Wem gehören die Daten? – Rechtliche Aspekte der digitalen Souveränität in der Wirtschaft

Julia Froese(✉) und Sebastian Straub
Institut für Innovation und Technik (iit), Steinplatz 1,
10623 Berlin, Deutschland
Froese@iit-berlin.de,Straub@iit-berlin.de

Zusammenfassung. Ausgehend von einer konkreten Diskussion in der Luftfahrtbranche über Zugriffs- und Nutzungsrechte an den Daten, die durch Flugzeuge generiert werden, nimmt dieser Beitrag die rechtlichen Aspekte rund um das Thema „Datenhoheit" in den Blick. Aufbauend auf einer Darstellung der gegenwärtigen Rechts- und Interessenlage, allgemein und insbesondere in der Dreieckskonstellation Maschinenhersteller-Plattformbetreiber-Maschinennutzer in Bezug auf Rechte an Daten, werden Hinweise für eine mögliche vertragliche Ausgestaltung gegeben und bestehende Regelungslücken einschließlich ihrer möglichen Folgen aufgezeigt. Ferner wird kurz auf weitere, vom Ausgangsproblem mittelbar betroffene juristische Fragen eingegangen. Schließlich erfolgt eine Auseinandersetzung mit möglichen Ansätzen zur Beseitigung der bestehenden Regelungslücken, Rechtsunsicherheiten und daraus resultierender Probleme.

Schlüsselwörter: Datenhoheit · Datenplattformen · Verfügungsrechte · Nutzungsrechte · Vertragsgestaltung · Datenschutz

1 Einleitung

„IN DER LUFTFAHRT TOBT DER KAMPF UM DIE DATENHOHEIT" – Hintergrund dieser Artikelüberschrift aus dem letzten Jahr (vgl. zum gesamten Text Koenen 2019) ist die durch den Flugzeughersteller Airbus betriebene Plattform „Skywise", welche die durch Flugzeuge generierten Daten dazu nutzen will, vorbeugende Wartungs- und Reparaturdienstleistungen anzubieten. Für sich genommen ist es zunächst einmal eine gute Idee, durch Nutzung der maschinengenerierten Daten entsprechende Dienste auf den individuellen Wartungsbedarf anzupassen – so werden unter anderem die Ressourcen des Maschinennutzers geschont. Nichtsdestotrotz stoßen die Pläne von Airbus auf Kritik bei der Lufthansa Technik AG (LHT). Diese sind selbst ein Anbieter von Wartungs-, Reparatur- und Überholungsdienstleistungen von Flugzeugen; die LHT sieht aber nicht primär ihr eigenes Geschäft in Gefahr. Vielmehr gehe es um die Unabhängigkeit der Airlines, in ihrer Rolle als Kunden

E. A. Hartmann (Hrsg.): *Digitalisierung souverän gestalten,* S. 86–97, 2021.
https://doi.org/10.1007/978-3-662-62377-0_7

der Dienstleistung. Würden die Daten nicht transparent verarbeitet, seien die Airlines nicht in der Lage, einen etwa gemeldeten Reparaturbedarf nachzuvollziehen. Allerdings: Wenn eine Fluggesellschaft einen solchen Dienstleistungsvertrag mit einem anderen Unternehmen abschließt, so könnte doch eigentlich unterstellt werden, dass alle Beteiligten sich in Kenntnis der Bedingungen auf diese Geschäftsbeziehung eingelassen haben. Folglich könnte man sich fragen, was vorliegend dann überhaupt das Problem ist. Eine Besonderheit jedoch, nämlich die Verbindung von Maschinenhersteller und Plattformbetreiber, führt hier zu der eigentlichen und viel grundsätzlicheren Frage: Wem gehören die Daten, die durch die Nutzung einer Maschine entstehen? Darf der Zugriff untersagt werden? Wenn ja, wem und durch wen?

Im Übrigen zeigt der Umstand, dass hier überhaupt Uneinigkeit herrscht und diskutiert wird, dass vorliegend im Großen und Ganzen gleichberechtigte Parteien aufeinandertreffen und ein Wettbewerb besteht. Beispielsweise haben auch der US-amerikanische Flugzeughersteller Boeing (der neben Airbus für Lufthansa produziert) und die LHT selbst ähnliche Systeme entwickelt (vgl. auch Oldenburg). Dies ist aber nicht überall so. Auch in Branchen, in denen die Nutzer von Maschinen keine Fluggesellschaften sind, sondern Einzelpersonen wie etwa Landwirte oder Autofahrer, wird das Potenzial der durch die Maschinen generierten Daten, erkannt und genutzt. Ob man überhaupt als Maschinennutzer Einfluss auf den Vertragsinhalt nehmen kann, der mit dem Maschinenhersteller und/oder Plattformbetreiber abgeschlossen wird, ist also mindestens genauso relevant wie die Frage, welche Regelungen getroffen werden sollten, um der Interessenlage zu entsprechen.

Die Thematik Datenhoheit/Datenverfügbarkeit, die auch die aufgeworfenen Fragen beinhaltet, bildet den Fokus dieses Beitrags. In Abschn. 2 erfolgt zunächst eine Darstellung der gegenwärtigen Rechtslage, eine Auseinandersetzung mit vertraglichen Ausgestaltungsmöglichkeiten beziehungsweise zwingender Grenzen hierbei sowie eine Identifizierung teilweise bestehender Regelungslücken und ihrer möglichen Folgen. In diesem Zusammenhang wird die Bedeutung der verschieden ausgeprägten Machtverhältnisse in unterschiedlichen Branchen relevant.

In Abschn. 3 wird aufgezeigt, welche weitergehenden Fragen (wie beispielsweise Beschäftigtendatenschutz oder Haftung für durch fehlerhafte Daten entstandene Schäden) in diesem Zusammenhang relevant werden können. Die Hintergründe, Interessenlage und mögliche Folgen für die vertragliche Ausgestaltung zwischen den Parteien werden kurz beleuchtet. An dieser Stelle noch ein Hinweis: Die dargestellten Fallkonstellationen sollen dazu dienen, das angesprochene Problem zu veranschaulichen. Im Interesse der Übersichtlichkeit wird die Rechtslage in Bezug auf die für die jeweilige Betrachtung nicht relevanten Tatbestandsmerkmale daher vereinfacht und nicht in all ihren juristischen Details wiedergegeben, auf diese wird in den entsprechenden Fußnoten hingewiesen.

Nach einer zusammenfassenden Darstellung des identifizierten Handlungsbedarfs erfolgt in Abschn. 4 eine Auseinandersetzung mit verschiedenen Lösungsmöglichkeiten und bereits existierenden Vorschlägen.

2 Datenhoheit

Das Beispiel Airbus/Lufthansa zeigt anschaulich die bestehende Problemlage: Trotz ihrer wirtschaftlichen Bedeutung sieht die Rechtsordnung kein Eigentumsrecht oder ein vergleichbares absolutes Recht an Daten vor. Dies mag auf den ersten Blick verwundern, denn die Bedeutung von Daten als Wirtschaftsgut wird seit Jahren in Politik und Wirtschaft hervorgehoben. In der Debatte werden Daten häufig als das „Öl des 21. Jahrhunderts" bezeichnet. Bei dieser Metapher wird jedoch regelmäßig die Natur von Daten verkannt. Anders als Rohstoffe sind Daten kein knappes Gut, nicht verbrauchbar und im Übrigen beliebig häufig vervielfältigbar. Die Schaffung eines Dateneigentums wurde auf politischer Ebene zeitweise in Erwägung gezogen (vgl. zum Beispiel den Koalitionsvertrag zwischen CDU, CSU und SPD 2018) und (auch auf europäischer Ebene) intensiv evaluiert (vgl. Barbero et al. 2017; Arbeitsgruppe „Digitaler Neustart" der Justizministerkonferenz 2017), bislang ohne Ergebnis. Aus diesem Grund lohnt es sich, einen Blick auf den rechtlichen Status Quo zu werfen. Wie nachfolgend gezeigt wird, gibt es eine Reihe gesetzlicher Vorschriften, welche Daten beziehungsweise die darin enthaltenen Informationen oder Inhalte schützen und einem Rechtssubjekt in dem jeweiligen gesetzgeberischen Kontext Verfügungsrechte gewähren.

2.1 Dateneigentum

In Bezug auf die zivilrechtliche Behandlung von Daten ist zunächst festzustellen, dass die Vorschriften des Bürgerlichen Gesetzbuches (BGB) kein Eigentumsrecht an Daten vorsehen. Das betrifft sowohl Einzeldaten als auch den Gesamtbestand von Daten, etwa in Form einer Datenbank. Daten sind keine körperlichen Gegenstände (§ 90 BGB) und daher den sachenrechtlichen Regelungen des BGB nicht zugänglich. Die Zuweisung von Daten erfolgt also im Grundsatz rein faktisch: Derjenige, der technisch in der Lage ist, auf Daten zuzugreifen und diese zu verarbeiten, kann dies tun. Ausnahmen hiervon können sich aus einzelnen Gesetzen ergeben, die je nach Regelungszweck eine bestimmte Art von Daten erfassen oder eine konkrete Schutzrichtung haben, etwa das Urheberrecht, das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) oder die Regelungen des Datenschutzrechts. Die Nutzung von Daten kann darüber hinaus auch durch vertragliche Vereinbarungen beschränkt werden.

2.2 Urheberrechtlicher Schutz von Daten und Datensammlungen

Das Urheberrecht dient dem Schutz von kreativen Leistungen und gewährt dem Urheber für einen begrenzten Zeitraum weitgehende Verwertungsrechte. Voraussetzung ist jedoch stets das Vorliegen einer persönlichen geistigen Schöpfung (§ 2 Abs. 2 UrhG). Notwendig ist hierfür ein menschlicher Schaffensprozess. Diese „anthropozentrische Ausrichtung des Urheberrechts" (Wandtke 2019) führt dazu,

dass rein maschinell generierte Erzeugnisse wie Daten keinen Urheberrechtsschutz genießen.[1] Möglich (und auch ausdrücklich gesetzlich vorgesehen) ist jedoch der Schutz von Datenbanken. Ein Datenbankwerk ist ein Sammelwerk, dessen Elemente systematisch oder methodisch angeordnet und einzeln, mit Hilfe elektronischer Mittel oder auf andere Weise, zugänglich sind (§ 4 Abs. 2 UrhG). Bei ungeordnet aneinandergereihten Rohdaten fehlt es in der Regel an einer systematischen oder methodischen Anordnung (vgl. OLG Köln 2006). Zu beachten ist, dass sich der Schutz lediglich auf die Struktur der Datenbank, nicht jedoch auf den Inhalt, also die Einzeldaten, bezieht. Zudem müssen Datenbankwerke (als Unterfall von Sammelwerken) aufgrund der Auswahl oder Anordnung der Elemente eine persönliche geistige Schöpfung sein (§ 4 Abs. 1 UrhG). Das bedeutet, dass die wesentlichen Merkmale der Datenbank durch einen Menschen vorgegeben sind und die Datenbank eine gewisse Originalität aufweisen muss (vgl. EuGH 2012). Rein automatisierte erstellte Datenzusammenstellungen sind folglich kein Datenbankwerk im Sinne von § 4 Abs. 2 UrhG.

Daneben können Daten (mittelbar) als Teil einer Datenbank durch das Recht des Datenbankherstellers geschützt sein (§§ 87a ff. UrhG). Dieses ebenfalls im UrhG geregelte Leistungsschutzrecht kommt dem Hersteller einer Datenbank zugute und schützt die Investition in den Aufbau und die Pflege der Datenbank. Wie beim urheberrechtlichen Datenbankwerk werden Einzeldaten nicht geschützt, sondern lediglich die Datenbank in ihrer Gesamtheit. Anders als beim Datenbankwerk nach § 4 Abs. 2 UrhG ist keine zugrunde liegende geistige Schöpfung erforderlich. Notwendig ist aber, dass die Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Der Hersteller einer Datenbank kann sich gegen die Übernahme seiner Datenbank als Ganzes oder wesentlicher Teile des Inhalts der Datenbank zur Wehr setzen. Von praktischer Bedeutung ist dabei der Umstand, ab welchem (quantitativen) Schwellenwert von einer wesentlichen Entnahme die Rede ist. Der BGH geht davon aus, dass es sich bei einem Anteil von 10 % des Gesamtdatenvolumens der Datenbank noch nicht um einen wesentlichen Teil der Datenbank im Sinne von § 87b Abs. 1 UrhG handelt (vgl. BGH 2010). Zielen jedoch wiederholte Entnahmen darauf ab, die Datenbank insgesamt oder einen nach Art oder Umfang wesentlichen Teil zu verwerten, liegt ein Eingriff in die Rechte des Datenbankherstellers vor (BGH 2010).

2.3 Schutz von Geschäftsgeheimnissen

Gerade im Kontext von maschinengenerierten Daten nimmt der Schutz von Betriebs- und Geschäftsgeheimnissen eine immer wichtigere Rolle ein. Daten können Aufschluss über sensible Unternehmensvorgänge geben, wie etwa die betriebliche Auslastung und damit gegebenenfalls die Auftragslage. Bislang wurden

[1] Das gilt auch für Erzeugnisse, die durch künstliche Intelligenz geschaffen wurden, sofern die KI (und nicht der Mensch) den Schaffensprozess maßgeblich beeinflusst (vgl. Ehinger/Stiemerling 2018).

Betriebs- und Geschäftsgeheimnisse durch die Regelungen des Gesetzes gegen den unlauteren Wettbewerb (UWG) geschützt. Mit dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), welches im April 2019 in Kraft getreten ist, ergeben sich weitreichende Änderungen. Das GeschGehG dient dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung (§ 1 GeschGehG). Geschäftsgeheimnis ist eine Information, die geheim (und daher von wirtschaftlichem Wert) ist, durch angemessene Geheimhaltungsmaßnahmen geschützt wird und bei der ein berechtigtes Interesse an der Geheimhaltung besteht (§ 2 Nr. 1 GeschGehG). Liegen diese Voraussetzungen vor, gewährt das GeschGehG Schutz vor unberechtigter Erlangung, Nutzung oder Offenlegung, indem es dem geschädigten Unternehmen weitreichende Ansprüche gegen den Rechtsverletzer zugesteht (vgl. §§ 6 ff. GeschGehG). Betrachtet man die genannten Voraussetzungen im Einzelnen, wird in der Praxis der Nachweis der Einhaltung von angemessenen Geheimhaltungsmaßnahmen am schwersten zu führen sein. Denn hierzu gehören nicht nur technische, sondern auch organisatorische und rechtliche Maßnahmen. Das Gesetz selbst legt jedoch nicht fest, welche Maßnahmen zum Schutz von sensiblen Informationen konkret ergriffen werden müssen. Es liegt daher bei den Unternehmen, ihre Informationen zu klassifizieren und bei Annahme einer hohen Schutzbedürftigkeit risikoadäquate Schutzmaßnahmen zu ergreifen. Im Falle einer Rechtsverletzung muss das betroffene Unternehmen nachweisen können, dass die getroffenen Geheimhaltungsmaßnahmen angemessen waren.

Werden sensible Betriebsdaten an eine Plattform weitergegeben – weil dies zur Erfüllung des Vertragszwecks erforderlich ist –, ist sicherzustellen, dass der Plattformbetreiber ebenfalls die notwendigen Geheimhaltungsmaßnahmen gewährleistet. Im Rahmen der Vertragsgestaltung ist darauf hinzuwirken, dass der Plattformbetreiber entsprechende technische und organisatorische Schutzmaßnahmen ergreift.

2.4 Datenschutzrecht

Mit der unmittelbaren Geltung der EU-Datenschutzgrundverordnung (DSGVO) seit Mai 2018 hat zudem der Datenschutz an Bedeutung gewonnen. Kommt es zu einer Verarbeitung von personenbezogenen Daten, ist der Anwendungsbereich des DSGVO regelmäßig eröffnet. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (Art. 4 Nr. 1 DSGVO). Dabei kann sich die Zuordnung zwischen Information und Person direkt oder indirekt ergeben. Im betrieblichen Kontext können oftmals anhand von Maschinen- oder Standortdaten Rückschlüsse auf die dahinterstehende Person, wie etwa den die Maschine bedienenden Arbeitnehmer oder den Fahrzeugführer (hierzu siehe unter Abschn. 3.2), gezogen werden.

Zwar sehen die Vorschriften der DSGVO kein Dateneigentum an personenbezogenen Daten vor, dennoch kann der Betroffene im begrenzten Rahmen Einfluss auf die Datenverarbeitung nehmen. Die DSGVO gewährt in diesem Zusammenhang etwa das Recht auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung (Art. 15–18 DSGVO). Weisen die verarbeiteten Daten tatsächlich keinerlei Personenbezug auf, findet die DSGVO keine Anwendung.

2.5 Vertragsrecht

Der bisherige Beitrag hat gezeigt, dass die bestehende Rechtsordnung Daten nur fragmentarisch schützt. Die genannten Normen begründen zwar kein Dateneigentum im eigentlichen Sinne, sie gewähren dem jeweilig Berechtigten im begrenzten Rahmen aber eine faktische Exklusivität an Daten bzw. Datensammlungen. Zur Gewährleistung einer vollumfänglichen Datenhoheit ist man in der Praxis zumeist auf vertragliche Regelungen angewiesen. Der Vorteil einer vertraglichen Regelung ist ohne Zweifel deren Flexibilität. Die vertraglichen Rechte und Pflichten der Parteien können entlang der jeweiligen Interessenslagen individuell ausgehandelt werden. Hierbei gilt der Grundsatz der Vertragsfreiheit. Das bedeutet, dass es den Vertragsparteien – vorbehaltlich der vorangehend dargestellten gesetzlichen Grenzen – grundsätzlich selbst überlassen ist, Datenzugangs- und Datennutzungsrechte zu regeln. Der hierdurch entstehende Handlungsspielraum kann aus Sicht des Wettbewerbs zugleich nachteilig sein. Denn es besteht die Gefahr, dass Unternehmen ihre Marktmacht einsetzen und sich umfangreiche Datenzugangs- und Datennutzungsrechte einräumen lassen (so auch Vogel 2020, der in diesem Zusammenhang auch von der Gefahr der Entstehung von Datenmonopolen spricht, siehe Abschn. 4). Hiervon betroffen wären vor allem kleine und mittlere Unternehmen, die in vertikalorientierten Wertschöpfungsketten in der Regel unterlegen sind.

Die Vertragsgestaltung kann darüber hinaus sehr aufwändig sein. Leistungspflichten in Bezug auf datenbezogene Prozesse lassen sich nur schwerlich in die gesetzlich vorgesehenen Vertragstypen einordnen. Die klassischen Vertragstypen können daher lediglich Grundlage für individuell ausgehandelte Vertragswerke sein (vgl. Körber/König 2020). Die Vertragsparteien können datenbezogene Pflichten in einem allgemeinen Vertrag aufnehmen (etwa im Rahmen eines Kauf- oder Wartungsvertrags) oder aber in einem gesonderten Vertrag regeln (vgl. Hoeren/Uphues 2020). Der Vertrag sollte den Leistungsgegenstand genau bezeichnen. Es muss also festgelegt werden, welche Daten konkret übermittelt werden und wer welche Leistungen erbringen muss. Neben der Festlegung eines Nutzungszwecks sollte auch der Umfang der Nutzungsrechteeinräumung bestimmt werden, also, was genau der Empfänger mit den Daten machen darf und ob er – hat er die Daten einmal erhalten – andere von der Nutzung ausschließen darf.[2] Aus Sicht des Maschinennutzers, des „Kunden“ im o. g. Beispiel, ist eine Regelung vorzugswürdig, nach welcher er selbst weiterhin auf die Daten zugreifen darf. Je nach Konstellation kann es sogar interessengerecht sein, diese offen verfügbar zu machen (vgl. Vogel 2020, der hierin ein mögliches Mittel zur Vermeidung der Entstehung von Datenmonopolen sieht). Auf der anderen Seite kann es gerade bei unternehmenssensiblen Daten geboten sein, Pflichten hinsichtlich der Datensicherheit festzulegen (siehe Abschn. 2.3).

Auch kann es notwendig sein, den technischen Ablauf des Datentransfers genau festzulegen, beispielsweise, Schnittstellen und Datenformate zu bestimmen und etwaige Mitwirkungspflichten der Vertragspartner zu benennen (vgl. Hoeren/Uphues 2020).

[2] In Betracht kommt die Einräumung eines ausschließlichen oder eines einfachen Nutzungsrechts.

Neben den bereits genannten spezialgesetzlichen Schutzrechten, aus denen sich Grenzen ergeben, existieren weitere allgemeine gesetzliche Regelungen zum Schutz vor allem der in manchen Konstellationen typischerweise unterlegenen beziehungsweise schwächeren Vertragspartei. Zu nennen sind in diesem Zusammenhang vor allem § 138 BGB, wonach ein „sittenwidriges" Rechtsgeschäft nichtig ist, sowie die Beschränkungen des Rechts der allgemeinen Geschäftsbedingungen (AGB, geregelt in §§ 305 ff. BGB). AGB sind „alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwenderin) der anderen Vertragspartei bei Abschluss eines Vertrags stellt" (§ 305 BGB). Werden AGB wirksam in den Vertrag einbezogen, unterliegen die dort enthaltenen Bestimmungen der Inhaltskontrolle gemäß § 307 BGB. Dies hat zur Folge, dass Bestimmungen unwirksam sind, wenn sie den Vertragspartner entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Die in den genannten Normen enthaltenen sogenannten unbestimmten Rechtsbegriffe wie „unangemessene Benachteiligung" oder „gute Sitten" entfalten ihre volle Wirksamkeit allerdings erst bei richterlicher Konkretisierung durch die Bildung von Fallgruppen und sind bis dahin eher ungeeignet, für Rechtssicherheit zu sorgen.

Die Vertragsfreiheit kann schließlich aber auch durch das Wettbewerbsrecht beschränkt sein. Die Einräumung von Datenrechten kann in diesem Zusammenhang kartellrechtliche Implikationen aufweisen (vgl. hierzu im Detail Körber/König 2020). Durch Art. 101 Abs. 1 AEUV werden insbesondere Vereinbarungen zwischen Unternehmen untersagt, welche geeignet sind, den Wettbewerb zu beeinträchtigen und zu einer Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs führen. Dies betrifft vor allem Unternehmen, die auf horizontaler Ebene miteinander kooperieren; hier müssen die vertragliche Vereinbarung auf ihre wettbewerbsrechtliche Kompatibilität hin überprüft werden. Die wettbewerbsrechtlichen Missbrauchsverbote wie zum Beispiel § 19 GWB schließlich dienen dazu, den unterlegenen Vertragspartner vor benachteiligenden Vereinbarungen zu schützen, die der andere Vertragspartner nur aufgrund seiner beherrschenden Marktstellung durchsetzen kann.

3 Weitergehende Fragen in diesem Zusammenhang

3.1 (Beschäftigten-) Datenschutz

Dort wo Menschen mit Maschinen interagieren, können potenziell auch personenbezogene Daten anfallen. Dabei handelt es sich um Informationen, die einen direkten oder indirekten Bezug zu einer Person (in diesem Fall zu einem Beschäftigten) zulassen. Diese Daten sind durch die Vorgaben der DSGVO in ihrer Verkehrsfähigkeit erheblich eingeschränkt. Schon alleine zur Vermeidung der haftungsrechtlichen Folgen eines Verstoßes müssen die Vorgaben der DSGVO im Rahmen der Vertragsverhandlungen zwischen dem die Maschine nutzenden Unternehmen und dem Plattformbetreiber unbedingt beachtet werden.

Nach der DSGVO ist die Verarbeitung personenbezogener Daten nur unter bestimmten Voraussetzungen gestattet. In Art. 6 sind verschiedene Erlaubnistatbestände aufgezählt, die eine Datenverarbeitung legitimieren können, wie etwa die

Einwilligung oder die Datenverarbeitung aufgrund eines berechtigten Interesses. Bei der Verarbeitung von personenbezogenen Daten im Beschäftigtenkontext gewährt die DSGVO in Art. 88 den Mitgliedsstaaten zudem Handlungsspielraum. Deutschland hat im Rahmen dieser Öffnungsklausel die Vorschrift des § 26 BDSG geschaffen. Danach dürfen für Zwecke des Beschäftigungsverhältnisses personenbezogene Daten verarbeitet werden, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigtenverhältnisses erforderlich ist. Daneben kann die Verarbeitung von Beschäftigtendaten auch durch eine Einwilligung oder eine Kollektivvereinbarung (z. B. eine Betriebsvereinbarung) legitimiert werden.

Die Einwilligung erweist sich dabei zumeist als ungeeignete Rechtsgrundlage. Zum einen muss die Einwilligung freiwillig erteilt werden, was wegen der wirtschaftlichen Abhängigkeit des Beschäftigten gegenüber dem Unternehmen nicht ohne Weiteres angenommen werden kann (vgl. im Detail hierzu Vogel/Klaus 2019). Zum anderen ist eine Einwilligung aufgrund ihrer jederzeitigen Widerrufbarkeit kein adäquates Mittel, um eine konstante rechtssichere Basis zu schaffen.

Vor diesem Hintergrund ist der Abschluss einer Kollektivvereinbarung nach § 26 Abs. 4 BDSG vorzugswürdig. Sofern im Unternehmen ein Betriebsrat besteht, muss bei der Implementierung von neuen Technologien ohnehin das in § 87 Abs. 1 Nr. 6 BetrVG angeordnete Mitbestimmungsrecht beachtet werden. Danach hat der Betriebsrat bei der Einführung und Anwendung von technischen Einrichtungen mitzubestimmen, die dazu geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Die die betriebliche Mitbestimmung wahrende Betriebsvereinbarung kann so also gleichzeitig die Rechtsgrundlage für die Datenverarbeitung bilden.

3.2 Haftung für Folgeschäden

Im Rahmen der Beziehung zwischen Plattformbetreiber und Kunden ist nicht nur die Klärung von Datenhoheit und Zugriffsrechten, sondern auch die Qualität der Daten selbst entscheidend (vgl. Ensthaler et al. 2019; Gieschen et al. 2019). Wenn bestimmte Prozesse vom Ergebnis einer Datenverarbeitung abhängen oder die Datenverarbeitung Auslöser für weitere Schritte (beispielsweise, wie eingangs genannt, eine Reparatur) sein soll, können dem Kunden aufgrund fehlerhafter Werte oder fehlerhafter Übermittlung Folgeschäden entstehen. Dies können wirtschaftliche Einbußen durch eine infolge unterbliebener Wartung nicht funktionstüchtige Maschine, ein Produktionsstillstand bzw. Lieferengpässe, aber auch Gesundheit und Leben anderer Menschen sein.

Ist vertraglich nichts weiter vereinbart, ist die Rechtslage auf den ersten Blick eindeutig: Der Plattformbetreiber haftet für durch eine fehlerhafte Datenverarbeitung entstandene Schäden, sofern er diese zu vertreten hat,[3] also mindestens fahrlässig handelt, § 276 BGB. Ein Unternehmen muss sich hierbei unter den Voraussetzungen des § 278 BGB die Fahrlässigkeit seiner Mitarbeitenden zurechnen lassen. Problematisch aus Sicht des Kunden ist vorliegend also nicht, dass ihm keine

[3] Unabhängig von der Anspruchsgrundlage – in Betracht kommt hier eine Haftung aus Vertrag gem. § 280 BGB oder auch eine Haftung aus Delikt gem. 823 Abs. 1 BGB.

gesetzlichen Rechte zustehen würden, sondern die Frage, wann diese greifen. Wann ist eine Datenverarbeitung „fehlerhaft“ und kann man dies in technischer Hinsicht immer zweifelsfrei feststellen? Wann kann man dem Plattformbetreiber fahrlässiges Handeln vorwerfen?

Nach § 276 Abs. 2 BGB handelt fahrlässig, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. Was erforderlich ist, wird anhand eines objektiven Maßstabs nach den im Verkehrskreis des Betroffenen üblichen Verhaltensanforderungen bestimmt (vgl. Schmidt 2020). Hier sollte vorab geklärt werden, wem welche möglichen Fehler zuzurechnen sind und das für diese Beurteilung erforderliche Maß an Transparenz und Informationsaustausch als vertragliche Nebenpflichten festgelegt werden. Ferner ist es innerhalb gewisser Grenzen möglich, eine gesetzlich vorgesehene Haftung vertraglich auszuschließen. Je nach Interessenlage und Verhandlungsmasse sollte also darauf hingewirkt werden, dies entweder herbeizuführen oder zu vermeiden. Die Vereinbarung eines Haftungsausschlusses für leichte Fahrlässigkeit des Plattformbetreibers etwa dürfte in dessen Sinne sein (vgl. Gieschen et al. 2019), aber natürlich eher weniger dem Interesse des Kunden entsprechen und von diesem soweit möglich verhindert werden.

3.3 Mangelgewährleistung und Beweislasten

Auch mit Blick auf die Darlegungs- und Beweislasten im Rahmen des schuldrechtlichen Gewährleistungsrechts könnte eine Konstellation, in der ausschließlich der Plattformbetreiber auf die Maschinendaten zugreifen kann und Einsicht in diese hat, aus Sicht des Kunden zu Unstimmigkeiten führen: Dem Kunden[4] als Nutzer der Maschine steht gegenüber dem Hersteller[5] bei einem Mangel am Vertragsgegenstand (bei Gefahrübergang) ein Recht auf Nacherfüllung zu, mit anderen Worten: Funktioniert die Maschine nicht, wie sie soll, kann der Kunde vom Hersteller verlangen, dass dieser den Fehler behebt, also die Maschine repariert[6]. Unabhängig vom konkret zugrunde liegenden Rechtsverhältnis kommt es letzten Endes auf einen Punkt entscheidend an: Auf den Ausschluss der Nacherfüllung bei Verantwortlichkeit des Gläubigers für den Fehler, vgl. § 323 Abs. 6 BGB. Auch hier muss mindestens Fahrlässigkeit vorliegen, um diese Verantwortlichkeit zu bejahen. Den Beweis dafür, dass der Kunde für den Fehler verantwortlich ist (etwa durch unsachgemäße Bedienung

[4] Die Bezeichnung „Kunde“ steht hier entsprechend der eingangs skizzierten Konstellation stellvertretend für denjenigen, der nach dem konkreten Vertrag die Maschine besitzen soll; in Betracht kommen neben einem Kaufvertrag als weitere Vertragstypen auch Pacht oder Leihe beziehungsweise wie oben schon genannt ein Rechtsverhältnis sui generis.

[5] Dieser Anspruch besteht auch gegen einen Zwischenhändler, also allgemein gegenüber demjenigen, der dem Kunden die Maschine verschafft hat. Der Einfachheit halber und entsprechend dem Eingangsbeispiel wird im Folgenden von einem Verhältnis Hersteller – Nutzer ausgegangen.

[6] Auch dies gilt unabhängig vom konkret zugrunde liegenden Schuldverhältnis; im Folgenden wird stellvertretend auf die Regelungen des allgemeinen Schuldrechts zurückgegriffen.

der Maschine oder falsche Lagerung), muss der Hersteller als Schuldner des Gewährleistungsanspruchs erbringen und wird sich hierfür der Daten bedienen, die die Maschine ihm geliefert hat.

Diesbezüglich können unter anderem folgende Fragen relevant werden: Wie kann der Kunde dies widerlegen, wenn er nicht auf die Daten zugreifen kann? Darf sich zur Beweiserbringung Daten bedient werden, die Rückschlüsse auf den Arbeitnehmer und seine Arbeitsleistung zulassen? Gilt der Beweis durch anonymisierte Daten als erbracht?

4 Fazit

Es zeigt sich, dass die hier skizzierten Problemkonstellationen zum Teil bereits mit bestehenden Rechtsnormen gelöst werden können. Auch sind vertragliche Regelungen aufgrund ihrer Flexibilität eine gute Ergänzung in gesetzlich ungeregelten Bereichen. Dies gilt aber nur, soweit zwischen den Parteien annähernd gleiche Verhandlungspositionen herrschen. Die Vertragsnormen, die einen unterlegenen Vertragspartner benachteiligen, finden zwar ihre Grenze in den zwingenden Regelungen des Schuldrechts. Die darin enthaltenen unbestimmten Rechtsbegriffe benötigen allerdings eine gewisse Konkretisierung, um für Rechtssicherheit zu sorgen.

Welche konkreten Folgen die teilweise ungeklärte Rechtslage im Bereich der Datenhoheit für manche Branchen langfristig haben wird, ist nicht absehbar. Klar ist jedoch, dass eine bestehende Rechtsunsicherheit hemmend auf die wirtschaftliche Entwicklung wirkt und sei es nur durch einen zögerlichen Einsatz neuer Technologien. Teilweise wird auch vor der Gefahr der Entstehung von Datenmonopolen gewarnt (vgl. u. a. Vogel 2020).

Die gesetzliche Regelung eines Eigentums an Daten ist allerdings keine Lösung: Wie oben bereits kurz angesprochen, ist die dem Eigentum als absolutem Recht zugrunde liegende Interessenlage nicht mit derjenigen vergleichbar, die bei einer Rechtsbeziehung zu Daten als nichtkörperlichen Rechtsobjekten besteht (so auch Vogel 2020): Ein einzelnes Datum kann anders als ein verkörperter Gegenstand beispielsweise keine Wertminderung erfahren, wenn man es benutzt. Auch wenn man es vervielfältigt, bleibt es dasselbe Datum – dann in mehrfacher Ausführung. Unter anderem daran würde zudem die gesetzliche Festlegung der Kriterien, anhand derer eine Eigentümerschaft zugeordnet werden soll, wenn nicht scheitern, so zumindest sehr komplex werden. Durch die vielfältigen Entstehungsmöglichkeiten von Daten und die unterschiedliche Bedeutung eines Datums je nach Kontext, kann es beispielsweise in einer Situation richtig sein, die Eigentümerschaft nach dem Entstehungs- bzw. Schaffungsprozess zuzuordnen, in einer anderen Situation erscheint eine Zuordnung desselben Datums nach dem Kriterium der persönlichen Betroffenheit sachgerecht. Eine gesetzliche Regelung wäre entweder zu unbestimmt oder würde nicht jeden Fall erfassen oder müsste so kleinteilig sein, dass sie schwerlich handhabbar wäre.

Ein Ansatz ist die von Vogel 2020 vorgeschlagene Etablierung von Musterverträgen, deren Verwendung durch Selbstverpflichtungserklärungen sichergestellt werden könnte. So könnte die branchenspezifische Interessenlage jeweils optimal

adressiert werden. Den unterlegenen Vertragspartner schützt dies natürlich nur, sofern er bei der Erstellung der jeweiligen Regelwerke maßgeblich beteiligt wird beziehungsweise seine Interessen angemessen vertreten werden. Flankiert werden könnte dies außerdem durch Zertifizierungssysteme, die nach außen hin sichtbar machen, welche Unternehmen sich zur Nutzung der Musterklauseln verpflichtet haben.

Die mögliche Korrektur unerwünschter vertraglicher Regelungen durch das Kartellrecht, auf die von der Justizministerkonferenz 2017 verwiesen wurde, ist ebenso durchaus denkbar, jedoch genauso wie die zwingenden vertragsrechtlichen Grenzen erst bei einer Konkretisierung der auch hier bestehenden unbestimmten Rechtsbegriffe[7] geeignet, für Rechtssicherheit zu sorgen. Diesbezüglich könnte gegebenenfalls eine Erleichterung des Zugangs zu den Gerichten und/oder ein zügigerer Verfahrensgang die richterliche Klärung beziehungsweise Konkretisierung durch die Etablierung von Fallgruppen herbeiführen. Dass dies möglich ist, zeigt beispielsweise das Arbeitsrecht: Aufgrund der existenziellen Bedeutung für den Einzelnen sind die Hürden für die Erhebung einer Kündigungsschutzklage niedriger als bei einer „normalen" zivilrechtlichen Klage. Das Arbeitskampfrecht wiederum ist ein gutes Beispiel dafür, wie ein (Teil-) rechtsgebiet fast ausschließlich richterrechtlich geprägt ist. Dadurch, dass die Rechtsprechung bestehendes Recht lediglich anwendet und auslegt und den gesetzlich vorgegebenen Rahmen anhand eines bestimmten Sachverhalts konkretisiert, kann sie flexibler und interessengerecht neue Entwicklungen berücksichtigen.

Literatur

Arbeitsgruppe Digitaler Neustart der Konferenz der Justizministerinnen und Justizminister der Länder – Bericht vom 15. Mai 2017

Barbero, M., Cocoru, D., Graux, H., Hillebrand, A., Linz, F., Osimo, D., Siede, A., Wauters, P.: Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability. Europäische Union (2017)

Beschluss der Konferenz der Justizministerinnen und Justizminister der Länder (2017)

Bundesgerichtshof (BGH), Urteil vom 01.12.2010 – I ZR 196/08

Ehinger, P., Stiemerling, O.: Die urheberrechtliche Schutzfähigkeit von Künstlicher Intelligenz am Beispiel von Neuronalen Netzen. In: Computer & Recht, S. 761–770. Verlag Dr. Otto Schmidt, Köln (2018)

Ensthaler, J., Haase, M., Straub, S., Gieschen, J.-H.: Bedeutsame Rechtsbereiche für die Smart Service Welt – Vermeidung von Haftung und Rechtsverstößen. In: Begleitforschung Smart Service Welt – iit – Institut für Innovation und Technik in der VDI/VDE (Hrsg.) Sichere Plattformarchitekturen – Rechtliche Herausforderungen und technische Lösungsansätze, S. 8–11. Berlin (2019)

Europäischer Gerichtshof (EuGH), Urteil vom 01.03.2012, C-604/10

[7] S. z. B. § 19 GWB: das Verbot der „missbräuchlichen Ausnutzung" einer marktbeherrschenden Stellung, die u. a. vorliegt, wenn dadurch ein anderes Unternehmen „unbillig behindert" wird.

Gieschen, J.-H., Seidel, U., Straub, S.: Rechtliche Herausforderungen bei Smart Services – Ein Leitfaden. In: Bundesministerium für Wirtschaft und Energie (Hrsg.) Begleitforschung zum Technologieprogramm Smart Service Welt. Bundesministerium für Wirtschaft und Energie, Berlin (2019)

Hoeren, T., Uphues, S.: Big Data in Industrie 4.0. In: Frenz, W. (Hrsg.) Handbuch Industrie 4.0.: Recht, Technik, Gesellschaft, S. 113–131. Springer, Berlin (2020)

Koenen, J.: In der Luftfahrt tobt der Kampf um die Datenhoheit. Handelsblatt (2019). https://www.handelsblatt.com/unternehmen/industrie/lufthansa-technik-und-airbus-in-der-luftfahrt-tobt-der-kampf-um-die-datenhoheit/24007658.html?protected=true. Zugegriffen: 12. Aug. 2020

Körber, T., König, C.: Vertragsrecht 4.0. In: Frenz, W. (Hrsg.) Handbuch Industrie 4.0.: Recht, Technik, Gesellschaft, S. 237–256. Springer, Berlin (2020)

Lufthansa Technik Homepage (2020). https://www.lufthansa-technik.com/. Zugegriffen: 12. Aug. 2020

Oberlandesgericht Köln (OLG Köln), Urteil vom 15.12.2006 – 6 U 229/0

Oldenburg, B.: Auf dem Weg zum Google der Lüfte. Innofrator (2020). https://www.innofrator.com/auf-dem-weg-zum-google-der-luefte/. Zugegriffen: 12. Aug. 2020

Schmidt, A.: Schuldrecht. In: Weber, C. (Hrsg.) Creifelds, Rechtswörterbuch. Beck, München (2020)

Vogel, P., Klaus, A.: Zulässigkeit der Verarbeitung von GPS-Daten im Arbeitsverhältnis. In: Stich, V., Schumann, J., Beverungen, D., Gudergan, G., Jussen, P. (Hrsg.) Digitale Dienstleistungsinnovationen, S. 393–496. Springer, Heidelberg (2019)

Vogel, P.: Datenhoheit in der Landwirtschaft 4.0. In: Gansdorfer, M. et al. (Hrsg.) Digitalisierung für Mensch, Umwelt und Tier. Referate der 40. GIL-Jahrestagung. Bd. Gesellschaft für Informatik, Bonn (2020)

Wandtke, A.A.: Urheberrecht, 7. Aufl. De Gruyter, Berlin (2019)