmehr wird es häufig um eine Eröffnung des Zugangs zum Gerät, zur Programmierung oder, noch treffender: zum Kunden gehen. Die wirtschaftliche Zielrichtung ist darauf gerichtet, den Kunden ansprechen zu können, die Kundenbeziehung aufzubauen und die Leistung, die der Kunde nachfragt, zu erbringen.

In den bestehenden wettbewerblichen Ansprüchen ist der Fokus auf den Zugang zu Daten gerichtet. Damit werden einige wichtige Konstellationen verfehlt oder jedenfalls auf ein Zugangsziel gelenkt, das dem Handwerk im Zweifel nicht immer nutzt. Als Zugangsziel eines allgemeinen Zugangsanspruchs wäre das Ziel in den Mittelpunkt zu rücken, Zugang zum Kunden zwecks Leistungserbringung zu erhalten. Technische Hürden dürften dem nicht entgegenstehen, ein rechtlicher oder technischer Ausschluss dürfte nicht erlaubt sein.

c) Materielle Voraussetzungen

Ein Zugangsanspruch setzt in quasi allen Szenarien, die im Recht bekannt sind – vom Notwegerecht über die Zwangslizenz bis zur PSD2-Richtlinie – eine Art „Notlage" voraus. Es müssen gewisse materielle Voraussetzungen

gegeben sein, sodass die Zugangseröffnung eigentlich der einzige Weg ist, will man nicht dem Petenten das Tätigwerden verunmöglichen. In den kartellrechtlichen Fällen wird dies typischerweise durch das Minimal-Kriterium der Unerlässlichkeit gewährleistet, wenn nicht – wie etwa bei der sog. „new product rule" im *IMS Health*-Fall – sogar weitergehende materielle Voraussetzungen gestellt werden.[337]

Im privaten Wirtschaftsverkehr, der vom allgemeinen Wettbewerbsrecht geregelt wird, ist eine allgemeine Zugangsgewährungspflicht unüblich. So kann etwa ein Marktbetreiber den Zugang zum Markt ebenso von Voraussetzungen abhängig machen wie der Inhaber eines Patents.

Die möglichen materiellen Voraussetzungen lassen sich aber in gewisser Weise verallgemeinern. Diese Verallgemeinerung könnte die Kriterien für einen Zugangsanspruch vorgeben, wenn man die bisherigen Ansprüche in §§ 19, 20 GWB für unzureichend hält. Mit folgenden Kriterien, die an die bisherige Praxis angelehnt sind, aber weniger schwierig zu erfüllen sind, ließe sich einfacherer Zugang erlangen:

- Liegt zwischen den Parteien ein Ungleichgewicht vor? (Asymmetrie)
- Hat der Zugangspetent keine alternativen Möglichkeiten, um weiterhin geschäftlich tätig zu bleiben? (Unerlässlichkeit)
- Ist die Zugangseröffnung volkswirtschaftlich oder rechtlich geboten? Werden so beispielsweise Effizienzgewinne, Innovationen, eine bessere Befriedigung der Nachfrage oder eine faire Chancenverteilung ermöglicht? (normatives Kriterium)
- Wird der Wettbewerb geschädigt, wenn der Zugang nicht eröffnet wird? (Wettbewerbsbeeinträchtigung)
- Liegt eine objektive Rechtfertigung für die Zugangsverweigerung vor? (Ausnahmen)

Das Kriterium der Asymmetrie ist eher nachweisbar als Abhängigkeit oder Marktmacht. Das normative Kriterium geht über das hinaus, was bislang in vergleichbaren Fällen verlangt wird.[338] Das ist insofern gerechtfertigt als, anders als im Immaterialgüterrecht, keine mit Verfassungsrang ausgestatteten eigentumsartigen Rechtspositionen zur Debatte stehen: Weder Daten, noch Kundenkontakte genießen eine derartige Stellung. Vielmehr ist die Zuordnung von Daten zu einem tatsächlichen Inhaber häufig Resultat einer zufälligen Position oder Folge einer vertraglichen Konstellation, die aber nur in seltenen Fällen Gegenstand von Verhandlungen mit

337 EuGH, 29.4.2004, Rs. C-418/01, ECLI:EU:C:2004:257 – *IMS Health.*

338 Vgl. *Schweitzer/Haucap/Kerber/Welker*, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, 2018, S. 187 f.

Leistung und Gegenleistung war, und die auch nicht immer auf hohen Investitionen beruht. Hat sich beispielsweise ein Fahrzeughersteller eine Einwilligung zur Nutzung personenbezogener Daten beim Kauf des Autos einräumen lassen, wird das im Regelfall nicht auf einem Aushandlungsprozess beruhen, bei dem der Käufer im Gegenzug einen erheblichen Nachlass auf den Kaufpreis erhalten hat und sich bewusst dagegen entschieden hat, der Werkstatt ebenfalls Zugang zu diesen Daten zu geben. Die vom Hersteller dann gesammelten Daten werden nicht vom Hersteller kreiiert oder generiert, sondern bestenfalls festgehalten. Die Investitionen für einen entsprechenden Sensor sind abzugelten, sie dürften aber überschaubar sein.

Im Immaterialgüterrecht (das für die Kriterien hier Pate stand) ist es gerade Kern der Sache, dass der Inhaber des Schutzrechts darüber entscheidet, wer in der Verwertungskette zum Zuge kommen soll, damit die Investitionen amortisiert oder seine berechtigten persönlichen Interessen am Schutzgegenstand angemessen gewahrt werden. Damit nimmt das Immaterialgüterrecht eine Ausnahme vom Wettbewerbsgedanken vor. Diese Ausnahme soll sich aber gerade nicht in anderen Bereichen fortsetzen. Der übliche Gang des Wettbewerbs ist, dass der Verbraucher zum Schiedsrichter wird und entscheidet, wer eine Leistung erbringen soll. Dieses Recht soll der Verbraucher auch im digitalen Zeitalter weiter innehaben – und die Schiedsrichterposition im Wettbewerb nicht an einen Vermittler verlieren. Der Gatekeeper entscheidet im Zweifel, wie dargelegt, auch nicht im Sinne des Kunden, sondern hat die Möglichkeit, seine Position als vermittelnder Agent zu mehreren Marktseiten hin missbräuchlich auszunutzen und in erster Linie seine eigenen Interessen zu befördern. Angesichts der fehlenden Informationen für den Verbraucher und der mangelnden Transparenz gelingt dies. In dieser Verdrängung des Verbrauchers aus seiner Schiedsrichter-Position liegt aber gerade eine korrekturbedürftige Fehlentwicklung.

Das hat auch der Bundesgerichtshof in seiner *Facebook*-Entscheidung 2020 deutlich gemacht: Der BGH hat entschieden, dass die mangelnde Einflussmöglichkeit des Verbrauchers auf die Datennutzung bei Facebook ein Missbrauch von Marktmacht durch das Netzwerk ist. Entscheidungssouveränität des Konsumenten ist demnach ein zentrales Element der Marktwirtschaft – auch im digitalen Zeitalter.[339] *Drexl* hat mit seiner Schrift zur „wirtschaftlichen Selbstbestimmung des Verbrauchers" nachge-

339 BGH, Beschl. v. 23.6.2020 – KVR 69/19; GRUR 2020, 1318; vgl. *Podszun*, GRUR 2020, 1268.

wiesen, dass es in einer modernen Marktwirtschaft gerade darauf ankommt, die Entscheidungshoheit des Verbrauchers zu sichern.[340] Anderenfalls funktioniert der Mechanismus Wettbewerb, der die Zusammenführung (und damit Auswahl) der Leistungspartner steuert, nicht mehr. Die Verbraucherentscheidung darf somit nicht durch eine Steuerung seitens der Vermittler ersetzt werden.

Das Kriterium der Wettbewerbsbeeinträchtigung ist der marktwirtschaftlichen Ordnung eingeschrieben. Eine Schädigung des Wettbewerbs sollte freilich genügen. Dafür spricht, dass gerade Plattformmärkte zur Monopolisierung neigen, also eine wettbewerbliche Gefahrenlage vorliegt. Wird stets erst eingegriffen, wenn der Markt bereits „gekippt" ist, ist das Wettbewerbsziel nicht mehr erreichbar.

Eine objektive Rechtfertigung für die Zugangsverweigerung könnte beispielsweise bei Sicherheitsbedenken oder Datenschutzfragen berücksichtigt werden.

Weiterführend wären solche Kriterien freilich nur, wenn gesetzliche Vermutungen etabliert würden. Andernfalls würden langwierige Auseinandersetzungen im Einzelfall die Zugangserlangung faktisch erheblich erschweren – gerade für strukturell unterlegene Parteien, die schlechter Rechtsschutz suchen können.

3. Sektorspezifische Zugangsansprüche

Wettbewerbliche Ansprüche knüpfen an die Marktmacht der Hersteller/Plattforminhaber an und greifen sodann an dem sich daraus ergebenden Machtgefälle zwischen den Marktteilnehmern ein. Ein allgemeiner Zugangsanspruch hat den Nachteil, dass er möglicherweise zu weitgehend eingreift. Eine Zwischenstellung könnten sektorspezifische Zugangsansprüche einnehmen. Darin läge wohl eine effektive Lösung der Zugangsproblematik, zumal sektorspezifisch auch Lösungen für technische Zugangsautomatismen gefunden werden könnten.[341]

340 *Drexl*, Wirtschaftliche Selbstbestimmung des Verbrauchers, 1998.
341 Vgl. *Drexl*, NZKart 2017, 339 und 415.

a) Vorbild-Regelungen

Bereits jetzt ist, wie dargestellt, etwa für die Kfz-Branche in einer eigenen EU-Verordnung ein Zugangsanspruch geregelt. So werden Kfz-Hersteller verpflichtet, den unabhängigen Marktteilnehmern die Reparatur- und Wartungsinformationen zu ihren Fahrzeugen in einem Standardformat leicht zugänglich diskriminierungsfrei zur Verfügung zu stellen.[342] Effektiv wird dieser Anspruch dadurch, dass er nicht von einer Einzelfallprüfung abhängig ist. Es muss nicht zuerst die besondere Marktmacht der Hersteller festgestellt werden, wofür langwierige Verfahren erforderlich sein können. Vielmehr wird der Zugang strukturell verankert, sodass die Nutzung des Anspruches als Standardprozedere automatisch abläuft und nicht als eine Art Sonderfall behandelt wird, der gesondert durchgesetzt werden muss. In den Kfz-Regelungen wird dem dadurch Sorge getragen, dass die Typengenehmigung der Fahrzeuge in der Regel erst dann erteilt wird, wenn der Zugang nachgewiesen wurde.[343]

Die sogenannte PSD-II Richtlinie[344] zeigt für den Sektor der Zahlungsdienste, dass auf diesem Wege auch allgemeine Schnittstellen für Drittanbieter geschaffen werden können. So verlangt Art. 66 Abs. 1 S. 1 RL (EU) 2015/2366, dass Drittanbieter die Möglichkeit haben müssen, durch das Konto des Bankkunden eine Zahlung auszulösen. Hierdurch wird ermöglicht, den Kunden neuartige Zahlungsservices anzubieten, die Zahlung selbst aber technisch über das „alte" Konto des Kunden durchzuführen. Im Gegenzug sind die Drittanbieter dazu verpflichtet, eine sichere Übermittlung der Zugangsdaten des Kunden zu gewährleisten und sich bei der Bank authentisch zu identifizieren.[345] Die Bank darf auch keine anderen Bedingungen oder Entgelte fordern, wenn ein Drittanbieter die Zahlung auslöst, als wenn dies der Kunde direkt tut.[346]

Die PSD-II Richtlinie führt dazu, dass eine für alle Drittanbieter offene Schnittstelle geschaffen wird und diese ihre Markthandlungen durchführen können. Wenn der Endkunde also einen solchen Drittanbieter nutzen möchte, kann er dies tun. Auf dem Markt können sich die Zahlungsauslösedienstleister durchsetzen, die die beste Leistung erbringen. Der sektor-

342 Siehe oben B.III.2.a.
343 Art. 6 Abs. 7 VO 715/2007.
344 Art. 66 f. VO (EU) 2015/2366. Siehe dazu oben B.III.2.b.
345 Art. 66 Abs. 3 b)-d) RL (EU) 2015/2366.
346 Art. 66 Abs. 4 c) RL (EU) 2015/2366.

spezifische Zugangsanspruch fördert also die Konsumentensouveränität und den Leistungswettbewerb.

b) Begrenzung

Die beiden genannten Regelungen sind auf kleine Anwendungsfelder und bestimmte Branchen begrenzt. Es handelt sich nicht um umfassende Zugangseröffnungen, sondern um Lösungen für konkrete Probleme in konkreten Wertschöpfungsketten. Genau das hat es ermöglicht, auf Einzelfallprüfungen zu verzichten und das Verfahren schlank zu halten. Zudem konnte nur eine solche Begrenzung des Zugangs zu technischen Lösungen führen, die automatisieren oder standardisiert Zugang gewähren, ohne dass es wesentlicher Umsetzungsschritte bedarf. Eine Negativwirkung für Innovation oder Investition geht angesichts der Begrenztheit des Anspruchs von diesem nicht aus. Insofern mahnen die genannten Modelle möglicherweise zur Bescheidenheit: Statt auf eine große Lösung zu pochen, die mit Innovationswirkungen und Bürokratie auch Probleme aufwirft, sollte zunächst die Lösung konkreter kleinerer Probleme verfolgt werden. Der Anspruch auf notwendige Reparaturinformationen wäre immerhin Nukleus für eine umfassende Lösung des Zugangsproblems.

Allerdings haben derartig eingegrenzte Lösungen auch einen Nachteil: Die Begrenzung auf bestimmte Branchen fördert deren Abschottung gegenüber Unternehmen, die nicht in der Branche aktiv sind. Die Vernetzung der Märkte, ihre Konvergenz, die ein Kennzeichen der Datenökonomie ist, wird so nicht abgebildet. Die adressierten Probleme sind im Umfang letztlich begrenzt – so ist das Kfz-Modell letztlich nur gedacht und geeignet, um Reparaturen zu ermöglichen. Dass die Kfz-Branche mit anderen Diensten zusammenwächst und Teil eines immer stärker datengetriebenen Mobilitätssektors ist, wird so nicht erfasst.

Gleichwohl ist das Modell ein wesentlicher Anfang, der praktikabler scheint als der Weg über allgemeinere Zugangsansprüche, die nur stumpfe Schwerter sind. Über sektoral begrenzte Zugangsautomatismen und Schnittstellenoffenlegungen können die Lernprozesse angestoßen werden, die erforderlich sind, damit in einem späteren Schritt echte übergreifende „Datenräume“ geschaffen werden können.

c) Automatisierung des Zugangs

Wesentliches Element dieser sektoralen Zugangsansprüche ist die Automatisierung des Zugangs, also der Verzicht auf eine Einzelfallprüfung.

Das entspricht zwar nicht der wettbewerblichen Lehre, doch lassen sich dafür Gründe finden: Erstens ist die wettbewerbliche Situation vielfach im Begriff zu kippen („tipping"). Die Erfahrungen bisher zeigen, dass eine Situation, in der eine Plattform oder der Inhaber eines digitalen Schlüssels sich durchgesetzt haben, im Nachhinein kaum mehr auflösbar ist. Dem ist durch eine frühzeitige Öffnung entgegenzutreten, damit auf nachfolgenden Marktstufen noch Wettbewerb entfaltet werden kann. Der automatisierte Zugangsanspruch ist damit der Schutzwall gegen das Abrutschen ins Monopol. Zweitens bedürfen auch die Hersteller und Datenoperatoren der Leistungen des Handwerks, z.B. weil Geräte eben einbau- oder reparaturbedürftig sind. Sie nutzen aber das strukturelle Übergewicht, das sie dank der digitalen Zugangskontrolle haben, aus, um Leistungserbringer in Abhängigkeitssituationen zu bringen. Hier ist ein Interessenausgleich angemessen. Dass damit auch die Werte der Konsumentensouveränität, des Leistungswettbewerbs und der Marktwirtschaft abgesichert werden, ergibt sich von selbst.

Neben etwaigen formellen Voraussetzungen sollten keine inhaltlichen Einzelfallentscheidungen erforderlich sein. Diese bergen Potenzial für Streitigkeiten und lange Verfahren.

d) Öffnung von Schnittstellen

In Wertschöpfungsnetzwerken, wie sie für das Internet of Things (IoT) typisch sind, sind Konstellationen denkbar, in denen zahlreiche Unternehmen, Dienstleister, Handwerker usw. an einem zentralen Operator hängen, der den Zutritt zur Leistungserbringung im Wertschöpfungsnetzwerk digital kontrolliert. In solchen IoT-Netzwerken steht dann nicht die individuelle Leistungserbringung im Vordergrund (wie etwa bei der Reparatur eines Autos), sondern die Mitwirkung in einem komplexen, vernetzen System. Als Beispiel kommen das Smart Home oder die Smart Factory in Betracht: Hier hat meist ein Unternehmen, das die zentrale Software steuert, den „digitalen Hausschlüssel" in seiner Kontrolle und kann das gesamte Wertschöpfungsnetzwerk steuern. Bei Errichtung, Wartung und Weiterentwicklung können zahlreiche verschiedene Handwerksunternehmen be-

teiligt sein, die aber allesamt Zugang zur Steuerungssoftware benötigen. Gerade solche Netzwerke können erhebliche Innovationen hervorbringen.

Der Zugang dazu sollte nicht durch automatisierte Zugangsansprüche gewährleistet werden, sondern durch offene Schnittstellen. Offene Programmierschnittstellen (APIs) eröffnen am ehesten die Möglichkeit eines unkomplizierten, direkten Zugriffs auf relevante Daten.

Das Vorbild dafür ist die PSD2-Richtlinie, die mit der offenen Schnittstelle den Zahlungsdienstleistermarkt samt seiner Innovationen entscheidend belebt, ja, erst ermöglicht hat. Nur wenn viele verschiedene Unternehmen mit ihren Leistungen andocken können und die Entscheidung nicht an den zentralen Operator delegiert wird (bzw. realistischer: von diesem strategisch nach Eigeninteressen gesteuert wird), können sich Smart Home, Smart Factory oder IoT-Anwendungen zu Foren entwickeln, in denen Innovationen blühen – und wo der eigentliche Nutzer (der Wohnungsinhaber, der Fabrikant, das IoT-Netzwerk) entscheiden kann, welche Leistungen den Wettbewerb gewinnen.

Seine Rechtfertigung findet dieses Modell in Konsumentensouveränität und Leistungswettbewerb. Auch die Innovationskraft wird gesteigert. Die digitalen Schlüsselinhaber bei komplexeren Leistungsnetzwerken dürfen nicht in die Rolle kommen, alle Leistungen zentral zu steuern. Das wäre nicht mehr die europäische Marktwirtschaft, die ihre Stärke gerade aus dem Unternehmergeist des Einzelnen schöpft.

Auch hier wären, wie im Vorbild der PSD2-Richtlinie, bestimmte Vorgaben vorzusehen, damit beispielsweise die Sicherheit gewährleistet bleibt. Selbst mit entsprechenden Einschränkungen würde eine offene Schnittstelle aber noch immer zahlreichen Unternehmen Zugang ermöglichen.

Sektoral spezifisch könnte das konkrete Zugangsziel definiert werden. In der Regel werden es nicht bloße Messdaten sein, sondern im Zweifel Zugang zu einem Dashboard, auf dem diese Daten bereits aufbereitet sind oder Zugang zu einer spezifischen Software. Eine Vergütung ist denkbar.

Alternativ könnten eine Investitionsschutzfrist plus Portabilitätsregelung vorgesehen werden: So ließe sich ein zeitlich begrenzter Schutz der Schnittstelle (z.B. für 2–3 Jahre) vorsehen, der in diesem Zeitraum eine gewisse Steuerung und Monopolisierung erlaubt. Damit könnten die Investitionen und die Innovationskraft des ursprünglichen Betreibers abgegolten werden. Danach wäre dann aber die Leistung des Operators abgegolten, die Schnittstelle wäre zu öffnen, Daten müssten portabel gemacht werden.

Die offene Schnittstelle müsste freilich auch genutzt werden – seitens des Handwerks müsste es Angebote geben, daran anzudocken und in die digitale Struktur der IoT-Netzwerke vertieft einzudringen.

e) Branchenspezifische Ausgestaltung

Den beiden hier hervorgehobenen Modellen ist gemein, dass sie sektorspezifisch ausgestaltet sind. In ihre Ausgestaltung ist das Know How der gesamten Branche eingeflossen, auf Eigenheiten konnte eingegangen werden. Der klare gesetzgeberische Impuls – Eröffnung des Zugangs – wurde so zielgerichtet implementiert.

Je nach den Besonderheiten der Branchen und der Märkte kann ein gesondertes Regime vorzusehen sein. Mal mag ein reiner Datenzugang ausreichend sein, mal mag die Teilhabe an einem komplexen Infrastrukturnetz mit dem Erfordernis eines differenzierten Vergütungsmodells erforderlich werden. Die Reparatur digital gesteuerter Kühlanlagen mag andere Regelungsaspekte mit sich bringen als der Zugang zu einer Augenoptiker-Plattform. Daher sollten derartige Zugangsverpflichtungen branchenspezifisch ausgestaltet werden, damit spezifische Bedingungen und Besonderheiten berücksichtigt werden können – so wie es im Kfz-Bereich auch gelöst ist. Dabei darf aber, insbesondere bei frühzeitiger Regelung, die Macht und künftige Macht, die von digitaler Kontrolle ausgeht, nicht unterschätzt werden. Die Lehre aus den Erfahrungen der letzten Jahre ist gerade, dass die Macht digitaler Player enorm rasch wachsen kann und dann nicht mehr bestreitbar ist.

Um die konkrete Ausgestaltung passgenau zu schaffen, sollten Branchenverbände oder Kammern die Gestaltung federführend übernehmen oder jedenfalls daran beteiligt werden. Auf die Erfordernisse kleiner und mittlerer Unternehmen ist besondere Rücksicht zu nehmen. Dementsprechend dürfen technische Lösungen nicht zu komplex sein oder mit hohen Anfangsinvestitionen verbunden sein. Ggf. muss ein Zugang über Kooperationen und Verbände ermöglicht werden.

4. Realisierung, Bedingungen und Vergütung

Wird Zugang eingeräumt, ist zu klären, wie Zugang gewährt wird, also welche Form der Eröffnung auf technischer Ebene stattfindet, welche Bedingungen gestellt werden und welche Vergütung zu leisten ist. Diese Fragen werden auch durch die Novellierung des Kartellrechts nicht geklärt, sodass sie zu Stolpersteinen in der Praxis werden können, selbst wenn der grundsätzliche Anspruch gewährt wird. Die Fragen stellen sich in allen Zugangsmodellen, egal ob es sich um einen kartellrechtlichen, einen allgemeinen oder einen sektoralen Zugangsanspruch handelt.

a) Modalitäten der Zugangseröffnung

Die Einräumung von Zugang ist ein technischer Vorgang, der eines Umsetzungsakts bedarf. Die Umsetzung kann mit zahlreichen Schwierigkeiten einhergehen. In der Vergangenheit hat beispielsweise die immer wieder erschwerte und verzögerte Öffnung des Fährhafens Puttgarden Geschichte geschrieben – und aufgezeigt, wie kompliziert es ist, Zugang praktisch wirksam werden zu lassen, wenn der Verpflichtete konfrontativ sabotiert.[347] Im *Microsoft*-Fall musste ein Monitoring Trustee eingesetzt werden, bis zur Umsetzung der von der EU-Kommission verlangten Schnittstellenöffnung mussten mehrere hohe Geldbußen gegen Microsoft verhängt werden.[348]

Besonders schwierig ist die Zugangsgewährung, wenn Daten zugänglich gemacht werden sollen. Hier stellt sich die Frage, welche Daten genau erfasst werden müssen, welche Daten benötigt werden und in welchem Format die Daten wann zugänglich zu machen sind. Werden Daten benötigt, ist zu spezifizieren, wie aktuell die Daten zu sein haben und ggf. in welcher Frequenz sie zu aktualisieren sind (Updatepflicht). Es wäre etwa denkbar, dass sich ein Unternehmen, das zur Zugangsgewährung widerwillig verpflichtet worden ist, seiner Verpflichtung entzieht, indem es auf einer CD-Rom einen Datensatz bereitstellt, der den Empfänger zu spät erreicht und der für den Empfänger nicht lesbar oder mangels Aktualität uninteressant ist. Hier stellt sich eine Vielzahl von Sabotagemöglichkeiten, bis Zugang in einer Form gewährt wird, die für die Zwecke des Zugangspetenten sinnvoll ist.

In derartigen Fällen stoßen Gerichte auch an die Grenzen ihrer Tenorierungsmöglichkeiten, da die Verpflichtung einerseits bestimmt genug ausfallen muss, andererseits im Vorhinein kaum zu ermessen ist, welche Daten in welcher Form wie vorgelegt werden müssen.

Häufig wird der Zugang nicht zwingend zu Daten vermittelt, sondern etwa zu einem Dashboard, das weiteren Zugriff in einer lesbaren Form vermittelt oder auf dem die Daten so vorliegen, dass sie einsehbar sind. Zu klären ist, ob dies genügt, um die Leistung zu erbringen. Auch hier ist

347 Der Fall dieser "Vogelfluglinie" wird teilweise nachgezeichnet in *Podszun*, ZWeR 2012, 48, 54 m.w.N. Den dort genannten deutschen Entscheidungen waren bereits mehrere EU-Entscheidungen vorgelagert, siehe z.B. Europäische Kommission, 21.12.1993, Entsch. 94/119/EG – *Hafen von Rødby*.

348 Europäische Kommission, 27.2.2008, COMP/34.792 – *Microsoft* (*periodic penalty payment*).

denkbar, dass relevante Daten fehlen oder ein erweiterter Zugang erforderlich ist, wenn die Leistungserbringung komplexer wird.

Zum Teil verlangen Gatekeeper, dass bestimmte Software verwendet werden muss, ohne die ein Auslesen von Daten oder ein Zugang nicht möglich ist. Es kann sein, dass diese Software nicht allgemein verfügbar ist oder wiederum ein Lizenzvertrag mit dem Gatekeeper (oder einem verbundenen Unternehmen) abgeschlossen werden muss oder im Gegenzug zahlreiche Daten des Handwerksunternehmens ausgelesen werden können. Dann verbergen sich möglicherweise hinter diesen Hilfsmaßnahmen weitere Wettbewerbsbeschränkungen oder Einschränkungen für den Zugangspetenten.

Denkbar ist auch, dass für die Gewährung des Zugangs der Abschluss eines Lizenzvertrags verlangt wird. Dieser Lizenzvertrag kann dann wiederum Teile enthalten, die erst wieder geprüft werden müssen und die möglicherweise rechtswidrig sind. Dadurch kann sich wiederum eine Verzögerung oder eine Erschwernis des eigentlich bereits erstrittenen Zugangs ergeben.

Der Datenzugang muss auch in zeitlicher Hinsicht determiniert werden. Je nach Bedürfnis kann es genügen, kurz und einmalig Zugang zu gewähren. Es kann aber auch Situationen geben, in denen ein Zugang mehrfach oder dauerhaft eröffnet sein soll. Auch diese zeitliche Schiene mag wiederum zu Verzögerungen und neuen Streitigkeiten führen.

Es gibt keine *one-size-fits-all*-Lösung für das hier aufgezeigte Problem der Modalitäten. Es soll insbesondere verdeutlicht werden, dass der eigentlich zugesprochene Anspruch bei der Geltendmachung zahlreiche Ungewissheiten mit sich bringen kann, die zu Verzögerungen und neuen Rechtsstreitigkeiten führen können, ohne dass dies im Vorhinein im Rahmen eines wettbewerblichen Zugangsanspruchs geregelt werden kann.

Erforderlich ist aber, dass mit Gewährung des Zugangs auch die wesentlichen Modalitäten feststehen. Diese sind:

- Konkretes Zugangsziel,
- Umfang des Zugriffs,
- mit dem Zugang verbundene Rechte (z.B. reine Betrachtung oder auch Bearbeitung),
- Details der technischen Ermöglichung des Zugangs (Schritt für Schritt),
- ggf. erforderliche Hilfsmittel oder Zusatzrechte für den Zugang,
- Mitwirkungspflichten der jeweiligen Parteien für den Zugang,
- Dauer der Zugangseröffnung,
- Frequenz des Zugriffs,

– Aktualität des zur Verfügung gestellten Materials (Livestream oder aktuelle Daten),
– zu beachtende technische oder rechtliche Besonderheiten.

Ein gesetzlicher Zugangsanspruch, der nicht jedes Detail festlegt, wird nicht ohne Code of Conduct der Praxis (siehe oben) oder einen raschen Streitschlichtungsmechanismus (siehe unten) auskommen, wenn der Anspruch wirksam sein soll.

b) Beschränkungen und Bedingungen

Die Zugangsbedingungen können einen erheblichen Einfluss auf das kommerzielle Ergebnis haben. Wenn der Gatekeeper die Möglichkeit hat, Bedingungen zu stellen (sei es auf vertraglicher Basis oder weil ihm dieses Recht nicht verwehrt ist), können sich solche Bedingungen erheblich auswirken. Zu denken ist neben den genannten Modalitäten z.B. an Verwendungsbeschränkungen hinsichtlich der Daten, die Verpflichtung zur Abnahme von Ersatzteilen, das Verlangen einer Zustimmung zur Datensammlung, die Verpflichtung zur Registrierung beim Gatekeeper, die Beschränkung sonstiger Kundenkontakte oder des Ausbaus von Kundenkontakten, die Verpflichtung auf die Einhaltung bestimmter Standards, Dokumentationspflichten, die Verpflichtung zur Nutzung bestimmter Software, das Verlangen nach Preisgabe bestimmter Daten, die Einräumung von Rechten an geschütztem Material – der Phantasie sind kaum Grenzen gesetzt.

Teil der Umsetzung kann etwa sein, dass im Gegenzug der Handwerker, der Zugang erlangt hat, seine Leistungsdaten oder andere Daten an denjenigen abgeben muss, der Zugang vermittelt. Eine entsprechende Übertragung von Informationen kann einen hohen wirtschaftlichen Wert für den datenerhebenden Zugangsgewährer haben, sodass dessen Marktposition wiederum gestärkt wird.

Das ist aber keineswegs zwangsläufig so. Es ist auch eine asymmetrische Datenteilungspflicht denkbar, mit der kleinere Unternehmen privilegiert werden. Die Gegenseitigkeit der Datenoffenlegung könnte so verhindert werden, sodass zwar ein Datenfluss zu den Kleinen, aber kein Datenabfluss zu den Großen stattfindet.

Erlangt der Handwerker Kenntnis von bestimmten Daten, kann ihm diesbezüglich eine weitergehende Verwendungsbeschränkung auferlegt werden, sodass die Daten nicht für weitere Leistungen verwendet werden können. Erhält beispielsweise ein Handwerker in einem Smart Home Zu-

gang zu den notwendigen Servicedaten und erkennt aus den Verbrauchsdaten, dass neben der angefragten Wartung für Gerät 1 auch Gerät 2 wartungsbedürftig ist, dürfte ggf. keine Wartung an Gerät 2 durchgeführt werden, oder es müsste erst erneut Zugang angefragt werden. Damit wird der Kundenservice beschnitten, dem Handwerker entgehen Zusatzgeschäfte oder es sind Provisionszahlungen zu leisten.

Bei der Zugangsgewährung selbst und in Folge der Zugangsgewährung bei Tätigkeiten und Geschäftsabschlüssen kann es zu Fehlern und Schädigungen kommen. Die Frage ist, wer die Haftung dafür übernehmen muss. Gewährt beispielsweise ein Gatekeeper Zugang zu einem Datensatz, überträgt mit dem Datensatz aber einen Virus, kann dies Folgeschäden für den Zugangspetenten haben. Repariert der Zugangspetent etwas im Smart Home und stellt dabei die Software falsch ein, sodass es danach zu einem Systemabsturz kommt, kann auch dies Schadensersatzansprüche auslösen. Eine Vielzahl von Gestaltungen ist denkbar, etwa eine Beschränkung der Haftung, eine Überwälzung der Haftung auf die andere Partei, eine Versicherungslösung oder eine gesetzliche Haftungslösung.

Die Gerichte werden nur sehr vorsichtig zusätzliche Bedingungen formulieren, solange das im Gesetz nicht angelegt ist. Vielmehr wird typischerweise das Aushandeln der Details auf den Verhandlungsweg verwiesen. Das wiederum kann den einmal erstrittenen Zugangsanspruch aufgrund der denkbaren Bedingungen und der notwendigen Verhandlungen entwerten. Wenn Zugang nicht zügig und umfassend gewährt wird, bleibt Zugang wertlos – die Kunden können nicht warten, bis erst höchstrichterlich entschieden ist, ob ein Handwerker eventuell Zugang erhält. In der Zwischenzeit wird es aus Kundensicht immer die bequemere Lösung sein auf einen Dienstleister zu setzen, den der Gatekeeper bereithält.

Zu klären ist daher, ob mit der Zugangseröffnung weitere Bedingungen oder Beschränkungen rechtlicher Art verbunden sein sollen. Zudem ist die Haftung zu klären.

Wiederum gilt, was zu den Modalitäten der Zugangseröffnung gesagt wurde: Kommt es nicht zu gesetzlichen Vorgaben (dazu oben), sind Codes of Conduct oder Streitschlichtungsmechanismen unerlässlich. Ein Mustervertrag könnte entsprechende Standards, ggf. branchenabhängig, durchsetzen.

c) Vergütung

Ein verpflichtender Zugang muss typischerweise nicht kostenfrei, sondern nur gegen ein angemessenes Entgelt gewährt werden. Der Gatekeeper muss für das Sammeln der Daten oder den Aufbau einer Plattform belohnt werden. Andernfalls wird der Anreiz, digitale Geschäftsmodelle weiterzuentwickeln, Daten zu sammeln und zu analysieren, die bisher noch niemand analysiert hat, oder innovative IoT-Systeme aufzubauen, erheblich geschwächt. Das gilt besonders, wenn mit dem Aufbau einer derartigen Infrastruktur nicht unerhebliche Kosten verbunden sind.

Probleme bereitet naturgemäß, welche Vergütung angemessen ist. Dabei stellt sich zum einen die Frage nach dem Vergütungsmodell. Denkbar ist eine einmalige oder regelmäßig wiederkehrende Zahlung, aber auch eine Bezahlung abhängig vom erwirtschafteten Gewinn, der erst durch die Zugangserlangung möglich wird. Wiederum liegt eine Einzelfalllösung näher als eine allgemeine Regel.

Denkbar ist, auf die aus dem Patentrecht geltenden FRAND-Bedingungen (fair, reasonable and non-discriminatory) zurückzugreifen, die beim sogenannten Zwangslizenzeinwand relevant sind. Dies wurde bereits 2017 von der Europäischen Kommission in ihrer Mitteilung zum Aufbau einer europäischen Datenwirtschaft erwogen.[349] Die FRAND-Grundsätze sind zudem bereits Leitbild für verschiedene Sekundärrechtsakte der Union (vgl. oben B.II.2). Dabei verweisen die Gerichte typischerweise auf den Weg der Aushandlung zwischen den Parteien (ggf. nach einem vorgegebenen Muster).[350] Ob ein Vertragsangebot FRAND-gemäß ist, ist von den Gerichten aber vollumfänglich überprüfbar.[351]

Der Grundsatz, dass die Parteien die Lizenzbedingungen und damit die Vergütung selbst aushandeln müssen, lässt sich auch für die Vergütung in Datenzugangskonstellationen fruchtbar machen.[352] Die Parteien können im Zweifel deutlich besser beurteilen, welches Vergütungsmodell und welche Vergütungshöhe im vorliegenden Fall angemessen ist. Damit bleibt

349 Europäische Kommission, Mitteilung zum Aufbau einer europäischen Datenwirtschaft, 2017, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017DC0009&from=DE S. 15.

350 Grundlegend EuGH, 16.7.2015, Rs. C-170/13, ECLI:EU:C:2015:477, GRUR 2015, 764 – *Huawei/ZTE*; BGH, 5.5.2020, Az. KZR 36/17, WuW 2020, 478 – FRAND-Einwand m. Anm. *Kellenter*.

351 Vgl. OLG Karlsruhe, 8.9.2016, Az. 6 U 58/16, BeckRS 2016, 17467, Rz. 36; OLG Düsseldorf, 17.11.2016, Az. I-15 U 66/15, BeckRS 2016, 21067, Rz. 14 ff.

352 Befürwortend auch *Staudenmayer*, IWRZ 2020, 147, 156.

zwar die Frage offen, wie die Gerichte die Vergütung bestimmen müssen, wenn sich die Parteien nicht nur hinsichtlich einzelner Fragen wie z.B. der konkreten Summe, sondern über grundlegende Fragen wie das Vergütungsmodell streiten. Dies sollte aber mit zunehmender Fallpraxis auf dem Markt immer leichter werden. Dennoch bleibt die Frage der Vergütung zentral und von enormer Schwierigkeit für die Praxis, da die Maßstäbe noch nicht wirklich konturiert sind.

Die FRAND-Lösungen haben in der immaterialgüterrechtlichen Praxis immer wieder auch zu erheblichen Schwierigkeiten geführt. Letztlich ist bis heute unklar, wie der „gerechte Preis" bestimmt werden sollte. Falls hier keine Brancheneinigung in Sicht ist oder ein rascher Streitschlichtungsmechanismus eingreift, empfiehlt sich ein innovatives Modell der Preisbestimmung: Beide Seiten legen ein Angebot vor, von dem ein unabhängiger Richter nur eines auswählen kann – ohne es verändern zu können.[353] Das zwingt beide Seiten zur Berücksichtigung einer Zumutbarkeitsgrenze.

5. Durchsetzung

Schließlich muss die institutionelle Ausgestaltung eines Zugangsanspruchs geklärt werden. Hier stellt sich die Frage, wie ein entsprechender Anspruch durchgesetzt werden kann. Verschiedene Modelle kommen in Betracht: So ist grundlegend zu trennen zwischen einer behördlichen und einer privaten/zivilrechtlichen Durchsetzung. Denkbar ist, dass die Zugangsverweigerung mit Sanktionen belegt ist (z.B. Bußgeld, erhöhte Haftung). Das Verfahren kann in besonderer Weise ausgestaltet werden, z.B. als Eilverfahren. Über den Erfolg entscheidet auch die Verteilung der Beweislast, die abweichend geregelt werden kann.

a) Ausgestaltung des Anspruchs

Der Anspruch lässt sich grundlegend zivilrechtlich verankern als ein Recht des einzelnen Unternehmers auf Zugangsgewährung (vgl. § 33 Abs. 1 GWB). Eine klassisch-zivilrechtliche Lösung würde bedeuten, dass zunächst Zugang individuell begehrt werden muss, bei Verweigerung aber

353 Vgl. *Jakobs*, Standardsetzung im Lichte der europäischen Wettbewerbsregeln, 2012. Siehe auch *Franz/Podszun*, ZWeR 2015, 207.

eine gerichtliche Überprüfung mit der Gewährung eines Zugangsrechts erfolgen kann. Dieses Modell würde stärker auf die individuellen Verhältnisse im konkreten Fall ausgerichtet sein. Es wäre eine ex post-Lösung, die, wie im Kartellrecht üblich, den Fehler nachträglich zu erkennen und zu beseitigen sucht, nachdem dazu ökonomisch umfassend vorgetragen wurde.

Dieses Modell ist in seiner Wirksamkeit für eine Vielzahl kleinerer Fälle kaum geeignet.

In Diskussionen über die Regeln für digitale Märkte (die als besonders schnell und dynamisch gelten) gewinnen daher ex ante-Regelungen an Überzeugungskraft. Solche Regelungen wären eher als „regulatorisch", nicht „wettbewerblich" zu bezeichnen. Dabei wäre von Anfang an ein Zugangsrecht gegeben, das automatisch gilt und keiner weiteren Umsetzung bedarf. Der Zugangsanspruch wäre damit gesetzlich verankert und würde automatisch greifen. Der Digital Markets Act-Vorschlag der Europäischen Kommission geht in diese Richtung.

Das Modell der offenen Schnittstellen ist die Verwirklichung eines umfassenden Automatismus.

Der Unterschied schlägt sich in der Durchsetzung nieder: Eine Norm, deren Verletzung auf der Hand liegt, weil die Vorschrift von vornherein gilt und kaum Auslegungsspielräume lässt, ist stärker als eine Vorschrift, deren Voraussetzungen erst im Einzelfall geprüft und nachgewiesen werden müssen. Hier ist länglichen Argumentationsketten Tür und Tor eröffnet.

b) Rechtsdurchsetzung

Wettbewerbliche Ansprüche, etwa aus § 20 GWB, werden im Zweifel durch das Bundeskartellamt, häufiger aber in Form privater Rechtsdurchsetzung bei Gericht umgesetzt. Diese Verfahren können lang dauern und durch mehrere Instanzen gehen. Der Fall der Jaguar-Vertragswerkstatt, die im Netz der Jaguar-Organisation bleiben wollte, nahm beispielsweise 2013 am Landgericht Frankfurt am Main seinen Ausgang – mutmaßlich nach längeren fruchtlosen Verhandlungen. Der BGH entschied 2016 darüber und verwies zurück ans Oberlandesgericht Frankfurt, das 2017 entschied. Von dort wurde offenbar erneut der Gang zum BGH gegangen, der Fall

wurde im Februar 2021 noch als beim BGH unter dem Az. KZR 2/18 „anhängig“ gemeldet.[354] So lange kann kein Handwerker warten.

Aber auch beim allgemeinen Zugangsanspruch oder bei sektoralen Ansprüchen, ja, selbst beim Modell offener Schnittstellen ist denkbar, dass sich in der Praxis Streitfragen rund um die Zugangseröffnung ergeben.

Die ungewissen Aussichten bei einem gerichtlichen Verfahren, die Kosten und der Zeitablauf stellen die Betroffenen vor die Entscheidung, ob sie das Prozessrisiko samt Kostenrisiko wirklich tragen wollen. Auch können Konstellationen vorkommen, in welchen solche Verfahren – selbst wenn sie aussichtsreich sind – allein wegen ihrer langen Verfahrensdauer und entsprechend zu späten Entscheidung für den Betroffenen nicht sinnvoll sind und dieser rational davon absehen müsste.

Anstelle einer gerichtlichen Entscheidung sollte für Streitfragen über Ob und Wie des Zugangs eine rasche Streitschlichtung vorgesehen werden. Eine solche könnte etwa durch ein privates Schiedsgericht oder eine Ombudsperson vorgenommen werden.[355] Dies wäre gegenüber einem Gerichtsverfahren schneller und kostengünstiger. Die staatlichen Gerichte leisten eine angemessen schnelle Konfliktlösung in solchen Konstellationen bislang nicht. Daher kann ein Zugangsanspruch – gerade wegen der vielen möglichen Detailfragen zu Modalitäten, Vergütung und Bedingungen, nur wirksam sein, wenn es einen hocheffizienten, raschen Konfliktlösungsmechanismus gibt. Dabei sollte ein solcher allerdings nicht von den Superplattformen vorgegeben und dominiert werden, wie es derzeit zum Teil üblich ist.

Denkbar wäre, die Durchsetzung solcher Ansprüche unter Beteiligung der Selbstverwaltungskörperschaften (z.B. Handwerkskammern) zu lösen. Sie könnten sich mit anderen Institutionen in Branchenvereinbarungen auf ein Streitschlichtungssystem verständigen, das angeboten wird und ggf. auch verpflichtend vorzusehen ist.

Ein gesondertes Problem könnte für die Weitergabe personenbezogener oder sonstiger geschützter Daten entstehen. Für diesen Fall sollten „Datentreuhänder“ eingesetzt werden, die als Clearing-Stellen darauf achten, dass besonders sensitive Daten nicht weitergereicht werden. Einen entsprechen-

354 Siehe zur Verfahrenshistorie https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=OLG%20Frankfurt&Datum=21.12.2017&Aktenzeichen=11%20U%206/14.

355 Dazu auch *Podszun*, Gutachten F zum 73. Deutschen Juristentag, 2020, S. F100.

den, aber nicht besonders weitgehenden Vorschlag hat die EU-Kommission im Data Governance Act unterbreitet.[356]

Die Schaffung weiterer Institutionen (Datentreuhänder, Streitschlichtungsstellen, Ombudspanels) ist zunächst mit höheren Kosten und ggf. zusätzlicher Bürokratie verbunden. Die zeitlichen und finanziellen Kosten eines vollen Gerichtsverfahrens sind aber für derartige Streitigkeiten nicht mehr vertretbar.

c) Regelungstechnik

Für die Umsetzung spielen Beweislastregeln eine erhebliche Rolle. Der Zugangspetent ist, nach den allgemeinen Grundsätzen, beweisbelastet für seine Behauptungen. Die Hürde für die Beweiserbringung wird durch die Beweislastverteilung gesteuert. Bei digitalen Geschäftsmodellen fehlt den Parteien häufig der Einblick, was überhaupt passiert und wie sie ggf. Zugang erlangen können. Materielle Voraussetzungen und Rechtfertigungen sind schwer überprüfbar.

Echte Abhilfe kann daher nur geschaffen werden, wenn es Automatismen, gesetzliche Vermutungen oder für den Petenten günstige Beweislastverteilungen gibt. Dazu könnte insbesondere mit dem Instrument der sekundären Darlegungslast gearbeitet werden. Die objektive Rechtfertigung ist schon im bestehenden Modell Sache desjenigen, der die Zugangsstelle besetzt hält. Bei offenen Schnittstellen ist die Anfälligkeit für Beweisschwierigkeiten besonders gering.

IV. Data-Governance-Lösungen

Alternativ zu eher punktuellen Zugangsansprüchen sind Ansätze zu verstehen, die unter dem Schlagwort „Data Governance“ diskutiert werden, und die die Regelungsaufgabe, Zugang zu eröffnen, noch grundlegender ange-

356 Europäische Kommission, 25.11.2020, Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz), COM(2020) 767 final. Vgl. zum Konzept der Datentreuhänder *Blankertz*, Designing Data Trusts, Stiftung Neue Verantwortung, 2020; siehe auch Kommission Wettbewerbsrecht 4.0, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, 2019, S. 43.

hen.[357] Die Regelungen beziehen sich überwiegend auf den Zugang zu Daten, auch wenn – wie dargelegt – die Zugangsziele weiter zu fassen sind.

1. Eigentumslösung mit Zuordnungsmodell

Zunächst könnte auf der Hand liegen, dass durch die Schaffung eigentumsartiger Rechte an Daten Klarheit erzielt werden könnte. Ein solches Recht würde zumindest eine robuste Zuordnung erreichen, sodass bestimmte Gruppen im Ausgangspunkt ein Recht an Daten als „Verhandlungschip" erhalten würden. In einem weiteren Schritt könnten dann Verhandlungslösungen für Zugang entstehen oder gesetzliche Schranken der Rechtsausübung vorgesehen werden.

Hierbei ist jedoch zu beachten, dass aufgrund des dann bestehenden Rechts an den Daten jeder nachfolgende Eingriff kompensations- und rechtfertigungsbedürftig ist. Dieses Problem stellt sich insbesondere, wenn das Dateneigentum dem Sacheigentum mit entsprechend hohem Schutz aus Art. 14 GG bzw. Art. 17 EU-GRCh gleichgestellt ist. Ein Schutz an Daten, wie er unter dem Schlagwort „Dateneigentum" diskutiert wird, würde die Zugangsproblematik daher eher komplizieren denn vereinfachen.

a) Schaffung von Rechten an Daten als Option

Die Schaffung von weitergehenden Rechten an Daten wird in der rechtspolitischen Diskussion als mögliche Lösung der Zugangsproblematik erwogen. Die dahinterstehende Logik folgt der sog. Property Rights-Theorie: Nur wenn Datenrechte normativ einem Inhaber zugewiesen werden, entsteht die für einen florierenden Handel erforderliche Rechtssicherheit, die den Zuordnungswechsel sicher ermöglicht. Das Ergebnis wirkt paradox: Es wird ein Ausschließlichkeitsrecht (wie Eigentum) geschaffen, damit Ausschlusseffekte anschließend rechtssicher durch vertragliche Lösungen abgemildert werden können.

---

357 Vgl. *Kerber*, From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems, MAGKS 40–2020, spezifisch zu connected cars *Kerber/Gill*, JIPITEC 10 (2019), 244; *Drexl*, Designing Competitive Markets for Industrial Data, Max Planck Institute for Innovation & Competition Research Paper No. 16–13, 2016, vgl. auch *Zech*, A legal framework for a data economy in the European Digital Single Market: rights to use data, JIPLP 11 (2016), 460.

Beispielhaft für das Modell von „data ownership", einem Dateneigentumsrecht, steht die bereits zitierte Studie, die 2017 für das Bundesministerium für Verkehr und digitale Infrastruktur vorgelegt wurde und mit der eine „Eigentumsordnung" für Mobilitätsdaten vorgeschlagen wurde.[358]

Hinsichtlich der Zuordnung von Rechtspositionen an Informationen wurde vorgeschlagen, diese derjenigen Person zuzuweisen, die die wesentliche Investition vornimmt, um Daten zu generieren. Terminologisch wird hier von einem Skripturakt gesprochen, der von einem Skribenten vorgenommen wird – durch den Skripturakt werde die Datenerzeugung angestoßen (und so die Information festgehalten und damit überhaupt erst zum Datum).[359] Um festzustellen, wer diese Person ist, werden mehrere Kriterien festgelegt:

> „Als wessen Verdienst ist die Generierung eines Datums anzusehen? Wer bewirkt den Skripturakt? Erstellt der Skribent das Datum für jemand anderen (bspw. Im Rahmen eines Arbeitsverhältnisses, Auftragsverhältnisses, etc.)? In Bezug auf maschinengenerierte Daten ist zu ermitteln, wer die Entwicklungs- und Produktionskosten trägt und ob diese gegebenenfalls im Rahmen der Anschaffung durch Dritte mittels einer Gegenleistung vergütet werden. Ebenfalls in Bezug auf den datengenerierenden Gegenstand ist zu ermitteln, wer die laufenden Kosten für die Unterhaltung des datengenerierenden Gegenstands trägt (Wartung, Instandsetzung, etc.). Wer trägt die Kosten für den benötigten Speicherplatz?"[360]

Nach diesen Kriterien werden die Daten, die beim Autofahren generiert werden, in der Regel wirtschaftlich dem Autohalter zugeordnet, der die Investition in den Kauf und Betrieb des Fahrzeugs getätigt hat. Der Kfz-Hersteller wird demgegenüber für seine Kosten durch die Bezahlung des Fahrzeugs entschädigt, wird aber im Wege vertraglicher Übertragung der Daten am Ende wieder der wirtschaftlich Berechtigte.

---

358 Bundesministerium für Verkehr und digitale Infrastruktur, „Eigentumsordnung" für Mobilitätsdaten?, 2017. Siehe auch *Tjong Tjin Tai*, EuCML 2018, 136.

359 Bundesministerium für Verkehr und digitale Infrastruktur, „Eigentumsordnung" für Mobilitätsdaten?, 2017, S. 101 m.w.N.

360 Bundesministerium für Verkehr und digitale Infrastruktur, „Eigentumsordnung" für Mobilitätsdaten?, 2017, S. 104 f.

b) Unterschied zu Sachgütern und immateriellen Leistungen

Bei der Diskussion um die Zuweisung von Daten im Sinne eines eigentumsartigen Ausschließlichkeitsrechts müssen Unterschiede zwischen Sacheigentum und Daten beachtet werden: Daten sind nicht-rivale Güter. Das bedeutet, dass sie ohne Wertverlust von mehreren Personen parallel genutzt werden können. Sie können auch immer wieder genutzt werden, nutzen sich also nicht ab.[361]

Eine schöpferische Idee oder eine spezifische Leistung liegt bei der Generierung von Daten in aller Regel nicht vor. Das unterscheidet Daten von den im Immaterialgüterrecht geschützten Informationen (etwa dem Inhalt eines Buches). Das gilt selbst für die Investition: Zwar müssen manche Daten aufwändig erhoben werden, das Entstehen der Information selbst ist aber häufig nicht mit Aufwand verbunden: Die Zahl der Vorgänge, die von einer Maschine bearbeitet werden, entsteht durch das Arbeiten der Maschine. Die einzige Investition liegt im Anbringen eines Zählers, es ist aber nicht die Information selbst, die Aufwand erfordert. Das liegt in der Natur von Daten als Informationen, die reale Vorgänge abbilden – die Vorgänge passieren nicht, um Informationen zu generieren, sondern Informationen entstehen automatisch durch die entsprechenden Vorgänge.

Erfassung, Sammlung, Analyse, Verwertung von Daten – das ist der Kern der Investition, nicht aber das Entstehen der Daten selbst. Der Schutz dieser Leistungen kann – wie dargestellt – ggf. über Schutzrechte erfolgen, etwa wenn für die Sammlung und Anordnung von Informationen ein Datenbank-Schutzrecht gewährt wird. Davon ist aber der Schutz des Datums selbst zu differenzieren.

c) Kritik an einer Schutzrechts-Lösung

Ein an Eigentumsrechte angelehnter Schutz, der zukünftig geschaffen werden könnte, wäre kontraproduktiv für die Verteilungsprobleme der Wirtschaft und für die Innovationskraft.

Das Münchner Max-Planck-Institut für Innovation und Wettbewerb hat in einer Stellungnahme festgestellt, dass es weder eine rechtliche noch eine wirtschaftliche Rechtfertigung für die Schaffung eines Ausschließlichkeits-

361 Es gibt demnach bei Daten nicht das Problem der "Tragik der Allmende" (tragedy of the commons).

rechts an Daten gibt.[362] Es gibt keinen Rechtsgrundsatz, dass Daten ausschließlich einem bestimmten Rechtssubjekt zuzuordnen sind. Aus ökonomischer Sicht warnt das Max-Planck-Institut vor Interventionen, die die Entwicklung von Märkten behindern könnten. Es lässt sich nicht eindeutig vorhersagen, wie sich ein exklusives Recht an Daten in der Praxis auswirken würde. Die Autoren weisen ausdrücklich darauf hin:

> „Nach heutigem Kenntnisstand gibt es auch keine wirtschaftlichen Gründe für die Anerkennung von Ausschließlichkeitsrechten an Daten. Im Gegenteil, dies würde die Gefahr einer Beeinträchtigung der unternehmerischen Freiheit und der Wettbewerbsfreiheit, die Gefahr einer Behinderung der Geschäftstätigkeit anderer Marktteilnehmer, die vom Zugang zu Daten abhängig sind, und negative Auswirkungen für die Entwicklung nachgelagerter Datenmärkte mit sich bringen. Bedenken ergeben sich wegen der Stärkung von vorhandener Datenmacht und der Schaffung neuer Marktmacht auf der Grundlage von Daten, was wettbewerbswidrige Marktzutrittsschranken begünstigen würde."[363]

In dieser Aussage sind die wesentlichen Gründe benannt, die gegen eine exklusive Zuweisung eines Rechts an Daten sprechen. Hier wird die Gefahr der Abhängigkeit derjenigen Unternehmen, die auf nachgelagerten Märkten tätig sind, gesehen.[364] Die Gefahr, dass Wettbewerb durch ausschließliche Zugriffsmöglichkeiten zurückgedrängt wird, wird als schädlich gekennzeichnet. Es kommt durch Exklusivzuweisungen zur Stärkung von Datenmacht, was Asymmetrien mit sich bringt, die einer wettbewerblichen und fairen Entwicklung abträglich sind. Es müsste mit verschiedenen Maßnahmen gegengesteuert werden, um diese Negativfolgen eines Dateneigentums auszubalancieren. Ein generelles Marktversagen, das die Einführung eines Schutzrechts rechtfertigen würde, vermögen die Autoren folglich nicht zu erkennen. Sie bringen vielmehr einen Gedanken aus dem Informationsrecht gegen das Dateneigentum in Stellung: Daten verkörpern Informationen. Informationen aber sollen in einer Gesellschaft frei sein. Der freie Zugriff auf Informationen, der Austausch und die Nutzung

362 MPI, Data Ownership and Access to Data, Position Statement 16 August 2016. Kritisch auch *Schöler* in: FS Harte-Bavendamm, 2020, S. 82 ff. m.w.N.

363 MPI, Data Ownership and Access to Data, Position Statement 16 August 2016, S. 2.

364 In der Studie für das Bundesverkehrsministerium waren diese Folgeeffekte, wie oben gesehen, ja gänzlich ausgeblendet geblieben.

von Informationen sind wesentliches Kapital einer offenen Gesellschaft. Informationsmonopole sind weder gesellschaftlich noch wirtschaftlich sinnvoll.

Hinzu treten erhebliche Nachteile für Innovationswirkungen: Die Zusammenführung von Daten, der Blick auf Daten durch verschiedene, diverse Unternehmen eröffnet gerade erst das technologische Potential der Datenökonomie. Gerade das Handwerk, das als besonders innovativ gilt und das einen direkten Anwendungsbezug hat, hat das Potenzial für weitere Entwicklungen und Verbesserungen. Das setzt aber einen relativ ungehinderten Zugang zu Daten voraus. Eine ausschließliche Zuweisung von Daten zu einer Person konterkariert diesen essentiellen Bestandteil der „big data"-Potenziale.

Würde beispielsweise der Halter das ausschließliche Recht an den Daten haben, die beim Autofahren erzeugt werden, wäre das Innovationspotential beinahe gänzlich verschenkt: Die Koordination der Telematik im Straßenverkehr wäre von der Zustimmung der Fahrzeughalter abhängig. Sichert sich der Fahrzeughersteller oder -verkäufer den Zugriff auf die Daten (da er der erste ist, der mit dem Käufer eines Fahrzeugs in Kontakt kommt, hat er auch die besten Möglichkeiten, ein Einverständnis in entsprechende Geschäftsbedingungen zu erhalten), wären Zulieferer, Kfz-Werkstätten, Verkehrsplaner, Forscher, Mobilitätsanbieter und alle anderen, die im Segment Fahrzeug- und Verkehrsentwicklung tätig sind, für eine Nutzung auf die Zustimmung des Herstellers angewiesen. Das würde Innovationsbarrieren aufbauen und die Transaktionskosten in die Höhe treiben: Für jede Nutzung könnte eine Lizenzgebühr verlangt werden, es wären Verhandlungen erforderlich. Der technologische Vorteil der Datenerhebung im Auto würde verpuffen.

Die Einführung eines Eigentumsrechts an Daten würde auch hohe Kosten verursachen. Die zu klärenden Fragen – welche Daten, welche Inhalte, welche Berechtigten, welcher Schutzumfang, welches Schutzniveau, welche Durchsetzung, welche Ausnahmen und Schranken usw. – würden erheblichen politischen und rechtlichen Aufwand voraussetzen, ohne dass auch nur annähernd zu erwarten wäre, dass die Fragen erschöpfend beantwortet werden.

Wesentliches Argument für die Einführung eines Dateneigentumsrechts ist die Überlegung, dass durch die Festlegung eines Inhabers Daten besser greifbar und handelbar und damit verwertbar werden. Die Annahmen einer solchen Property Rights-Theorie greifen allerdings schon nicht: Anders als bei Sachgütern droht bei fehlender Zuweisung keine „Übernutzung" oder „Abnutzung" von Daten, da sie ja gerade nicht-rival sind und

vielfach nutzbar sind. Es muss auch keine Leistung belohnt werden (samt entsprechender Anreizwirkung), da die Datenentstehung kollateral/automatisch erfolgt. Andere externe Effekte, die durch eine Rechtszuweisung internalisiert würden, sind nicht erkennbar.

Lehnt man sich an den Schutz des geistigen Eigentums als Vorbild für eine solche Rechtszuweisung an, sollte beachtet werden, dass gerade Schutzsysteme wie das Urheber- und Patentrecht zu Negativwirkungen geführt haben, die immer sichtbarer werden: Im Bereich der Telekommunikation beispielsweise haben die beteiligten Unternehmen kaum mehr Bewegungsfreiheit („freedom to operate"), da sie in einem engen Korsett von Patenten anderer Unternehmen befangen sind. Sperrpatente führen mittlerweile zu Innovationsschranken, obwohl die Idee des Schutzrechts war, Innovation anzureizen.

Es ist leicht ersichtlich, dass bei Daten eine ähnliche Gefahr droht: Einzelne Dateninhaber könnten mit ihren Rechten wichtige Entwicklungen blockieren oder Monopolrenten extrahieren, die für Innovation und Preisentwicklung schädlich wären.

Fritz Machlup hat bereits 1958 in einer berühmten Studie ein kritisches Fazit zu den Auswirkungen des Patentrechts gezogen:

> „Wenn wir kein Patentsystem hätten, wäre es unverantwortlich, auf der Grundlage unseres derzeitigen Wissens über die wirtschaftlichen Folgen dieses Systems die Einführung eines solchen Systems zu empfehlen."[365]

Die Vorbehalte von Ökonomen gegenüber der Schaffung neuer Schutzrechte sind seitdem eher gestiegen. Für den Bereich der Daten ist weder eine Fehlentwicklung dieser Art erkennbar, noch ist auch nur im Ansatz ersichtlich, wie ein Dateneigentumsrecht sinnvoll ausgestaltet werden könnte, ohne dass monopolistische Strukturen entstünden und Innovationspotentiale verloren gingen. Die Schaffung weitergehender Rechte an Daten ist daher gegenwärtig abzulehnen.[366] Die Zugangsthematik würde dadurch erschwert, nicht erleichtert. Das ist auch deshalb stimmig, da es, wie bereits gesehen, nicht zwingend der Zugriff auf bestimmte Rohdaten oder Informationen ist, sondern der Zugang zum Kunden, auf den sich das eigentliche unternehmerische Interesse richtet. Zugang zu Daten ist für Handwerksbetriebe kein Selbstzweck, sondern notwendige Vorbedin-

365 *Machlup*, An Economic Review of the Patent System, Study for the US Senate, 1958, S. 80.

366 So auch *Resta* in: Pertot, Rechte an Daten, 2020, S. 244.

gung, um ein Gerät reparieren, eine Heizung warten oder ein Smart Home ausbauen zu können.

Es sollte jedoch noch einmal ins Bewusstsein gerufen werden, dass rein faktisch exklusive Zugriffsrechte bereits bestehen können und zum Teil auch abgesichert werden.[367]

2. Modell der offenen Datenräume

Einige politische Initiativen auf europäischer und deutscher Ebene sind in die Richtung eines Modells offener Datenräume (EU-Kommission) oder eines Daten-für-alle-Modells (SPD) entwickelt worden.

a) EU-Daten-Governance-Verordnung

Auf europäischer Ebene wird der Problematik der heterogenen Regelungslandschaft mit der Datenstrategie Rechnung getragen, die 2020 vorgestellt wurde.[368] Erste Ansätze für ein vielversprechendes Modell offener Datenräume lassen sich erkennen. Sie sind im Vorschlag der Europäischen Kommission für eine Europäische Daten-Governance-Verordnung niedergelegt.[369]

Die Zielsetzung ist durchaus vielversprechend. Die EU-Kommission hat drei Punkte vorgesehen, die sie künftig erleichtern will:

Erstens sollen Daten des öffentlichen Sektors zur Weiterverwendung bereitgestellt werden, auch wenn diese Daten den Rechten anderer unterliegen.[370] Für 2021 wurde ein noch zu entwickelnder „Durchführungsrechtsakt über hochwertige Datensätze" angekündigt, der jedenfalls einen kostenlosen Zugangsanspruch zu Datensätzen der öffentlichen Hand in maschinenlesbarer Form schaffen soll.[371] Der Informationsbestand der öffentlichen Hand kann, so die Idee, durch eine weitergehende Öffnung zum

367 Siehe das Beispiel der Automobilwirtschaft unter D.II.1.

368 Europäische Kommission, Mitteilung vom 19.2.2020, Eine europäische Datenstrategie, Dokument COM(2020) 66 final.

369 Europäische Kommission, Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz), 25.11.2020, COM(2020) 767 final.

370 Europäische Kommission, Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz), 25.11.2020, COM(2020) 767 final, Kap. II des VO-Vorschlags.

371 Europäische Kommission, COM(2020) 66, S. 15.

Nukleus neuer Ideen, Erfindungen und Geschäftsideen werden. Schon jetzt gibt es erste Zugangsrechte zu „Public Sector Information".[372]

Es soll außerdem der „Datenaltruismus" gefördert werden, also die Datenspende für nicht-gewerbliche Zwecke.[373]

Für die vorliegende Untersuchung besonders interessant ist, dass die „gemeinsame Datennutzung durch Unternehmen gegen Entgelt in jedweder Form" erleichtert werden soll.[374] Dazu wird ein rechtlicher Rahmen für Datendienstleister gesetzt, aus dem heraus sich Konturen ergeben, wie sich die Kommission die Unterstützung gerade der kleineren und mittleren Unternehmen vorstellt. Die nach den geplanten Vorschriften vorgesehenen Datendienstleister sollen als Mittler agieren, die den Datenaustausch zwischen verschiedenen Personen organisieren und dabei berechtigte Interessen und Rechte wahren, etwa bei personenbezogenen Daten („Datentreuhänder"). Dazu sind eine Anmeldung dieser Mittler (zu denen auch Plattformanbieter, Datenbankdienstleister und Datengenossenschaften gehören können) bei einer Behörde vorgesehen sowie ein Katalog an Bedingungen, die derartige Dienstleister einhalten müssen.[375] Durch die Regulierung dieser Dienste soll offenbar ein Rechtsrahmen geschaffen werden, der das notwendige Vertrauen im B2B-Datenaustausch schafft, um die Nutzung solcher Dienste zu fördern. Dazu muss ein hohes Sicherheitsniveau gewährleistet werden und die Wettbewerbsvorschriften müssen beachtet werden. Dafür darf in gewissem Umfang Interoperabilität hergestellt werden. Einen eigenen Anreiz zur Teilnahme an derartigen Austauschverfahren setzt die Verordnung allerdings nicht.

Weitergehend sieht die Kommission in ihrer Datenstrategie – eher unverbindlich – die Schaffung von „europäischen Datenräumen" in bestimmten Sektoren vor, die durch eine Kombination aus rechtlichen und

372 Vgl. die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors.

373 Europäische Kommission, Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz), 25.11.2020, COM(2020) 767 final, S. 1.

374 Europäische Kommission, Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz), 25.11.2020, COM(2020) 767 final, Kap. IV.

375 Europäische Kommission, Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz), 25.11.2020, COM(2020) 767 final, Kap. III.

technischen Rahmenbedingungen geschaffen werden sollen. Die Zielbestimmung lautet:

> „Ziel ist die Schaffung eines einheitlichen europäischen Datenraums, eines echten Binnenmarkts für Daten, der für Daten aus aller Welt offensteht, in dem sowohl personenbezogene als auch nicht-personenbezogene Daten, darunter auch sensible Geschäftsdaten, sicher sind und in dem Unternehmen auch leicht Zugang zu einer nahezu unbegrenzten Menge hochwertiger industrieller Daten erhalten."[376]

Die Umsetzung dieses doch eher hochtrabend formulierten Ziels bleibt einstweiligen wolkig. Offenbar soll durch einen klaren Rechtsrahmen und Governance-Strukturen eine größere Sicherheit beim Datenaustausch geschaffen werden. Der Data Governance Act als erste vorgeschlagene Maßnahme leistet dazu nur einen kleinen Beitrag. Bei den weiteren Schritten ist aus Sicht des Handwerks insbesondere darauf zu achten, dass die entsprechende Rechtsetzung nicht durch solche Unternehmen dominiert wird, die in ohnehin besonders datenmächtig sind.

b) Daten für alle-Gesetz

In Deutschland hatte die damalige SPD-Vorsitzende Andrea Nahles 2019 den Vorschlag eines „Daten für alle-Gesetzes" unterbreitet. Die Forderung besteht aus drei Kernpunkten:

> „Nutzung von nicht-persönlichen Daten als Gemeingut; Aufbrechen von Datenmonopolen durch eine Datenteilungspflicht für marktdominante Unternehmen; Schaffen von Anreizen zum Datenteilen und Etablierung und Ermöglichung eines sicheren europäischen Datenraums unter Wahrung des Datenschutzes."[377]

Damit wird zum einen die oben skizzierte Idee des europäischen Datenraums aufgegriffen. Akzentuiert wird, dass die Sicherheit von Daten, der Schutz personenbezogener Daten, der Respekt vor Geschäftsgeheimnissen und Immaterialgüterrechten sowie eine Verlässlichkeit und Vertrauens-

376 Europäische Kommission, 19.2.2020, Eine europäische Datenstrategie, COM(2020) 66 final.

377 *Nahles*, Digitaler Fortschritt durch ein Daten-für-Alle-Gesetz, Diskussionspapier, 12.2.2019, S. 5.

würdigkeit von – behördlich überwachten – Datendienstleistern gewährleistet ist.

Weitergehend sind die beiden anderen Punkte: Die Nutzung nicht-persönlicher Daten als Gemeingut konkretisiert Nahles dahingehend, dass

> „Daten, die als Gemeingut anzusehen sind, grundsätzlich einer Nutzung zugänglich zu machen sind. Dazu zählen Daten in vollständig anonymisierter und aggregierter Form wie Mobilitätsdaten oder Geodaten. Die Daten sollten von öffentlichen und privaten Akteuren zugänglich gemacht und ggfs. auch in vertrauenswürdigen Datenräumen zusammengeführt werden, um sie zivilgesellschaftlichen, aber auch privatwirtschaftlichen Akteuren für soziale oder auch ökonomische Innovationen zur Verfügung zu stellen. Wie das Zusammenführen konkret ausgestaltet wird (Treuhand, Stiftung, etc.) und welcher Aufsichtsbehörden bzw. Institutionen es dazu bedarf, ist zu diskutieren."[378]

Damit werden zwar Zugangsprobleme individueller Art (zu einem konkreten Smart Home z.B.) nicht gelöst, es würde aber ein großes Innovationspotenzial freigesetzt, das von vielen verschiedenen Akteuren genutzt werden könnte. Dieser Vorschlag ist äußerst weitreichend, weil er letztlich die komplette Offenlegung vieler nicht-personenbezogener Daten umfassen könnte. Für datenbasierte Innovationen wäre das ein großer Schritt.[379]

Der andere entscheidende Schritt wäre die Datenteilungspflicht für marktbeherrschende Unternehmen. Die Autorin schlägt vor:

> „Sobald ein Unternehmen einen bestimmten Marktanteil für eine bestimmte Zeit überschreitet, muss es einen Teil seiner Daten anonymisiert öffentlich machen. Andere Unternehmen sollen dann mit diesen Daten arbeiten können und eigene Produkte und Dienste an den Markt bringen."[380]

Diese Lösung würde einen Automatismus beinhalten und würde damit über die Einzelfallgewährung von Zugang, wie im Kartellrecht, hinausgehen. Die Anonymisierung würde wiederum die Signifikanz für den Einzelfall aufheben. Auch sonstige geschützte Daten und Analysedaten würden wegen der darin vorhandenen Wertschöpfung von der Teilungspflicht aus-

---

378 *Nahles*, Digitaler Fortschritt durch ein Daten-für-Alle-Gesetz, Diskussionspapier, 12.2.2019, S. 5.

379 Siehe auch *Busch*, Der Mittelstand in der Plattformökonomie, WISO Diskurs 8/2019, S. 18.

380 *Nahles*, „Die Tech-Riesen des Silicon Valleys gefährden den fairen Wettbewerb", Handelsblatt 13.8.2018.

drücklich ausgenommen. Handwerker brauchen für ihre konkrete Leistungserbringung konkrete, individualisierte Daten.

Der Vorschlag der SPD ist ein weitgehender Impuls, hilft aber für die hier interessierende Problematik nur begrenzt weiter. Es lassen sich daran aber in besonderer Weise interessante Aspekte ablesen: Die DS-GVO mit dem Schutz personenbezogener Daten hat in eine regulatorische Falle geführt, indem kategorisch um die Weitergabe personenbezogener Daten herum ein Problem aufgebaut wird. Ob es überhaupt (angesichts der auch in der DS-GVO vorgesehenen Ausnahmetatbestände) ein Problem gibt, tritt angesichts der Komplexität der DS-GVO in den Hintergrund. Ebenso bleibt unklar, ob beispielsweise die Weitergabe von Heizungsdaten von einem Smart Home-Betreiber an einen Handwerksbetrieb tatsächlich ein Problem darstellt, das durch Datenschutzvorschriften gestoppt werden sollte.

Der Vorschlag wirft aber auch Licht auf die Problematik der Rohdaten: Vielen Handwerksbetrieben würde mit der Öffentlichmachung großer Teile von Rohdaten marktbeherrschender Unternehmen nicht geholfen, sie könnten damit nicht viel anfangen. Datenanalyse ist nicht ihre Kernkompetenz. Auch wenn die Fähigkeiten in diesem Feld wachsen (und von handwerksnahen Verbänden und Dienstleistern angeboten werden können), bleibt der Kern der Leistungserbringung auf anderen Feldern. Dafür sind nicht Rohdaten erforderlich, sondern häufig eher Zugang zu einem Dashboard oder zu bearbeiteten Daten oder zum Kunden. Der Fairness halber ist anzumerken, dass der Fokus des „Daten für alle"-Vorschlags auch nicht in der Abmilderung des hier behandelten Problems liegt, sondern in der Ermöglichung von Innovation auf breiter Basis durch verschiedene Akteure, die Zugriff auf Daten erhalten sollen, die sonst faktisch monopolisiert werden können. Dafür ist der Vorschlag geeignet.

c) Stufenmodelle

Ein weiteres Datenzugangsmodell sieht eine Klassifikation von Daten je nach Art der Daten, nach Schutzbedürfnissen und kommerzieller Bedeutung vor. Daten könnten nach bestimmten Kriterien so geclustert werden. In einer Art Stufenmodell könnte Zugang dann differenziert ausgestaltet werden: Je nach Klassifikation kann dann verschiedenen Gruppen von Anspruchstellern Zugriff auf die Daten gewährt werden.

Dieses Modell kann insbesondere Datenschutzbedenken und anderen berechtigten Interessen Rechnung tragen. Allerdings ist die Aufspaltung von Daten in verschiedene Cluster praktisch wohl nur schwerlich möglich.

3. B2B-Kooperationen als Chance des Handwerks

Zugangsansprüche gegenüber Dritten sind immer nur ein Behelf. Sie sind, wenn das Verfahren konfrontativ läuft, schwierig durchzusetzen, von zahlreichen komplexen Rechtsfragen überlagert, es muss in der Regel eine Vergütung entrichtet werden, die technische Umsetzung ist nicht trivial. Handwerksunternehmen, die Zugangsansprüche geltend machen müssen, sind in der Defensive.

Für das Handwerk mit seiner fragmentierten Struktur ist es deshalb von zentraler Bedeutung, eine eigene Datenmacht oder wettbewerbliche Gegenmacht aufzubauen und so in eine aktiv gestaltende Position in der Datenökonomie zu rücken. Ohne die Leistungserbringung seitens der individuellen Handwerksbetriebe vor Ort funktioniert kein Smart Home und fährt kein Auto. Es gibt daher grundsätzlich auch ein großes Bedürfnis der Datenkonzerne – die ja keinen Tisch schreinern und kein Zahnmodell einpassen können – mit dem Handwerk zusammenzuarbeiten.

Der Aufbau einer entsprechenden Gegenmacht müsste über B2B-Kooperationen oder Datenpool-Lösungen funktionieren. In den Pools wären Daten, Software u.a. essentielle Digitalwerkzeuge zu sammeln und zur Verfügung zu stellen. So könnte Verhandlungsmacht aufgebaut werden, es könnten eigene, interoperable Datenformate entwickelt werden, das Datensharing würde erleichtert.

Die so gebildeten B2B-Plattformen würden die Eigenständigkeit und die kommerziellen Interessen der angeschlossenen Betriebe wahren. Dazu müsste freilich eine gemeinsame Anstrengung der Handwerksunternehmen (ggf. nach Gewerken sortiert) erfolgen. Es wären auch rechtliche Weichenstellungen vorzunehmen, die im Folgenden skizziert werden sollen. Wenn hier von Datenpools die Rede ist, so lassen sich die Ausführungen auch auf IoT-Netzwerke und sonstige B2B-Kooperationen übertragen.

a) Definition von Datenpools

Datenpools sind digitale Infrastruktureinrichtungen, in denen Unternehmen in Bezug auf einen bestimmten Markt oder Dienst, oder genereller in

Bezug auf eine Industrie oder ein digitales Ökosystem Daten austauschen oder digitale Werkzeuge vorhalten.[381] Eine derartige Zusammenführung von Daten kann für bestimmte Innovationen zwingend erforderlich sein, so z.B. um autonom-fahrende Fahrzeuge zu ermöglichen.[382] In anderen Bereichen mag zwar keine zwingende Notwendigkeit bestehen, um eine Ware oder Dienstleistung anbieten zu können, allerdings sind Effizienzvorteile denkbar. So können Kosten für Forschung und Entwicklung gesenkt werden, wenn Daten oder Forschungsergebnisse miteinander geteilt werden.[383]

In Datenpools sollten Daten und digitale Werkzeuge gesammelt und den Pool-Teilnehmern zur Verfügung gestellt werden. Der Datenpool-Betreiber dürfte nicht mit eigenem Gewinnerzielungsinteresse handeln (um den Missbrauch und den Aufbau eines neuen Marktbeherrschers zu vermeiden) und würde im Wesentlichen die Organisation des Datenaustauschs, die Rechtewahrung und die Herstellung von Interoperabilität gewährleisten – ähnlich den Vorstellungen der Europäischen Kommission für Datendienstleister (siehe oben).

In Datenpools vereinbaren Unternehmen und andere Akteure, ihre Daten zu bündeln, d.h. in eine gemeinsame Infrastruktur einzuspeisen. Die Verteilung oder der Zugriff auf den Pool kann auf unterschiedliche Weise organisiert werden, in der Regel über einen Betreiber, der die Interoperabilität der Daten sicherstellt. Teilnehmer des Pools können in der Regel auf die Daten anderer zugreifen und diese in irgendeiner Form nutzen. Datenpools sind vergleichbar mit Patentpools, wie sie in den Leitlinien zum Technologietransfer der EU-Kommission definiert sind.[384] Die im Pool gesammelten Informationen werden in der Regel allen Mitgliedern in der ursprünglichen oder einer modifizierten Form zur Verfügung gestellt.

b) Bedingungen der Pool-Mitgliedschaft

Für jeden Pool müsste eine Satzung ausgearbeitet werden, die die Nutzungsbedingungen darlegt. Solche Satzungen könnten branchenweit Maß-

381 Vgl. *Lundqvist*, EuCML 2018, 146.
382 *Lundqvist*, EuCML 2018, 146, 147.
383 *Lundqvist*, EuCML 2018, 146, 147.
384 Europäische Kommission, Leitlinien zur Anwendung von Artikel 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Technologietransfer-Vereinbarungen, ABl. 2014 C 89/03, Rn. 244.

stäbe setzen. Mustersatzungen der Verbände würden die Transaktionskosten senken. Das würde das mühsame Aushandeln oder Festlegen aller Bedingungen im Einzelfall ersparen. Die Modelle sollten auf den folgenden Kernbestimmungen beruhen:

Der Zugang zu Daten wird nicht bilateral, sondern auf Poolbasis gewährt: Die Daten werden in einen Pool eingebracht und müssen auf Gegenseitigkeits-Basis zugänglich gemacht werden. Alle relevanten Unternehmen der Branche können dem Pool beitreten. Ob auch Industrieunternehmen und Datenunternehmen beitreten können, wäre eine wirtschaftliche Überlegung, die zu klären wäre.

Der Pool soll von einem Unternehmen betrieben werden, das nicht in den Märkten tätig ist, für die der Pool gedacht ist. Ein solches Unternehmen könnte sich unparteiisch mit den technischen Fragen der Datenverwaltung, Datensicherheit und Interoperabilität befassen.

Der Betrieb des Pools wird durch die Satzung bestimmt, die auf einem Standardmodell basiert, das von den Wettbewerbsbehörden oder der Europäischen Kommission bestätigt wird. Um Governance-Probleme zu minimieren, wählt der Pool eine Ombudsperson, die anstehende Probleme unbürokratisch entscheidet.

Die Daten im Pool müssen regelmäßig aktualisiert werden, typischerweise in einem Live-Streaming-Szenario. Der Betrieb des Pools sollte zunächst auf eine Laufzeit von ca. drei Jahren begrenzt sein (mit der Möglichkeit der Verlängerung). Damit würde die Bindung angesichts des noch experimentellen Charakters von vornherein begrenzt.

Auf Antrag eines Unternehmens wird die finanzielle Entschädigung für das Einstellen der Daten in den Pool durch einen externen, unabhängigen Gutachter festgelegt, im Übrigen wäre die Vergütung entweder auf Reziprozitätsbasis bereits abgegolten, oder es müsste eine FRAND-artige Lösung gefunden werden. Denkbar wäre alternativ auch, dass jedes Unternehmen die Konditionen für seine Daten im Rahmen einer Auswahl verschiedener Lizenzmodelle selbst bestimmen kann.

Die Bedingungen wären in den Musterlizenzen festgelegt, vergleichbar mit den verschiedenen Lizenzen für Inhalte im Internet (z.B. Creative-Commons-Lizenz). Die Wahl der Bedingungen führt zu Gegenseitigkeit und kann die Vergütung beeinflussen. Falls die Bedingungen das Wettbewerbsziel des Pools unerreichbar machen, kann die Ombudsperson entscheiden.

Die hier skizzierten Bedingungen sollen vor allem gewährleisten, dass eine reibungslose Kooperation in derartigen B2B-Netzwerken möglich ist und Transaktionskosten gering bleiben. Zudem ist darauf zu achten, dass

es für alle Unternehmen (auch solche unterschiedlicher Größe) Anreize gibt, am Pool zu partizipieren. Nur dann können sich die Chancen solcher Handwerker-Pools umfassend entfalten.

c) Perspektiven der Kooperation

Das Datenpool-Modell hat auch die Europäische Kommission in den Blick genommen. 2017 hat sie vorgeschlagen, das Problem der standardessentiellen Patente durch eine derartige Lösung zu minimieren – insbesondere durch die Standardisierung der Lizenzierungsvorgaben, sodass Streitpunkte, die zu langwierigen Konflikten führen können, gar nicht erst entstehen könnten.

Die Europäische Kommission sollte beginnen, mit Vertretern der Wirtschaft zusammenzuarbeiten, um Standards für Vereinbarungen zur gemeinsamen Nutzung von Daten oder Datenpools festzulegen. Idealerweise würde die Kommission mehrere „Modelle" für Satzungen von Datenpools vorlegen. Diese Standardmodelle wären der Bezugspunkt in Fällen, in denen der Zugang zu Daten beantragt wird.

Die Kooperation von Handwerksunternehmen dürfte sich nicht nur in einem Datenaustausch-Programm mit standardisierten Lizenzen erschöpfen. Es müsste zugleich der Ausgangspunkt für den Aufbau eigener Dateiformate, Innovationen und Produkte sein – die Zusammenarbeit des Handwerks könnte hier den Anstoß zu ganz neuen, handwerkstauglichen Geschäftsmodellen leisten, die die Vereinzelung aufbrechen und die kollektive Stärke des Handwerks nutzen.

d) Vereinbarkeit mit dem Wettbewerbsrecht

Kooperationsmodelle, wie sie hier zur Schaffung eigener handwerklicher Zugangslösungen angedacht sind, sind kein völlig neues Phänomen. Sie sind auch schon Gegenstand kartellrechtlicher Entscheidungen geworden, da sie durchaus wettbewerbliche Probleme aufwerfen können.

In mehreren Fällen hat das Bundeskartellamt inzwischen über die Bildung von B2B-Plattformen entschieden, bei denen auch der Datenaustausch Thema war. Die kartellrechtlichen Leitlinien aus der *Asnef-Equifax*-Rechtsprechung des EuGH, die sich auch in den sog. Horizontalleitlinien der Europäischen Kommission niedergeschlagen haben, sind nach wie vor

ein Stolperstein für derartige Kooperationsmodelle.[385] Gibt es solche Data-Pools erst einmal, sind in den Markt neu eintretende Unternehmen in praktisch gleicher Weise auf den Datenzugang angewiesen, wie dies bei standardessenziellen Patenten der Fall ist.[386]

Der bekannte EU-Wettbewerbsrechtsfall *John Deere*, in dem es um die staatlich veranlasste "UK Agricultural Tractor Registration Exchange" ging, war ein System des Informationsaustausches, das man heute als Datenpool bezeichnen würde. In diesem Fall registrierten die Hersteller und Importeure von Traktoren bestimmte Daten bei einem britischen Verband. Erklärtes Ziel war es, die Dienstleistungen in ländlichen Gebieten zu verbessern. Tatsächlich wurde festgestellt, dass die damalige Vereinbarung über die gemeinsame Nutzung von Daten eine Beschränkung des Wettbewerbs und der Importe darstellte und eine Marktzutrittsschranke für andere Unternehmen bildete. Es kam zur kartellrechtlichen Untersagung.[387]

Das Recht des Informationsaustauschs im Kartellrecht bleibt in permanenter Entwicklung. Heute haben Datenpools eine neue quantitative und qualitative Dimension – und sie können eine enorme Bedeutung für den Wettbewerb erlangen. Datenpools dienen stärker denn je der Innovation. Während der Informationsaustausch im Fall *John Deere* vor allem dem Zweck diente, einzelne Leistungen der beteiligten Unternehmen besser zu verteilen, mag dies bei den heutigen Pools anders sein. Zumindest in einigen Fällen können die Pools Big-Data-Anwendungen ermöglichen, was eine Voraussetzung für eine Freistellung nach Art. 101 Abs. 3 AEUV wäre. Wenn neue Produkte oder Technologien entwickelt werden oder ein Feld für größere datengesteuerte Systeme eröffnet wird, sollte das Kartellrecht nicht im Weg stehen, da es innovationsoffen ist.

Aus wettbewerbsrechtlicher Sicht stellen sich bei der Organisation der Zusammenarbeit von Unternehmen derselben Branche zwei Probleme: Die Rolle des Betreibers der Plattform hat das Potenzial zum Machtmissbrauch. Zudem können Unternehmen die Koordinationsmechanismen nutzen, um sich in wettbewerbswidriger Weise abzusprechen.

Das erste Problem wird in den oben genannten Modellen durch die Verpflichtung zu einem unabhängigen, neutralen Betreiber und einer markt-

385 EuGH, 23.11.2006, Rs. C-238/05, ECLI:EU:C:2006:734 – *Asnef-Equifax*; Europäische Kommission, Leitlinien zur Anwendbarkeit von Artikel 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit, ABl. 2011 C 11/1, Rn. 55 ff.; vgl. *Podszun/Bongartz*, BB 2020, 2882, 2888 f.; *Lundqvist*, EuCML 2018, 146, 150.

386 *Richter/Slowinski*, IIC 2019, 4, 22.

387 EuGH, 28.5.1998, Rs. C-7/95 P, ECLI:EU:C:1998:256 – *John Deere*.

unabhängigen Governance-Struktur adressiert. Diese Lösung kommt der Entscheidung des Bundeskartellamts im Fall der Klöckner-Plattform *XOM Metals* nahe, wo es eine Trennung des Poolbetriebs von den anderen mit dem Pool verbundenen Geschäften von Klöckner forderte.[388]

So sollten Gatekeeping-Probleme (z.B. nicht oder zu unlauteren Bedingungen gewährter Zugang zum Pool) vermieden werden, die für andere Fälle typisch sind. Die Unabhängigkeit des Betreibers soll auch das Risiko von Exklusivverträgen, Kopplungsgeschäften oder anderen Praktiken vermeiden, die unter anderen Bedingungen von den so entstehenden Netzwerken ausgehen können.

Das Koordinationsproblem wird von den Wettbewerbsbehörden häufig sehr kritisch gesehen. In den Vorschlägen der EU-Kommission für ein Daten-Governance-Gesetz wird offenbar vorausgesetzt, dass lediglich ein wettbewerblich neutraler Austausch, etwa anonymisierter Daten, stattfindet. Das würde allerdings der Problematik nicht gerecht: Zwar kann ein Datenpool wettbewerbsabschottende Wirkung entfalten. Diese Wirkungen sind jedoch aufzuwiegen mit dem Innovationspotenzial und der Bildung wettbewerblicher Gegenmacht.

Angesichts der besonderen Herausforderungen der digitalen Ökonomie, gerade auch für KMU, scheint es geradezu notwendig, einen stärkeren Datenaustausch und eine vernetzte Zusammenarbeit zu ermöglichen – zumindest zeitlich begrenzt, quasi als Experiment unter den Augen der Wettbewerbsbehörde. B2B-Kooperationen gelten gerade für kleinere Unternehmen als unabdingbar.[389] Will man nicht die Monopolisierung ganzer Geschäftszweige durch Dateninhaber zulassen, muss es auch für KMU Möglichkeiten geben, eine gewisse Datenmacht aufzubauen. Das würde über die Pools organisiert. Hier muss sich die Europäische Kommission rechtspolitisch weiter bewegen. Das gilt auch für das Datenschutzrecht.

388 Bundeskartellamt, Fallbericht vom 27.3.2018, Aufbau einer elektronischen Handelsplattform für Stahlprodukte (XOM Metals GmbH), abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Kartellverbot/2018/B5-1-18-01.pdf. Siehe auch *Podszun/Bongartz*, BB 2020, 2882.

389 Vgl. *Haucap/Kehder/Loebert*, B2B-Plattformen in Nordrhein-Westfalen: Potenziale, Hemmnisse und Handlungsoptionen, 2020, S. 68 ff.; Kommission Wettbewerbsrecht 4.0, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, 2019, S. 58.