Stellungnahme

Rechtsfragen der digitalisierten Wirtschaft: Datenrechte

September 2019

Zusammenfassung[1]

Die digitalisierte Wirtschaft ist für ihre Entwicklung auf die Möglichkeit zur Nutzung von Daten angewiesen. Zugangs- und Nutzungsrechte für Daten kennt das geltende Recht aber nur für bestimmte Datenbestände oder als Reflex anderer Rechte. So erfassen z. B. Persönlichkeitsrecht, Sacheigentum am Datenträger und das Recht am geistigen Eigentum Daten nur mittelbar. Rechte an Daten selbst sind im geltenden Recht nicht allgemein, sondern nur in bestimmten Bereichen normiert (z. B. im Datenschutzrecht, im Gesetz zum Schutz von Geschäftsgeheimnissen, im Strafrecht oder in Spezialgesetzen). Dies wird vielfach als Lücke gesehen, die es zu schließen gelte. Daher wird bereits seit längerem diskutiert, Eigentumsrechte an Daten selbst oder gesetzliche Ansprüche auf Datenzugang einzuführen.[2]

Auch wenn **die geltenden Gesetze** Rechtsbeziehungen für Daten nicht lückenlos regeln, **decken** sie **den praktischen Regelungsbedarf weitgehend ab**. Das Prinzip der Vertragsfreiheit ermöglicht in ausreichendem Maße den Zugang zu Daten. Datenerzeuger und Dateninhaber besitzen faktische Zugangs- und Kontrollmöglichkeiten, welche sie mit Mitteln des Vertragsrechts steuern und übertragen können. Um die Möglichkeiten des geltenden Rechts besser nutzen zu können, sollten jedoch noch **bestehende Anwendungsschwierigkeiten und Rechtsunsicherheiten**, z. B. bei der Auslegung der Datenschutz-Grundverordnung (DS-GVO) oder bei der kartellrechtlichen Beurteilung von Datenkooperationen zwischen Unternehmen beseitigt und der **Open-Data-Ansatz weiter gefördert** werden.

Im Übrigen hat der Gesetzgeber bereits damit begonnen, auf abgegrenzte Regelungsbereiche zugeschnittene und aufeinander abgestimmte Rechte und Pflichten im Umgang mit Daten zu schaffen.[3] Dieser **Ansatz der begrenzten Regulierung** von Datenrechten erscheint gegenüber einer allgemeinen gesetzlichen Regelung für Daten **vorzugswürdig**. Denn dadurch können die Verschiedenartigkeit und die jeweils unterschiedlichen Nutzungszusammenhänge von Daten besser berücksichtigt, die jeweils spezifischen Interessen der Beteiligten besser zum Ausgleich gebracht und die besonderen Anforderungen im jeweiligen Regelungsbereich zielgenauer adressiert

[1] Vgl. auch die separate Kurzdarstellung der Bitkom-Position auf der Bitkom-Homepage
[2] Einige dieser Vorschläge werden in Kapitel 6 dieses Positionspapiers diskutiert.
[3] Vgl. dazu einige Beispiele unter Ziffer. 5.4 d dieser Stellungnahme

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Thomas Kriesel
Bereichsleiter Steuern,
Unternehmensrecht und -finanzierung
T +49 30 27576-146
t.kriesel@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

werden. Wie unterschiedlich der Regelungsbedarf und die auszugleichenden Interessen sind, zeigt der Blick in verschiedene Anwendungsbereiche der digitalisierten Wirtschaft.[4]

Auch zukünftig sollte **Datenzugang** – unter Beachtung der Datenschutzvorgaben – grundsätzlich **auf dem Prinzip der Vertragsfreiheit und damit auf Freiwilligkeit beruhen**. Vorhandene Datenbestände stiften den größten Nutzen, wenn Unternehmen bei ihrer Nutzung freiwillig und kooperativ zusammenarbeiten. Auch zeichnet sich bereits ab, dass sich die Bereitstellung von Datenzugang zunehmend als eigenes Geschäftsmodell etabliert und somit eventuell auftretende Defizite bei der Versorgung mit Daten weitgehend vom Markt selbst beseitigt werden können.

Ein Tätigwerden des Gesetzgebers ist nicht angezeigt, solange kein strukturelles Marktversagen nachweisbar ist**. Ein gesetzlicher Anspruch auf Datenzugang** sollte **nur zur Behebung eines** solchen **Marktversagens** im Kartellrecht **oder bei nachgewiesenen Lücken im Rechtsschutz** für anerkannte Rechtsgüter (z. B. informationelle Selbstbestimmung, Investitionsschutz) **oder zur Sicherung der Funktionsfähigkeit wichtiger digitaler Infrastrukturen** für **genau bezeichnete Datenbestände** und i**n gesetzlich begrenzten Anwendungsbereichen** eingeführt werden. Dabei muss Ziel sein, Innovationen zu ermöglichen und nicht zu hemmen, Investitionen in der Volkswirtschaft wirksam zu schützen und Überregulierung zu vermeiden. Widerstreitende Interessen müssen zu einem angemessenen Ausgleich gebracht und die Datennutzung zweckgebunden ausgestaltet werden. Der Einführung eines eigentumsähnlichen Rechts an Daten und einer voraussetzungslosen Verpflichtung zum Datenteilen (Zwangslizenzierung von Daten) steht Bitkom sehr skeptisch gegenüber.

[4] Einige dieser Anwendungsbereiche sind in Kapitel 7 dieses Positionspapiers beispielhaft dargestellt.

bitkom

Inhalt

Seite

1 Einleitung

Für digitale Geschäftsmodelle sind Daten ein wichtiger Produktionsfaktor. Zur Entwicklung der digitalen Wirtschaft sollen daher Daten für möglichst viele Interessenten, Geschäftsmodelle und Anwendungsszenarien nutzbar gemacht werden. Um die Nutzung von Daten zu verbessern, wird von Teilen der Politik und Wissenschaft vorgeschlagen, neue Zugangs- und Nutzungsrechte oder sogar ein Eigentumsrecht an Daten einzuführen.[5] Diese Stellungnahme gibt einen Überblick über die Diskussion und stellt die Position des Bitkom dar.

2 Datenkategorien

Die juristische Betrachtung von „Daten“ differenziert nach verschiedenen Ebenen und nach verschiedenen rechtlichen Zusammenhängen. So lässt sich zunächst eine semantische Ebene (Informationsgehalt der Daten) und eine technische Zeichenebene (Codierung auf dem Datenspeicher) unterscheiden. Diese Unterscheidung hat auch eine rechtliche Bedeutung. Die Frage nach dem rechtlichen Schutz für den Informationsgehalt von Daten führt in den Anwendungsbereich des geistigen Eigentums (Urheberrecht, gewerblicher Rechtsschutz). Unbefugte Veränderungen der Codierung auf einem Datenträger sind dagegen als Eingriff in das Sacheigentum am Datenträger anzusehen und damit sachenrechtlich und ggf. auch strafrechtlich relevant.

Aus technischer Sicht sind Daten maschinenlesbar codierte Zeichen, die als physikalischer oder elektronischer Zustand auf einem Datenträger gespeichert sind und zwischen Speichermedien übertragen werden können.[6] Auf der semantischen Ebene fügen sich Daten zu Eigenschaftsangaben, Sachverhalten und Zusammenhängen, d. h. zu Informationen zusammen. Kleinste informationstragende Einheit ist ein einzelnes Roh-Datum, also z. B. ein Mess- oder Zahlwert, eine Ortskennzeichnung, eine Laser- oder Sensorerfassung, ein Name. Sinn und Informationsgehalt ergeben sich aus Einzeldaten allerdings erst durch ihre Verknüpfung und durch gegenseitigen Bezug in einem Datensatz. (Einzel-)Daten müssen in Beziehung gesetzt werden z. B. zu einer Person, einem Objekt oder einem Ort. Nur so liefern sie Informationen zum Aufenthaltsort einer Person, zur Beschaffenheit eines Materials, zum Fertigungstakt einer Maschine oder zur Niederschlagsmenge an einem Ort.

In rechtlichen Zusammenhängen sind des Weiteren personenbezogene und nicht personenbezogene Daten zu unterscheiden, da das Recht an den Umgang mit personenbezogenen Daten besondere Anforderungen stellt. Als personenbezogene Daten

[5] Einige dieser Vorschläge werden in dieser Stellungnahme in Kapitel 6 diskutiert.
[6] Vgl. in diesem Sinn auch die strafrechtliche Bestimmung von Daten in § 202a Abs. 2 StGB

gelten alle „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ (Art. 4 Nr. 1 DS-GVO).[7] In der Kategorie der personenbezogenen Daten bildet das Recht weitere Klassen besonders sensibler personenbezogener Daten, die Grundlage einer rechtlich missbilligten Diskriminierung sein können: ethnische Herkunft, politische Meinung, religiöse Überzeugung, Gewerkschaftszugehörigkeit, Gesundheitszustand, Alter, sexuelle Orientierung. Diese besonderen Kategorien von Daten genießen sowohl im Datenschutzrecht als auch in sonstigen Gesetzen wie dem AGG einen besonderen Schutz, auch wenn sich der Schutzbereich der beiden Regelungsbereiche nicht vollständig deckt. Teilweise sind personenbezogene Daten auch Gegenstand eines eigenen Schutzrechts (z. B. Recht am eigenen Bild).

Nicht personenbezogen sind solche Daten, die keinen Zusammenhang zu einer konkret identifizierbaren Person aufweisen. Dies können Daten über Tiere, Maschinen, Produkte, Produktions- und Logistikprozesse, Umwelt- oder Naturzustände, Marktgegebenheiten oder auch anonymisierte Daten über Menschen sein. Für diese Arten von Daten gilt das Datenschutzrecht nicht, ihre Erhebung und Verarbeitung ist im Rahmen der allgemeinen Gesetze zulässig. Während die Unterscheidung zwischen personenbezogenen Daten einerseits und nicht personenbezogenen Daten andererseits in der Theorie klar erscheint, ist die Unterscheidung in der Praxis vielfach nicht so eindeutig und verursacht teilweise erhebliche Rechtsunsicherheiten und Anwendungsschwierigkeiten.[8]

Weitere Differenzierungen nimmt das Recht vor, um Investitionen in die Gewinnung von Informationen zu schützen. So besteht z. B. ein besonderer rechtlicher Schutz für Daten, die in den Anwendungsbereich eines Leistungsschutzrechts fallen, für Daten, deren Entstehung auf einem besonderen geistigen Schöpfungsakt beruht, und für Geschäftsgeheimnisse. Einen solchen Schutz genießen sog. Rohdaten gerade nicht. Bei Rohdaten handelt es sich um Daten, die z. B. durch Sensoren lediglich gesammelt, nach Erhebung aber noch nicht verarbeitet wurden.[9]

3 Datenbedarf in der digitalisierten Wirtschaft

Daten ermöglichen es Unternehmen, ihre Geschäftsmodelle zu verfeinern, ihre Angebote zu verbessern und zu individualisieren oder ganz neue Geschäftsmodelle zu entwickeln. Den Datenbedarf in der digitalisierten Wirtschaft sollen einige Beispiele verdeutlichen.

[7] Sobald Daten auf ein bestimmtes Subjekt oder Objekt bezogen sind, sind diese Daten bereits als Informationen anzusehen.
[8] So werden z. B. Daten über das Nutzungsverhalten einer Suchmaschine zwar von einer Vielzahl natürlicher Personen verursacht, sie können aber auch als bloße abstrakte Statistikdaten erhoben werden.
[9] Vgl. Mitteilung der EU-Kommission COM(2017) 9 final vom 10. 01.2017 „Aufbau einer europäischen Datenwirtschaft“, S. 9

Die Überwachung von Maschinen- und Geräten durch eine ständige Erhebung und Auswertung von Prozess- und Zustandsdaten und eine darauf gestützte frühzeitige und zielgenaue Wartung reduziert Ausfälle und Ausfallzeiten dieser Maschinen und Geräte (Predictive Maintenance) und ermöglicht zielgenaue Produkt- und Serviceverbesserungen.

Die Modellierung eines Produkts über Veränderung, Anpassung und Verbesserung von Produktionsdaten in einem virtuellen Raum beschleunigt den Konstruktionsprozess und hilft bei der Vermeidung von Produktions- und Transportkosten (Digital-Twin-Technology, Additive Manufacturing).

Die Analyse von Daten ermöglicht Voraussagen über zukünftiges Kaufverhalten und zukünftigen Produktbedarf (Predictive Analytics) oder besser auf die Bedürfnisse von Verbrauchern angepasste Produktangebote (individualisierte Versicherungstarife, individualisierte Werbung).

Automatischer Datenaustausch ist Voraussetzung für das Internet of Things oder das vernetzte sowie das autonome Fahren. Um die vielfach benötigten Daten besser nutzbar zu machen, etablieren sich zunehmend Datenplattformen. Sie vernetzen Datennutzer und Datenbereitsteller, führen Datenbestände zusammen, bereiten sie auf, stellen sie zur Nutzung bereit und verwalten Zugriffs- und Nutzungserlaubnisse (Consent).

Den hier nur beispielhaft genannten Geschäftsmodellen ist gemein, dass sie auf Datenzugang und auf die Möglichkeit zur Nutzung von Daten angewiesen sind. Für viele Geschäftsmodelle ist allerdings keine zeitlich unbegrenzte Verwendung von Daten erforderlich. Die Nutzung der Daten kann zweckgebunden und zeitlich begrenzt ausgestaltet werden. Dadurch lassen sich einem Datenzugang entgegenstehende Interessen in einer Volkswirtschaft ggf. besser zum Ausgleich bringen.

4 Unterschiedliche Dateninteressen

4.1 Datenschutz

Es kann wohl inzwischen als gesellschaftlicher Grundkonsens in der EU gelten, dass auch bei zunehmender Vernetzung und zunehmend intensiver Datennutzung die Souveränität des Einzelnen über seine Daten erhalten, wenn nicht sogar erhöht werden soll. Hierzu dient insbesondere das Datenschutzrecht, das jedoch nicht Daten an sich, sondern Privatsphäre und informationelle Selbstbestimmung von Personen (Datensouveränität) schützen soll. Verbraucher, Geschäftspartner oder Privatleute wollen in verschiedenen Zusammenhängen jeweils eigenständig entscheiden, wer zu welchen Zwecken ihre Daten einsehen und nutzen kann. Sie werden also zunächst an einem Abwehranspruch gegen

den Zugriff auf Daten aus ihrer Privatsphäre interessiert sein und Zugriffs- bzw. Nutzungsrechte für diese Daten nur im Einzelfall und nach eigener Entscheidung gewähren. Mit der Datensouveränität hängt eine Techniksouveränität zusammen, also die Möglichkeit, zu bestimmen, welche Applikationen in welchem Umfang auf welche Daten zugreifen und an wen diese Daten übermittelt werden sollen. Um eine solche Techniksouveränität herbeizuführen, müssen aber Mindestanforderungen an die Benutzerfreundlichkeit erfüllt sein.

4.2 Entwicklung datengetriebener Geschäftsmodelle

Unternehmen, die neue datengetriebene Geschäftsmodelle anbieten wollen, sind an einem möglichst umfassenden Datenzugang und an weitgehenden Nutzungsrechten interessiert. Dabei wollen sie sich möglichst nicht vorab auf bestimmte Arten von Daten festlegen, um sich die Realisierung weiterer oder erweiterter Datengeschäftsmodelle offen zu halten. Vielfach entsteht auch erst bei der Untersuchung eines Datenbestandes die Idee für ein neues Geschäftsmodell oder für eine innovative Aufbereitung der Daten. Des Weiteren liegt Unternehmen daran, neue Geschäftsmodelle mit Daten zunächst im überschaubaren Rahmen ausprobieren zu können, ohne bereits in einer solchen Experimentierphase mit datenrechtlichen Vorgaben konfrontiert zu werden. Die Entwicklung von datengetriebenen Geschäftsmodellen kann jedoch an der Datenschutz-Grundverordnung (DS-GVO) scheitern. So werfen z. B. die Bestimmung eines berechtigten Interesses an der Datenverarbeitung oder das Erfordernis der Zweckbestimmung bei der Verarbeitung personenbezogener Daten erhebliche Probleme bei der Entwicklung datengetriebener Geschäftsmodelle auf.[10] Vor diesem Hintergrund sind Unternehmen an verbesserter Rechtssicherheit und an einem eindeutigen Erlaubnistatbestand zur Verarbeitung personenbezogener Daten für Big-Data-Analysen interessiert.[11]

4.3 Optimierungsinteresse

Insbesondere im Bereich von Industrie 4.0 sind Anbieter von Maschinen, Maschinen- und Fahrzeugteilen oder Dienstleistungen an Informationen über Nutzung, Funktionalität, Anfälligkeit, Verschleiß und Eignung für bestimmte Prozesse interessiert. Die Anbieter benötigen die Daten z. B. zur Optimierung ihrer Produkte, zur Erfassung von Kundenwünschen, zur Verbesserung ihres Leistungsangebots, zur Erhöhung von Nutzerfreundlichkeit und Produktsicherheit und zur Einschätzung von Ansprüchen auf Gewährleistung oder Schadensersatz. Die Erhebung dieser Daten kann technisch

[10] Für die Nutzung personenbezogener Daten in einem noch zu entwickelnden Geschäftsmodell ist die Einholung einer vorherigen zweckbestimmten Einwilligung naturgemäß schwierig.
[11] Z. B. wäre eine Klarstellung der Datenschutzbehörden wünschenswert, inwieweit und unter welchen Voraussetzungen pseudonymisierte Daten für die Entwicklung neuer Geschäftsmodelle verarbeitet und genutzt werden dürfen.

vergleichsweise unkompliziert durch Anbringung von Hard- und Software-Elementen an den Maschinen und Maschinenteilen erfolgen. Andererseits werden an diesen Daten auch die Betreiber und Nutzer der Maschinen ein Interesse haben bzw. die Weiterleitung dieser Daten unterbinden wollen, wenn aus den Daten Geschäftsgeheimnisse ausgelesen werden könnten oder wenn sie eigene Nutzungsinteressen verfolgen.

4.4 Investitionsschutz

Unternehmen werden in die Erhebung und Auswertung von Daten nur investieren, wenn sie sich aus dieser Investition einen wirtschaftlichen Vorteil oder einen Vorteil im Wettbewerb versprechen. Ein solcher Vorteil ist nicht erzielbar oder gerät in Gefahr, wenn z. B. aus erhobenen Daten gewonnene Erkenntnisse ohne angemessene Kompensation mit Wettbewerbern geteilt werden müssen. In solchen Fällen werden die Unternehmen die Investition oder auch die Erhebung der Daten einstellen oder beschränken. Damit fallen dann aber ggf. auch kostenfreie oder günstige Angebote weg, die mit der Datenerhebung verbunden sind.

4.5 Wettbewerbsschutz

Am Markt etablierte Unternehmen sehen oftmals ihre Marktposition durch neue datengetriebene Geschäftsmodelle gefährdet und werfen diesen die Ausnutzung unfairer Wettbewerbsbedingungen vor. Daher fordern sie Mindeststandards für Geschäftsmodelle, um gleiche Bedingungen für alle Wettbewerber zu erreichen, teilweise aber auch darüber hinaus Rechtsregeln, die ihr bestehendes Geschäftsmodell und die Exklusivität ihres Datenbestands schützen. Allerdings führen nicht die Daten selbst, sondern Möglichkeiten zur Analyse und zur Informationsgewinnung zu Wettbewerbsvorteilen, sodass Datenzugriff allein noch keinen wirtschaftlichen Erfolg garantiert.

Andererseits sollte die Verfügungsmacht eines Unternehmens über große Datenmengen nicht andere Unternehmen, die nicht über eine ähnliche Datenmacht verfügen, von der Marktteilnahme abhalten. Die Herrschaft über große Datenmengen darf also nicht zu einem Exklusivzugang zu bestimmten Marktsegmenten führen, wenn dieser nicht das Resultat eines fairen Wettbewerbs ist. Jedoch darf ein Datenzugang, der aus Gründen des fairen Wettbewerbs eingeführt wird, nicht seinerseits zu einer dauerhaften Schlechterstellung der Unternehmen führen, die den Datenzugang zu gewähren haben.

5 Datenrechte des geltenden Rechts

Im Folgenden wird ein Überblick über Vorschriften des geltenden Rechts gegeben, die schon gegenwärtig auf Daten anzuwenden sind und den Umgang mit Daten regeln.

5.1 Rechtlicher Schutz von Daten

Einen Schutz für Daten und für die Verfügungsmöglichkeiten über Daten gewährt das Gesetz demjenigen, dem die Daten von Rechts wegen zugewiesen sind. Solche Zuweisungen sind aufgrund von verschiedenen rechtlichen Konzepten denkbar (vgl. dazu die folgende Darstellung). Die rechtliche Zuweisung von Daten begründet eine rechtlich anerkannte Stellung des Dateninhabers, die regelmäßig mit einem Recht auf Abwehr von Datenzugriffen durch Dritte verbunden ist.

a) Sacheigentum

Den umfassendsten zivilrechtlichen Schutz weist das geltende Recht dem Eigentümer zu. Nach § 903 S. 1 BGB berechtigt das Eigentum an einer Sache den Eigentümer, mit der Sache nach Belieben zu verfahren, die Bedingungen für die Nutzung der Sache zu bestimmen und andere Personen von einer Einwirkung auf die Sache auszuschließen. Die eigentumsrechtlichen Vorschriften des BGB (§§ 903 ff. BGB) sind jedoch für körperliche Gegenstände (Sachen) konzipiert und daher für unkörperliche Gegenstände wie Daten nicht anwendbar.[12]

An dieser intuitiv einleuchtenden Einordnung könnten angesichts der Rechtsprechung Zweifel entstehen. Denn die Rechtsprechung behandelt teilweise den ebenfalls unkörperlichen Gegenstand Software als Sache.[13] Diese Einordnung der Rechtsprechung ist jedoch auf das Vertragsrecht beschränkt geblieben. Die Rechtsprechung wollte damit die Anwendbarkeit der vertragsrechtlichen Gewährleistungsrechte bei Softwaregeschäften sicherstellen und auf diese Weise das vertragsrechtliche Äquivalenzinteresse des Softwareerwerbers schützen. In diesem Zusammenhang hat die Rechtsprechung stets den Aspekt der Verkörperung auf einem Datenträger betont.

Gegen eine Anwendung der Vorschriften zum Sacheigentum auf Daten spricht letztlich vor allem das Wesen von Daten als nicht-rivale, nicht-exklusive und nicht-abnutzbare Gegenstände. Das Sachenrecht für bewegliche Sachen wurde dagegen geschaffen als Rechtsordnung für eine exklusive Zuordnung von nicht beliebig multiplizierbaren Gegenständen, die durch Nutzung an Wert verlieren.[14]

Das Sacheigentum des BGB umfasst allerdings den Schutz von Datenträgern, da diese wiederum Sachen sind. Über den Eigentumsschutz an Datenträgern sind die darauf

[12] Vgl. z. B. MüKoBGB/Stresemann, 8. Aufl. 2018, BGB § 90 Rn. 25; Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder, Bericht vom 15. Mai 2017, S. 34; Determann: „Gegen Eigentumsrechte an Daten", in: Zeitschrift für Datenschutz 2018, 503, 505
[13] z. B. BGH, Urteil vom 15. 11.2006, Az. XII ZR 120/04 Rn. 15
[14] Ein Eigentum an Daten lehnt auch das LG Konstanz ab (vgl. Urteil vom 10.05.1996, Az. 1 S 292/95).

gespeicherten Daten mittelbar mitgeschützt. Die unbefugte Änderung oder Löschung von Daten ist daher als Eingriff in das Eigentum am Datenträger anzusehen, der zu Schadensersatz führen kann (z. B. nach § 823 Abs. 1 BGB), wenn die Nutzungs- und Verfügungsmöglichkeiten des Berechtigten über Daten und Datenträger (Integritätsinteresse) durch den unbefugten Eingriff beeinträchtigt sind.[15]

Die bloße Kenntnisnahme oder das bloße Kopieren von Daten ohne deren Veränderung ist allerdings kein Eingriff in das Eigentum am Datenträger. Denn das bloße Kopieren beeinträchtigt die Integrität und die Nutzbarkeit von Daten und Datenträger nicht. Wegen des nicht-rivalen Charakters von Daten können mehrere Personen nach Kopieren gleichzeitig einen identischen Datenbestand nutzen, ohne dass der Datenbestand dadurch an Nutzwert verliert. Der Integritätsschutz am Datenträger begründet also kein Eigentumsrecht an den einzelnen Daten.[16] Das Kopieren von Daten kann zwar widerrechtlich sein, wenn damit gleichzeitig ein Schutz von Vertraulichkeit oder Exklusivnutzung des Datenbestandes (z. B. aufgrund von Datenschutz oder Geheimnisschutz) gebrochen wird. Dies ist aber auf der Ebene eines Eingriffs in das Sacheigentum am Datenträger unbeachtlich, da damit ein anderes Schutzgut (geistiges Eigentum am Informationsgehalt der Daten, Vertraulichkeitsschutz für Datenbestände) betroffen ist.

b) Besitz

Wer Daten gespeichert hat oder über ungehinderten Datenzugriff und Datenkontrolle verfügt, hat eine beherrschende Position über diese Daten inne. Diese rein tatsächliche Position könnte als Besitz i.S.d. §§ 854 ff. BGB anzusehen sein und damit auch eine rechtliche Bedeutung haben. Ihrem Wortlaut nach sind die Besitzvorschriften des BGB wie auch die Eigentumsvorschriften auf Sachen, also körperliche Gegenstände ausgerichtet. Eine direkte Anwendung dieser Vorschriften auf Daten scheidet daher wie beim Eigentum aus. Dennoch erkennt das Recht eine Dateninhaberschaft und dadurch begründete Verfügungsmöglichkeiten über einen Datenbestand und eine entsprechende Schutzbedürftigkeit an (z. B. in § 303a StGB).[17] Während die Sacheigentumsvorschriften mit dem Wesen von Daten nicht in Einklang zu bringen sind, besteht also eine solche unüberbrückbare Differenz zu den Besitzvorschriften nicht. Insofern liegt eine analoge Anwendung dieser Vorschriften nahe, falls sich Lücken im Rechtsschutz auftun sollten. Der

[15] So z. B. OLG Karlsruhe, Urteil vom 07.11.1995, Az.3 U 15/95
[16] Wie bei der Frage, ob Daten als Sachen i.S.d. §§ 903 ff. BGB zu behandeln sind, besteht bei der Frage, ob das bloße Kopieren von Daten ein Eingriff in das Sacheigentum am Datenträger darstellt, kein allgemeiner Konsens.
[17] So auch Hoeren: „Datenbesitz statt Dateneigentum“, in: MMR 2019, S. 5, 6f., der aus der berechtigten Inhaberschaft an Daten eine rechtliche Zuordnung in Form eines „Datenbesitzes“ ableitet.

berechtigte Besitzer könnte gegen unberechtigte Dritte z. B. Ansprüche wegen Besitzstörung oder Besitzentziehung (§§ 861, 862 BGB) geltend machen.

c) Geistiges Eigentum

Da das Sachenrecht des BGB für Daten nur in Anwendung gebracht werden kann, wenn die Verkörperung der Daten (technische Ebene) betroffen ist, liegt es nahe, Rechte an Daten selbst im Recht des geistigen Eigentums (z. B. Urheberrecht, Patentrecht, Knowhow-Schutz) zu suchen, das zum Schutz immaterieller Güter etabliert wurde. Hierfür kommen mehrere Schutztatbestände in Betracht.

So gewährt das Leistungsschutzrecht an Datenbanken (§§ 87a ff. UrhG) dem Datenbankhersteller das alleinige Recht, den Inhalt der Datenbank zu vervielfältigen, zu verbreiten und zu veröffentlichen. Damit sollen die wesentlichen Investitionen des Datenbankherstellers in die Beschaffung, Überprüfung und Darstellung der Daten geschützt und die Nachahmung dieser Darstellung verhindert werden. Der Datenbankhersteller kann also u. a. die Vervielfältigung der Datenbank oder wesentlicher Teile davon durch Dritte abwehren. Von diesem Schutz sind jedoch die einzelnen Daten in der Datenbank nur mittelbar umfasst, d. h. nur insoweit, als sich daraus die besondere Struktur, Ordnung oder Darstellung des Datenbestandes ergibt. Werden nur einzelne Datensätze, nicht aber wesentliche Teile aus der Datenbank kopiert, greift der Datenbankherstellerschutz nicht ein.[18] Auch sind Investitionen in die Erzeugung von Daten, die im Anschluss in der Datenbank dargestellt werden, nicht vom Datenbankherstellerrecht umfasst.[19] Datenbestände, die lediglich als Nebenprodukt eines Geschäftsbetriebs anfallen, sollen ebenfalls nicht dem Datenbankschutz unterfallen.[20]

Der Schutz des Urhebers nach §§ 2 Abs. 2, 4 Abs. 2 UrhG umfasst im Übrigen lediglich strukturgebende Ideen oder Werke von einer gewissen Schöpfungshöhe. Auf einzelne Daten erstreckt sich dieser Schutz nicht. Denn der Erzeugung einzelner Daten (insbesondere bei automatisierter Erzeugung durch Sensoren oder Messeinrichtungen) liegt regelmäßig kein persönlich geistiger Schöpfungsakt zugrunde.[21]

[18] Vgl. EuGH, Urteil vom 09.11.2004 (Rs. C-203/02 „The British Horseracing Board“), Rn. 69ff., und OLG Hamburg, Urteil vom 24.10.2012, Az. 5 U 38/10
[19] EuGH, Urteil vom 09.11.2004 (Rs. C-203/02 „The British Horseracing Board“), Rn. 38 – 42 und EuGH, Urteil vom 09.11.2004 (Rs. C-444/02 „Fixtures Marketiung“), Rn. 53
[20] Vgl. z. B. BGH, Urteil vom 01.12.2010 - I ZR 196/08, Rn. 35, sowie zu diesem Themenkomplex auch die Erörterung von Hornung/Hofmann in: Hornung (Hrsg.): „Rechtsfragen der Industrie 4.0“, Nomos 2018, S. 25 mit Hinweis auf EuGH, Urteil vom 09.11.2004 (Rs. C-338/02 „Fixtures-Fußballspielpläne“)
[21] Teilweise ist die Begrenzung des Rechtsschutzes auf eine neuartige Idee und ihre technische Umsetzung im jeweiligen Schutzgesetz selbst geregelt. So erstreckt sich z. B. der Halbleiterschutz nach § 1 Abs. 4 HalblSchG ausdrücklich nicht auf die auf einem Halbleiter gespeicherten Informationen.

Inhalt des Patentschutzes nach § 9 Nr. 3 PatG ist das alleinige Recht des Patentinhabers, durch ein patentgeschütztes Verfahren hergestellte Erzeugnisse anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu den genannten Zwecken entweder einzuführen oder zu besitzen. Eine bestimmte Datenfolge kann Erzeugnis in diesem Sinn sein. Als solches ist ihre Verwertung vom Patentschutz umfasst, wenn die Datenfolge sachlich-technische Eigenschaften aufweist, die ihr durch das patentgeschützte Verfahren aufgeprägt wurden. Ein Datenbestand, der lediglich die erfindungsgemäß gewonnenen Erkenntnisse enthält, fällt dagegen nicht unter den Patentschutz.[22]

Insgesamt gewährt das Recht des geistigen Eigentums einen rechtlichen Schutz nur für eine bestimmte Leistung, also für eine persönliche geistige Schöpfung, eine getätigte Investition oder für eine Erfindung. Sind im Rahmen der Generierung von Daten solche Leistungen nicht anzuerkennen (z. B. für Sensordaten und sonstige Rohdaten aus Maschinen), gelten die Daten als gemeinfrei. Das bedeutet, der Nutzung durch jedermann steht ein Recht des geistigen Eigentums nicht entgegen. Die Datennutzung kann dennoch durch andere Gesetze (z. B. zum Schutz von Geschäftsgeheimnissen) untersagt sein.

d) Datenschutzrecht

Die Datenschutz-Grundverordnung der EU (DS-GVO) und ergänzende nationale Vorschriften gewähren einen besonderen Schutz für personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO. Begünstigter dieses Rechtsschutzes ist die betroffene Person. Der Schutz ist so umgesetzt, dass für datenverarbeitende Stellen (z. B. Behörden und Unternehmen) die Verarbeitung personenbezogener Daten (z. B. Erhebung, Speicherung, Analyse) grundsätzlich verboten und nur auf der Grundlage eines Erlaubnistatbestands nach Art. 6 DS-GVO zulässig ist.[23]

Die Rechtsposition des Betroffenen im Datenschutzrecht lässt sich aber nicht als Alleinzuweisung seiner Daten, als Ausschließlichkeits-, als Vermögens- oder als Verwertungsrecht begreifen. Vielmehr ist es ein Entscheidungsrecht darüber, wer zu welchem Zweck die Daten verarbeiten darf. Es ist aber auch kein Alleinentscheidungsrecht.[24] Denn der nationale Gesetzgeber kann die Verarbeitung personenbezogener Daten für bestimmte Zwecke erlauben oder vorschreiben (vgl. Art. 6 Abs. 3 S. 1 i.V.m. Abs. 1 c) DS-GVO). Die DS-GVO selbst erlaubt z. B. die Verarbeitung

[22] Vgl. BGH, Urteil vom 27.09.2016 , Az. X ZR 124/15, und BGH, Urteil vom 21.08. 2012, Az. X ZR 33/10 (Videosignal-Codierung)
[23] Datenverarbeitung im Privatbereich ist von diesem Verbot weitgehend ausgenommen, da die DS-GVO nach ihrem Art. 2 Abs. 2 c) für Datenverarbeitung im Rahmen persönlicher oder familiärer Tätigkeiten nicht anwendbar ist.
[24] Nach der Rechtsprechung Bundesverfassungsgericht sind personenbezogene Informationen ein Abbild der sozialen Realität und gerade nicht dem Betroffenen alleine zuzuordnen (BVerfG, Urteil vom 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83 „Volkszählungsurteil“)

personenbezogener Daten zur Erfüllung eines Vertrages oder bei Vorliegen berechtigter Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1a) bzw. Abs. 1f) DS-GVO). Für Unternehmen sind die abstrakt formulierten Erlaubnistatbestände mit erheblicher Rechtsunsicherheit verbunden, die schwer hinzunehmen ist, wenn datengetriebene Innovation ermöglicht werden soll.[25]

Das Entscheidungsrecht der betroffenen Person wird durch verschiedene unterstützende Rechte ergänzt, z. B. Informationsrechte, einen Anspruch auf Datenübertragung sowie Rechte auf Einschränkung der Datenverarbeitung oder auf Löschung der Daten. Wird der konkrete Personenbezug durch Anonymisierung entfernt oder liegt kein Personenbezug vor, findet das Datenschutzrecht keine Anwendung. Die Anforderungen an eine rechtlich anerkannte Anonymisierung sind aber bisher nicht abschließend geklärt.

e) Schutz von Geschäftsgeheimnissen

Bisher richtete sich der Investitionsschutz für wettbewerbsrelevante unternehmerische Informationen nach dem UWG. Betriebs- und Geschäftsgeheimnisse waren nach § 17 UWG gegen unbefugtes Offenbaren geschützt. Der Schutz nach § 17 UWG galt z. B. für Konstruktionsdaten einer Maschine oder Prozessdaten einer Produktionsanlage, die erkennbar geheim bleiben sollten.[26] Dies sollte Unternehmen ermöglichen, einen selbst erarbeiteten Informationsvorsprung im Wettbewerb gegenüber Konkurrenten abzusichern.

Mit Wirkung zum 26.04.2019 trat für den Schutz von Knowhow das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) an die Stelle des UWG.[27] Das GeschGehG unterscheidet nicht mehr zwischen Betriebs- und Geschäftsgeheimnissen, sondern fasst beides in der Kategorie der Geschäftsgeheimnisse zusammen. Gegenüber der bisherigen Rechtslage haben sich auch Schutzumfang und Schutzvoraussetzungen geändert. Danach sind Informationen als Geschäftsgeheimnisse nur geschützt, wenn das Unternehmen angemessene Maßnahmen zur Geheimhaltung dieser Informationen getroffen hat. Auf diese Weise hat es ein Unternehmen weitgehend selbst in der Hand, welche Informationen als Geschäftsgeheimnis dem gesetzlichen Schutz unterfallen. Allerdings sieht das Gesetz nur einen möglichen Schutz von Informationen vor, einzelne Rohdaten wären damit wohl nicht vom Schutzbereich erfasst.

[25] Peitz/Schweitzer: „Ein neuer europäischer Ordnungsrahmen für Datenmärkte?“, in: NJW 2018, 275, 276 ff. für die Erlaubnistatbestände in Art. 6 Abs. 1a und Abs. 1f) DS-GVO
[26] Zum Begriff des Betriebs- und Geschäftsgeheimnisses vgl. BGH, Urteile vom 27.04.2006, Az. I ZR 126/03, und vom 26.02.2009, Az. I ZR 28/06.
[27] Das Gesetz setzt die Geschäftsgeheimnisrichtlinie der EU 2016/943 in deutsches Recht um.

Gesetzlich geschützt ist vor allem die Vertraulichkeit von Geschäftsgeheimnissen. Eine „Wissensexklusivität" soll dem Inhaber des Geschäftsgeheimnisses die ungestörte profitable Nutzung eigener Innovationsaktivitäten und des damit erarbeiteten Informationsvorsprungs sichern. Entsprechend sind der unbefugte Zugang und das unbefugte Kopieren von Geschäftsgeheimnissen verboten (§§ 4, 23 GeschGehG). Bei Verletzung seines Geschäftsgeheimnisses kann der Inhaber sowohl gegen denjenigen vorgehen, der das Geheimnis unberechtigt kopiert oder offengelegt hat, als auch gegen Dritte, die das Geheimnis im Anschluss unbefugt nutzen (§§ 6 ff. GeschGehG). Dabei sind die Rechte des Geheimnisinhabers umfassend, sie reichen von Auskunftsrechten über Rechte auf Unterlassung, Herausgabe bzw. Löschung bis zu Schadensersatzansprüchen. Allerdings dürfen produktimmanente Informationen durch Untersuchung frei auf dem Markt verfügbarer Produkte aufgedeckt (Reverse Engineering) und in der Folge weiter verwendet werden (§ 3 Abs. 1 Nr. 2 GeschGehG). Insoweit liegt keine Verletzung eines Geschäftsgeheimnisses vor.

f) Deliktsschutz

Ein unbefugter Eingriff in bestimmte Rechtspositionen und Rechtsgüter führt nach Deliktsrecht (insbesondere § 823 BGB) zu Schadensersatzansprüchen. Die Vorschrift des § 823 Abs. 1 BGB gewährt Ersatzansprüche für schädigende Eingriffe in das Sacheigentum und ähnliche Rechte. Unbefugtes Verändern eines gespeicherten Datenbestandes führt daher als Eingriff in das Eigentum am Datenträger zu Ansprüchen nach § 823 Abs. 1 BGB.[28]

Nicht so eindeutig ist, ob auch der Informationsgehalt der gespeicherten Daten einen deliktischen Schutz genießt. Zu bejahen ist dies jedenfalls für personenbezogene Daten als Ausfluss des allgemeinen Persönlichkeitsrechts; denn das allgemeine Persönlichkeitsrecht gehört zu den von § 823 Abs. 1 BGB geschützten Rechtsgütern.[29] Darüber hinaus wird teilweise auch ein vermögenswertes Verfügungsrecht am eigenen Datenbestand als Schutzgut des § 823 Abs. 1 BGB befürwortet.[30] Ein solches Recht wurde aber bisher nicht genauer konturiert und ist von der Rechtsprechung bisher nicht aufgegriffen worden.

Ein Schutz vor unberechtigtem Zugriff auf einen Datenbestand gewährt im Übrigen das Strafrecht mit den §§ 202a, 202b, 202c StGB. Auch §§ 303a und 303b StGB verbieten die unberechtigte Löschung, Veränderung, Beschädigung und Zerstörung von Daten. Ein Eigentum an den Daten ist nicht Voraussetzung für den strafrechtlichen Schutz, dieser steht jedem berechtigten Dateninhaber zu.[31] Geschütztes Rechtsgut des § 303a StGB ist

[28] OLG Oldenburg, Beschluss vom 24.11.2011, Az. 2 U 98/11)
[29] Vgl. z. B. BGH, Urteil vom 01.12.1999, Az. I ZR 49/97 (KG)
[30] MüKoBGB/Wagner, 7. Auflage 2017, BGB § 823, Rn. 294-298
[31] Dennoch bietet das Strafrecht keinen lückenlosen Schutz; denn fahrlässige Veränderungen von Datenbeständen sind nicht von den Datenstraftatbeständen erfasst.

die Datenintegrität und die ungehinderte und ausschließliche Verfügungsbefugnis über Daten, nicht aber die rechtliche Zuordnung von Daten. Das bloße Kopieren von Daten ist daher nicht Tathandlung.

Sind Strafvorschriften einschlägig, kann ein unbefugter Zugriff auf die mit den Strafvorschriften geschützten Rechtsgüter auch zivilrechtlich nach § 1004 BGB analog abgewehrt bzw. nach § 823 Abs. 2 BGB mit einem Anspruch auf Schadensersatz verfolgt werden. Der Strafrechtsschutz greift zugunsten desjenigen ein, der die Speicherung von Daten unmittelbar durch Eingabe, durch Start eines Speicherprogramms oder durch bestimmungsgemäße Verwendung eines zur Datenerzeugung und -aufzeichnung bestimmten Gerätes bewirkt hat (Dateninhaber). Allein aus der Herstellung und dem Verkauf eines Gerätes zur Datenerzeugung kann – wenn eine entsprechende Vereinbarung fehlt – eine Berechtigung an den damit erzeugten Daten nicht abgeleitet werden.[32]

5.2 Rechte zur Erhebung von Daten

Eine allgemeine Erlaubnis für die Erhebung, Sammlung, Nutzung oder Auswertung von Daten für private oder unternehmerische Zwecke ist im deutschen Recht nicht vorhanden. Andererseits ist die Erhebung, Vervielfältigung, Sammlung und Nutzung von Daten durch Unternehmen auch nicht generell verboten. Denn anders als für eine Datenerhebung zu staatlichen Zwecken ist für die Erhebung von Daten im Privatrechtsverkehr eine gesetzliche Ermächtigungsgrundlage nicht erforderlich. Allerdings sind bei der Datenerhebung zu privaten oder unternehmerischen Zwecken verschiedene rechtliche Grenzen zu beachten, die sich aus den Vorschriften über den rechtlichen Schutz von Daten ergeben (vgl. oben unter Ziffer 5.1, z. B. aus Datenschutz oder Geschäftsgeheimnisschutz).

Hat ein Dateninhaber Daten in rechtmäßiger Weise erlangt (z. B. durch eigene Erhebung oder durch Kauf), so kann er an dem rechtmäßig erlangten Datenbestand zwar kein Eigentum begründen. Ihm stehen aber dennoch gewisse Abwehransprüche gegen einen unbefugten Datenzugriff Dritter zu. Der Dateninhaber genießt z. B. den Schutz des Strafrechts gegen unbefugte Veränderungen, Löschungen oder Manipulationen von Datenbeständen und die Überwindung von Sicherungsvorrichtungen für die Daten. Daneben kommen Ansprüche aus Geschäftsgeheimnisschutz oder wegen Besitzstörung in Betracht, falls eine analoge Anwendung der Besitzschutzvorschriften für Daten anerkannt wird.

[32] OLG Naumburg, Urteil vom 27.08.2014, Az. 6 U 3/14

5.3 Verwertungsrechte an Daten

Daten können – rein tatsächlich – von demjenigen verarbeitet und verwertet werden, der sie im Einklang mit dem geltenden Recht erhoben und in seinem Verfügungsbereich gespeichert hat. Soweit das Recht des geistigen Eigentums sich auf Daten erstreckt, stehen die Verwertungsrechte an erhobenen Daten dem Inhaber exklusiv zu. So gibt das Recht dem Inhaber von urheberrechtlich geschützten Daten z. B. Verwertungsrechte (§ 15 UrhG) oder die Befugnis, Nutzungsrechte an Dritte zu übertragen (§ 31 UrhG).

Allerdings gelten die Verwertungsrechte für zulässigerweise erhobene Daten nicht absolut. So dürfen unter bestimmten Voraussetzungen Informationen, die als Geschäftsgeheimnis oder durch das Urheberrecht geschützt sind, auch durch Dritte genutzt werden (vgl. z. B. § 3 GeschGehG, §§ 44a ff. UrhG). Auch für zulässigerweise erhobene personenbezogene Daten gibt es gesetzliche Nutzungsbeschränkungen und Zweckbindungen. Wurden personenbezogene Daten für einen bestimmten Zweck aufgrund einer Einwilligung der betroffenen Person erhoben, so ist für eine Nutzung dieser Daten außerhalb der von der Einwilligung gedeckten Nutzung (Zweckänderung) eine weitere Erlaubnis notwendig, es sei denn, die Weiterverarbeitung ist noch vom ursprünglichen Erlaubnistatbestand gedeckt (sog. kompatible Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO).

Darüber hinaus spricht das Recht z. B. dem Eigentümer (§§ 987, 988 BGB), dem Käufer (§ 446 S. 2 BGB) oder dem berechtigten Besitzer (§ 993 Abs. 1 BGB) die Nutzungen einer Sache zu. Nutzungen sind nach § 100 BGB auch Gebrauchsvorteile einer Sache. Darüber, ob die bei Gebrauch einer Sache entstehenden wirtschaftlich verwertbaren Daten als Gebrauchsvorteil im Sinn des § 100 BGB anzusehen sind, besteht keine Einigkeit.[33] Da das Recht das Sacheigentum und den berechtigten Besitz einer Sache umfassend schützt und in diesen Schutz als Reflex auch die Nutzungs- und Verfügungsmöglichkeiten über eine Sache einbezieht, liegt es nahe, Daten als Gebrauchsvorteile i.S.d. § 100 BGB anzusehen, die zumindest von der Gesetzestendenz her dem Eigentümer bzw. vorrangig dem berechtigen Besitzer zugewiesen sind. Leitet ein Rechtsinhaber sein Recht zur Verwertung von Daten aus einem Recht am Datenträger ab, so ist zu beachten, dass die Rechte an den Daten und die Rechte am Datenträger auseinanderfallen können. An den Daten können besondere Rechte bestehen (z. B. Urheberrechte), die einem anderen Rechtsträger zugewiesen sind als dem Eigentümer oder dem Besitzer des Datenträgers.

[33] Dafür teilweise Hieke :„Big Data - Zum gesetzlichen Schutz und der rechtlichen Zuordnung von Daten“ und Zech: „Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers““, in: CR 2015, S. 127 ff., 142; dagegen Studie für das Bundesministerium für Verkehr und digitale Infrastruktur „Eigentumsordnung“ für Mobilitätsdaten?, August 2017, S. 59

5.4 Gewährung von Datenzugang

Datenzugang kann verschiedene Formen annehmen. In Betracht kommen

- das Kopieren von Datenbeständen,
- die bloße Einsichtnahme in Datenbestände,
- Recherche- oder Analysemöglichkeiten,
- Schaffung einer Schnittstelle zum Auslesen von Daten,
- Parallelspeicherung bei Datenentstehung,
- Übertragung von Daten,
- Herausgabe von Daten.

Dabei ist auch zu unterscheiden, ob Datenzugang zu Rohdaten oder zu Informationen gewährt werden soll.

Das geltende Recht unterscheidet nicht systematisch zwischen verschiedenen Formen des Datenzugangs und konkretisiert diesen nur in Einzelfällen. So enthält Art. 20 der DS-GVO Vorgaben für die Übertragung personenbezogener Daten (Informationen). Herausgabe von Daten bedeutet nach der Rechtsprechung, dass der zur Herausgabe Verpflichtete die herauszugebenden Daten an den Berechtigten zu übermitteln und bei sich selbst zu löschen hat.[34]

a) Zivilgesetzlicher Datenzugang

Ein allgemeines Recht auf Datenzugang bzw. eine korrespondierende Pflicht, Zugang zu Daten zu gewähren, ist im geltenden Zivilrecht nicht verankert. Daher hat zunächst rein faktisch derjenige Zugang zu Daten, der sie mit den von ihm entwickelten oder erworbenen Methoden und Instrumenten im rechtlich zulässigen Rahmen (d. h. unter Beachtung der bestehenden Schutzrechte) erhebt und in seinem Verfügungsbereich speichert (Datenhoheit). Die Begründung einer solchen Verfügungsmacht ist zwar rechtlich nicht in jedem Fall mit einem besonderen Schutzrecht abgesichert, aber bei rechtskonformer Erlangung der Datenverfügungsmacht kann diese Verfügungsmacht dem Dateninhaber auch nicht streitig gemacht werden.

b) Kartellrechtlicher Datenzugang

Im Kartellrecht besteht nach der aus Art. 102 AEUV abgeleiteten sog. Essential-Facilities-Doktrin unter bestimmten Voraussetzungen ein Anspruch auf Teilhabe an einer für den Marktzugang notwendigen Ressource („essential facility“). Entsprechend kommt ein

[34] BGH, Urteil vom 17.04.1996, Az. VIII ZR 5/95

Anspruch auf Datenzugang in Betracht, wenn die Verweigerung eines solchen Zugangs als Missbrauch einer marktbeherrschenden Stellung anzusehen wäre. Bezogen auf Datenmärkte ist bisher nicht letztgültig geklärt, wann eine marktbeherrschende Stellung anzunehmen ist. Ein wichtiges Kriterium bei der Beurteilung ist der exklusive Zugriff auf wettbewerbsrelevante Daten (vgl. § 18 Abs. 3a GWB). Eine marktbeherrschende Stellung auf einem Datenmarkt muss wohl anzunehmen sein, wenn anderen Unternehmen ohne Zugang zu den notwendigen Daten der Marktzutritt verwehrt bleibt und das den Marktzugang suchende Unternehmen die benötigten Daten nicht selbst generieren oder von Dritten erwerben kann.

Der kartellrechtliche Anspruch auf Zugang zu Erzeugnissen oder Dienstleistungen auf der Grundlage der Essential-Facilities-Doktrin wird durch die Rechtsprechung bewusst auf Situationen beschränkt, in denen außergewöhnliche Umstände vorliegen. Denn Unternehmen können berechtigterweise den Zugang Dritter zu Ressourcen verweigern, soweit ihnen für diese Ressourcen ein gewerbliches Schutzrecht zusteht.[35] Außergewöhnliche Umstände liegen nach der Rechtsprechung des EuGH nur vor, wenn mehrere Bedingungen kumulativ erfüllt sind: Der verweigerte Ressourcenzugang muss das Angebot eines neuen, von Verbrauchern potenziell nachgefragten Erzeugnisses verhindern; die Weigerung darf nicht gerechtfertigt sein; und die Weigerung muss geeignet sein, jeglichen Wettbewerb auf einem abgeleiteten Markt auszuschließen.[36] Allein die Tatsache, dass ein Unternehmen über eine Ressource verfügt, die andere Unternehmen benötigen, reicht also noch nicht zur Begründung eines Anspruchs auf Datenzugang. Außerdem muss ein solcher Anspruch nach der Essential-Facilities-Doktrin nicht kostenfrei, sondern nur gegen einen angemessenen finanziellen Ausgleich gewährt werden. Schließlich sind bei der Herausgabe von personenbezogenen Daten auf der Grundlage der Essential-Facilities-Doktrin die Vorgaben des Datenschutzes zu beachten.[37]

Weiterhin darf ein Unternehmen eine relative Marktmacht gegenüber kleinen und mittleren Unternehmen, die von ihm abhängig sind, nicht ausnutzen (§ 20 Abs. 1 GWB). Auch hieraus könnte sich im Einzelfall ein Anspruch auf Datenzugang (ggf. gegen Entgelt) ergeben.

Hat ein Unternehmen einem anderen Unternehmen freiwillig Zugang zu seinen Datenbeständen gewährt, so darf es weitere Unternehmen von einem entsprechenden Datenzugang nicht willkürlich ausschließen. Das bedeutet, anderen Unternehmen ist für

[35] EuGH, Urteil vom 26.11.1998 (Rs. C-7/97 „Bronner"), Rn. 38 - 41
[36] EuGH, Urteil vom 29.04.2004 (Rs. C-418/01 „IMS Health"), Rn. 38
[37] Die französische Wettbewerbsbehörde hat in einer Entscheidung gegen GDF Suez auf Herausgabe von Kundendaten aus Wettbewerbsgründen zur Beachtung des Datenschutzes der herausgabepflichtigen Gesellschaft zur Auflage gemacht, ihre Kunden zu informieren und ihnen ein Widerspruchsrecht gegen die Datenherausgabe einzuräumen, vgl. Décision n° 14-MC-02 du 9 septembre 2014, Rn. 294.

denselben Zweck und unter identischen Bedingungen Datenzugang zu gewähren, wenn dem kein anzuerkennender Sachgrund entgegensteht. Dieser Grundsatz ergibt sich aus Art. 102 Buchstabe c AEUV und § 19 Abs. 2 Nr. 1 GWB. Insoweit genießt der kartellrechtliche Schutz des Wettbewerbs auch Vorrang vor dem Patentrechtsschutz.[38]

c) Vertragsrechtlicher Datenzugang

Im Vertragsrecht sind für bestimmte Vertragsbeziehungen und insbesondere bei Beendigung einer Vertragsbeziehung Ansprüche auf Herausgabe von Daten normiert, z. B. für Geschäftsbesorgungsverträge (§ 667 BGB), bei Rücktritt vom Vertrag (§ 346 Abs. 1 BGB) oder für die Übertragung von personenbezogenen Daten (Art. 20 DS-GVO). Vertragsrechtliche Herausgabeansprüche für Daten bestehen aber eben nur im Rahmen eines Vertragsverhältnisses, bei Erfüllung der Voraussetzungen in der Anspruchsgrundlage und nur gegen den jeweiligen Vertragspartner.

Nach dem zivilrechtlichen Grundsatz der Vertragsfreiheit können allerdings zwischen zwei Unternehmen Erhebung, Erwerb, Austausch oder Zugang zu Daten vertraglich geregelt werden, soweit dadurch keine Rechte betroffen sind, die nicht den Vertragsparteien selbst zustehen. Darüber hinaus kann sich der Zugang zu personenbezogenen Daten ebenfalls aus einem Vertrag ergeben. Die Verarbeitung von personenbezogenen Daten des Vertragspartners ist nach Art. 6 Abs. 1b) der DS-GVO erlaubt, soweit die Verarbeitung der Daten für die Abwicklung des Vertrages erforderlich ist.[39] Einer Einwilligung der betroffenen Person oder einer anderen Rechtsgrundlage für die entsprechende Datenverarbeitung bedarf es insoweit nicht.

Allerdings setzt das Kartellrecht dem Datenaustausch zwischen Unternehmen Grenzen. Nach Art. 101 Abs. 1 AEUV, § 1 GWB sind Vereinbarungen zwischen Unternehmen und aufeinander abgestimmte Verhaltensweisen verboten, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken. Ein regelmäßiger, evtl. sogar automatisierter Datenaustausch zwischen Marktteilnehmern wird von diesem Verbot erfasst, wenn es sich dabei um den Austausch wettbewerblich sensibler Informationen handelt. Ein Austausch strategischer Informationen mit potenziellen Wettbewerbern ist daher mit kartellrechtlichen Risiken behaftet. In den vergleichsweise noch jungen Datenmärkten gibt es vielfach noch Schwierigkeiten bei der Bestimmung wettbewerblich sensibler Informationen, bei der Identifizierung potenzieller Wettbewerber oder bei der Marktabgrenzung. Auch ist unklar, wie Vorkehrungen ausgestaltet sein müssen, um die Übermittlung bzw. den Empfang wettbewerblich

[38] BGH, Urteil vom 13.07. 2004, Az. KZR 40/02 („Standard-Spundfass“)
[39] Zur Auslegung dieser Rechtsgrundlage vgl. Leitlinie 2/2019 des Europäischen Datenschutz-Ausschusses vom 09.02.2019.

sensibler Daten zu verhindern. Diese Unsicherheiten können die Bereitschaft von Unternehmen zum Datenaustausch beeinträchtigen.

Das Insolvenzrecht steht einer Durchsetzung vertraglicher Ansprüche auf Herausgabe, Nutzung und Verwertung von Daten nicht entgegen.[40] Zwar werden Daten nach § 35 InsO zur Insolvenzmasse gezogen, wenn z. B. ein Cloud-Nutzer Daten in den Verfügungsbereich eines insolventen Cloud-Betreibers übertragen hat. Soweit es sich bei den vertragsgegenständlichen Daten um personenbezogene Daten handelt, geht jedoch die Datenschutz-Grundverordnung dem Insolvenzrecht vor, sodass die Insolvenz des Dateninhabers den Übertragungsanspruch nach Art. 20 Abs. 1 DS-GVO oder den Löschungsanspruch nach Art. 17 DS-GVO nicht beeinträchtigt. Dabei wird der Insolvenzverwalter zum Verantwortlichen i.S.d. Datenschutzrechts.

Aber auch nicht-personenbezogene Daten können in der Insolvenz des Cloud-Anbieters herausverlangt werden, obwohl an ihnen keine dinglichen Rechte bestehen. Entscheidet sich der Insolvenzverwalter gemäß §§ 103 ff. InsO für die Fortführung des Cloud-Vertrages, kann der Cloud-Nutzer die vertraglichen Ansprüche, die ihm bislang gegen den Cloud-Betreiber zustanden, nunmehr gegen den Insolvenzverwalter geltend machen.[41] Entscheidet sich der Insolvenzverwalter gegen die Fortführung des Vertrages, so ist jedenfalls für die Daten, die der Cloud-Betreiber vom Cloud-Nutzer nach § 667 Alt. 1 BGB erhalten hat, ein Anspruch auf Aussonderung nach § 47 InsO anerkannt.[42] Auch in der Insolvenz des Cloud-Betreibers bleibt also der Cloud-Nutzer Herr über die Daten, die er selbst eingegeben oder übermittelt hatte. Ein bloßer schuldrechtlicher Anspruch kann zur Aussonderung berechtigen, wenn der Gegenstand, auf den er sich bezieht, nach Inhalt und Zweck der gesetzlichen Regelung als massefremd anzusehen ist.[43] Erst recht führt ein eigenes Recht an Daten (z. B. aus dem Leistungsschutzrecht an Datenbanken oder aus Geschäftsgeheimnisschutz) zu einer Aussonderungsberechtigung nach § 47 InsO.

d) Spezialgesetzlicher Datenzugang

Neben Datenrechten des allgemeinen Zivilrechts finden sich Datenzugangsrechte und Pflichten zur Gewährung von Datenzugang zwischen Unternehmen in Sondergesetzen für bestimmte abgegrenzte Regelungsbereiche. So müssen Automobilhersteller Zugang zu Reparatur- und Wartungsinformationen der von ihnen produzierten Fahrzeugtypen über

[40] Daher sieht die Bundesregierung in ihrer Antwort vom 04.03.2019 (BT-Drs. 19/8108) auf eine kleine Anfrage der FDP-Fraktion im Bundestag für das Insolvenzrecht derzeit keinen gesetzgeberischen Handlungsbedarf.
[41] Vgl. Bericht der Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder vom 15.05. 2017, S. 61
[42] OLG Düsseldorf, Urteil vom 27.09. 2012, Az. I-6 U 241/11
[43] BGH, Urteil vom 10.02.2011, Az. IX ZR 73/10; Bericht der Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder vom 15.05.2017, S. 62 ff.

das Internet gewähren.[44] Straßenverkehrsteilnehmern sind im Rahmen intelligenter Verkehrssysteme Straßen-, Verkehrs- und Reisedaten zur Verfügung zu stellen.[45] Ebenfalls im Verkehrsbereich gilt die Pflicht, neue Fahrzeugtypen mit einem eCall-System auszustatten. Dieses System sendet bei einem schweren Verkehrsunfall unmittelbar und automatisch einen Notruf, der die genauen Standortdaten, Unfallzeitpunkt, Anzahl der Insassen, Fahrzeugtyp und Art des Treibstoffs enthält.[46]

Die gesetzlichen Grundlagen für die Digitalisierung der Energieversorgung enthalten sehr konkrete Vorgaben zur Erhebung, zur Nutzung und zum Austausch von Daten.[47] Die detaillierte Regelung ist nicht zuletzt deswegen erforderlich, weil es dabei vor allem um personenbezogene Daten geht, deren Erhebung und Verarbeitung mit den Belangen des Datenschutzes abgewogen und in Einklang gebracht werden müssen.

Als weiteres Beispiel kann der Datenaustausch im Zahlungsverkehr angeführt werden. Das Zahlungsdiensteaufsichtsgesetz verpflichtet kontoführende Zahlungsdienstleister (in der Regel Banken), Drittanbietern (z. B. FinTechs) Informationen zu übermitteln, die zur Durchführung von Zahlungsvorgängen oder für Kontoinformationsdienste erforderlich sind.[48] Über eine eigene Schnittstelle des Zahlungsdienstleisters können Drittanbieter Überweisungen auslösen, Kontoinformationen herunterladen oder die Deckung von Kartenverfügungen abfragen. Informationsübermittlung und Zahlungsvorgänge setzen aber jeweils eine ausdrückliche Zustimmung des Zahlers bzw. Kontoinhabers voraus.

Die genannten Regelungen zur Gewährung von Datenzugang beschränken sich auf die Datennutzung und Datenbereitstellung in gesetzlich abgegrenzten Bereichen. Sie beziehen ihre Rechtfertigung aus den Zusammenhängen mit den jeweils geregelten Spezialmaterien (Funktionsfähigkeit einer bestimmten Infrastruktur). Die auszutauschenden Informationen sind dabei gesetzlich festgelegt. Daneben dienen die Datenzugangsregelungen auch dazu, für die Wettbewerber auf einem bestimmten Markt gleiche Voraussetzungen für den Informations- und Marktzugang zu schaffen.

---

[44] Vgl. Art. 6 der EU-VO Nr. 715/2007 vom 20.06.2007; der Hersteller kann allerdings nach Art. 7 der EU-VO Nr. 715/2007 Gebühren für den Datenzugang erheben. Zu weiteren Einzelheiten dieser Pflicht zur Gewährung von Datenzugang vgl. OLG Frankfurt, Urteil vom 23.02.2017, Az. 6 U 37/16

[45] Rechtsgrundlagen sind die Richtlinie 2010/40/EU und das Intelligente Verkehrssysteme Gesetz. Gemäß ihrer am 30. 11.2016 veröffentlichten Strategie will die EU-Kommission darüber hinausgehend einen direkten Informationsaustausch zwischen Fahrzeugen ermöglichen (vgl. Pressemitteilung der EU-Kommission vom 30.11.2016).

[46] Die Pflicht zur Ausrüstung von Fahrzeugen mit E-Call-Systemen ergibt sich aus der Verordnung (EU) 2015/758, der vom eCall-System übermittelte Mindestdatensatz ist im Standard EN 15722:2011 festgelegt.

[47] Vgl. §§ 49 ff. des Messstellenbetriebsgesetzes

[48] Vgl. §§ 45 ff. des Zahlungsdiensteaufsichtsgesetzes, das zur Umsetzung der zweiten Zahlungsdiensterichtlinie (EU) 2015/2366 (PSD2) dient. Diese Vorgaben treten allerdings erst im Laufe des Jahres 2019 in Kraft.

5.5 Zwischenfazit

Ein eigenes Schutzrecht, das sich direkt auf Daten selbst bezieht, kennt das geltende Recht nur für personenbezogene Daten und Geschäftsgeheimnisse. Solche Schutzrechte beinhalten auch eine Zuordnung der Daten zu einem bestimmten Berechtigten. Ansonsten ergeben sich Datenrechte nur mittelbar aus anderen Rechten (z. B. aus dem Sacheigentum am Datenträger, aus dem geistigen Eigentum am datenproduzierenden Gerät oder aus dem Leistungsschutz für Datenbanken). Auf diese Weise schützt das geltende Recht Daten vor Zugriffen durch Dritte, soweit die Daten vom Persönlichkeitsrecht des Einzelnen, von einem Leistungsschutzrecht, einem Urheberrecht oder vom Integritätsschutz für den Datenträger miterfasst sind. Darüber hinaus gewährt das Recht in begrenztem Maße nicht-ausschließliche Nutzungs- und Zugriffsrechte an Daten in bestimmten gesetzlich definierten Spezialbereichen. Diese Datenzugriffsrechte werden durch korrespondierende Pflichten des Dateninhabers flankiert. Da mit einer Pflicht zur Gewährung von Datenzugang immer auch ein Eingriff in die unternehmerische Freiheit des Dateninhabers verbunden ist, wird gesetzlicher Datenzugang nur in besonderen Sachlagen und bei Erfüllung strenger Tatbestandsvoraussetzungen gewährt.

Die Gewinnung und Verwertung von Daten und Informationen ist im geltenden Recht zulässig, soweit kein Recht zur exklusiven Zuweisung der Information, zum Schutz vor unbefugtem Kopieren der Information oder zum Schutz der Verfügung über einen Datenbestand vorrangig zu beachten ist. Dem Daten- oder Informationserzeuger kommt daher zwar kein gesetzlich kodifiziertes Recht, aber doch eine faktische Verfügungsmöglichkeit an den von ihm erzeugten Daten zu. Zur Abwehr unbefugter Eingriffe in diese Verfügungsmöglichkeit können durchaus Vorschriften des geltenden Rechts (z. B. Strafrechtsschutz, Geschäftsgeheimnisschutz) in Stellung gebracht werden. In den durch einschlägige Schutzrechte vorgegebenen Grenzen kann jede Art von Datenrechten durch Vertrag begründet und geregelt werden.

6 Ansätze zur Einführung neuer Datenrechte

Das weitgehende Fehlen von Rechten, die sich auf Daten selbst beziehen, wird vielfach als unbefriedigend empfunden. Die EU-Kommission hat daher mit einer Mitteilung vom Januar 2017 eine Diskussion über die Notwendigkeit einer datenrechtlichen Regulierung eröffnet und verschiedene Regelungsansätze untersucht.[49] Im Kern der Betrachtung stehen dabei sog. Rohdaten. Damit sind maschinell erzeugte nicht-personenbezogene Daten gemeint, die nach ihrer Erhebung noch nicht bearbeitet oder analysiert wurden,

[49] Vgl. Mitteilung der EU-Kommission COM(2017) 9 final vom 10. 01.2017 „Aufbau einer europäischen Datenwirtschaft“ und das zugehörige Arbeitspapier der EU-Kommission: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0002&from=NL

sodass sie nicht vom Schutz für geistiges Eigentums oder für Geschäftsgeheimnisse erfasst werden. Die Mitteilung sieht zwar keinen zwingenden Bedarf für eine gesetzliche Regulierung des Zugangs zu Daten. Vielmehr geht sie vor allem der Frage nach, mit welchen Mitteln Anreize zum Teilen von Daten geschaffen, Lock-In-Effekte vermieden, aber auch Investitionen geschützt werden können. Die Einführung neuer Datenrechte wird aber auch nicht ausgeschlossen. Seitdem werden die Einführung neuer Datenrechte und verschiedene Maßnahmen zur Förderung des freien Datenverkehrs intensiv diskutiert. Einige Vorschläge dazu werden im Folgenden einer Betrachtung unterzogen.

6.1 Einführung eines Dateneigentums

Zur Stärkung und Förderung der Datenökonomie wird teilweise die Einführung eines „Dateneigentums“ im Sinne eines Ausschließlichkeitsrechts für Daten gefordert. Der Berechtigte soll den Zugriff auf „seine“ Daten durch Dritte ausschließen können, damit er den wirtschaftlichen Wert der Daten besser realisieren kann und in der Konsequenz Anreize zur Schaffung weiterer Daten hat. Darüber hinaus soll ein Eigentum an Daten für mehr Rechtssicherheit sorgen und die Effizienz von Datenmärkten verbessern.

In ihrer Mitteilung vom Januar 2017 diskutiert die EU-Kommission neben verschiedenen anderen Ansätzen auch ein Ausschließlichkeitsrecht des Datenerzeugers. Danach soll der Eigentümer oder der langfristige Nutzer eines datenerzeugenden Geräts über die Nutzung der mit dem Gerät erzeugten Daten bestimmen dürfen.[50] Allerdings ist die EU-Kommission inzwischen selbst von der Idee eines Dateneigentums wieder abgerückt. In ihrer Mitteilung zum Aufbau eines europäischen Datenraums stellt sie stattdessen die freiwillige Gewährung von Datenzugang zwischen Unternehmen untereinander in den Mittelpunkt der Betrachtung und als unterstützenswertes Ziel dar.[51]

Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) will die Verfügungsrechte an Daten aus einem Kraftfahrzeug demjenigen zuweisen, auf den die Erstellung der Daten zurückgeht. Damit sollen Fahrzeugdaten dem Halter zustehen, der das Fahrzeug erworben hat.[52] Eine im Auftrag des BMVI erarbeitete Studie schlägt vor, ein eigentumsähnliches Verfügungsrecht an Daten demjenigen zuzuordnen, „der bei wirtschaftlicher Betrachtungsweise für die Erstellung und Speicherung des Datums verantwortlich ist“.[53]

[50] Vgl. Mitteilung der EU-Kommission COM(2017) 9 final vom 10. 01.2017 „Aufbau einer europäischen Datenwirtschaft“, S. 14
[51] Vgl. Mitteilung der EU-Kommission COM(2018) 232 final vom 25.04.2018 zum „Aufbau eines gemeinsamen europäischen Datenraums“, S. 10 ff.
[52] Vgl. Strategiepapier des BMVI zur Digitalen Souveränität
[53] Studie „Eigentumsordnung für Mobilitätsdaten“, Studie für das BMVI, August 2017, S. 104 f. und S. 107 f.

Bitkom-Position

Eine neue eigentumsähnliche Rechtsposition für Daten wäre in ein schon bestehendes Geflecht aus Datenrechten einzufügen. Es würde mit bestehenden Rechten (z. B. Schutz von Geschäftsgeheimnissen, Datenschutz) und Interessen (z. B. IT-Sicherheit, Investitionsschutz) in Konflikt geraten und wäre mit diesen zum Ausgleich zu bringen. Ein vom Gesetzgeber vorab vorzunehmender Interessenausgleich in einer gesetzlichen Regelung würde zu vielen sachwidrigen Ergebnissen oder sogar zu einer Nichtanwendbarkeit der Norm in Einzelfällen führen.

Selbst wenn sich ein Ausgleich mit bestehenden Rechten erreichen ließe (z. B. durch Beschränkung des Anwendungsbereichs auf maschinell erzeugte Rohdaten), so wäre vermutlich ein Eigentumsrecht an Daten für eine bessere und verbreitetere Nutzung vorhandener Datenbestände durch möglichst viele Akteure eher kontraproduktiv. Denn eigentumsähnliche Rechte implizieren das Recht und damit die Versuchung, andere von Zugriff und Nutzung auszuschließen, die Bedingungen für den Datenzugang durch andere einseitig zu diktieren und die Exklusivität von Datenbeständen zu begründen. Es ist also zu befürchten, dass ein Eigentumsrecht Tendenzen zur Abwehr von Datenzugang und Datennutzung Vorschub leistet und freien Datenfluss behindert. Zur Vermehrung existierender Datenbestände wäre ein Dateneigentum nicht notwendig. Denn auch ohne dieses steigt der bestehende Datenbestand kontinuierlich an, sodass ein Marktversagen bei der Produktion von Daten nicht ersichtlich ist.

Das Eigentum setzt die feste Zuordnung eines Gegenstands zu einem Eigentümer voraus. Als „Dateneigentümer“ kommt z. B. in Betracht:

- derjenige, der das zur Datenerzeugung genutzte Verfahren zur Verfügung stellt,
- derjenige, auf dessen Geräten aufgezeichnete Daten gespeichert sind,
- derjenige, in dessen Eigentum die zur Datenerhebung verwendeten Geräte stehen,
- derjenige, dessen Verhalten durch die Daten erfasst wird („Datenerzeuger“),
- derjenige, der Daten zu neuen Informationen verarbeitet („Datenverarbeiter“),
- derjenige, der die tatsächliche Möglichkeit hat, über die Daten zu verfügen,
- derjenige, der Daten am sinnvollsten nutzen und verwerten kann.

Eine allgemeine gesetzliche Zuordnung eines Eigentumsrechts zu einem dieser Beteiligten ohne Ansehung der konkreten Situation wäre zufällig, wenn nicht sogar willkürlich und für viele konkrete Anwendungsfälle fragwürdig. Sie birgt die Gefahr der automatischen Entrechtung anderer Interessengruppen, die nach dem geltenden Recht bereits Rechte an Daten innehaben. Da die rechtliche Zuordnung von Daten im Rechtsverkehr nicht über einen Rechtsscheintatbestand wie sichtbarer Besitz oder Registereintragung kenntlich

gemacht werden kann, sind bei Feststellung und Nachvollziehbarkeit von rechtlicher Zuordnung und rechtmäßigem Erwerb von Datenbeständen Unsicherheiten und erhöhter Aufwand zu erwarten.

Würde ein Recht an Daten zudem nach dem Vorbild des deutschen Sacheigentums entwickelt, besteht außerdem die Gefahr, dass es auf den Anwendungsbereich des deutschen Rechts beschränkt bliebe, da andere EU-Mitgliedstaaten eine andere zivilrechtliche Eigentumsordnung haben als das deutsche Recht (z. B. fehlt in anderen Rechtsordnungen die Trennung zwischen Verpflichtungs- und Verfügungsgeschäft).

Nicht zuletzt ist die Systematik der zivilrechtlichen Eigentumsvorschriften auf körperliche Gegenstände (Sachen) und auf deren exklusive Zuweisung an einzelne Berechtigte ausgerichtet. Eine am Sacheigentum orientierte Ausformung von eigentumsähnlichen Rechten für Daten würde dem Wesen von Daten, das durch Nicht-Rivalität, Nicht-Exklusivität und Nicht-Abnutzbarkeit gekennzeichnet ist, widersprechen. Daten können fast beliebig und ohne nennenswerten Aufwand kopiert werden, können daher von mehreren Nutzern gleichzeitig verarbeitet werden und unterliegen keiner Abnutzung. All dies ist bei körperlichen Gegenständen anders und rechtfertigt insoweit ein absolutes Recht für das Sacheigentum.[54] Der Einführung eines eigenständigen Dateneigentums steht Bitkom aus den genannten Gründen sehr skeptisch gegenüber.[55]

6.2 Leistungsschutzrecht für Daten

Die bestehenden Regelungslücken insbesondere für unbearbeitete Maschinendaten hat zu Vorschlägen für die Schaffung eines neuen Leistungsschutzrechts geführt, das dem Bearbeitungsrecht in § 950 BGB nachgebildet ist.[56] Eine direkte Anwendung von § 950 BGB in der geltenden Fassung wäre für Datenbestände nicht möglich, da die Vorschrift ein eigentumsähnliches Recht des Bearbeiters nur für neu entstehende bewegliche Sachen gewährt.

Begründet wird die Einführung eines Leistungsschutzrechts für Daten mit dem für die strukturierte Erhebung der Daten erforderlichen Aufwand im gewerblichen Bereich. Das neue Recht soll eine bessere Amortisation des für die Datenerhebung erforderlichen Aufwands ermöglichen. Seiner Konzeption nach begründet es ein nicht ausschließliches Zugriffs- und Nutzungsrecht des Maschinenherstellers für Maschinendaten, die beim Einsatz der Maschine generiert werden. Im Gegenzug erhält der Maschineneigentümer /

[54] Hoeren: „Datenbesitz statt Dateneigentum“; in MMR 2019, S. 5f.
[55] Ablehnend z. B. auch vzbv: Rechte an Daten – „Regulierungsbedarf aus Verbrauchersicht?“
[56] Ensthaler: „Industrie 4.0 und die Berechtigung an Daten“, in: NJW 2016, 3473 ff.

Maschinennutzer, der die jeweiligen Daten beim Einsatz der Maschine hervorbringt, einen Anspruch auf angemessenen Ausgleich.

Bitkom-Position:

Ein Leistungsschutzrecht für denjenigen, der eine Datenerzeugung ermöglicht, muss mit bestehenden Rechten, insbesondere mit Kartellrecht, Datenschutzrecht und Geschäftsgeheimnisschutz, in Einklang gebracht werden. Sind solche Rechte zu berücksichtigen, müsste wohl ein Leistungsschutzrecht des Maschinenherstellers zurücktreten und es wäre insgesamt nicht viel gewonnen. Eine Schwierigkeit wird auch darin bestehen, gemeinfreie Daten widerspruchsfrei von solchen Informationen abzugrenzen, an denen bereits anderweitige Rechte bestehen.

Fraglich ist, in welchen Fällen ein ansonsten nicht vergüteter Aufwand für eine Datenerhebung mit einem Leistungsschutzrecht aufgefangen werden muss. Denn der Aufwand für die Schaffung der Voraussetzungen für eine Datenerhebung wird bereits mit Kaufpreis bzw. Pachtzins für die Maschine abgegolten sein.

In vielen Konstellationen wäre es durchaus sinnvoll und für die Datenökonomie förderlich, Herstellern den Zugang zu Daten aus der Nutzung ihrer Produkte zu ermöglichen (z. B. zur Produktverbesserung). Dies sollte aber nicht auf der Grundlage eines vorrangig dem Hersteller zugewiesenen Exklusivrechts erfolgen, sondern als vertraglich vereinbartes Datenzugangsrecht, das gleichrangig mit anderen Datenzugangsrechten (z. B. dem Recht des Maschineneigentümers) besteht. Denn eine Lösung für den notwendigen Interessenausgleich wird sich wohl nur für individuelle Einzelfälle über vertragliche Vereinbarungen lösen lassen.

6.3 Datenschutz für alle Daten (E-Privacy-Verordnung)

Die Datenschutz-Grundverordnung (DS-GVO) hat einen umfassenden rechtlichen Schutz für personenbezogene Daten etabliert, hinter dem nationale Rechtsordnungen der Mitgliedstaaten nicht mehr zurückfallen dürfen. Als sektorspezifische Ergänzung hierzu hat die EU-Kommission den Entwurf für eine Verordnung über die Vertraulichkeit der elektronischen Kommunikation (sog. E-Privacy-Verordnung) vorgelegt.[57] Der Entwurf enthält neben Vorschriften zur Vertraulichkeit der Kommunikation von natürlichen Personen auch Vorgaben für Kommunikationsdienstleister, für die automatische Kommunikation von vernetzten Geräten und Maschinen über das Internet der Dinge und

[57] Vorschlag COM(2017) 10 final vom 10.01.2017 für eine Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG

zur Vertraulichkeit elektronischer Kommunikationsdaten als solches. Sämtliche Kommunikationsdaten sollen nur bei Erfüllung besonderer, gegenüber der DS-GVO noch verschärfter Erlaubnistatbestände verarbeitet werden dürfen. Da in der Datenwirtschaft so gut wie alle Daten über elektronische Kommunikationsmittel erhoben und ausgetauscht werden, bedeutet der weite Anwendungsbereich der E-Privacy-Verordnung eine Ausdehnung des Datenschutzes auf alle Daten. Die Vorgaben der Verordnung sollen durch Datenaufsichtsbehörden der Mitgliedstaaten durchgesetzt werden. Da der Entwurf der E-Privacy-Verordnung in vielerlei Hinsicht umstritten und zwischen den Rechtsetzungsorganen der EU noch nicht ausverhandelt ist, sind die endgültigen Vorgaben in diesem Bereich derzeit nicht absehbar.

Bitkom-Position

Zwar ist das Ziel der E-Privacy-Verordnung, personenbezogene Daten in der elektronischen Kommunikation zu schützen, anzuerkennen. So muss insbesondere das Abfangen und Überwachen von Daten aus der Kommunikation zwischen Personen untersagt sein, um einen effektiven Grundrechtsschutz zu gewährleisten. Die Ausweitung von Datenschutzvorgaben auf sämtliche Kommunikationsdaten wirkt jedoch den Zielen eines möglichst breiten Datenzugangs und einer verbesserten Datennutzung für die digitale Wirtschaft entgegen.

Daten aus der automatischen Kommunikation zwischen Maschinen (M2M-Kommunikation) stellen für die deutsche Wirtschaft einen immer wichtigeren ökonomischen Wert dar. Die Anwendung von Datenschutzgrundsätzen auf Maschinendaten würde dazu führen, dass diese Daten nur sehr restriktiv erhoben und verarbeitet werden dürften. Dies würde bereits etablierte Abläufe in der Wirtschaft in Frage stellen und Spielräume für Innovationen im Bereich Industrie 4.0 und dem Internet der Dinge sowie in anderen neuen Geschäftsfeldern stark verengen. Sollten die vorgesehenen restriktiven Erlaubnistatbestände zu geltendem Recht werden, wäre bereits die Erhebung und unternehmerische Auswertung von Daten (vorbehaltlich einer Einwilligung) unzulässig, sodass sich die Frage nach der rechtlichen Zuordnung derartiger Daten erübrigt.

Schließlich ist das Verhältnis der E-Privacy-Verordnung zur DS-GVO noch nicht abschließend geklärt, die Anwendungsbereiche beider Regelungsregime sind noch nicht trennscharf voneinander abgegrenzt. Zusammen mit den vielen im Datenschutz noch ungelösten und umstrittenen Auslegungs- und Anwendungsfragen würde dies die schon

bestehende Rechtsunsicherheit weiter erhöhen, was sich ebenfalls innovationshemmend auswirkt.[58]

6.4 (Zwangs-)Lizenzierung von Daten

In ihrer Mitteilung vom Januar 2017 hat die EU-Kommission die Idee in die Diskussion eingeführt, eine Pflicht zur Einräumung von Nutzungsrechten (Lizenzierung) an Daten gegen eine faire, vernünftige und nicht-diskriminierende Vergütung (FRAND) bei berechtigten Interessen einzuführen.[59] Insoweit könnte man von einer Zwangslizenzierung von Daten sprechen.

Bitkom-Position

Die Vergabe von Nutzungsrechten an Daten (Lizenzierung) setzt zunächst voraus, dass das Gesetz solche Rechte einem vorrangig Berechtigten zuerkennt (z. B. Urheber), der sie dann in der Folge Dritter einräumen kann. Rechte an Daten selbst erkennt das geltende Recht aber nur in wenigen Fällen an (vgl. oben). Andererseits ist für die Datennutzung auch keine Lizenz, sondern nur der tatsächliche Datenzugang erforderlich, soweit keine vorrangigen Datenrechte Dritter zu beachten sind.

Ein gesetzlicher Zwang, rechtmäßig erhobene Daten mit anderen Unternehmen zu teilen, bedarf einer besonderen Rechtfertigung, die über das Ziel einer Förderung der Datenökonomie hinausgehen muss. Die Schaffung eines erweiterten Zugangs zu Daten ist kein erstrebenswertes Ziel an sich[60], sondern muss der Förderung einer innovationsfreundlichen Digitalwirtschaft mit gleichen Wettbewerbschancen für alle Unternehmen dienen. Daher könnte eine gesetzliche Pflicht zur Datenlizenzierung bei Vorliegen von strukturellem Marktversagen gerechtfertigt sein. Sie bedarf jedoch des Beweises, dass gesetzlicher Zwang die am besten geeignete Abhilfemaßnahme darstellt, um Wettbewerbskonformität und Markteffizienz herzustellen. Denn damit wäre ein recht weitgehender Eingriff in die unternehmerische Handlungsfreiheit und in den zivilrechtlichen Grundsatz der Vertragsautonomie verbunden. Letzterer schließt die Freiheit ein, sich einen Vertragspartner selbst auszusuchen bzw. einen Vertrag nicht abzuschließen.

[58] Weitere Bedenken gegen die E-Privacy-Verordnung hat Bitkom in verschiedenen Stellungnahmen zusammengetragen (vgl. z. B. Stellungnahme vom 27.04.2017 und Stellungnahme vom 01.07.2019)
[59] Vgl. Mitteilung COM(2017) 9 final vom 10. 01.2017 „Aufbau einer europäischen Datenwirtschaft", dort S. 15 und das begleitende Staff Working Paper SWD(2017) 2 final vom 10.01.2017, dort S. 37 f.
[60] Vgl. Peitz/Schweitzer: „Ein neuer europäischer Ordnungsrahmen für Datenmärkte?"; in: NJW 2018, 275, 279

Weiterhin ist zu berücksichtigen, dass die Marktmacht von Datenmonopolisten, die mit ihren Diensten den Markt bereits dominieren, bei Zahlung für die Nutzung der von ihnen meist unentgeltlich erworbenen Daten weiter zementiert wird. Andererseits ist durchaus zweifelhaft, dass Unternehmen vermehrt Daten erheben, wenn ein damit begründbarer Wettbewerbsvorsprung aufgrund einer zwingenden Bereitstellung der Daten für andere Unternehmen wieder entfällt.

Als Voraussetzung für einen Datenzugangsanspruch muss ein möglicher Anspruchsberechtigter wissen, welche Daten er von welchem Dateninhaber herausverlangen kann. Ein solches Wissen zur Anspruchskonkretisierung wird aber beim möglichen Anspruchsinhaber nicht immer vorhanden sein. Denn Daten können in höchst unterschiedlichen Zusammenhängen anfallen, sodass eine Einheitslösung für alle Daten kaum zielführend sein kann.

Schließlich zeigt auch der Streit um Bereitstellung und Nutzungsvergütung für sog. standardessentiellen Patente, dass sich allgemein akzeptierte Kriterien und Berechnungsgrundlagen für FRAND-Lizenzentgelte kaum finden lassen.

6.5 „Daten für alle“

Anfang 2019 hatte die SPD ein Diskussionspapier für ein "Daten-für-alle-Gesetz" veröffentlicht.[61] Danach sollen Möglichkeiten der Datennutzung und damit verknüpfte Mehrwerte gesellschaftlich breiter geteilt, Innovation gefördert und der Marktmacht digitaler Quasi-Monopole auf Datenmärkten entgegengewirkt werden. Das Konzept sieht vor, nicht-personenbezogene und anonymisierte Daten als öffentliches Gut für eine breite Nutzung der Allgemeinheit zur Verfügung zu stellen. Solche Daten (z. B. Mobilitäts- oder Geodaten) sollen sowohl von öffentlichen als auch von privaten Akteuren in vertrauenswürdige Datenräume übermittelt und dort allen Interessenten zugänglich gemacht werden.

Darüber hinaus sollen Unternehmen mit einer marktdominanten Stellung gesetzlich verpflichtet werden, ihre Daten der Allgemeinheit und ihren Wettbewerbern zur Verfügung zu stellen. Bei personenbezogenen Daten soll vor Weitergabe eine vollständige Anonymisierung erfolgen. Nach geltendem Recht besonders geschützte Informationen wie Geschäftsgeheimnisse, gewerbliche Schutzrechte oder wettbewerbssensible Daten sind von dieser Teilungspflicht ausgenommen. Vielmehr sollen gesetzlich konkrete Anwendungsbereiche festgelegt werden, in denen die Daten geteilt werden müssen (z. B. anonymisierte Daten aus der Nutzung von Suchmaschinen und anderen Internetdiensten

[61] Diskussionspapier der Parteivorsitzenden der SPD Andrea Nahles „Digitaler Fortschritt durch ein Daten-für-alle-Gesetz“ vom 12.02.2019

oder aus dem Electronic Shopping). Schließlich enthält das Diskussionspapier Überlegungen zur Schaffung von sonstigen Anreizen zum Daten-Teilen (z. B. Herstellung von Rechtsicherheit für kooperative Datenpartnerschaften, Schaffung technischer Standards und vertrauenswürdiger Datenpools für die Zusammenführung von Maschinendaten).

Bitkom-Position

In seinem Ziel, den Datenzugang für Unternehmen zu verbreitern und die Bedingungen zum freiwilligen Datenaustausch zu verbessern, ist der Vorschlag der SPD zu unterstützen. Dieses im Zivilrecht anzusiedelnde Ziel vermischt der SPD-Vorschlag jedoch mit dem wettbewerbsrechtlichen Ansatz, die Dominanz von US-Unternehmen in Datenmärkten zurückzudrängen. Eine Datenteilungspflicht soll dabei nicht erst den Missbrauch einer marktbeherrschenden Stellung sanktionieren, sondern bereits die Entstehung von Marktmacht verhindern. Markterfolg hängt aber nicht allein von der Masse der verfügbaren Daten ab, sondern maßgeblich vom Knowhow bei Verarbeitung und Nutzung der Daten. Die Marktmacht großer Unternehmen rührt auch daher, dass sie bereits am längsten mit großen Datenmengen arbeiten und entsprechend viel Knowhow aufgebaut haben. Hinzu kommt das praktische Problem, Datenmärkte abzugrenzen und eine marktdominante Position in Datenmärkten belastbar festzustellen.

In seiner Reaktion auf Geschäftsmodelle großer US-amerikanischer Datenplattformen stellt der SPD-Vorschlag personenbezogene Daten in den Fokus. Dieser Ansatz passt für die deutsche Wirtschaft nur bedingt, da die Stärke und der Knowhow-Vorsprung der deutschen Wirtschaft vor allem in der Verarbeitung von Maschinendaten (z. B. Sensordaten aus Maschinen) liegen.[62] Wenn große deutsche Unternehmen zum Teilen dieser nicht dem Datenschutz unterliegenden Maschinendaten gezwungen werden, würden sie in ihrer Marktposition gegenüber ausländischen Unternehmen im Wettbewerb geschwächt. Denn von einer generellen Pflicht zum Datenteilen würden vor allem die großen Tech-Plattformen mit ihrem bereits vorhandenen Knowhow und ihrer gut ausgebauten Infrastruktur zur Erfassung und Analyse von Daten profitieren. Es ist daher zu befürchten, dass eine Pflicht zum Datenteilen US-Konzerne eher begünstigt als ihre Einflussmöglichkeiten begrenzt. Eher zielführend wären Überlegungen, über Datenkooperationen in ausgesuchten Bereichen den Aufbau von Datenpools durch europäische Unternehmen gezielt zu fördern, um deren Datenmacht und Knowhow zu bündeln und ein Gegengewicht zu außereuropäischen Konzernen aufzubauen (z. B. für Zwecke des maschinellen Lernens).

[62] Allerdings gibt es verschiedene Bestrebungen, Deutschland als Datenstandort über maschinenbezogene Daten hinaus zu stärken, z. B. im „Projekt für ein Financial Big Data Cluster am Finanzplatz Frankfurt am Main“.

Zur Beachtung der DS-GVO sieht die SPD in ihrem Vorschlag die Anonymisierung personenbezogener Daten vor deren Weitergabe vor. Wie aber eine der DS-GVO entsprechende Anonymisierung praktisch durchzuführen ist, ist derzeit eine der drängendsten unbeantworteten Fragen im Datenschutzrecht. Mangels ausreichender rechtlicher Vorgaben ist eine Anonymisierung mit vielen Unsicherheiten für den Betroffenen und das anonymisierende Unternehmen verbunden. Es wäre unbillig, dem zur Datenteilung verpflichteten Unternehmen diese Risiken aufzuerlegen, ohne zugleich entsprechende Haftungsbegrenzungen zu gewähren. Problematisch sind auch die technischen Möglichkeiten, Datensätze wieder zu de-anonymisieren. Die Anonymisierung beeinträchtigt auch in der Regel den Wert von Daten, etwa in Bezug auf die Genauigkeit der auf ihrer Basis trainierten Systeme Künstlicher Intelligenz.

Eine Verpflichtung zur Datenherausgabe wäre für den Dateninhaber ohne Einschränkung nur möglich, wenn keine vorrangigen Rechte oder rechtliche Vorgaben für die Daten bestehen. Daher sollen Geschäftsgeheimnisse, gewerbliche Schutzrechte oder wettbewerbssensible Daten von der Teilungspflicht ausgenommen werden. Weiterhin wären wohl auch Vorgaben der IT-Sicherheit, der Schutz kritischer Infrastrukturen oder Rechte Dritter z. B. aus Entwicklungskooperationen zu beachten. Es dürfte insgesamt kaum eine wirtschaftsfördernde Wirkung haben, wenn der Dateninhaber solche Rechte vor Datenherausgabe klären und seine Datenbestände entsprechend organisieren müsste; denn er hätte Aufwand, der insoweit nur Dritten zugutekäme.

Unklar ist weiterhin, wie ein leicht verwertbares, maschinenlesbares Format aussehen soll, in dem die Daten zur Verfügung gestellt werden sollen. Funktionierende Datenportabilität ist ein seit langem ungelöstes Problem, das sich mit einem deutschen Gesetz nicht beheben lassen wird.

Viel grundsätzlicher ist allerdings die Frage, wer in Europa überhaupt noch in datengetriebene Geschäftsmodelle investieren würde, wenn Daten Allgemeingut wären. Denn ökonomisch würde dies kaum Sinn ergeben. Kein Startup würde Mittel z. B. für die mühsame Digitalisierung von Röntgenbildern aufbringen, wenn es die Ergebnisse dieser Mühen anschließend kostenfrei als Allgemeingut der Konkurrenz zur Verfügung stellen müsste. Unter der Prämisse, dass Anreize für Datenerhebung und Investitionen in Datengeschäftsmodelle nicht beeinträchtigt werden dürfen, kann es nicht Daten für alle geben.

6.6 Datenzugang bei wettbewerbsrechtlicher Indikation

Ein Anspruch auf Zugang zu Daten sowie eine korrespondierende Pflicht zur Gewährung von Datenzugang lassen sich nicht nur im allgemeinen Zivilrecht einführen, sondern

könnten auch – allerdings mit anderen Voraussetzungen – im Kartellrecht etabliert werden. Entsprechende Vorschläge werden sowohl auf EU-Ebene[63] als auch auf nationaler Ebene[64] geäußert. Die Ideen gehen dahin, Pflichten für marktmächtige Digitalunternehmen einzuführen, Zugang zu ihren Datenbeständen zu gewähren.

Da die Voraussetzungen für einen Anspruch auf Datenzugang nach der Essential-Facilities-Doktrin sehr hoch sind und in der Praxis selten vom Anspruchsteller nachgewiesen werden können, wird über eine Absenkung der Anforderungsschwelle für einen Datenzugang und über eine entsprechende Ergänzung des GWB nachgedacht.[65]

Bitkom-Position

Ein fairer Wettbewerb zwischen allen Marktteilnehmern und eine von Marktverzerrungen ungehinderte Verwirklichung neuer Geschäftsideen sind für alle Märkte, insbesondere auch für Datenmärkte erstrebenswert. Die Ausbildung einer besonderen datenbasierten Marktmacht ist bisher jedoch allenfalls für personenbezogene Daten zu konstatieren und im Einzelfall zu prüfen. Für die Verarbeitung und Nutzung solcher Daten hat die Datenschutzgrundverordnung vorrangig zu beachtendes Recht gesetzt und insoweit auch die Wettbewerbsbedingungen für die Erhebung und Auswertung größerer Datenbestände bis zu einem gewissen Grad vereinheitlicht. Vor Schaffung eines kartellrechtsindizierten Datenzugangs für personenbezogene Daten müsste zunächst geklärt werden, wie dieser Herausgabeanspruch mit der Datenschutz-Grundverordnung in Einklang gebracht werden kann. So könnte vor Weitergabe von Daten eine aufwändige und mit vielen Unsicherheiten verbundene Anonymisierung erforderlich werden. Ursprünglich personenbezogene Daten können nach Entfernung des Personenbezugs viel von ihrem Nutzwert einbüßen. Denn vielfach liegt der Wert eines unternehmerischen Datenbestandes gerade in der Möglichkeit, darüber direkte Kundenverbindung und Kundenkommunikation herzustellen oder ein Kundenverhalten auszuwerten.

In der digitalisierten Wirtschaft ist Datenzugang zwar wichtig, aber nicht allein entscheidend für wirtschaftlichen Erfolg eines Unternehmens. Noch wichtiger sind die Instrumente und Methoden (Algorithmen), die zur Bearbeitung von Datenbeständen und zur Gewinnung neuer Informationen eingesetzt werden. Diese Instrumente sind nach geltendem Recht weitgehend durch Rechte des geistigen Eigentums oder als Geschäftsgeheimnis geschützt. Dieser Schutz darf durch neue Datenzugangsrechte

[63] Notiz der EU-Ratspräsidentschaft zum Thema KI, S. 7 für KI-Lerndaten
[64] Haucap/Schweitzer/Kerber: „Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen", Gutachten im Auftrag des BMWi vom 29.08.2018" oder die SPD-Vorsitzende Andrea Nahles in einem Gastbeitrag für das Handelsblatt vom 13.08.2018
[65] Vgl. Haucap/Schweitzer/Kerber: „Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen", S. 138 ff.

keinesfalls ausgehebelt oder umgangen werden. Auch wenn also kartellrechtlich unter bestimmten Voraussetzungen ein Zugang zu Rohdaten begründet werden könnte, müssten diese Voraussetzungen für einen Zugang zu Informationen (bearbeitete Daten) noch deutlich enger sein. Jedenfalls müssen praktikable Regelungen zum Ausgleich mit anderen Datenrechten gefunden werden.

Auch wäre der Anreiz für Unternehmen zur Generierung von Daten geringer, wenn sie den mit der Verfügungsmöglichkeit über diese Daten ggf. verbundenen Wettbewerbsvorteil sogleich wieder verlieren, weil sie die Daten mit Wettbewerbern teilen müssen. Eine zu enge Marktregulierung kann eine dynamische Marktentwicklung hemmen. Vor diesem Hintergrund ist ein kartellrechtlicher Datenzugang als ultima ratio anzuerkennen, wenn eine zu starke Marktdominanz einzelner Unternehmen zu einer Datenkonzentration und zum Ausschluss einzelner Marktteilnehmer vom Datenzugang führt. Solche Marktungleichgewichte können im Geschäftsverkehr zwischen Unternehmen (B2B-Märkte) nicht allgemein unterstellt werden. Um sie identifizieren zu können, wären praktisch handhabbare Fallgruppen eines Missbrauchs von Marktmacht zur Behinderung des Datenzugangs von Wettbewerbern zu entwickeln. Außerdem müssten die derzeit bestehenden Schwierigkeiten bei der Abgrenzung von Datenmärkten überwunden und Kriterien für eine marktbeherrschende Stellung in Datenmärkten fortentwickelt werden.

Soll ein Anspruch auf Zugang zu Daten geschaffen werden, der auch bei Weigerung des Anspruchsgegners gerichtlich durchgesetzt und vollstreckt werden kann, müssen die Datenbestände, auf die sich ein rechtlicher Zugriffsanspruch erstrecken soll, genau bezeichnet und definiert werden können.

6.7 Open Data

Dem Konzept von Open Data liegt die Idee zugrunde, vorhandene Datenbestände freiwillig oder aufgrund einer Selbstverpflichtung für jeden Interessierten entgeltfrei und ohne Einschränkungen für Zugriff und Nutzung bereitzustellen. Bestände an Open Data werden vor allem durch den Staat bereitgestellt, um die Datenwirtschaft zu fördern, eine bessere Nutzung vorhandener Daten zu ermöglichen und die Entwicklung innovativer Dienstleistungen voranzutreiben.[66]

Die zum öffentlichen Zugriff zur Verfügung gestellten Daten müssen bestimmte Anforderungen erfüllen. Sie dürfen nicht personenbezogen sein bzw. müssen vom Betroffenen für die öffentliche Bereitstellung freigegeben sein. Sie müssen frei von

[66] Vgl. schon Richtlinie 2003/98/EG vom 17. 11.2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-Richtlinie), deren Änderung durch Richtlinie 2013/37/EU vom 26.6.2013 und den Kommissionsvorschlag zur Überarbeitung der PSI-Richtlinie vom 25.4.2018 COM(2018) 234 final

Urheberrechten bzw. vom Urheberrechtsinhaber für die öffentliche Zugänglichmachung bereitgestellt worden sein. Sie dürfen nicht dem Schutz kritischer Infrastrukturen unterliegen und ihre Bereitstellung darf nicht zu Lücken in der IT-Sicherheit führen. Und schließlich dürfen sie nicht der Vertraulichkeit oder der Geheimhaltung unterliegen.

Das Konzept von Open Data findet aber auch in der Wirtschaft zunehmend Verbreitung. Denn die Bereitstellung von Daten ohne direkte Gegenleistung kann sehr wohl auch aus eigennützigen Motiven erfolgen. So können Unternehmen von einem freiwilligen Pooling ihrer Daten profitieren, indem sie z. B. gemeinsam neue Nutzungsmodelle für die Daten entwickeln. Eine freiwillige Kooperation kann durch vertragliche Absprachen abgesichert werden. So könnte z. B. ein Maschinenbetreiber dem Maschinenhersteller Datenzugang zu den Maschinendaten einräumen, soweit dies für eine Wartung der Maschine erforderlich ist. Der Maschinenbetreiber könnte dann zu Service-Zwecken den Datenzugang freischalten.

Bitkom-Position

Das Open-Data-Konzept kann auf der Grundlage des geltenden Rechts verwirklicht werden (im Privatrechtsbereich vor allem durch Verträge) und kann dazu beitragen, die Diskussion um Datenrechte zu entschärfen. Denn es setzt auf freiwilliges Teilen von vorhandenen Datenbeständen zum Nutzen von allen Beteiligten. Die bestehenden Ansätze für Open Data sollten daher anerkannt und gefördert werden. Hierzu sollte der Staat weitere bei ihm gespeicherte Datenbestände für die unternehmerische Nutzung freigeben und für Unternehmen Anreize setzen, freiwillig Daten für den Austausch mit anderen Unternehmen bereitzustellen (z. B. durch Aufbau neutral gemanagter Datenpools mit anonymisierten und aggregierten Daten aus verschiedenen Bereichen bei gleichzeitigem Schutz vor unrechtmäßigem Zugriff). Da der Datenzugang für alle Interessierten nach denselben Bedingungen gewährt wird, ist dadurch keine Marktbeschränkung zu befürchten, sondern Marktbeschränkungen wird entgegengewirkt.

Der Vorteil von Open Data besteht auch darin, dass zur Teilung bereitgestellte Datenbestände nicht vorab allgemein beschrieben werden müssen. Denn soweit Open Data auf Freiwilligkeit beruht, werden diese Datenbestände vom Dateninhaber selbst festgelegt. Soweit Open Data auf Selbstbindung des Staates beruht, können die zu teilenden Daten nach Bedarf und technischen Möglichkeiten bestimmt werden.

Das Konzept und die positiven Auswirkungen von Open Data sind weitgehend unumstritten. Rechtliche und praktische Unsicherheiten gibt es jedoch beim „Wie“ des Datenzugangs. Denn der Datenbereitsteller trägt die Verantwortung dafür, dass die bereitgestellten Daten den oben beschriebenen Anforderungen an Datenschutz, IT-

Sicherheit usw. entsprechen. Der Umgang mit Ansprüchen Dritter und ggf. daraus resultierenden Haftungsansprüchen muss daher pragmatisch geregelt werden.

Es wäre wünschenswert, Nutzern die freiwillige Übermittlung ihrer personenbezogenen Daten an ein Unternehmen oder an einen Datenpool zu erleichtern („Datenspende"). Dabei müssen die Transparenz für den Nutzer und die Zweckbindung eine besondere Bedeutung haben. Der Nutzer muss in Anlehnung an die DS-GVO vorab erkennen können, wer welche Daten für welche Zwecke verarbeitet und wie diese Zweckbindung durchgesetzt wird.

7 Anwendungsbereiche

Nachdem in diesem Positionspapier bisher allgemeine Regelungsansätze für Datenrechte dargestellt und diskutiert wurden, soll nunmehr die Situation in einigen Anwendungsbereichen der digitalisierten Wirtschaft untersucht werden.

7.1 Vernetztes Fahren

Das Interesse unterschiedlicher Marktakteure an der Sammlung und Verwertung von Daten aus dem vernetzten Fahrzeug ist groß und nimmt weiter zu. Daher werden in modernen Fahrzeugen sehr große Mengen an Daten generiert. Dabei werden nicht nur technische Daten (z. B. zu Motorendrehzahl, Batteriezustand, Abnutzung von Bremsscheiben und Reifen) erfasst, sondern auch Umwelt- und Umgebungsdaten, Daten zum Fahrverhalten, Daten über Fahrer und Beifahrer und Daten für das vernetzte und das automatisierte Fahren (vollautonomes Fahren ohne jegliche Beteiligung des Fahrers erlaubt das deutsche Straßenverkehrsrecht derzeit noch nicht).

Ein bereits umgesetzter Anwendungsfall des vernetzten Fahrens ist das Platooning. Dabei werden mindestens zwei Lkw über Fahrassistenz- und Steuersysteme derart digital miteinander verbunden, dass sie in geringem Abstand hintereinander fahren können.

Beim vernetzten Fahren lassen sich Daten nach verschiedenen Funktionszusammenhängen unterscheiden.[67] In Betracht kommende Datenkategorien sind:

[67] Zu verschiedenen Datenkategorien in vernetzten Fahrzeugen und im öffentlichen Personennahverkehr z. B. VDA (https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html) und VDV (https://www.vdv.de/politikbrief-01-2018.pdfx?forced=true, S. 7)

- Infrastrukturdaten: Daten aus der Kommunikation mit Verkehrsleitsystemen und intelligenten Infrastrukturen (z. B. Ampeln, Leitplanken), die auch im Offline-Modus bei unzureichender Mobilfunkabdeckung verfügbar sein sollten,
- Daten zur Fahrzeugführung (z. B. Steuerungs-, Funktions- und Signaldaten in Lenk-, Brems- und Sicherheitssystemen, die besonders vor unbefugtem Zugriff zu schützen sind),
- Daten zur Fahrzeugwartung und zur Funktionsfähigkeit der Fahrzeugsysteme (z. B. zum Fahrzeugzustand, Motorstatus, Ölstand, Kraftstoffverbrauch),
- Daten zum Verschleiß von Fahrzeugteilen,
- Daten zum Fahrverhalten (Fahrerdaten), z. B. Geschwindigkeit, Fahrstrecken, Bremsverhalten,
- Verkehrsdaten über Staugefahr, Geschwindigkeit des Verkehrsflusses, Verkehrsdichte,
- Umweltdaten, z. B. zu Wetter, Luftfeuchtigkeit, Straßenverhältnissen,
- Komfortdaten, z. B. zu Sitzeinstellungen, Belüftung, Insassen-Entertainment.

Mit „NEVADA“ (Neutral Extended Vehicle for Advanced Data Access)[68] hat die Automobilindustrie ein Konzept entwickelt, das die sichere Weitergabe von Daten aus Fahrzeugen ermöglichen und diese Daten für öffentliche Stellen (z. B. Polizei, Feuerwehr, Verkehrsbehörden) und Industrie nutzbar machen soll. Ziel des Konzepts ist es, die Entwicklung digitaler Innovationen und neuer Geschäftsmodelle zu unterstützen und gleichzeitig einen Beitrag zur weiteren Verbesserung der Straßenverkehrssicherheit zu leisten.

Die Daten sollen zunächst aus den Fahrzeugen an ein OEM-Backend übermittelt und dann nach einheitlichen Bedingungen entweder über eine standardisierte Schnittstelle von den Fahrzeugherstellern selbst oder von neutralen Servern bezogen und genutzt werden können. Zum Schutz der Fahrzeugsicherheit ist nach dem Konzept ausschließlich der Automobilhersteller befugt, die im Fahrzeug generierten Daten abzufragen oder Updates durchzuführen. Entsprechend trägt der Hersteller auch die Verantwortung für die Sicherheit des Fahrzeugs. Berechtigte Dritte (z. B. Versicherungen oder freie Werkstätten) können die Daten nach Kundenzustimmung diskriminierungsfrei aus dem Backend übermittelt bekommen. Zur Zuordnung von Nutzungsbefugnissen an Daten aus dem vernetzten Fahrzeug unterscheidet NEVADA mehrere Kategorien:[69]

- Kategorie 1 umfasst verkehrssicherheitsrelevante Daten zur Nutzung für Polizei, Feuerwehr, Verkehrs- und Straßenbaubehörden,
- Kategorie 2 für fahrzeugbezogene Daten, die für einen diskriminierungsfreien Zugriff durch Service-Dienstleister bereitstehen sollen,

[68] Vgl. z. B. die Erläuterung des Konzepts auf der Homepage des VDA
[69] Vgl. VDA-Position „Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten“, September 2016

- Kategorie 3a für markenspezifische Servicedaten, die Geschäftsgeheimnisse der OEM oder ihrer Partner enthalten,
- Kategorie 3b umfasst Daten für die Komponentenanalyse und Produktverbesserung, die OEM oder dessen Zulieferern zur Verfügung stehen sollen,
- Kategorie 4 enthält personenbezogene Daten der Fahrzeugnutzer, auf die ein Zugriff nur bei Vorliegen einer gesetzlichen Ermächtigung eröffnet wird.

Neben der Fahrzeugsicherheit kommt dem Datenschutz im vernetzten Fahrzeug eine besondere Bedeutung zu. Alle Fahrzeugdaten, die ohne größeren Aufwand einer bestimmten Person zugeordnet werden können, sind als personenbezogene Daten mit entsprechenden Datenschutzauflagen anzusehen. Von Gesetzes wegen (§ 45 StVG) sind jedenfalls all jene Daten als personenbezogen einzustufen, die zusammen mit einem Fahrzeugkennzeichen, mit einer Fahrzeug-Identifikationsnummer oder mit einer Fahrzeugbriefnummer erhoben werden oder mit diesen Kennzeichen in Verbindung gebracht werden können (wegen § 6g Abs. 4 Nr. 9 StVG z. B. alle Daten, die in der zentralen Datei beim Kraftfahrt-Bundesamt gespeichert werden). Die Rechte zur Bestimmung über die personenbezogenen Fahrzeugdaten (z. B. das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO) liegen zunächst beim Fahrzeug-Halter bzw. beim Fahrer. Zur Berücksichtigung der Anforderungen des Datenschutzes sieht das NEVADA-Konzept vor, dass der Fahrzeughalter jederzeit die volle Hoheit über seine aus dem Fahrzeug übertragenen persönlichen Daten hat. Er kann selbst entscheiden, welche Daten er wem zu welchem Zweck zur Verfügung stellen möchte und von welchen Anbietern er Services bezieht. So kann der Fahrzeughalter festlegen, welche Services mit den in seinem Fahrzeug generierten Daten verknüpft werden und diese Nutzungserlaubnis auch jederzeit widerrufen oder erweitern.[70]

Über die Zuweisung von Datenrechten und über Zugriffsberechtigungen auf die verschiedenen Datenkategorien ist bisher kein allgemeiner Konsens erzielt worden.[71] So ist bisher die Frage nicht letztgültig beantwortet, ob sämtliche Daten aus dem vernetzten Fahrzeug als personenbezogene Daten anzusehen sind, oder ob es im vernetzten Fahrzeug auch rein technische Daten gibt, die anonymisiert verarbeitet werden können. Neue eigentumsähnliche Rechte zur Abwehr oder zum Ausschluss eines Datenzugangs scheinen kaum geeignet, um automatisiertes Fahren und neue datenbasierte Mobilitätsdienstleistungen zu fördern. Vielmehr bietet vor allem ein diskriminierungsfreier Zugang zu den Fahrzeugdaten für alle Marktteilnehmer (z. B. Pannendienste, Mobilitätsanbieter, Kfz-Werkstätten, Ersatzteilhandel, Versicherer) die

[70] Vgl. die Erläuterung des Konzepts auf der Homepage des VDA
[71] Gemäß einer Bitkom-Umfrage aus 2018 spricht sich eine Mehrheit der befragten Bundesbürger dafür aus, dass Eigentümer bzw. Fahrer über die Nutzung von Daten aus dem vernetzten Fahrzeug entscheiden sollen.

Voraussetzung dafür, Telematik-Angebote und Dienstleistungen zu entwickeln oder bestehende Angebote aufrecht zu erhalten und zu verbessern.

Insgesamt ist die Rechtsentwicklung beim vernetzten und automatisierten Fahren noch nicht abgeschlossen. So denkt die EU-Kommission schon seit geraumer Zeit über eine Regulierung des Datenverkehrs aus dem vernetzten Fahrzeug nach.[72] Ziel dabei ist nicht zuletzt, für einen fairen Wettbewerb zwischen den Dienstleistern zu sorgen und den Zugang zu und die Wiederverwendung von Mobilitäts- und Fahrzeugdaten zu gewerblichen und nicht gewerblichen Zwecken zu verbessern. Dieses Ziel ist zu unterstützen. Zudem muss die IT-Sicherheit und die Resilienz in vernetzten Fahrzeugen eine absolute Priorität haben, da bei Lücken in der IT-Sicherheit von vernetzten Fahrzeugen Menschenleben unmittelbar gefährdet sind. Weder Fahrzeuginsassen noch die Erbringer von Mobilitätsdiensten sollten durch andere Marktteilnehmer beim Datenzugriff, bei der Datenfreigabe oder beim Datenaustausch überwacht werden können. Der Schutz personenbezogener Daten und die Datensouveränität von Fahrzeuginsassen (z. B. bei Erhebung von Daten über Fahrstil und Nutzungsverhalten) müssen auch im vernetzten und autonomen Fahren gewährleistet sein.

7.2 Vernetzte Produktion

In der vernetzten Produktion sind typischerweise mehrere Parteien an der Generierung von Daten beteiligt. Das geltende Recht gewährt unterschiedliche Rechtspositionen, die in solchen mehrseitigen Kooperationen zu widerstreitenden Rechten an den entstehenden Daten führen können. So könnten z. B. ein Maschineneigentümer aus seinem Eigentum an der Maschine, ein Maschinenhersteller aus Patentrecht, ein Maschinennutzer aus Geschäftsgeheimnisschutz und der an der Maschine eingesetzte Arbeiter aus Datenschutzrecht Rechte an den mit der Maschine produzierten Daten ableiten. Dieser Interessenkonflikt wird sich kaum angemessen durch eine gesetzliche Regelung, sondern nur auf individueller vertraglicher Grundlage lösen lassen.

Auch wenn Unternehmen für die Entwicklung neuer Leistungen einen Zugang zu Maschinendaten benötigen, die von einem anderen Unternehmen exklusiv kontrolliert werden, rechtfertigt dies allein noch nicht die Einführung eines entsprechenden gesetzlichen Zugangsrechts. Denn der leistungsfreie Zugang zu Ressourcen unter Ausnutzung des wirtschaftlichen Aufwands anderer ist einer Marktwirtschaft fremd. Darüber hinaus sind auch immer die Interessen des Dateninhabers zu berücksichtigen, die z. B. durch Geschäftsgeheimnisschutz auch rechtlich anerkannt sein können.

[72] Vgl. z. B. die Übersicht zu „Mobility and Transport" der DG MOVE und den Entwurf für eine delegierte Richtlinie Specifications for the provision of cooperative intelligent transport systems (C-ITS) mit sehr detaillierten Festlegungen in den Annexes.

Das geltende Recht enthält einerseits kein generelles Verbot, Produkt- und Maschinendaten zu erheben und auszuwerten, gewährt andererseits jedoch die Möglichkeit, einen Datenzugang auf abgegrenzte Datenbestände auszuschließen und diesen Zugangsausschluss auch rechtlich abzusichern. Zur Umsetzung von Anforderungen der vernetzten Produktion ist die Schaffung eines umfassenden einseitig zugeordneten gesetzlichen Exklusivrechts für Produkt- und Maschinendaten (also für Daten, die nicht vom besonderen Schutz für personenbezogene Daten erfasst sind) nicht erforderlich und nicht wünschenswert.

Die bestehende Rechtslage lässt den Unternehmen ausreichende Spielräume, Zugang zu und Nutzung von Maschinendaten vertraglich zu begründen bzw. abzusichern und entsprechend den Interessen der Vertragspartner auszugestalten. Es ist darauf zu achten, dass solche vertraglichen Regelungen zum Datenaustausch im Geschäftsverkehr zwischen Unternehmen nicht an den Anforderungen des AGB-Rechts (§§ 305 ff. BGB) zum isolierten Nachteil der deutschen Marktteilnehmer scheitern.

Allerdings wird zukünftig zu beobachten sein, ob ein fehlendes Zugriffsrecht an Daten die Entstehung neuer Geschäftsmodelle verhindert und die Nachteile von Datenmonopolen durch das Kartellrecht ausreichend adressiert werden. Erst dann, wenn dazu belastbare Erkenntnisse vorliegen, kann ein Handeln des Gesetzgebers in Betracht kommen.

7.3 Landwirtschaft

Zur Fortentwicklung der Digitalisierung in der Landwirtschaft ist die Verfügbarkeit von Daten zentrale Voraussetzung. Benötigt werden dafür öffentliche Daten und Informationen wie Geodaten, Informationen über Flurstücke, Katasterdaten, Gewässer- und Saumstrukturdaten, Rahmenwerte für Natur-, Boden- und Gewässerschutz, die insbesondere in staatlichen Behörden erhoben und verwaltet werden. Die Vernetzung und Analyse dieser Daten ermöglicht z. B. die präzisere Bewirtschaftung von Feldern und den effizienteren Einsatz von Ressourcen. Zudem bilden öffentliche Daten den Grundstoff für die Entwicklung neuer Anwendungen im Agrartechnologiebereich und fördern somit Innovationen und Unternehmensgründungen. Diese Daten sollten daher bundesweit hochaufgelöst, aktuell und kostenlos zur Verfügung gestellt werden. Während deutsche Unternehmen führend in der Entwicklung technologischer Anwendungen in der Landwirtschaft sind, erschweren mangelnde Vernetzung und Verfügbarkeit öffentlicher Daten Nutzung und stärkere Verbreitung dieser Anwendungen auf nationaler Ebene.

Um die Potenziale in der digitalisierten Landwirtschaft zu realisieren, ist vor allem die Ausweitung und Durchsetzung des Open-Data-Ansatzes geboten. Öffentliche Daten müssen durch Vernetzung bestehender Datenbanken, über frei zugängliche und

dokumentierte Schnittstellen und in einheitlichen und maschinenlesbaren Formaten über zentrale Plattformen unbürokratisch zugänglich gemacht werden.

Alle Überlegungen müssen jedoch die zentrale Rolle der Landwirte berücksichtigen. Lösungen werden sich nur durchsetzen, wenn die Landwirte an den entstehenden Vorteilen und Effizienzsteigerungen der Digitalisierung angemessen beteiligt werden. Dies gilt vor allem für Erhebung, Nutzung und Austausch digitaler Betriebs- und Bewirtschaftungsdaten. Daher sichert die gemeinsame Branchenempfehlung verschiedener Verbände den Landwirten umfassende Hoheit und Souveränität über digitale Betriebsdaten in der Landwirtschaft zu.[73]

7.4 Finanzdienstleistungen

Der Finanzsektor entwickelt sich immer stärker in Richtung Plattformökonomie. Nicht mehr der Verkauf von standardisierten Finanzprodukten steht im Fokus, sondern Dienstleistungen, die auf Kunden individuell zugeschnitten sind, von ihm nach Bedarf abgerufen und gesteuert werden können und über Internet und Smartphone zugänglich sind. Die Überlegungen für die Ausgestaltung von Produkten und Dienstleistungen im Finanzbereich richten sich wesentlich am Kunden, seinen Lebensumständen und seinen Bedürfnissen aus. Dementsprechend ist das Interesse an Daten und Informationen zum Kunden und seinem Verhalten hoch.

Daten erschließen Banken und sonstigen Finanzdienstleistern ganz neue Möglichkeiten zur Optimierung ihrer Geschäftsprozesse und für neue Dienstleistungen. Über die Kombination von Transaktionsdaten, Stammdaten des Kontoinhabers und externen Daten über Händler können Technologien des maschinellen Lernens genutzt und z. B. die Geldwäscheerkennung verbessert werden. Daten ermöglichen aber auch Verbrauchern Mehrwert im Vergleich zu herkömmlichen Angeboten des Finanzmarkts. Bankkunden könnten eine transparente und übersichtliche Zusammenstellung ihrer gesamten Vermögensverhältnisse erhalten, leichter Einsparmöglichkeiten und bessere Konditionen realisieren oder Kontomissbrauch früher als bisher erkennen. Möglich wäre auch eine proaktiv durch die Bank aktualisierte Budget- und Liquiditätsplanung für den Kunden.

Die Datenhoheit im Finanzbereich, also die Entscheidungsgewalt über Zugriff und Nutzung von Daten durch verschiedene Beteiligte, liegt jedoch nach geltender Rechtslage ausschließlich beim Kunden selbst. Dies ergibt sich bereits aus der DS-GVO, ist jedoch zusätzlich auch im Zahlungsdiensteaufsichtsgesetz (ZAG) geregelt. Zahlungsdienstleister dürfen personenbezogenen Daten nur mit der ausdrücklichen Zustimmung des Zahlungsdienstnutzers abrufen, verarbeiten und speichern (§ 59 Abs. 2 ZAG), und

[73] Vgl. Gemeinsame Branchenempfehlung „Datenhoheit des Landwirts“ vom 28.02. 2018

Informationen über eine Kontodeckung dürfen nur mit ausdrücklicher Zustimmung des Kontoinhabers zugänglich gemacht werden (§ 45 Abs. 1 Nr. 2 ZAG). Automatisiertes Auslesen von Transaktionen und Verknüpfung von Finanzdaten aus mehreren Quellen ist ohne aktives Zutun des Kontoinhabers nicht zulässig. Der Kunde muss bewusst für ein neues Angebot optieren. Hierzu muss er sich aber im Vorfeld mit dem Angebot auseinandersetzen. Dies ist in der Praxis vielfach ein Hindernis, da Kunden oftmals aus Unsicherheit eine ausdrückliche Zustimmung scheuen. Teilweise lassen sich neue Angebote auch erst nach Zusammenführung verschiedener Datenbestände modellieren und detailliert beschreiben. Seine Zustimmung zu einer solchen Zusammenführung wird der Kunde aber regelmäßig nur geben, wenn für ihn das Angebot und dessen Nutzen transparent sind. Schließlich ist der Grundsatz „Privacy by default“ mit den von Kunden gewünschten personalisierten Bankdienstleistungen und persönlicher Ansprache schwer in Einklang zu bringen.

7.5 Energieversorgung

Die Versorgung mit Energie erfolgt über ein zunehmend vernetztes System, in dem die Digitalisierung einen unverzichtbaren Beitrag leistet, um die Ziele Wirtschaftlichkeit, Umwelt- und Klimaverträglichkeit der Energieversorgung sowie Versorgungssicherheit miteinander zu vereinbaren. Energieerzeugung aus regenerativen Quellen und die Einbindung von Kunden lässt die Zahl der Akteure im Energiesystem wie Elektromobile, Wärmepumpen, Speicher, Photovoltaik- und Windkraftanlagen sprunghaft steigen. Neue Geschäftsmodelle entstehen: Solarmodule werden Teil virtueller Kraftwerke, kleinste Strommengen automatisiert gehandelt, Autobatterien und Stromheizungen für die Stabilisierung des Stromnetzes genutzt. Ein intensiver Datenaustausch dient dabei zum einen der Koordination der zunehmend komplexen Lastflüsse sowie der notwendigen Flexibilisierung in den Transport- und Verteilnetzen (Smart Grid) und zum anderen zur Entwicklung von Geschäftsmodellen (z. B. im Rahmen der Elektromobilität) auf Grundlage des verpflichtenden Smart-Meter-Rollouts. Wie Digitalisierung und Datenaustausch bei der Erreichung von Energie- und Klimazielen helfen können, zeigen folgende Beispiele:

- Mehr Transparenz über die eigene Energiebilanz und die Nutzung von Energieprofildaten für private Haushalten bis hin zu Industriestandorten;
- Reduzierung der Treibhausgasemissionen durch bessere Integration erneuerbarer Energien;
- Zuverlässiger und effizienter Stromnetzbetrieb durch eine bessere Auslastung der installierten Kapazität;
- Energiehändler und -einzelhändler können ihre Bilanzgruppe genauer prognostizieren, um den Bedarf an Regel- oder Ausgleichleistung zu minimieren;

- Technologieanbieter können Informationen zur Performance von installierten Betriebsmitteln erhalten, die dazu beitragen, die Produkte effizienter und zuverlässiger zu machen und so insgesamt die Nachhaltigkeit des Energiesystems zu verbessern.

Nach den aktuell im Energiebereich geltenden Rechtsgrundlagen liegen Datenhoheit und Datenkontrolle in intelligenten Messsystemen („Smart Meter“) beim Endverbraucher, d.h. beim Nutzer eines Energieanschlusses. Erhebung, Verarbeitung und Nutzung von Daten aus einer Messeinrichtung darf nur nach Einwilligung des Anschlussnutzers erfolgen (§ 50 MsbG) und ist auf gesetzlich benannte Beteiligte beschränkt (§ 49 MsbG). Um die Datenhoheit des Verbrauchers abzusichern, sind die Kernprinzipien „privacy by design“ und „privacy by default“ sowie strengste Vorgaben zur Datensicherheit zu beachten. Als Standardeinstellung werden über den Privatkunden keine Daten außer zum Jahresverbrauch an den Netzbetreiber kommuniziert. Entsprechend müssen Stromlieferanten gemäß § 40 Abs. 5 Satz 2 EnWG immer auch einen Tarif anbieten, bei dem nur nach insgesamt verbrauchter Strommenge abgerechnet wird. Der Privatverbraucher entscheidet, wem er Zugang zu seinen Daten gewährt, muss sich dann aber teilweise selbst um die Übermittlung der Daten kümmern, speziell wenn er Daten Mehrwertdienstleistern außerhalb der Energiewirtschaft zur Verfügung stellen will. Diese Bereitstellung erfolgt durch standardisierte Schnittstellen, welche auch den Austausch mit anderen Wirtschaftszweigen ermöglichen. Nach § 51 MsbG übernimmt der Gateway-Administrator (GWA) die Aufgabe, die Einwilligungen und rechtlichen Voraussetzungen zum Datenaustausch zu prüfen und zu verwalten.

Die Echtzeit-Energiewirtschaft der nahen Zukunft wird ein dezentrales Ökosystem der Daten brauchen: Daten sollten frei und unter der Kontrolle des berechtigten Akteurs zu jedem anderen Akteur im Energiesystem (z. B. Verbraucher, Netzbetreiber, Erzeuger, Mehrwertdienstleister etc.) fließen. Gleichzeitig bleiben die Daten und die Einwilligung zur Nutzung der Daten so oft und so nah wie möglich an ihrer Quelle, während der Zugriff und die Verwaltung der Daten durch den Berechtigten an allen möglichen Orten, Kanälen, Anwendungen und Zeitpunkten im Ökosystem erfolgen kann. Dabei liegt die Entscheidung immer bei den beteiligten Akteuren. Mit anderen Worten: Daten, Anwendung, IT und Governance werden physisch entkoppelt, während sie in einem gemeinsamen Rahmen arbeiten.

Allerdings zählen Energienetze zu den kritischen Infrastrukturen. Daraus ergeben sich für die ausgetauschten Daten besondere Schutz- und Sicherheitsanforderungen sowie eine Zweckbindung beim Datenaustausch, sodass Energieinfrastrukturunternehmen ihre Daten nicht uneingeschränkt bereitstellen können. Außerdem dürfen die Chancen der beteiligten Infrastrukturunternehmen im Wettbewerb nicht dadurch reduziert werden, dass sie einseitig und ohne Kompensation zur Datenherausgabe verpflichtet werden. Für

energiewirtschaftliche Daten, die von Infrastrukturunternehmen erzeugt werden und nicht einzelne Nutzer betreffen, (z. B. Netzauslastung zu bestimmten Zeiten) muss daher klar definiert und abgegrenzt sein, welche Daten zu welchem Zweck weitergegeben werden müssen.

Die Debatte über die Organisation des dezentralen Datenaustauschs in Energienetzen nimmt Fahrt auf, insbesondere auf europäischer Ebene. Im Wesentlichen können die Rahmenbedingungen über die bestehenden Möglichkeiten privatrechtlicher Verträge und über brancheneigene Open-Data-Vereinbarungen angemessen festgelegt werden. Punktuell könnten branchenspezifische Regelungen durch den Gesetzgeber oder durch eine unabhängige, neutrale Organisation sinnvoll werden.

8 Fazit und Bitkom-Empfehlungen

An Daten können unterschiedliche Rechte bestehen. Zu unterscheiden sind dabei: eigentumsähnliche Zuweisung von Daten zu einem Berechtigten und eine damit verbundene Schutzposition, Verfügungsrechte, Zugriffsrechte, Nutzungsrechte, Abwehrrechte, Rechte auf Integrität und Vertraulichkeit eines Datenbestandes und Schadensersatzansprüche bei unberechtigtem Datenzugriff oder unberechtigter Datennutzung.

a) Schutz von Daten durch eigentumsähnliche Rechte

Eine umfassende eigentumsähnliche Zuordnung von Daten selbst zu einem Berechtigten ergibt sich aus dem geltenden Recht nicht. Eine Exklusivnutzung von Daten und ein exklusives Recht zur Bestimmung über das „Schicksal“ eines bestimmten Datenbestandes sieht das geltende Recht nur bei Erfüllung besonderer Voraussetzungen vor (z. B. wenn die Daten von einem Patentschutz erfasst werden oder als Geschäftsgeheimnis anzusehen sind). Ansonsten gewährt das Recht für Daten nur einen indirekten Schutz in Verbindung mit dem Schutz eines anderen Rechtsguts (z. B. Persönlichkeitsrecht, Eigentum am Datenträger). Dieser indirekte Schutz und die sich daraus ableitenden Rechte an Daten haben jeweils eigene Voraussetzungen, einen unterschiedlich weiten Schutzumfang und unterschiedliche Verfügungsberechtigte (Personen, die jeweils über das Schicksal der Daten bestimmen können). Reichweite und Schutzumfang sind aber noch nicht für alle diese Rechte im Detail festgelegt.

Auch wenn sich aus dem Eigentum am datenproduzierenden oder datenspeichernden Gerät tendenziell eine Verfügungsbefugnis über die damit produzierten Daten ergibt (Daten als Nutzungen i.S.d. § 100 BGB), führt dies nicht zu einem eigentumsähnlichen Exklusivrecht an den Daten selbst. Die Verfügungsbefugnis kann von anderen rechtlichen

Zuweisungen überlagert werden. So kann z. B. aus dem Patentrecht an einem datengenerierenden Gerät eine Zuweisung der Daten zum Patentinhaber abzuleiten sein. Das Strafrecht sieht eine Zuweisung von Daten an denjenigen vor, der die Aufzeichnung von Daten bewirkt hat, und das Datenschutzrecht sichert der betroffenen Person weitgehende Verfügungsrechte über ihre Daten. Soweit spezielle Rechte an Daten selbst anzuerkennen sind, gehen diese der Zuweisungstendenz aus dem Eigentum am Datenträger vor.

b) Rechte auf Datenzugang

Für Datenzugang, Bereitstellung, Übertragung und Nutzung von Daten kennt das geltende Recht in Spezialgesetzen für begrenzte Bereiche bereits zwingende Vorgaben. Soweit solche Rechte nicht bestehen, sind Unternehmen am Erheben und Verarbeiten von Daten nicht gehindert, auch wenn im geltenden Recht ein allgemeines Datenzugangsrecht fehlt. Denn im Privatrechtsverkehr ist eine gesetzliche Ermächtigungsgrundlage nur für die Verarbeitung von personenbezogenen Daten erforderlich. Insbesondere im Bereich maschinengenerierter Daten kann es dagegen auch Datenbestände geben, die nicht von einer geschützten Rechtsposition erfasst werden.

c) Bitkom-Empfehlungen zur Weiterentwicklung des geltenden Rechts

Es erscheint im Hinblick auf die weitere Entwicklung der Datenökonomie wenig zielführend, den nicht-rivalen Charakter von Daten durch Einführung von eigentumsähnlichen oder sonstigen Ausschließlichkeitsrechten für Daten einzuschränken.

Das unterstützenswerte Ziel, möglichst viele in der Privatwirtschaft erzeugte Daten möglichst vielen Akteuren für eine wirtschaftlichen Nutzung zugänglich zu machen, lässt sich aber auch nicht durch einen allgemein-gesetzlich geregelten Datenzugang sowie eine korrespondierende gesetzliche Pflicht zur Bereitstellung von Daten erreichen. Ein allgemeiner, voraussetzungs- und leistungsloser Anspruch auf Datenzugang dürfte das Interesse der zur Herausgabe verpflichteten Unternehmen an Datenerzeugung stark dämpfen. Außerdem wären die Rechte von Dateninhabern an einer Exklusivnutzung ihrer Datenbestände (z. B. aus gewerblichem Rechtsschutz, Geschäftsgeheimnisschutz) zu beachten und mit dem Interesse am Datenzugang zum Ausgleich zu bringen. Denn bei Überlegungen zur Einführung neuer Datenrechte können die Grundentscheidungen und Vorgaben des geltenden Rechts für Daten nicht unberücksichtigt bleiben, auch wenn sie nicht lückenlos und nicht widerspruchsfrei sind. Da in ganz verschiedenen Wirtschaftsbereichen jeweils unterschiedliche Interessen und Rechte an Daten zum Ausgleich zu bringen sind, dürfte die Kodifizierung eines allgemeinen zivilrechtlichen Datenzugangsrechts (bzw. einer spiegelbildlichen Pflicht zur Gewährung eines

Datenzugangs) kaum in allen Fällen zu angemessenen und befriedigenden Ergebnissen führen. Ein Anspruch auf Datenzugang wäre außerdem nur erfüllbar und durchsetzbar, wenn er ausreichend konkretisiert werden kann. Angesichts der Vielfalt an Daten und deren unterschiedlicher Nutzungszusammenhänge dürfte eine solche Konkretisierung durch den Gesetzgeber kaum möglich sein.

Der Zugang zu Daten ist bereits nach geltendem Recht hinreichend gewährleistet und sollte auch zukünftig primär zwischen den beteiligten Unternehmen auf vertraglicher Basis geregelt werden. Damit sollte Datenzugang grundsätzlich auf dem Prinzip der Vertragsfreiheit und damit auf Freiwilligkeit beruhen und somit das Ergebnis individueller Verhandlungen zwischen den Marktakteuren sein. In einem Vertragsverhältnis können die notwendigerweise zu regelnden Fragen z. B. zu den bereitzustellenden Daten, zu Art, Dauer und technischen Voraussetzungen des Datenzugangs, zur Datenqualität, zu einer evtl. notwenigen Rechtseinräumung und zum Entgelt ausreichend konkret und den Anforderungen der Parteien entsprechend geregelt werden. Die Praxis zeigt, dass ein Datenaustausch auf vertraglicher Basis grundsätzlich funktioniert und dass sich darüber neue Geschäftsmodelle mit Daten etablieren lassen.

Erst wenn sich abzeichnet, dass über Vertragslösungen ein ausreichender Datenfluss in einzelnen Bereichen nicht erreichbar ist, sollte darüber nachgedacht werden, sektorbeschränkte und zweckgebundene Datenzugangsrechte unter gesetzlich definierten Bedingungen und für genau definierte bzw. kategorisierte Datenbestände einzuführen. Als mögliche Begründung für einen solchen Datenzugang kommt der kartellrechtswidrige Missbrauch einer marktbeherrschenden Stellung, generelles Marktversagen oder ein übergeordnetes volkswirtschaftliches Interesse am Datenzugang in einem abgegrenzten Markt in Betracht. Eine nach diesen Gesichtspunkten begründete gesetzliche Initiative sollte nur ins Auge gefasst werden, wenn andere wettbewerbsrechtliche Maßnahmen oder branchenspezifische, nicht-gesetzliche Initiativen (z. B. im Rahmen der Selbstregulierung) dem diagnostizierten Marktversagen nicht abhelfen können.

Auch bei einem kartellrechtlich motivierten Eingriff des Gesetzgebers müssen berechtigte Interessen aller Beteiligten (z. B. aus Leistungsschutz oder zur Aufrechterhaltung von IT-Sicherheit) identifiziert, abgewogen und entsprechend berücksichtigt werden. Ein Ausgleich verschiedener berechtigter Interessen ist bei Beschränkung auf einen möglichst kleinen Anwendungsbereich besser beherrschbar und es ist auch besser überschaubar, um welche Daten es geht, wie die Marktverhältnisse sind und wie die Marktbeteiligten nach welchen besonderen Sachanforderungen miteinander vernetzt und am Datenfluss teilhaben sollten. Um berechtigte Interessen der zum Datenzugang verpflichteten Unternehmen angemessen zu berücksichtigen, könnte kartellrechtlich gerechtfertigter

Datenzugang mit einer zeitlichen Befristung versehen und nur zweckbeschränkt gewährt werden.

Schließlich sollte im Rahmen des Open-Data-Ansatzes der Zugang zu Daten des Staates und die Nutzung dieser Daten weiter ausgebaut werden. Die Attraktivität dieses Ansatzes im Unternehmensbereich kann erhöht werden, indem der Aufbau von Datenpools gefördert wird und die kartellrechtlichen Grenzen von Datenkooperationen geklärt und ggf. geweitet werden.