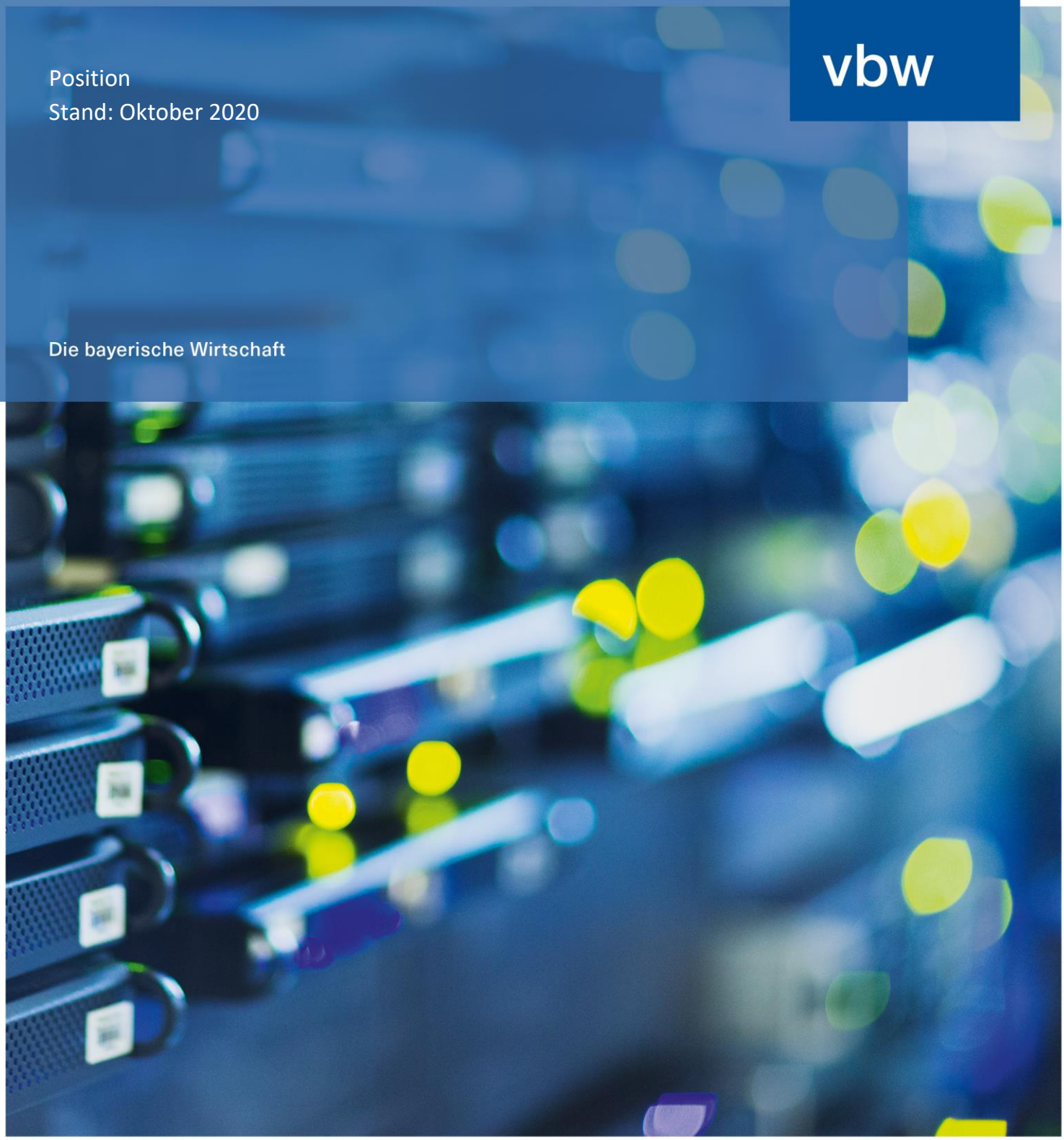
Digitalisierung

Datenwirtschaft

vbw

Position
Stand: Oktober 2020

Die bayerische Wirtschaft



Vorwort

Datenwirtschaft: Allgegenwärtig und noch zu wenig fassbar

Einerseits erscheint es spät, im Jahr 2020 erstmals ein Positionspapier zur Datenwirtschaft zu veröffentlichen, weil digitale Technologien längst alle Sektoren und Branchen durchdringen und die Wirtschaft im Ganzen prägen. Von einem abgrenzbaren Teilbereich kann nicht mehr die Rede sein. Wirtschaft ganz ohne Datennutzung ist mittlerweile ein Nischenbereich.

Andererseits ist es immer noch fast zu früh, weil so viele Einzelaspekte noch weit von einer abschließenden Klärung entfernt sind und so vieles im Fluss ist, dass die Materie bisweilen wenig greifbar erscheint. Während sich beinahe jedes bayerische und deutsche Unternehmen auf die eine oder andere Art mit der Nutzung von Daten befasst, steht das Thema erst bei einer sehr kleinen Minderheit im Zentrum des Geschäftsmodells.

Gerade weil die Potenziale der Datenwirtschaft enorm sind, muss aber der Versuch unternommen werden, sowohl am Standort optimale Rahmenbedingungen für unsere Unternehmen zu ermöglichen, als auch die zahlreichen Diskussionen und Regulierungsvorhaben auf einige Kernanliegen zu fokussieren.

Wenn wir eine globale Spitzenstellung in der Datenwirtschaft erreichen wollen, ist es von ganz entscheidender Bedeutung, dass wir ein chancenorientiertes und innovationsfreundliches Umfeld schaffen – mit einer Regulierung, die Fairness gewährleistet und Sicherheit gibt, aber nirgendwo mehr als nötig einengt. Wir müssen das Bewusstsein für die immensen Möglichkeiten einer intelligenten und verantwortungsbewussten Datennutzung stärken.

Bertram Brossardt
12. Oktober 2020

Inhalt

Position auf einen Blick

Chancen der Datenwirtschaft nutzen

Die Datenwirtschaft bietet große Chancen für alle Branchen und Sektoren, aber auch für jeden Einzelnen. Es gilt, diese bestmöglich zu nutzen. Dazu sind insbesondere die folgenden Aspekte zu beachten:

- Der Wert von Daten muss besser messbar werden. Darauf muss dementsprechend öffentlich geförderte Forschung einen Schwerpunkt setzen. Insbesondere bilanzielle Fragen sollten geklärt werden.
- Auch der Mehrwert der Digitalisierung und dort vor allem datenbasierte Geschäftsmodelle muss besser erfasst werden können. Dazu müssen die Grundlagen der volkswirtschaftlichen Statistik modernisiert werden.
- Wir brauchen kein Dateneigentum, aber auch kein Recht auf „Daten für alle“. Vertragliche Regelungen müssen Vorrang haben. Für den Insolvenzfall wären klarstellende Regelungen durchaus wünschenswert.
- Es gibt gegenwärtig keinen Anlass, bei der Zuordnung des Mehrwerts regulierend einzugreifen. Der Staat sollte eher bei der Vermittlung eines realistischen Bilds von der Datenwirtschaft ansetzen. Im Steuerrecht besteht kein akuter Handlungsbedarf – insbesondere wäre es nicht zielführend, über diesen Weg zu einer generellen Bepreisung von Daten zu gelangen.
- Datenschutzvorgaben müssen praxisgerecht ausgestaltet und angewendet werden. Vor allem die Anonymisierung muss ohne große Hürden rechtssicher möglich sein. Sachdaten dürfen allenfalls ausnahmsweise wegen einer (theoretischen) Personenbeziehbarkeit der DSGVO unterfallen.
- Bei der Umsetzung der neuen EU-Richtlinien für digitale Inhalte und für den Warenhandel müssen auch die Pflichten der Verbraucher bei einer Hingabe von Daten als Gegenleistung geregelt werden. Eine Erweiterung des Anwendungsbereichs auf Unternehmen ist nicht sachgerecht. Insgesamt sollte die Umsetzung so wenig wie möglich in die bewährte Systematik des BGB eingreifen.
- Neue Haftungsregelungen sollten nicht geschaffen werden, weil das geltende Recht gut geeignet ist, die wesentlichen Konstellationen interessengerecht aufzulösen. Geklärt werden sollten dagegen die rechtliche Behandlung von Updates, auch im B2B-Bereich, der Fehlerbegriff bei Software sowie Fragen im Zusammenhang mit dem Regress des Herstellers der physischen Sache. Generell dürfen die Anforderungen an den einzelnen Hersteller – ob von Hardware oder Software – in einem zunehmend komplexen Umfeld nicht überspannt werden.
- Souverän agierende Verbraucher sollten ein gefördertes Leitbild sein. Wichtig ist, dass jeder Einzelne Verantwortung für sein Handeln übernimmt. Weitere Informationspflichten sollten allenfalls sehr zurückhaltend eingeführt werden – zielführender wären Vereinfachungen und einheitlichere Standards (beispielsweise Piktogramme) hinsichtlich der bereits bestehenden Pflichten.

Position auf einen Blick

- Für eine erfolgreiche europäische und nationale Datenwirtschaft müssen die richtigen Rahmenbedingungen geschaffen werden. Dazu zählen erweiterte Regeln für die Verfügbarkeit von Daten (Open Government Data, Datenspenden) und intelligente Cloud-Lösungen. In vielen Bereichen wäre Regulierung eher kontraproduktiv, so zum Beispiel im Hinblick auf Industrieplattformen, und muss unterbleiben. Im wichtigen Bereich IT-Sicherheit muss viel stärker auf Kooperation und Beratung gesetzt werden als auf die Ahndung von Verstößen. Forschung und Entwicklung müssen nachhaltig gestärkt werden, um den Vorsprung zu den führenden Nationen zu verringern.
- Corporate digital responsability und digitale Nachhaltigkeit sind sinnvoll, müssen aber freiwillige Konzepte bleiben. Umgekehrt müssen die Potenziale digitaler Technologien für Nachhaltigkeit, namentlich den Klimaschutz, umfassend gehoben werden.
- Auch die allgemeinen Rahmenbedingungen für erfolgreiches Wirtschaften am Standort müssen selbstverständlich stimmen. Zu nennen sind hier unter anderem das Arbeitsrecht, Bezahlbarkeit und Versorgungssicherheit im Energiebereich oder das Steuerrecht.

Als Fazit lässt sich sagen, dass die aktuellen Initiativen der EU und des Bundes zur Datenwirtschaft viele zielführende Aspekte enthalten, die Schwerpunkte aber stärker auf dem Ermöglichen des Neuen als auf dem Schutz vor potenziellen Gefahren liegen sollten. Während letztere gut mit dem bestehenden Instrumentarium zu bewältigen sind, müssen die Chancen noch deutlich besser genutzt werden.

1 Daten als „Rohstoff“ und Vermögensposition

Die Bedeutung des Zugriffs auf Daten in ausreichender Menge und Qualität löst Diskussionen über Zuordnung und Zugang aus

Datenwirtschaft oder Datenökonomie (Data Economy) sind als Begriffe inzwischen in den allgemeinen Sprachgebrauch übergegangen. Sie sind allerdings nicht eindeutig definiert und nicht trennscharf von anderen Bereichen der digitalen Transformation abzugrenzen, da Daten letztlich immer eine wichtige Rolle spielen.

Die vorliegende Position konzentriert sich auf Daten als vertragliche Leistung und Gegenleistung sowie Geschäftsmodelle, die maßgeblich darauf basieren, Daten zu nutzen, auszutauschen, zu handeln und zu monetarisieren. Big Data- und KI-gestützte Anwendungen sowie datenzentrierte Plattformen zählen daher in jedem Fall zum Kernbereich der Datenwirtschaft.

1.1 Definitionen

1.1.1 Daten, Informationen und Wissen

Eine einheitliche Legaldefinition für „Daten“ existiert bislang nicht. Verschiedene Ansätze finden sich unter anderem im Datenschutzrecht, im Strafrecht oder im Bereich der Normung. Generell lässt sich sagen, dass ein Datum eine maschinell verarbeitbare Folge von Zeichen (Zahlen, Buchstaben oder Symbolen) ist. Durch den Kontext (Kombination verschiedener Daten) kann sich aus dem Datum eine Information und damit eine Bedeutung ergeben. Wissen entsteht durch die Verknüpfung von Daten beziehungsweise Informationen und deren Interpretation.

1.1.2 Arten von Daten

Eine wichtige Unterscheidung ist zunächst diejenige zwischen personenbezogenen Daten und Sachdaten. Personenbezogene Daten beziehungsweise Informationen, die dem besonderen Schutz des Datenschutzrechts (namentlich der DSGVO) unterliegen, sind solche, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen und Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. In anderen Vorschriften (z. B. TKG, TMG) wird ferner zwischen den für den Vertragsschluss notwendigen *Bestandsdaten* (z. B. Adresse, Kontodaten) und bei der Interaktion entstehenden *Nutzungs-* bzw. *Verkehrsdaten* (z. B. besuchte Seiten) unterschieden. *Inhaltsdaten* betreffen demgegenüber den Inhalt der Kommunikation. Ob es sich jeweils um personenbezogene Daten handelt hängt davon ab, ob sie mit einem bestimmten Nutzer verknüpft sind.

Digitale Daten können in (semi-)*strukturierter* oder *unstrukturierter* Form vorliegen beziehungsweise gespeichert werden. Strukturierte Daten basieren auf einem Ordnungssystem und ihnen können z. B. Begriffe zugeordnet werden. Rohdaten sind alle (noch unbearbeiteten) Daten in ihrem ursprünglich – zum Beispiel durch einen Sensor – erfassten Format.

Aggregierte Daten sind Daten, die je nach Systemanforderung zusammengefasst, kategorisiert oder interpretiert worden sind. In datenschutzrechtlicher Hinsicht relevant ist, dass aggregierte Daten durch das Zusammenführen der Daten von mindestens drei Personen nicht mehr auf eine einzelne Person beziehbar sind, sondern lediglich der Gruppenwert erkennbar bleibt. Damit unterliegen sie nicht mehr dem Regelungsbereich der DSGVO.

Position der vbw

Die datenschutzrechtlichen Vorgaben – insbesondere Einwilligungserfordernis, Datensparsamkeit und Zweckbindung – stellen im internationalen Vergleich relativ hohe Hürden für eine wirtschaftliche Nutzung von Daten auf. Diese Grundsätze müssen daher praxisgerecht ausgelegt werden. Insbesondere muss eine Anonymisierung rechtssicher und ohne überzogene Anforderungen möglich sein. Bisher macht die DSGVO keine klaren Vorgaben, viele Details sind umstritten. Eine Anonymisierung sollte auch nicht als neuer Verarbeitungsvorgang gewertet werden, da anderenfalls Fehlanreize gesetzt würden, darauf – obwohl unter Datenschutzgesichtspunkten wünschenswert – gleich ganz zu verzichten.

Die Nutzung von Sachdaten darf keinen zusätzlichen Einschränkungen unterworfen werden. Insbesondere im Hinblick auf personenbeziehbare Daten ist das – auch gesamtgesellschaftliche – Interesse an einer hohen Datenverfügbarkeit immer angemessen zu berücksichtigen. Personenbeziehbarkeit darf also nicht immer dann schon angenommen werden, wenn die Herstellung eines entsprechenden Bezugs theoretisch möglich sein könnte.

Die Landesdatenschutzbehörden müssen angemessen ausgestattet sein und auf Beratung statt Sanktionierung ausgerichtet werden. Wenn keine Vereinheitlichung in der Entscheidungspraxis gelingt, kann eine Zentralisierung erforderlich werden. Sehr sinnvolle Leistungen wären rechtssichere Musterverträge und eine rechtsverbindliche Auskunft (analog etwa zu Bauvoranfragen).

1.2 Bedeutung von Daten für die Wertschöpfung

Die häufig gebrauchte Analogie, Daten seien der entscheidende Rohstoff der Zukunft, ist zugleich wahr und irreführend. Sie sind ein Rohstoff in dem Sinne, dass Wertschöpfung erst bei der Weiterverarbeitung entsteht. Daten sind nur dann wirklich wertvoll, wenn man sowohl über einen konkreten Verwendungszweck als auch über die rechtlichen (z. B. Einwilligung in den Verwendungszweck) und technischen Mittel (z. B. Algorithmen)

verfügt, um sie wirtschaftlich zu nutzen, und auch dann in aller Regel nur, wenn sie mit einer Vielzahl anderer Daten kombiniert werden können. Irreführend ist die Redewendung insoweit, als sie den Eindruck vermittelt, Daten seien per se sehr wertvoll und dem „Urheber“ oder „Inhaber“ des einzelnen Datensatzes (also des kleinen Rohstoffvorkommens) stehe damit in jedem Fall eine beachtliche Vergütung zu, wobei hier in der Regel noch ganz klassisch an eine monetäre Vergütung gedacht wird, nicht an Dienstleistungen.

1.2.1 Daten als Wirtschaftsgut

Wirtschaftsgüter (beziehungsweise Vermögensgegenstände im handelsrechtlichen Sinn) können neben Sachen auch Rechte oder tatsächliche Zustände, konkrete Möglichkeiten oder Vorteile für den Betrieb sein, deren Erlangung der Kaufmann sich etwas kosten lässt, die einer besonderen Bewertung zugänglich sind und zumindest mit dem Betrieb übertragen werden können.

Daten *können* nach dieser weiten Definition also jedenfalls Wirtschaftsgüter sein. Entsprechend wurden sie auch schon von der Rechtsprechung eingeordnet; auch verschiedene gesetzgeberische Entscheidungen zeigen, dass von einer entsprechenden Einordnung ausgegangen wird (näher dazu unten).

1.2.2 Besonderheiten von Daten, Informationen und Wissen

Ob Daten beziehungsweise das aus ihnen generierte Wissen auch Produktionsfaktoren sind, ist noch nicht entschieden. Im Gegensatz zu den klassischen Produktionsverfahren zeichnen sie sich dadurch aus, dass sie bei Verwendung nicht „verbraucht“ werden.

Die ökonomischen Besonderheiten der Digitalisierung liegen vor allem darin, dass das in Daten oder Datenmodellen verkörperte Wissen nahezu kostenlos kopiert werden kann, und die Grenzkosten für die Verbreitung einer zusätzlichen Information ebenfalls nahe Null liegen (sogenannte doppelte Nullgrenzkosteneigenschaft). Auch für die „Lagerung“, also die Speicherung der Daten beziehungsweise des Wissens entstehen im Vergleich zu realen Gütern vernachlässigbare Kosten. Diese Eigenschaften sind eng mit den Besonderheiten des zentralen „Produkts“ Software verbunden: Hohen Fixkosten bei der Entwicklung stehen niedrige Kosten für Kopien und Verbreitung gegenüber, was zu einer hohen Skalierbarkeit führt.

Ein Rohstoff im klassischen Sinne sind Daten angesichts ihrer besonderen Eigenschaften jedenfalls nicht. Eher als mit Öl – wie anfänglich oft geschehen – könnte man sie eher mit regenerativen Energiequellen wie der Sonnenenergie vergleichen, aber auch diese Analogie greift zu kurz.

1.2.3 Effekte der Digitalisierung auf die Wertschöpfung

Datenverarbeitung und -speicherung bilden die Grundlage der digitalen Transformation. Drei zentrale Eigenschaften kennzeichnen die Digitalisierung: Die Vernetzung von Menschen und Dingen, die Virtualisierung von Produkten und Prozessen sowie der Austausch von Daten und Wissen. Auf der Kombination dieser drei Eigenschaften und der Auswertung und Weiterentwicklung von Daten und Wissen bauen zunehmend automatisierte und autonome Systeme auf.

Eine intelligente Nutzung von Daten kann in allen Branchen neue Wertschöpfung schaffen durch

- *Optimierung von Prozessen* (Beispiel Building Information Modeling: Der digitale Zwilling ermöglicht in der Bauwirtschaft die durchgängige Nutzung von digitalen Gebäudeinformationen über den gesamten Lebenszyklus eines Bauwerks).
- *Produktverbesserungen* beziehungsweise *neue Produkte* (Beispiel individualisierte Medizin).
- optimierte oder neue *Geschäftsmodelle* (Beispiel predictive maintenance als – gegebenenfalls ergänzende – Dienstleistung).

Der Beitrag der Digitalisierung zur gesamtwirtschaftlichen Wertschöpfung ist heute schon hoch und soll allen Prognosen zufolge weiter steigen. Das physische Produkt bleibt wichtig, die wirtschaftliche Nutzung von Daten erweitert aber das Wertschöpfungsspektrum deutlich. Alleine dem zunehmenden Einsatz von Big Data-Verfahren wird ein Beitrag von 0,3 Prozentpunkten zum jährlichen Wachstum zugeschrieben. Im Jahr 2015 prognostizierte die EU-Kommission, dass sich die Wertschöpfung aus der Datennutzung etwa durch produktbezogene Dienstleistungen wie vorausschauende Wartung und Instandsetzung im Binnenmarkt innerhalb von fünf Jahren mehr als verdoppeln kann – bis auf vier Prozent des BIP der Europäischen Union im Jahr 2020.

Die volkswirtschaftliche Statistik ist heute aber noch nicht in der Lage, diese Effekte abzubilden. Tatsächlich lassen sich aus den amtlichen Zahlwerken sogar insgesamt nur eher schwache Auswirkungen der Digitalisierung ablesen. Zu den Erklärungsansätzen zählt, dass wir uns noch in einer Investitionsphase befinden, deren Effekte erst mit Verzögerung sichtbar werden und dass die volkswirtschaftliche Gesamtrechnung Aspekte wie eine gestiegene Konsumentenrente nicht abbildet (näher siehe *Neue Wertschöpfung durch Digitalisierung*, vbw 2017). Die vbw hat daher in einer bislang zweimal durchgeführten Studie auf Basis einer Unternehmensbefragung empirische Daten erhoben. Hochgerechnet auf die gesamte deutsche Wirtschaft kann danach die den digitalen Produkten und Dienstleistungen zurechenbare Wertschöpfung auf rund 500 Milliarden Euro geschätzt werden (Stand 2018/2019) – bei der ersten Untersuchung 2016 / 2017 waren es noch 332 Milliarden Euro. Das entspricht einem Zuwachs um 50 Prozent; die Erwartungen wurden sogar noch übertroffen.

Position der vbw

Es muss eine Verbesserung der statistischen Grundlagen angestrebt werden. Wichtig sind insbesondere eine Ergänzung der Indikatoren und die bessere Verknüpfung amtlicher Daten. Eine stärkere Berücksichtigung von Qualitäts- und Nutzenänderungen und ein Ausbau der Erfassung des intellektuellen Kapitals könnten die Produktivitätsmessung deutlich genauer machen. Ein weiterer Weg ist der Aufbau eines Längsschnittpanels der bayerischen beziehungsweise deutschen Wirtschaft, bei dem im Wege der Unternehmensbefragung über Jahre hinweg strukturgleich die relevanten Daten erhoben werden. Unsere eigenen Erhebungen gehen in diese Richtung. Als weiterer Schritt sollte im Rahmen der volkswirtschaftlichen Gesamtrechnung ein Satellitenkonto digitale Wirtschaft entwickelt werden, dass dann auch die Abbildung der Verflechtungen mit allen anderen Wirtschaftsbereichen ermöglicht.

1.3 Der Wert von Daten

Die Bestimmung eines konkreten Werts ist in vielerlei Hinsicht wichtig. Das gilt natürlich für die Festlegung einer angemessenen Gegenleistung (Entgelt), ob es um Unternehmen beziehungsweise Unternehmensteile oder reine Datenbestände geht. Auch für die Bilanzierung, die Festlegung von internen Verrechnungspreisen oder bei einer Bewertung im Rahmen konzerninterner Umstrukturierungen ist eine Wertermittlung entscheidend. Weitere Aspekte sind die Ermittlung einer (potenziellen) Schadenshöhe z. B. bei einem Verlust der Daten und ihre Bedeutung als Produktionsfaktor für das eigene Unternehmen, um strategische Entscheidungen (z. B. Versicherungsschutz, Maßnahmen zur Gefahrenabwehr, Investitionen in die Möglichkeiten zur Datenanalyse etc.) auf einer belastbaren Grundlage treffen zu können. Für jeden Einzelnen ist überdies die Frage relevant, was (ihm) seine persönlichen Daten wert sind, wenn er darüber entscheidet, ob er sie als „Zahlungsmittel“ einsetzt.

1.3.1 Wertermittlung: Objektive Ansätze

Um es vorwegzunehmen: Keine der gängigen Methoden für die finanzielle Bewertung immaterieller Vermögensgegenstände kann sich für die Bewertung von Daten aufdrängen. Im Allgemeinen kommen drei Ansätze in Betracht, die im Folgenden am Beispiel personenbezogener Daten skizziert werden.

Marktwertorientierte Verfahren orientieren sich an dem tatsächlich auf dem Markt erzielbaren Preis. Für Daten, namentlich für Einzeldaten, sind kaum Informationen zu Marktpreisen verfügbar. Ein denkbarer Ansatz sind die Marktpreise für Profile (z. B. Kreditvergabe, Marketingzwecke), die allerdings eine große Schwankungsbreite von einigen Cents bis ca. 30 Dollar für ein Profil aufweisen; eine Verallgemeinerung ist schwierig. Auch der Ansatz, die eigenen Daten als Teil des Unternehmenskapitals zu verstehen und den Wert aus großen Transaktionen (z. B. Übernahmen datengetriebener Unternehmen) abzuleiten,

kann allenfalls eine grobe Näherung leisten. So waren es etwa 55 Dollar pro Nutzer bei der Übernahme von WhatsApp durch Facebook und gut 20 Dollar bei Instagram, mehr als 200 Dollar beim Kauf von Skype durch Microsoft. Der Kaufpreis für Skype beispielsweise – seinerzeit etwa das Zehnfache des Jahresumsatzes – spiegelt mit Sicherheit mehr wider als den Wert von Nutzerdaten, namentlich Unternehmens-Knowhow. Diese Werte wären dann jeweils noch durch die Anzahl der Daten pro Nutzer zu dividieren.

Kostenorientierte Verfahren orientieren sich an den geschätzten Reproduktionskosten für den zu bewertenden Vermögensgegenstand (historische Kosten, Wiederbeschaffungskosten), also unter anderem dem Aufwand für Speicherung, Verarbeitung und Aufbereitung. Diese Informationen stehen dem Unternehmen, das über die Daten verfügt, in der Regel zur Verfügung, auch wenn die Zuordnung im Einzelfall schwierig sein mag. Unberücksichtigt bleiben hier allerdings die Vorteile, die aus einer Nutzung gezogen werden können.

Ertragsorientierte Verfahren ermitteln den Wert aus den zukünftigen finanziellen Überschüssen, die dem immateriellen Vermögenswert zugeordnet werden können. Das spiegelt die Investorensicht fraglos am besten wider. Konkrete Verfahren wie beispielsweise eine Lizenzpreisanalogie speziell für Daten fehlen aber auch hier. Bei Google und Facebook ist immerhin bekannt, dass sie mehr als 90 Prozent ihres Umsatzes mit Werbung machen, für die die Nutzerdaten nicht die alleinige, aber eine entscheidende Voraussetzung sind. Dass Facebook alleine im Jahr 2019 knapp 70,7 Milliarden Dollar Umsatz und rund 18,5 Milliarden Dollar Gewinn gemacht hat zeigt zwar, was sich mit dem aktiven Datenbestand (und dem vorhandenen Knowhow) pro Jahr und Nutzer verdienen lässt, bedeutet allerdings noch nicht, dass diese Zahl objektivierbar wäre. Selbst auf den einzelnen Nutzer bezogen haben dessen Informationen, die er in Social Media teilt, keineswegs alle denselben Wert. Ein Urlaubsfoto, das Aufschluss über bevorzugte Zielregionen geben mag, ist beispielsweise vermutlich weniger wertvoll als das Bild eines Babys, das auf einen markanten Wendepunkt im Konsumverhalten schließen lässt.

Während es für personenbezogene Daten bereits schwer ist, einen verlässlichen Anhaltspunkt für einen Wert zu finden, ist die Lage bei Sachdaten noch einmal komplizierter. Hier gibt es keinen vergleichbaren Standardweg der wirtschaftlichen Nutzung von Daten wie den Einsatz für Werbezwecke.

Zwischen Unternehmen ist aber immerhin die Preissetzung vergleichsweise einfach: die Monetarisierung liegt in der Verantwortung des Unternehmens, das über die Daten verfügt, und ist eine Frage der Vertragsgestaltung beziehungsweise von Angebot und Nachfrage. In der Regel verbleibt der Mehrwert bei demjenigen, der mittels von ihm (weiter)entwickelter Verfahren aus Daten nutzbare Informationen generiert. Ein Regulierungsbedarf ist gegenwärtig nicht ersichtlich.

1.3.2 Wertermittlung bei Verbraucherdaten: Subjektive Ansätze

Verhandlungsspielräume oder überhaupt Verhandlungen gibt es im Verbraucherbereich in der Regel nicht. Den Wert der persönlichen Daten aus der Sicht von Verbraucher*innen wird typischerweise mittels zweier gegensätzlicher Ansätze gemessen:

– mit dem angenommenen Wert *der persönlichen Daten*, also dem Preis, für den die Person bereit ist, ihre Daten offenzulegen („Willingness to Accept“ - WTA).
– mit dem angenommenen Wert *der Privatsphäre*, also dem Preis, den die Person bereit ist zu bezahlen, um ihre persönlichen Daten zu schützen („Willingness to Pay“ - WTP).

Grundsätzlich sind weniger Personen bereit, Geld für Privatsphäre auszugeben (WTP) als sie bereit sind, für den gleichen Preis einen Teil ihrer Privatsphäre aufzugeben (WTA). Diese Bewertungen sind unter anderem von der Verwendung der Daten und dem Vertrauen der Verbraucher*innen in die Datenverarbeiter abhängig.

– Nach dem WTA-Ansatz geben Verbraucher*innen den Preis an, für den sie bereit sind, ihre persönlichen Daten zu verkaufen oder Nutzungsrechte daran einzuräumen. Danach ergeben sich Preise von 15 bis 100 Euro für bestimmte Datensätze. Das sind in Ermangelung breitenwirksamer Angebote für den „Datenverkauf“ aber reine Laborwerte und ohne jede Validierung am Markt. Klar ist allerdings, dass die Verbraucher den Wert ihrer Daten deutlich überschätzen, wie verschiedene Studien zeigen. Im Rahmen einer regelmäßig durchgeführten Studie der TU Darmstadt liegen die Schätzungen der Teilnehmer regelmäßig um das drei- bis vierfache über den gemittelten Gewinnen pro Nutzer auf den entsprechenden Plattformen.
– Kostenpflichtige Services, die die Privatsphäre ihrer Nutzer*innen berücksichtigen, bilden ein Gegenmodell zu Gratis-Angeboten, die persönliche Daten kommerziell nutzen. Wie hoch liegt die WTP für solche kostenpflichtigen Services? Die Antwort auf diese Frage hängt von den jeweiligen Daten ab, die geschützt werden sollen. Verbraucher*innen sind regelmäßig bereit, für den Schutz besonders sensibler persönlicher Daten niedrige einstellige Eurobeträge aufzubringen. Die vergleichsweise geringe Inanspruchnahme von entgeltlichen Dienstleistungen ohne Datenübertragung (über das zur Vertragsabwicklung Notwendige hinaus) und die eher geringe Zahlungsbereitschaft lassen jedenfalls den Schluss zu, dass es nicht im Sinne der Mehrheit der Verbraucher wäre, für digitale Leistungen stets einen Preis in Geld zu bezahlen (und im Gegenzug Daten stets vergütet zu bekommen).

Eine weitere Möglichkeit, den Wert der persönlichen Daten aus Sicht der Verbraucher*innen zu veranschaulichen, ist die Bemessung des Schadens im Falle einer unerwünschten Offenlegung der persönlichen Daten und anhand der materiellen (Preisnachteile durch dynamic pricing bei der Weiterleitung z. B. von geografischen Daten, negatives Kreditrating) und nicht-materiellen Auswirkungen (z. B. Imageschaden). Grundsätzlich sollten diese Risiken allerdings in den oben genannten Schätzungen „eingepreist“ sein.

1.3.3 Position der vbw

Der Wert von Daten muss besser messbar werden. Dazu bedarf es intensiverer Forschung zur Methodik der Bewertung, auch speziell für den europäischen und deutschen Markt. Ansätze dazu verfolgt beispielsweise das Fraunhofer-Institut für Software- und Systemtechnik (ISST). Bestehende Erkenntnisse aus öffentlich geförderter Forschung müssen fortlaufend zusammengeführt werden. Die Öffentlichkeit muss über den Stand der Forschung transparent und verständlich informiert werden, gleichzeitig aber auch über die anderen Faktoren, die Daten überhaupt erst wertvoll machen.

Einstweilen kann Unternehmen nur geraten werden, den Wert anhand der verschiedenen skizzierten Verfahren zu ermitteln und gegebenenfalls zu kombinieren, auch unter Berücksichtigung der Zielgruppe im konkreten Anwendungsfall. Ein genereller Regulierungsbedarf besteht nicht (siehe oben 1.3.1).

1.3.4 Daten als Kapital und als Asset: Bilanzielle Fragen

Nach geltender Rechtslage werden Kundendaten nur dann bilanziert, wenn das Unternehmen für ihren Erwerb bezahlt hat (§ 246 HGB). Das ist jedenfalls bei einem Kauf der Daten im Einzelabschluss sowie von Unternehmensbereichen und der Übernahme ganzer Unternehmen im Konzernabschluss der Fall. Wie der Marktwert dieser Daten zu beziffern ist, wird nicht geregelt. Das Einschätzen des für die Bilanzierung maßgeblichen Werts ist schwierig, da sehr unterschiedliche Nutzungsmöglichkeiten denkbar sind beziehungsweise sich erst durch die Kombination mit weiteren Datensätzen ergeben und sich der Wert schnell ändern kann.

Selbst geschaffene immaterielle Vermögenswerte wie Kundenlisten, Informationen über Kundenpräferenzen oder Ähnliches unterliegen dagegen gemäß § 248 Absatz 2 HGB einem Bilanzierungsverbot. In die Bilanz können dann nur die Zahlungen für die Anschaffung der Software eingestellt werden, mit deren Hilfe die Daten erhoben wurden. Mit dem zunehmenden Einfluss internationaler Rechnungslegungsstandards (insbesondere der International Accounting Standards, IAS) auf deutsche Unternehmen rückt die Bilanzierung immaterieller Vermögenswerte aber immer stärker in den Vordergrund. Gleichzeitig wächst die Bedeutung von Daten für den Geschäftserfolg.

Die Interessenslage ist nicht einheitlich:
– Auf der einen Seite können Unternehmen ein Interesse daran haben, Abschreibungen zu vermeiden, um höhere Gewinne ausweisen zu können. Dann ist es vorteilhaft, Datenbestände nicht oder nur mit einem geringen Wert zu bilanzieren: Nach dem internationalen Rechnungslegungsstandard IFRS wird die Differenz zwischen Kaufpreis und beim Unternehmenskauf bilanzierten Vermögenswerten (Goodwill, Firmenwert) nicht abgeschrieben. Zusätzlich kann es attraktiv sein, keine zu große Transparenz über das eigene digitale Geschäftsmodell herzustellen.

– Auf der anderen Seite können Unternehmen ein Interesse daran haben, ihren maßgeblich auf Daten basierenden Unternehmenswert zu steigern beziehungsweise realistisch abzubilden, namentlich Start-ups, die eine Finanzierung benötigen.

Position der vbw

Jeder Regulierungsansatz muss sowohl den unterschiedlichen Interessen als auch den skizzierten Schwierigkeiten bei der Werterfassung angemessen Rechnung tragen. Die Diskussion muss aber jetzt geführt werden, sorgfältig und unter Einbeziehung aller Beteiligten. Zu klären ist dabei auch, ob Algorithmen einbezogen werden, die die Daten oft überhaupt erst wertvoll machen. Grundsätzlich sollte das Recht die wirtschaftliche Realität abbilden.

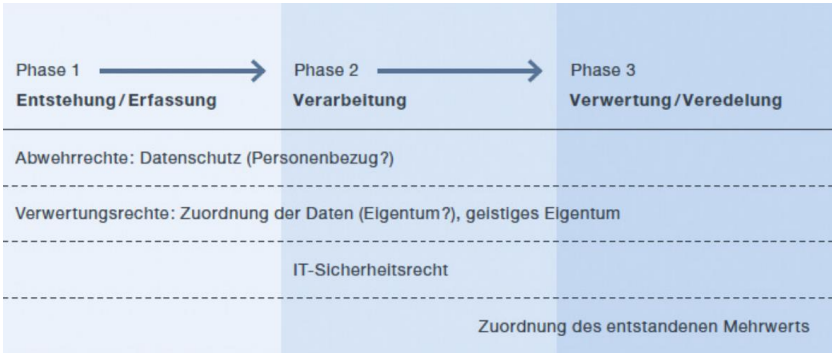
1.4 Rechtliche Einordnung und Zuordnung von Daten

Angesichts der großen und weiter wachsenden Bedeutung von Daten einerseits und der entsprechenden Interessen der verschiedenen Beteiligten andererseits sind Abwehr- und Verwertungsrechte zu klären sowie die Frage der Zuordnung eines entstehenden Mehrwerts zu beantworten.

1.4.1 Grundsätzliche Fragen

In einer vbw Studie hat Professor Dirk Heckmann dazu drei Phasen unterschieden.

3-Phasen-Modell



vbw/Heckmann, 2016

Die *erste Phase* der Datenentstehung und Datenerfassung stellt zumeist den Beginn der Wertschöpfungskette dar. In rechtlicher Hinsicht liegt hier die wesentliche Weichenstellung im Datenschutzrecht. Schon in der ersten Phase ist ferner die Frage aufzuwerfen, inwieweit die Akteure, ohne die die Datenbestände erst gar nicht erzeugt werden könnten,

an einem späteren Gewinn aus der Verarbeitung und Veredelung jener Daten zu beteiligen sind.

Das Datenschutzrecht bleibt in der *zweiten Phase* relevant, sofern ein Personenbezug (weiterhin) besteht. Hier stellt sich dann insbesondere die Frage, ob sich die Speicherung und Verarbeitung in dem durch die konkrete Rechtfertigung gesteckten Rahmen bewegt (Stichwort Zweckbindung). Zusätzlich müssen hier insbesondere Fragen des IT-Sicherheitsrechts beachtet werden. Das Urheberrecht kann relevant werden, wenn es um den Schutz von Datenbanken geht.

In der *dritten Phase* geht es schließlich entscheidend darum, den entstehenden Mehrwert – insbesondere über vertragliche Gestaltungen – den am Prozess Beteiligten zuzuordnen.

Am Beispiel der beim automatisierten und vernetzten Fahren entstehenden Daten kann illustriert werden, wie viele Beteiligte Interesse daran haben können. Die Aufzählung ist sicher nicht abschließend, und die Interessen sind sehr unterschiedlich gelagert; sie reichen vom Schutz der Privatsphäre über die Gewährleistung von Verkehrssicherheit bis hin zur Entwicklung neuer Geschäftsmodelle.

Daten und Interessenten am Beispiel Automobil

vbw, 2018

1.4.2 Regulierungsansätze

1.4.2.1 Dateneigentum, eigentumsähnliche Rechte

Eigentum an unkörperlichen Gegenständen ist nach geltendem Recht nicht möglich, eigentumsähnliche sonstige Rechte sind es ebenso wenig. Vielfach wurde gefordert, hier regulierend einzugreifen und ein neues ausschließliches Recht an Daten zu

schaffen. Vorteil wäre insbesondere die eindeutige, gegenüber jedermann wirkende Rechtsposition.

Position der vbw

Eigentumsähnliche Rechte an Daten sind abzulehnen. Sie würden anstelle eines Anreizes für ein stärkeres Wachstum der verfügbaren Datenmenge – das nachweislich auch ohne Dateneigentum exponentiell ist – eine künstliche Datenverknappung bewirken und so die Aussagekraft von Datenanalysen sowie die Nutzungspotenziale insgesamt verschlechtern. Letztlich würden davon ganz überwiegend diejenigen profitieren, die heute bereits in einer beherrschenden Stellung sind. Ein Dateneigentum oder ähnliche Ausschließlichkeitsrechte ließen sich zudem schlecht mit den Eigenschaften digitaler Güter vereinbaren: Grundsätzlich verbrauchen sich Daten nicht und können mit mehrfacher Nutzung sogar wertvoller werden, mehrere KI-Anwendungen können (auch parallel) auf demselben Datenbestand aufbauen. Über das Datenschutzrecht hinaus sollten also keine Ausschließlichkeitsrechte geschaffen werden, wenn man KI und Big Data nicht auf zivilrechtlichem Wege jede Innovationskraft nehmen will.

1.4.2.2 Zugangsrechte zu Daten

Nachdem es keine eigentumsähnliche Zuordnung gibt, können Daten grundsätzlich von allen Akteuren genutzt werden, die (faktisch) Zugang zu ihnen haben, wenn keine Zugriffs- oder Nutzungsbeschränkungen eingreifen. Solche Beschränkungen können sich insbesondere aus Straf-, Wettbewerbs- oder Datenschutzrecht ergeben. Auch vertragliche Regelungen können die Datennutzung beschränken.

Beispiel: Daten als Geschäftsgeheimnisse

Mit der EU-Geschäftsgeheimnisrichtlinie (umgesetzt durch das Gesetz zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung vom 18.04.2019) wurde ein einheitliches Mindestniveau für den Schutz von Know-how und vertraulichen Geschäftsinformationen geschaffen. Geschäftsgeheimnisse sind danach Informationen, auf die die folgenden Kriterien zutreffen:

- sie sind in dem Sinne geheim, als dass sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile allgemein bekannt oder ohne weiteres zugänglich sind,
- sie sind von kommerziellem Wert, weil sie geheim sind,
- sie unterliegen angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt und ein berechtigtes Interesse an der Geheimhaltung hat.

Dabei kommt es nicht auf einen objektiven Wert der Informationen an.

Nach Art. 4 Abs. 2 der Richtlinie beziehungsweise § 4 Abs. 1 GeschGehG liegt ein rechtswidriger Erwerb eines Geschäftsgeheimnisses vor, wenn elektronische Daten unbefugt kopiert werden, die der rechtmäßigen Kontrolle durch den Inhaber des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt. Damit trifft die Richtlinie auch eine Aussage über die Zuordnung der von ihr erfassten Daten. Zugleich wird klar, dass Maschinendaten grundsätzlich Informationen enthalten können, die als Geschäftsgeheimnis schutzfähig sind. Das kann bei Vorliegen der o.g. Kriterien etwa dann der Fall sein, wenn sie Rückschlüsse auf interne Produktionsabläufe, Auslastungsgrade oder Qualität der produzierten Ware zulassen.

Über die rechtlichen Aspekte hinaus gibt es eine faktische Wirkung hinsichtlich der Zugangsmöglichkeiten zu Sachdaten: Der Eigentümer der Sache hat in der Regel auch den Zugriff auf die von ihr erzeugten und erhobenen Daten, beziehungsweise die Möglichkeit, andere davon auszuschließen. Dies ist im Sinne eines Annexes zum Sacheigentum grundsätzlich hinzunehmen, zumal sich anderenfalls unter anderem Abgrenzungsschwierigkeiten im Hinblick auf Betriebs- und Geschäftsgeheimnisse stellen, während im privaten Bereich zumindest meistens die theoretische Möglichkeit einer Personenbeziehbarkeit der Daten besteht.

Nachdem zunächst vielfach ein „Dateneigentum“ diskutiert wurde (siehe oben), hat sich inzwischen der Trend komplett gewandelt, und es sollen nun nach verbreiteter Auffassung Daten immer allen „gehören“. Der Zugang zu einer bestimmten Art von Daten kann notwendig sein, um in einen Markt einzutreten oder datengetriebene Innovationen zu entwickeln. Es wird daher argumentiert, dass ein Zugangsrecht notwendig sei, um den Wettbewerb und eine gesamtwirtschaftlich effiziente Nutzung der Daten zu ermöglichen, und diskriminierende Zugangsbeschränkungen zu vermeiden.

Position der vbw

Dieses andere Extrem ist allerdings nicht minder riskant für eine zukunftsfähige Ausrichtung des Standorts und ebenso abzulehnen. Es ist entscheidend, Anreize für die Produktion werthaltiger Daten und Informationen zu erhalten. Die dafür von den entsprechenden Unternehmen eingesetzten Investitionen gilt es daher zu schützen und die faktische Kontrolle über die generierten Werte zu erhalten. Hinzu kommt, dass völlig unklar wäre, wer eigentlich von einem breiten Zugangsrecht profitieren würde: Sicher nicht der einzelne Nutzer, möglicherweise aber internationale Wettbewerber.

1.4.2.3 Für die Zuordnung von Daten auf vertragliche Lösungen setzen

Während eine Regulierung in diesem Bereich – mit unterschiedlichen Stoßrichtungen – seit Jahren diskutiert wird, lässt sich nach wie vor kein dringender Bedarf feststellen, dafür aber gravierende Schwächen der vorgeschlagenen Regelungsansätze. Es gilt daher, auf freiwillige vertragliche Regelungen (Zuordnungs- und Nutzungsvereinbarungen) zu Möglichkeiten und Grenzen der Datenverwertung, Gegenleistung und möglichen Haftungsfolgen zu setzen. Ein großer Vorteil liegt in der Flexibilität dieser Lösungen, die in den einzelnen Branchen auch ganz unterschiedlich ausfallen können. Für das oben skizzierte Beispiel der bei der Nutzung eines Pkw anfallenden Daten gibt es eine solche Branchenlösung bereits. Sie kann auch für andere Bereiche Vorbild sein.

Erst dann, wenn beispielsweise ein strukturelles Marktversagen in einzelnen Segmenten beobachtet werden könnte, müssten maßgeschneiderte legislative Lösungen entwickelt werden. Einstweilen bietet sowohl auf europäischer als auch auf deutscher Ebene das Wettbewerbs- und Kartellrecht ausreichende Instrumente für ein Einschreiten gegen etwaige „Datenmonopole“.

Hinweise für die Vertragsgestaltung

Auch vertragliche Lösungen setzen allerdings eine differenzierte und sorgfältige Herangehensweise durch die Beteiligten voraus, zumal es gegenwärtig keine gefestigte Rechtsprechung gibt, und Regelungen aus verschiedenen Bereichen zur Anwendung kommen. Zu beachten sind beispielsweise etwaige weitere Rechtspositionen an (einzelnen) Daten, die sich unter anderem aus den Anforderungen des Urheber- und Geheimnisschutzes ergeben können.

Angesichts der Relativität der Schuldverhältnisse – also ihrer Wirkung nur zwischen den Parteien des jeweiligen Vertragsverhältnisses, nicht gegenüber Dritten, die am Vertrag nicht beteiligt sind – kann es erforderlich sein, seine Vertragspartner zu verpflichten, bei allen weiteren Verträgen in der Kette bestimmte Rechte (beispielsweise Nutzungsbeschränkungen) vertraglich zu regeln, um einen Regress zu ermöglichen.

Wichtig ist auch eine Regelung zur Zuordnung von entstehenden Immaterialgüterrechten- beziehungsweise allgemein der aus der Nutzung der Daten generierten Wertschöpfung. Informationen über entsprechende Regelungsmöglichkeiten und Vertragsmuster wären hier eine sehr sinnvolle Hilfestellung seitens staatlicher Stellen.

Gerade Start-ups könnten stark davon profitieren, wenn sie praktische Unterstützung bei der rechtskonformen Gestaltung ihrer Geschäftsmodelle erhalten. Letztlich ist das im Vergleich zu den vielfach geforderten Experimentierräumen sowohl der rechtssicherere (die DSGVO etwa sieht keine Abweichungen vor) als auch der langfristig tragfähigere Weg.

1.5 Zuordnung des Mehrwerts

Vielfach sind Verbraucher der Ansicht, nicht ausreichend für die Preisgabe ihrer Daten kompensiert zu werden. Tatsächlich kann der Bürger mit seinen Daten in monetärer Hinsicht nicht viel anfangen. Eine Ausnahme sind insoweit vor allem individualisierte Versicherungstarife (am bekanntesten wohl als *pay as you drive*-Tarif in der Kfz-Versicherung). Hier kann der Verbraucher über die Freigabe seiner Daten gegen einen spürbaren Preisnachlass bei risikoadversem Verhalten entscheiden. Im Hinblick auf sonstige persönliche Daten (etwa Bewegungsdaten, Einkaufsverhalten) gibt es nur vereinzelt Geschäftsmodelle, die explizit auf einen „Verkauf“ setzen, sie werden aber in Deutschland von der Bevölkerung mehrheitlich abgelehnt und entsprechen von den Erlösen her sowieso nicht den verbreiteten Erwartungen (siehe oben 1.3.2). Auch die Unternehmen als potenzielle Kunden solcher Lösungen setzen lieber auf Systeme, die ihnen eine datenschutzkonforme Verwertung von Nutzerdaten ermöglichen.

Wo die „Selbstvermarktung“ nur in begrenztem Umfang klappt, ein Gefühl der Ungerechtigkeit aber bleibt, verlagern sich die Forderungen je nach politischer Ausrichtung hin zur Umverteilung (Teilhabe an Wertschöpfung, z. B. über steuerliche Lösungen), oder Zerschlagung der „Datenmonopole“ beziehungsweise der über sie verfügenden Unternehmen.

Die Akzeptanz datenbasierter Geschäftsmodelle ist in der Bevölkerung relativ niedrig, was in starkem Kontrast zum Maß der Nutzung gerade im privaten Bereich steht. Eine stabile Mehrheit von knapp unter 50 Prozent sagt, sie finde es nicht in Ordnung, dass „kostenlose“ Internetdienste wie Facebook oder Google Geld mit Nutzerdaten verdienen, aber sie müssten sich damit abfinden. Erstaunlicherweise steigt der Anteil derjenigen, die über diese Frage noch nie nachgedacht haben, seit Jahren an: Von 3,6 Prozent im Jahr 2012 auf 13,2 Prozent in der jüngsten Befragung von 2017. Auf der einen Seite spricht das nicht für den Erfolg der bisherigen Bemühungen zur Steigerung der Medienkompetenz, auf der anderen Seite mag das Ausdruck einer wachsenden Normalität des Geschäftsmodells gerade in der jüngeren Zielgruppen sein.

Allerdings besteht kaum ein Zweifel daran, dass Nutzern heute bewusst ist, dass ihre Daten beispielsweise in sozialen Netzwerken für wirtschaftliche Zwecke genutzt werden. Etliche Nutzer gehen sogar – ohne belastbare Grundlage – von noch einer viel weitgehenderen Verwendung ihrer Daten aus, etwa dem Einsatz privater Aufnahmen für Werbezwecke. Richtigerweise muss also daraus abgeleitet werden, dass die bloße theoretische Präferenz noch keinen Regulierungsbedarf begründen kann. Folgerichtig sind dagegen die Ansätze von Privacy by Design: Die Grundeinstellung ist auf Schutz der Privatsphäre gestellt, der Nutzer kann auf Grundlage bewusster Entscheidungen mehr preisgeben. Mehr als ein solches Nudging ist kaum zu rechtfertigen, da es auch zum Recht auf informationelle Selbstbestimmung gehört, mehr von sich preiszugeben, als es vielleicht die Mehrheit für vernünftig hielte.

Position der vbw

Es gibt gegenwärtig keinen Anlass, in die Zuordnung des Mehrwerts regulierend einzugreifen. Umverteilungsforderungen und allgemeine Zugangsrechte zu Daten blenden nicht nur den tatsächlichen monetären Wert aus und die eigentliche Leistung des Anbieters des datengetriebenen Geschäftsmodells, sie spiegeln nicht einmal den subjektiven Wert der Daten wider, wie er im Umgang des Einzelnen damit zum Ausdruck kommt.

Hier müssen zum einen die Unternehmen schon im eigenen Interesse an einer besseren und transparenteren Kommunikation arbeiten. Daneben sind aber auch staatliche Einrichtungen als „neutrale Instanzen“ gefordert, realistische Erwartungen zu wecken. Staat und Politik müssen Zusammenhänge und die Auswirkungen grundlegender Weichenstellungen frühzeitig und so transparent und verständlich wie möglich kommunizieren. Nur, wenn ökonomische Grundlagen bekannt sind – und dazu gehören in einer zunehmend digitalen Wirtschaft auch Grundzüge der Datenökonomie – ist eine sachliche Auseinandersetzung auch in der politischen Debatte möglich, die nicht alleine um Fragen der (Verteilungs-)Gerechtigkeit kreist.

1.6 Spezielle Zuordnungsfragen

1.6.1 Steuerrechtliche Aspekte von Datentransaktionen

Bisher unterliegen die eigentlichen Datentransaktionen weit überwiegend nicht direkt einer Besteuerung, da als Gegenleistung entweder Dienstleistungen unentgeltlich zur Verfügung gestellt werden (z. B. Nutzung einer Suchmaschine, einer App) oder Preisnachlässe gewährt werden (Treueprogramme, günstigere Versicherungstarife). Der Vorgang des Datensammelns ist in der Regel nicht erfasst. Je nach vertragsrechtlicher Einordnung des der Datensammlung zugrunde liegenden Geschäftsmodells (siehe oben) weist der Unternehmer dann beispielsweise für den entgeltlichen Teil der Leistung Umsatzsteuer aus; soweit es diesen aber nicht gibt, fehlt es jedenfalls für Daten an einer geeigneten Bemessungsgrundlage. Zwar wäre auch ein reines Tauschgeschäft grundsätzlich umsatzsteuerpflichtig, der dann maßgebliche Wert der getauschten Güter (§ 10 Abs 2 Satz 2 und Satz 3 UstG) ist aber nicht praxisgerecht zu bestimmen. Für die Schätzung von Centbeträgen (für die Datenüberlassung) ist das auch kaum zu rechtfertigen. Der Nutzer gibt letztlich nicht einmal eine vermögensrechtliche Position auf, weil er dieselben Daten parallel und ohne qualitative Einschränkung beliebig vielen weiteren Unternehmen zur Verfügung stellen kann. Oft ist zudem die Bereitstellung von Daten schon eine notwendige Voraussetzung für die Inanspruchnahme der digitalen Leistung, etwa bei Standortdaten für die Navigation.

Die Daten sind regelmäßig erst nach der Sammlung und Aufbereitung durch den Anbieter der kostenlosen Angebote handelbar und zählen dann im Falle einer Veräußerung (zum Beispiel in Form von Nutzerprofilen) oder Verwertung zu den besteuerten Umsätzen.

Das hat bereits zu Überlegungen geführt, Steuern sozusagen als Instrument für die Bepreisung von Daten einzusetzen, insbesondere aufgrund einer empfundenen Ungerechtigkeit der „kostenlosen“ Umverteilung. Der Weg könnte darin liegen, die Datenübertragung kostenpflichtig zu machen, so dass jedenfalls Umsatzsteuer anfiele und der Kunde eine Vergütung erhielte.

Position der vbw

Dagegen spricht unter anderem, dass – wie bereits erwähnt – der Kunde bereits heute eine Gegenleistung erhält, an der er offenbar auch interessiert ist, und dass er bei personenbezogenen Daten seine Einwilligung jederzeit widerrufen kann. Es wäre auch nicht nachvollziehbar, warum ausgerechnet ein Gut, das durch seine Nicht-Rivalität gekennzeichnet ist, immer zu bepreisen wäre, von den oben skizzierten Schwierigkeiten einer Preisfestsetzung ganz abgesehen.

Neben den rein praktischen Schwierigkeiten wäre es auch nicht sachgerecht, Daten in diesem Kontext anders zu behandeln als bei der Aufnahme in die Kundenkartei eines stationären Händlers. Daten werden seit Jahrzehnten auch von Unternehmen mit (bislang) nicht digitalen Geschäftsmodellen erhoben und genutzt, ohne dass die Verwendung als solche etwa zu Werbezwecken der Umsatzsteuer unterliegen würde. Was damit erwirtschaftet wird, unterliegt – im digitalen wie im analogen Geschäft – wiederum der Unternehmensbesteuerung beziehungsweise (zum Beispiel bei der Platzierung von Werbung) der Umsatzsteuer. Der Mehrwert, den die Personalisierung der Werbung mit sich bringt, wird schon durch die höhere Bemessungsgrundlage der Werbeleistung gegenüber dem Werbetreibenden von der Umsatzsteuer erfasst.

Würde jede Preisgabe von personenbezogenen Daten/Einwilligung in die Nutzung als Tätigkeit zur Erzielung wirtschaftlicher Vorteile eingestuft, dann verschwimmen schließlich die Grenzen zwischen Unternehmen und Verbrauchern zunehmend angesichts der wachsenden (parallelen) Inanspruchnahme solcher Angebote. Die Rolle als Verbraucher ändert sich aber nicht durch die spezielle Form der Gegenleistung.

Insgesamt lässt sich festhalten, dass gegenwärtig kein zwingender Handlungsbedarf im Steuerrecht besteht.

1.6.2 Daten in der Insolvenz

Gegenstand einer Insolvenzmasse können Daten nur sein, wenn sie zum Zeitpunkt der Eröffnung des Insolvenzverfahrens zum Vermögen des Schuldners gerechnet werden. Grundsätzlich haben Daten einen wirtschaftlichen Wert, der Bestandteil des Schuldnervermögens ist, wenn das Unternehmen sie in Ausübung seiner unternehmerischen Tätigkeit erzeugt beziehungsweise „gesammelt“ hat (siehe oben).

Schwierigkeiten bei der Zuordnung können sich insbesondere dann ergeben, wenn die Daten nicht beim Schuldner gespeichert sind, sondern beispielsweise in einer Cloud oder bei einem externen Dienstleister – und zwar sowohl in der Insolvenz des Cloud-Betreibers als auch in der Insolvenz des Unternehmens, das sie dorthin ausgelagert hat. Das OLG Düsseldorf hat in einer ähnlichen Konstellation (Insolvenz eines für die Verwaltung eines Unternehmens-Newsletters beauftragten Dienstleisters) einen Aussonderungsanspruch aufgrund eines Herausgabeanspruchs aus dem zugrundeliegenden Geschäftsbesorgungsvertrag bejaht. Der Insolvenzgläubiger konnte damit erfolgreich die Herausgabe, der zuvor zur Verfügung gestellten Abonnentendaten, verlangen.

Position der vbw

Eine Übertragung dieser Wertung jedenfalls auf die Insolvenz des Cloud-Anbieters erscheint möglich; angesichts der wachsenden Bedeutung von Cloud-Lösungen wäre eine Klarstellung aber durchaus wünschenswert.

Weiterführende Informationen

- *TechCheck 2019. Technologien für den Menschen.,* Zukunftsrat der Bayerischen Wirtschaft
- Studie *Neue Wertschöpfung durch Digitalisierung*, vbw 2017
- *Neue Wertschöpfung durch Digitalisierung. Analyse und Handlungsempfehlungen.*, Zukunftsrat der Bayerischen Wirtschaft, vbw 2017
- Studie *Daten als Wirtschaftsgut*, Prof. Dirk Heckmann, vbw 2018
- Studie *Big Data im Freistaat Bayern. Chancen und Herausforderungen.* Prognos/Heckmann, vbw 2016
- B*ig Data im Freistaat Bayern – Analyse und Handlungsempfehlungen*., Zukunftsrat der Bayerischen Wirtschaft, 2016
- Positionspapier *Künstliche Intelligenz*, vbw 2019
- Studie *Digitalisierung der bayerischen Wirtschaft*, IW 2019
- Positionspapier *Automatisiertes Fahren – Datenschutz und Datensicherheit*, vbw 2018

2 Daten als Vertragsgegenstand

Daten sind gleichermaßen Ware und Währung

So bedeutend Daten im Wirtschaftsleben bereits sind, so komplex und teilweise noch nicht abschließend geklärt ist die rechtliche Einordnung der verschiedenen Transaktionen.

2.1 Datenzentrierte Geschäftsmodelle

In der gesamten Wirtschaft vollzieht sich seit einigen Jahren eine Veränderung in den Leistungsbeziehungen, die maßgeblich durch die sich stetig verbessernden Möglichkeiten der Datenanalyse getrieben wird.

Im Ergebnis wandelt sich der klassische Austausch Produkt gegen Geld zunehmend zu hybriden Wertschöpfungsbeziehungen, in denen ergänzende Serviceleistungen hinzukommen. Mit zunehmendem Kundenkontakt werden mehr Informationen über die tatsächliche Nutzung der Sache, Anforderungen des Kunden und gegebenenfalls auch über ihren Wert für den Abnehmer übermittelt. Teilweise steht am Ende des Wandels eine Transformation des (Produktions-)Geschäfts in eine Dienstleistungsbeziehung („Lösungsanbieter“). Umgekehrt kombinieren Dienstleister ihr Leistungsspektrum mit – auf die aus der Datenanalyse bekannten Kundenanforderungen – maßgeschneiderten Produkten, zu beobachten beispielsweise bei Amazon.

Unter datenzentrierten Geschäftsmodellen sind insbesondere solche zu verstehen, bei dem Daten eine Schlüsselrolle für Wertschöpfung und/oder Wertangebot (siehe unten) des Unternehmens spielen und auch die Schlüsselaktivitäten datenorientiert sind (beispielsweise Datengenerierung, Datenverarbeitung, Datenanalyse oder Visualisierung). Es geht also um die Generierung von Produkten und Dienstleistungen, die sich direkt aus den Prozessdaten des Unternehmens, seiner Kunden oder externen Umwelt speisen. Dazu gehören auch hybride Dienstleistungen, wie eine datengestützte, vollautomatisierte Wartung industrieller Anlagen.

Auf Basis der ausgetauschten Daten wird es möglich, neue Angebote für die Kunden zu entwickeln. Die Grenzkosten eines zusätzlichen Nutzers gehen gegen Null, jedenfalls solange die Anwendungen als solche nicht sicherheitskritisch sind oder – zum Beispiel aufgrund erheblicher Rechenleistung – spürbaren Aufwand erzeugen. Über das Internet kann ein riesiger Markt in kürzester Zeit erreicht werden. Die Anbieter stehen dabei in direktem Austausch mit dem Endverbraucher und haben unmittelbaren Zugriff auf seine Daten. Die entstehenden softwarebasierten Ökosysteme binden die Nutzer und eine Vielzahl an Firmen mit neuen Geschäftsmodellen ein. Umgekehrt können Plattformen dazu führen, dass – auch branchenfremde – Dritte die Kundenschnittstelle besetzen und sich die Wertschöpfung verschiebt.

Die Entwicklung datenbasierter Geschäftsmodelle kann auf verschiedene Weise auf einzelne oder alle Ebenen des bisherigen Geschäftsmodells einwirken.

Veränderungen des Geschäftsmodells durch Datennutzung (Grundtypen)

Quelle: eigene Darstellung nach Geschäftsmodelle 4.0, Baukasten zur Entwicklung datenbasierter Geschäftsmodelle

Näheres hierzu und Hinweise für die entsprechenden Handlungsoptionen der Unternehmen enthalten die Handlungsempfehlungen des Zukunftsrats der Bayerischen Wirtschaft *TechCheck 2019. Technologien für den Menschen*.

So vielfältig wie die Geschäftsmodelle sind auch die möglichen Erlösmodelle; in der Praxis haben sie eine sehr unterschiedliche Verbreitung gefunden. Einige davon basieren auf einem mehrseitigen Verhältnis: Der eigentliche Nutzer des Angebots zahlt nicht für die Leistung des Anbieters, sondern ein Dritter (Unternehmen) für dessen Daten beziehungsweise die daraus gewonnenen Einsichten.

Erlösmodelle für digitale Angebote

– Abonnement (periodisches Entgelt)

– Nutzungsgebühr (Abrechnung nach Nutzungshäufigkeit oder beispielsweise der Anzahl bearbeiteter Datensätze)
– Kostenlose Basisversion mit optionalen – kostenpflichtigen – Zusatzleistungen (sogenanntes Freemium-Modell, wie es vielfach bei Gaming- oder Anwendungssoftware eingesetzt wird)
– Provision/Beteiligung an Erfolg des Services beim Kunden
– Werbefinanzierung
– Kauf und Verkauf von Daten
– Weiterverarbeitung der Daten zu neuen Services

Die drei letztgenannten sind mehrseitige Modelle. Insbesondere die Werbefinanzierung hat sich als sehr erfolgreich erwiesen und extrem weite Verbreitung bei B2C-Angeboten gefunden. Sie trägt allerdings auch zu der Illusion des privaten Nutzers bei, digitale Angebote seien grundsätzlich kostenlos (siehe näher oben, 1.5).

Dabei können datenbasierte Geschäftsmodelle und die aus der Datennutzung gewonnenen Ergebnisse auf unterschiedliche Art in die Systeme der Kunden eingebunden werden. In Betracht kommen beispielsweise
– Software as a Service (Cloud-Lösung): Der Auftragnehmer hostet und betreibt die Software, der Service wird via Internet zur Verfügung gestellt.
– On-Premise: Der Kunde betreibt die Software auf eigener Hardware, gegebenenfalls auch offline im eigenen Rechenzentrum.
– Integration in kundeneigene Software.

2.2 Vertragsrechtliche Einordnung, Daten als Leistung

Grundsätzlich gilt im deutschen Vertragsrecht das Prinzip der Vertragsfreiheit. Dieses beinhaltet zum einen das Recht, frei zu bestimmen, ob und mit wem ein Vertrag abgeschlossen werden kann (Abschlussfreiheit) und zum anderen das Recht, den Inhalt des Vertrags frei zu bestimmen (Gestaltungsfreiheit). Vertragliche Regelungen über Daten-Transaktionen sind deshalb möglich; für die Durchführung des Vertrags ist relevant, ob er einem der gesetzlich vorgesehenen Vertragstypen (Kaufvertrag, Tausch etc.) zugeordnet werden kann. Das hängt maßgeblich von den Gegebenheiten im Einzelfall ab.

Daten können dabei sowohl Leistungsgegenstand als auch Gegenleistung sein. Bei den datenbasierten Geschäftsmodellen im engeren Sinne sind unter anderem folgende Grundkonstellationen verbreitet:
– Datenverarbeitung beziehungsweise -analyse als Vertragsgegenstand (Beispiel Suchmaschinen)
– Datenverarbeitende Software als Vertragsgegenstand (Beispiel KI-Tools für die Automatisierung von unternehmensinternen Vorgängen)
– Digitale Angebote wie Apps oder Medieninhalte mit (Nutzer-)Daten als Gegenleistung

Mögliche Vertragstypen

- Der klassische Kaufvertrag (Sachkauf, §§ 433 ff. BGB) kommt nicht in Betracht, wenn die Daten nicht in einer Sache „verkörpert“ sind.
- Es kann sich um einen Kauf von Rechten und sonstigen Gegenständen (§ 453 BGB) handeln, auf den das Kaufvertragsrecht anwendbar ist, wenn die Datenüberlassung als dauerhafte/endgültige vorgesehen ist.
- Ein Werklieferungsvertrag (§ 650 BGB) wird nur in den Fällen passen, in denen die Daten erst noch erzeugt werden sollen.
- Der Werkvertrag (§ 631 BGB) kann dort passen, wo es um das Sortieren/Herstellen von bestimmten Datenpaketen geht, oder die Daten erst noch erhoben werden sollen.
- Ob ein Dienstvertrag (§ 611 BGB) oder eine Geschäftsbesorgung (§ 675 BGB) passt, hängt davon ab, ob ein konkreter Erfolg (z. B. die Nutzbarkeit der Daten im Hinblick auf die Datenschutzkonformität) geschuldet sein soll. Regelmäßig wird das gewollt sein und ein Dienstvertrag daher ausscheiden; denkbar sind aber verschiedene Konstellationen der Datenverarbeitung.
- Miete (§ 535 BGB) wird regelmäßig wegen der fehlenden Sacheigenschaft der Daten ausscheiden. Denkbar sind mietvertragliche Konstruktionen dagegen dort, wo es beispielsweise vorrangig um die Speicherung der Daten (z. B. in einer Cloud) geht.
- Für Dauerschuldverhältnisse beziehungsweise auf Zeit angelegte Leistungen kann dagegen die Pacht (§ 581 BGB) passen.

Oftmals werden typengemischte Verträge vorliegen, die danach beurteilt werden, wo ihr Schwerpunkt liegt; denkbar ist auch eine Einordnung als atypischer Vertrag. Damit finden auf die Leistungen die jeweils passenden vertragsrechtlichen Vorschriften Anwendung. Bei der Leistung des Unternehmers ist es das Kaufvertragsrecht (in entsprechender Anwendung), wenn es um die endgültige Überlassung des Leistungsgegenstands geht (z. B. eines E-Books), bei einer dauerhaften Bereitstellung einer Nutzungsmöglichkeit (z. B. einer Plattform, einer App) passen eher mietrechtliche Regelungen.

In der Praxis empfiehlt sich, das Gewollte möglichst genau zu regeln, um Auslegungsschwierigkeiten beziehungsweise der Zuordnung zu einem eigentlich nicht gewollten Vertragstyp mit den entsprechenden Rechtsfolgen vorzubeugen.

Für die Wirksamkeit eines Vertrags ist es erforderlich, die wesentlichen Vertragsinhalte festzulegen, also jedenfalls die gegenseitigen Hauptleistungspflichten. Die (gegebenenfalls inklusive Einwilligung) geschuldeten Daten müssen also hinreichend genau beschrieben werden. Gerade bei künftigen Datenerhebungen bei erneuter Nutzung des Angebots (z. B. über den Einsatz von Cookies) wird mindestens eine entsprechende Beschreibung des Vorgangs erforderlich sein. Geht es um personenbezogene Daten, muss zudem der Verarbeitungszweck festgelegt werden, weil das Datenschutzrecht insoweit durchschlägt.

Sonderfall Unternehmenstransaktionen

Der Kauf von Unternehmen (Asset Deal) beziehungsweise von Anteilen oder Beteiligungen (Share Deal) bringt in aller Regel auch die Übertragung von Datenbeständen mit sich, wobei es sich sowohl um Sachdaten als auch um personenbezogene Daten handeln kann. Beim Share Deal werden keine einzelnen Vermögenswerte übertragen, sondern Gesellschaftsanteile. Hier werfen auch personenbezogene Daten keine besonderen Schwierigkeiten auf, da die Veräußerung zunächst keine Auswirkungen auf die Rechtsverhältnisse zwischen dem Unternehmen und seinen Kundenbeziehungsweise Mitarbeitern hat. Der Asset Deal führt dagegen in der Regel zu einem Wechsel des Vertragspartners, so das datenschutzrechtliche Vorgaben zu beachten sind; im Hinblick auf Sachdaten muss schon im Rahmen der vorbereitenden Due Diligence geklärt werden, wie sich im Einzelnen die Rechtsverhältnisse daran ausgestalten, ob also Datenbestände beispielsweise einem vertraglichen Schutz unterliegen. Im Hinblick auf personenbezogene Daten sollte sich der Erwerber die rechtmäßige Erhebung nachweisen oder mindestens zusichern lassen.

Im B2C-Bereich kommen Daten als Leistungsgegenstand praktisch nur in der Konstellation vor, dass der Unternehmer Daten zur Verfügung stellt. Der Verkauf eigener Datensätze durch Verbraucher hat bislang keine praktische Bedeutung erlangt (siehe auch oben 1.5).

2.3 Daten als Gegenleistung

Während die oben skizzierte Einordnung immer relevant ist, stellen sich weitere Fragen, wenn die *Gegenleistung* nicht in einem Entgelt in Geld besteht, sondern in der Hingabe von Daten.

2.3.1 Datenschutzrechtliche Einwilligung

Bei personenbezogenen Daten stellt sich insbesondere die Frage, ob als Gegenleistung nur die Hingabe von Daten ist, oder (auch) die datenschutzrechtliche Einwilligung.

Anforderungen an das Einwilligungserfordernis nach der DSGVO

- Die Einwilligung als solche ist auch bei Daten als Gegenleistung nicht schon im Hinblick auf Art. 6 Abs. 1 b (zur Erfüllung eines Vertrags) entbehrlich, da dieser nur sicherstellen soll, dass der Vertragspartner zur Erfüllung überhaupt in der Lage ist, weil die Daten für die Vertragserfüllung etwa technisch erforderlich sind.
- Ein Verstoß gegen das Koppelungsverbot kann regelmäßig nicht angenommen werden. Art. 7 Abs. 4 DSGVO soll den Verbraucher vor Zwangslagen schützen, in die er geraten könnte, weil er auf eine Leistung angewiesen ist, beziehungsweise soll ihn davor

schützen, personenbezogene Daten preisgeben zu müssen, die nicht mit dem Austauschverhältnis im Zusammenhang stehen. Beides liegt in Standardfällen wie der Nutzung von Social Media etc. in der Regel nicht vor.

Nach wohl herrschender Ansicht ist es die Einwilligung, weil regelmäßig nur diese eine Rechtsgrundlage für die Datennutzung durch den Erwerber bereitstehe. Die Einwilligungserklärung ähnelt der Einräumung von Nutzungsrechten in einem Lizenzvertrag und könne nach den Vorschriften über Dauerschuldverhältnisse beurteilt werden.
Dagegen spricht allerdings unter anderem, dass nicht nur ein Anspruch auf Abgabe der Einwilligungserklärung bezweifelt wird (obwohl in dieser Konstellation Hauptleistungspflicht), sondern er in jedem Fall wegen des Persönlichkeitsrechts und der jederzeitigen Widerruflichkeit nicht rechtlich durchsetzbar wäre.

Position der vbw

Nach anderer – überzeugender – Ansicht ist die Einwilligungserklärung Wirksamkeitsvoraussetzung, die Hingabe von Daten dagegen die relevante Gegenleistung. Das dürfte sich letztlich auch mit dem Ansatz der Richtlinie über digitale Inhalte (siehe unten 2.5.1) besser in Einklang bringen lassen.

2.3.2 Spezialfall Ad-Blocker und Bezahlschranken

Insbesondere Nachrichtendienste verwenden verschiedene Formen digitaler Bezahlschranken, um Vertriebserlöse für die Inhalte zu erzielen (vgl. näher die vbw Studie *Digitale Bezahlschranken – Profit- oder Problembringer?*). Diese Schranken lassen sich allerdings vergleichsweise einfach umgehen. Da sich mit Ad-Blockern zudem auch Werbeanzeigen ausblenden lassen, sieht die Branche ihr auf diesen zwei Säulen beruhendes Erlösmodell insgesamt gefährdet. Teilweise wird daher ein Verbot von Ad-Blockern gefordert, so dass letztlich immer der Betreiber der Website entscheiden könnte, was der Nutzer zu sehen bekommt. Die Gegner eines solchen Verbots verweisen darauf, dass eine solche Regulierung über das Ziel hinausschießen würde und auch Sicherheitstools oder Privatsphäreneinstellungen von Browsern betroffen sein könnten. Es lasse sich auch schlecht mit der angestrebten Datensouveränität der Verbraucher in Einklang bringen.

Position der vbw

Das Thema Ad-Blocker sollte auf technischem Weg gelöst werden, nicht auf rechtlichem. Faktisch ist kaum ein Unterschied zur Fernsehwerbung erkennbar, wo auch kein Zuschauer gezwungen werden kann, sich diese anzusehen, statt das Programm aufzuzeichnen und vorzuspulen oder die kurzen Pausen anderweitig zu nutzen. Bereits heute findet ein

Wettlauf zwischen Anbieter- und Nutzerseite statt: Wo ein neuer Blocker auftaucht, wird im Gegenzug versucht, dessen Nutzung zu identifizieren und Angebote in diesem Fall nicht sichtbar zu machen.

Anders sieht die Lage allerdings dort aus, wo Bezahlschranken umgangen werden, um kostenpflichtig angebotene Inhalte unentgeltlich nutzen zu können. Der Sache nach handelt es sich hier ebenso um ein Erschleichen von Leistungen, wie es nach § 265a StGB in den dort aufgezählten Fällen (z. B. Beförderung, Zutritt zu einer Veranstaltung) strafbar ist. Es wäre nur folgerichtig, auch in diesen Fällen jedenfalls an eine Bußgeldbewährung zu denken.

2.4 Vertragsabwicklung und Rechtsfolgen

2.4.1 Rückabwicklung allgemein

Wird der Vertrag rückabgewickelt, insbesondere aufgrund eines Rücktritts, dann sind die gegenseitig gewährten Leistungen zurückzugewähren. Im Falle von Daten (aber auch digitalen Inhalten) ist eine Verpflichtung zur Löschung sachgerecht, da eine Herausgabe angesichts der fast beliebigen Vervielfältigbarkeit wenig zielführend wäre. Grundsätzlich müssen auch die erlangten Gebrauchsvorteile herausgegeben werden. Dem Wortlaut nach sind damit aber nur solche aus Sachen und Rechten gemeint, und dabei sollte es auch belassen werden, um keine unverhältnismäßigen Folgen auszulösen.

Eine Minderung kommt bei einer Hingabe von Daten als Entgelt in aller Regel nicht in Betracht, sondern nur die Begründung eines Rückgewährschuldverhältnisses (beispielsweise aufgrund einer Kündigung).

2.4.2 Widerruf der datenschutzrechtlichen Einwilligung

Ein grundsätzliches Problem ist, dass die datenschutzrechtliche Einwilligung beziehungsweise die Ausgestaltung als Verbot mit Erlaubnisvorbehalt ausschließlich den Schutz des Persönlichkeitsrechts im Blick hat, aber nicht auf wirtschaftliche Vorgänge zugeschnitten ist. Während sich im allgemeinen Vertragsrecht die Parteien nur in bestimmten Fällen wieder vom Vertrag lösen können, ist die datenschutzrechtliche Einwilligung jederzeit widerruflich, so dass der Vertragspartner gewissermaßen mit leeren Händen dasteht, wenn Daten in Verbindung mit der notwendigen Einwilligung die vertragliche Gegenleistung darstellten, und den Vertrag seinerseits nur noch kündigen kann. Ein solches einseitiges und voraussetzungsloses Reuerecht ist im Zivilrecht mindestens ungewöhnlich. Wenn Verträge über Daten ermöglicht und gefördert werden sollen, kann es nicht bei diesem Zwischenergebnis bleiben.

Mit der Kündigung wird regelmäßig auch – mindestens im Wege der Auslegung – ein Widerruf der datenschutzrechtlichen Einwilligung verbunden sein. Damit ist einerseits ein Löschungsanspruch nach der DSGVO verbunden, andererseits ein Anspruch auf Rückgewähr der Daten.

Ein pauschaler Verzicht auf die Widerruflichkeit ist wegen der grundrechtlich geschützten informationellen Selbstbestimmung wohl nicht möglich. Ein dingliches Nutzungsrecht, das widersprechende Verfügungen ausschließt, ließe sich weder mit Persönlichkeitsrechten noch mit der Natur von Daten vereinbaren.

Was allerdings zulässig sein muss, ist – ähnlich wie beim Recht am eigenen Bild – ein Verzicht auf das Recht zum Widerruf der Einwilligung in bestimmten Nutzungsszenarien. Wenn Daten ein Wirtschaftsgut sind, das Gegenstand von Verträgen sein kann, dann muss sich der im datenschutzrechtlichen Sinn „Betroffene“ auch an seinen vertraglich vereinbarten Dispositionen über diesen Vermögensbestandteil festhalten lassen. Danach gilt: Wenn der Vertrag jederzeit kündbar ist, dann ist auch die Einwilligung unbeschränkt widerruflich. Ist der Vertrag auf eine bestimmte Dauer geschlossen, dann ist ein vorzeitiger Widerruf vertragswidrig; beim punktuellen Leistungsaustausch sollte jedenfalls ein Widerruf in missbräuchlicher Absicht (um sich trotz Leistungserhalt der Gegenleistungspflicht zu entziehen) eine Schadensersatzpflicht auslösen können. Jedenfalls kann der Anbieter hier die Rückabwicklung des Vertrags erreichen. Konsequenterweise müsste ihm bei nicht vollständiger Erbringung der Gegenleistung ein Wertersatzanspruch für den von ihm geleisteten digitalen Inhalt oder ein Schadensersatzanspruch zustehen.

Praxistipp

Diese Fragen sind höchstrichterlich noch nicht geklärt. Eindeutig sanktionsbewehrt ist lediglich die Weiternutzung der Daten nach Widerruf der Einwilligung. Es könnte sich daher empfehlen, eine bedingte Entgeltpflicht/einen Wertersatzanspruch für den Fall eines (im Sinne des Vertrags) vorzeitigen Widerruf vorzusehen. Auch deren rechtliche Haltbarkeit ist allerdings nicht gewährleistet. Wird mit Vertragsschluss zugleich eine Einwilligung in die Anonymisierung der Daten eingeholt, sollte jedenfalls die Weiternutzung der anonymisierten Daten ohne erneute Einwilligung zulässig sein. Eine datenschutzrechtliche Pflicht zur Löschung erfolgreich anonymisierter Daten besteht nicht. Zu (künftigen) Neuerungen aufgrund des EU-Rechts vgl. unten.

Wenn auf europäischer Ebene Regelungen im Bereich der Datenwirtschaft getroffen werden, dann sollten auch Aspekte wie die genannten berücksichtigt werden. Echte Anreize für eine florierende europäische Datenökonomie setzen auch funktionierende Märkte voraus, auf denen nicht lediglich eine Seite verbriefte Rechte hat.

2.4.3 Haftungsfragen

Datengetriebene Prozesse und Produkte können fehlerhafte Ergebnisse liefern, so dass sich die Frage stellt, wer dafür einzustehen hat.

Ursachen für die Fehlerhaftigkeit können auf verschiedenen Ebenen auftreten, z. B.:
- bei der Programmierung
- aufgrund technischer Defekte der Hardware (z. B. Sensorik)
- im Rahmen der Interaktion mit anderen Maschinen oder Menschen
- im Rahmen der Verarbeitung beispielsweise Interpretation der Daten durch die Software
- durch externe Störquellen (zum Beispiel bei der Datenübertragung, aufgrund von Manipulation)

2.4.3.1 Rechtliche Einordnung

Ist die Software aufgrund eines *Programmierungsfehlers* mangelhaft, greift das Gewährleistungsrecht ein (Nacherfüllung, Minderung und Rücktritt sowie bei Verschulden auch Schadenersatzansprüche). Je nachdem, was vertraglich vereinbart ist, kann beispielsweise auch ein unpassender Test- oder Trainingsdatensatz für ein intelligentes System einen solchen Mangel auslösen. Voraussetzung ist allerdings, dass tatsächlich ein Vertrag mit dem Software-Ersteller vorliegt. Produkthaftung und Produzentenhaftung kommen gegenüber dem „Hersteller“ der KI schon deshalb nicht in Betracht, weil Software nach überwiegender Auffassung keine bewegliche Sache und damit kein Produkt in diesem Sinne ist. Es mag sein, dass sich die Wertungen nicht zuletzt angesichts der neuen EU-Richtlinien (siehe unten 2.5.1) verschieben. In den dort geregelten Fällen greifen jedenfalls zugunsten des Verbrauchers weitere Erleichterungen bei der Geltendmachung von Ansprüchen.

Grundsätzlich dasselbe wie bei der Software gilt auch für *Defekte der Hardware*. Zusätzlich kommen hier Ansprüche aus Produkthaftung (ProdHaftG) in Betracht, die verschuldensunabhängig eingreifen kann, wenn der Fehler bereits beim Inverkehrbringen vorlag und dieser Fehler dazu führt, dass ein Mensch getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache, die für den privaten Gebrauch oder Verbrauch bestimmt ist, beschädigt wird. Denkbar ist auch eine deliktische Haftung nach § 823 BGB (Produzentenhaftung, Verletzung eines Schutzgesetzes) – auch hier wird aber Verschulden vorausgesetzt (im Falle der Produzentenhaftung gegeben, wenn eine Verkehrssicherungspflicht verletzt wurde), und reine Vermögensschäden sind nicht ersatzfähig. Vorteil der Produkt- oder Produzentenhaftung ist aus Sicht des Geschädigten, dass der Hersteller des physischen Produkts – wenn die oben skizzierten Voraussetzungen vorliegen – letztlich auch für Fehler der mit dem Produkt verbundenen Software in Anspruch genommen werden kann, auch wenn sie nicht in seinem Unternehmen programmiert wurde. Der Hersteller kann seinerseits Regress nehmen, wenn er in einem vertraglichen Verhältnis zum Software-Ersteller steht, und nicht beispielsweise Open Source Software nutzt oder die Haftung anderweitig ausgeschlossen ist.

Im Zentrum der Diskussion stehen die Fälle, in denen der *Fehler im Rahmen der Datenverarbeitung* aufgetreten ist, und hier insbesondere der Einsatz lernender Systeme. In Betracht kommen hier neben Gewährleistungsrechten ebenfalls Ansprüche aus dem Bereich der Produkthaftung und der Produzentenhaftung. Schwierigkeiten ergeben sich hier daraus, dass gerade bei lernenden Systemen oftmals ein Sorgfaltsverstoß nur schwer nachweisbar ist, weil es an der Vorhersehbarkeit fehlt. Die verschuldensunabhängige Produkthaftung setzt ferner voraus, dass der Fehler schon beim Inverkehrbringen vorlag. Das kann zweifelhaft sein, wenn es sich um Entscheidungen aufgrund des erst später Erlernten handelt. Noch nicht abschließend geklärt ist auch, ob jedes Softwareupdate ein neues Inverkehrbringen des ausgestatteten Ursprungsproduktes darstellt, selbst wenn es nur eine Fehlerbehebung wäre.

Für den Fall, dass nur eine verschuldensunabhängige Haftung in Betracht kommt und ein Sorgfaltsverstoß nicht nachweisbar ist, wird die Einführung eines neuen Gefährdungstatbestands diskutiert, um Haftungslücken zu vermeiden. Dieser soll allein auf der Gefahrenquelle Automatisierung beziehungsweise Einsatz Künstlicher Intelligenz beruhen. Vorbild könnte etwa die Haftung des Fahrzeughalters nach § 7 Abs. 1 StVG sein. Die Europäische Kommission schlägt in ihrer Mitteilung „Building a EU Data Economy“ zwei konkrete Herangehensweisen vor, die sich gegenseitig unterstützen sollen. Dabei wird zwischen einem Risk-Generating Approach (ähnlich der Gefährdungshaftung) und einem Risk-Management Approach unterschieden.

Diskutiert wird ferner, dass der Hersteller auch für solche Schäden in die Pflicht genommen werden könnte, deren Entstehung er aufgrund der ihm übermittelten Daten (etwa Betriebs- und Zustandsdaten) hätte erkennen können und die dementsprechend gegebenenfalls vermeidbar gewesen wären.

Bei *externen Eingriffen* (z. B. Hacker-Angriff) kommt grundsätzlich nur das Deliktsrecht in Betracht. Während Verschulden des Angreifers immer vorliegt (Ansprüche aber nur selten durchsetzbar sind), kommt eine Haftung des Herstellers (Software und/oder Produkt) nur in Betracht, wenn der entsprechende Missbrauch nicht vorhersehbar und damit vermeidbar war, etwa durch angemessene Sicherheitsvorkehrungen. Letztere müssen allerdings entweder vertraglich vereinbart worden sein oder aufgrund besonderer gesetzlicher Vorgaben eingreifen (namentlich für kritische Infrastruktur). Für Verbraucher wird sich die Rechtslage insoweit demnächst ändern, zumal verpflichtende Updates vorgesehen sind (vgl. unten 2.5.1). Für Unternehmer bieten sich gemeinsam definierte und auf Risikoanalysen basierende Cybersicherheits-Richtlinien an; gegebenenfalls wird auch die Verwendung freiwilliger Sicherheitskennzeichnungen eine Wirksamkeitsvermutung ermöglichen. Auch hier stellt sich die Frage, inwieweit das Schließen von Sicherheitslücken durch Updates Einfluss auf die Gewährleistung für das Produkt hat.
Entsteht ein Schaden schließlich aufgrund eines Fehlers bei der *Datenübertragung* (z. B. Verbindungsabbruch), können sich Host- und Zugangsprovider nach dem TMG vielfach exkulpieren.

2.4.3.2 Bewertung der vbw

Grundsätzlich gilt es, eine angemessene Risikoverteilung zu finden, die innovationsfreundlich und fair gegenüber allen Marktteilnehmern ist.

Es ist gegenwärtig keine Regelungslücke erkennbar, die die Einführung eines neuen Tatbestands der Gefährdungshaftung notwendig machen würde. Die häufigsten Fälle lassen sich durch eine sachgerechte Abgrenzung nach Verantwortungsbereichen (z. B. welche Art von Daten verwendet werden, in welcher Umgebung das System eingesetzt wird) lösen, die idealerweise vertraglich klar abgebildet wird. Für Verbraucher wird ohnehin die für 2021 anstehende Umsetzung der EU-Richtlinien deutliche Erleichterungen bringen (siehe unten 2.5.1).

Die rechtliche Behandlung von Updates sollte insbesondere auch für den B2B-Bereich geklärt werden. Eine generelle Einordnung von Updates als neues Inverkehrbringen des Produkts würde zu einer Überdehnung der Produkthaftung führen. Insoweit muss zukünftig eine trennscharfe Definition erfolgen, die zwischen zusätzlichen Funktionalitäten für die KI, die dann daraus ein neues Produkt machen würden, und reinen Fehlerbehebungen unterscheidet. Aufgrund des sich ständig verändernden Zustandes von Software wird eine statische Produktdefinition immer weniger zielführend. Das erkennt auch die EU für Verträge mit Verbrauchern an (vgl. unten, Richtlinie für digitale Inhalte, 2.5.1), im Verhältnis zwischen Unternehmen muss das erst recht gelten.

Gleichzeitig muss die Frage des Anspruchsgegners beziehungsweise des Regresses in diesen Fällen beantwortet werden, um nicht den Hersteller des physischen Produkts faktisch in vielen Fällen alleine haftbar zu machen. Auch der – ebenfalls diskutierte – umgekehrte Weg, die Haftung (alleine) auf den Hersteller der KI zu verlagern, etwa über Produktbeobachtungspflichten, ist abzulehnen. Er kann zum einen den Einsatz des Systems nur bedingt beeinflussen, zum anderen wäre das der weiteren Entwicklung von KI-Anwendungen kaum zuträglich.

Zusätzliche Produkthaftungsansprüche gegenüber Unternehmen aufgrund der Vorhersehbarkeit von Schadensereignissen aufgrund der Verfügbarkeit von Rohdaten sollten nicht begründet werden. Zum einen bewegt sich das außerhalb des Verantwortungsbereichs des Herstellers, sofern es nicht um die Produktbeobachtungspflicht nach bisherigem Verständnis geht, zum anderen drohen Fehlanreize. Aus Sorge vor möglichen Haftungsansprüchen würden Produkthersteller sich diese Daten nach Möglichkeit gar nicht erst verschaffen, um nicht das Risiko einer (unterlassenen) Auswertung tragen zu müssen. Dies hätte vielfältige Nachteile für die Entwicklung einer europäischen Datenökonomie zur Folge.

Die Anforderungen an den einzelnen Hersteller – ob von Hardware oder Software – dürfen nicht überspannt werden. Aufgrund der enormen Komplexität und der kurzen Entwicklungszyklen können einzelne Unternehmen ab einer gewissen Interaktion und wechselseitiger Beeinflussung von software-gesteuerten Geräten nur bedingt Gewährleistung für das Funktionieren des Gesamtsystems übernehmen. Gerade für sicherheitskritische Anwendungen ist es jedoch entscheidend, das gesamte Ökosystem im Blick zu haben. Darin kann

eine Aufgabe für die entsprechenden staatlichen Stellen – beispielsweise das BSI oder auf europäischer Ebene die ENISA – gesehen werden, soweit es um sicherheitskritische Themen geht. Entscheidend ist aber, dass eine solche Aufgabe über Beratung und Empfehlung wahrgenommen wird, nicht mit repressiven Maßnahmen (vgl. auch 4.1.6 zur IT-Sicherheit).

Diskussionswürdig ist, ob der Fehlerbegriff im Bereich von Software präzisiert werden sollte, um zu einer angemessenen Haftungsverteilung auch im unternehmerischen Bereich beizutragen. Ein Beispiel sind die oben genannten „Eingangsdaten" für den Fall, dass dies vertraglich nicht ausdrücklich geregelt ist. Bekannt geworden sind einige Fälle, in denen die intelligenten Systeme mit vorurteilsbelasteten Datensätzen „gefüttert" wurden. Wenn Künstliche Intelligenz ethische Leitlinien verletzt (vgl. insoweit die Arbeiten der nationalen und europäischen Datenethikkommissionen), wäre mindestens eine Nachbesserungspflicht gut vertretbar, durchaus aber auch die Annahme eines Fehlers. Die EU-Kommission erörtert derzeit, wie sich die Regelungen der Produkthaftung diesbezüglich anpassen lassen.

Auch wenn Künstliche Intelligenzen hochkomplexe Systeme darstellen, deren Verhalten nur bedingt vorhersehbar ist und die teilweise selbstständig lernen können, handeln sie – jedenfalls derzeit noch – im Rahmen der von Menschen vorgegebenen Programmierungen. Auf den ersten Blick scheint die Entwicklung der Künstlichen Intelligenz das Zivilrecht vor neue Herausforderungen zu stellen. Tatsächlich offenbart sich bei näherem Hinsehen jedoch, dass die geltende Rechtsordnung, insbesondere mitsamt den bestehenden Rechtsinstituten im Haftungsrecht geeignet ist, die Risiken, die durch den Einsatz intelligenter Systeme entstehen, zuzuweisen.

Die Verteilung der Haftung für technische Ausfälle in der Datenübertragung und die bestehenden Privilegierungen müssen angesichts der wachsenden Bedeutung von Systemen, die auf durchgehende Verbindungen angewiesen sind, noch einmal kritisch geprüft werden.

2.5 Neuerungen auf der europäischen Ebene und ihre Auswirkungen

Mit zwei Legislativakten – Richtlinie für digitale Inhalte und Richtlinie für den Warenhandel – hat die EU im vergangenen Jahr regelnd in die oben skizzierten Vertragsverhältnisse eingegriffen. Von der EU-Regulierung war vielfach erwartet worden, dass sie jedenfalls für das Verhältnis zwischen Unternehmer und Verbraucher Klarheit in den oben skizzierten Zweifelsfragen schafft. Diesen Anspruch erfüllt sie nicht.

Beide Richtlinien beruhen auf dem Grundsatz der maximalen Harmonisierung, das heißt, dass die Mitgliedstaaten nicht von den Anforderungen abweichen können. Sie dürfen beispielsweise keine abweichenden Vorschriften über die Umkehr der Beweislast erlassen, oder auch keine Verpflichtung des Verbrauchers, den Anbieter innerhalb eines bestimmten Zeitraums über eine Vertragswidrigkeit zu informieren. Bei einigen Aspekten haben die EU-Mitgliedstaaten jedoch einen gewissen Spielraum, so dass sie über die Anforderungen

hinausgehen und in bestimmten Fällen (z. B. Haftung für versteckte Mängel, zusätzliche Ansprüche gegen Dritte außerhalb des Vertragsverhältnisses) das auf nationaler Ebene bereits geltende Verbraucherschutzniveau beibehalten und gegebenenfalls erweitern können.

Die Richtlinien gelten nur für Verbraucher. Den Mitgliedsstaaten steht es frei, den Anwendungsbereich auszudehnen, oder aber ein anderes Regime für die nicht erfassten Verträge (z. B. zwischen Unternehmen) vorzusehen. Zusätzlich können sie auch bestimmte eigentlich nicht erfasste Fallkonstellationen mit Verbraucherbezug in den Anwendungsbereich einbeziehen.

Ab dem 01.01.2022 müssen die Richtlinien in Deutschland angewendet werden; die Umsetzungsvorschriften sind bis zum 01.07.2021 zu erlassen.

2.5.1 EU-Richtlinie für digitale Inhalte

2.5.1.1 Anwendungsbereich und wesentliche Inhalte

Die *Richtlinie für Verträge über die Bereitstellung digitaler Inhalte und Dienstleistungen* (Richtlinie für digitale Inhalte, RL 2019/770 vom 20. Mai 2019) soll Lücken im Verbraucher- und Vertragsrecht schließen und regelt dazu unter anderem die vertragsgemäße Beschaffenheit digitaler Inhalte und Gewährleistungsrechte. Zusätzlich wird erstmals ausdrücklich arnerkannt, dass der Verbraucher die Gegenleistung für digitale Inhalte auch durch die Bereitstellung personenbezogener Daten erbringen kann („Zahlen mit Daten“).

Anders, als man im Laufe des Entstehungsprozesses vermuten konnte, wird eine Differenzierung nach bestimmten Vertragstypen nur sehr zurückhaltend vorgenommen. Betroffen sind praktisch alle Verträge in B2C-Bereich.

Anwendungsbereich

- Vom Regelungsbereich umfasst sind Inhalte und Daten, die in digitaler Form hergestellt und bereitgestellt werden (z. B. Musik, Online-Videos usw.), Dienstleistungen, die die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form ermöglichen (z. B. Cloud-Speicherung), Dienstleistungen, die den Austausch von Daten ermöglichen (z. B. Facebook, YouTube usw.) sowie alle dauerhaften Datenträger, die ausschließlich der Übermittlung digitaler Inhalte dienen (z. B. DVDs). Erfasst werden unter anderem auch Verträge über die Entwicklung individueller digitaler Inhalte nach den Anforderungen des Verbrauchers (z. B. Software) sowie die Bereitstellung von Dateien im Rahmen des 3D-Drucks.
- Bereichsausnahmen gelten unter anderem für Finanzdienstleistungen (etwa PayPal) und kostenlose und quelloffene Software (open source), sofern personenbezogene

Daten ausschließlich zur Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software verwendet werden.

- Digitale „Darstellungen eines Werts“ (elektronische Gutscheine, E-Coupons oder virtuelle Währungen, sofern sie nach nationalem Recht anerkannt sind) zählen zu den Zahlungsweisen im Sinne der Richtlinie, sind selbst jedoch keine digitalen Inhalte oder Dienstleistungen.
- Nicht erfasst sind „die Erbringung von Dienstleistungen, die keine digitalen Dienstleistungen sind, unabhängig davon, ob der Unternehmer digitale Formen oder Mittel einsetzt, um das Ergebnis der Dienstleistung zu generieren oder es dem Verbraucher zu liefern oder zu übermitteln“; gemeint sind ausweislich der Erwägungsgründe (Nr. 27) Verträge, deren Hauptgegenstand die Erbringung freiberuflicher Dienstleistungen ist (z. B. Übersetzungen, juristische Beratung). Bei den freiberuflichen Dienstleistungen ging aus den Erwägungsgründen zunächst hervor, dass der Ausschluss vom Anwendungsbereich nur dann gelten soll, wenn die Dienstleistung persönlich erbracht und lediglich das Ergebnis digital übermittelt wird. Die aktuelle Fassung ist insoweit enger. Trotzdem wird man von einer Anwendbarkeit der Richtline in bestimmten Konstellationen ausgehen können, weil automatisierte „freiberufliche“ Leistungen wie eine Übersetzungsplattform durchaus unter die Legaldefinition der digitalen Dienstleistung subsumiert werden können. Grundsätzlich ausgeschlossen sind ferner die Bereitstellung von digitalen Inhalten durch öffentliche Stellen (Open Data) oder Gesundheitsdienstleistungen (zum Beispiel Telemedizin).
- Fragen der Haftung (etwa für Daten und Verträge bei der Interaktion zwischen Maschinen) im Zusammenhang mit dem Internet der Dinge sollen gemäß Erwägungsgrund 17 gesondert geregelt werden.

Der für die Bereitstellung gewählte Weg (Herunterladen, Streamen, Webapplikation, Software as a Service etc.) ist unerheblich; lediglich Internetzugangsdienste sollen ausdrücklich nicht erfasst sein.

Nach der Richtlinie für digitale Inhalte werden Verbraucherinnen und Verbraucher künftig weitgehend geschützt sein, wenn sie für eine Dienstleistung bezahlen, aber auch wenn sie für diese Dienstleistung Daten zur Verfügung stellen. Personenbezogene Daten können zwar „nicht als Ware betrachtet werden“, es soll aber sichergestellt werden, dass der Verbraucher auch bei solchen Geschäftsmodellen vertragliche Rechtsbehelfe hat. Personenbezogene Daten dürfen nur im Einklang mit der DSGVO verarbeitet werden; im Falle eines Widerspruchs gehen diese vor. Die Richtlinie über digitale Inhalte regelt ausdrücklich nicht die Gültigkeit der Einwilligung oder deren Widerruf. Nicht erfasst werden Fälle, in denen der Unternehmer nur Metadaten wie Informationen zum Gerät des Verbrauchers oder zum Browserverlauf erhebt, es sei denn, der betreffende Sachverhalt gilt als Vertrag nach nationalem Recht. Ebenso wenig soll die Richtlinie in Fällen gelten, in denen der Verbraucher ausschließlich zwecks Erlangung des Zugangs zu digitalen Inhalten oder digitalen Dienstleistungen Werbung ausgesetzt ist, ohne mit dem Unternehmer einen Vertrag abgeschlossen zu haben.

Die Neuregelung sieht insbesondere vor, dass Verbraucher Anspruch auf eine Preisminderung oder eine Rückerstattung des vollen Preises haben, wenn Mängel nicht innerhalb eines angemessenen Zeitraums behoben werden können (grundsätzlich vorrangiger Anspruch auf unentgeltliche Herstellung des vertragsgemäßen Zustands). Wenn die digitalen Inhalte oder digitalen Dienstleistungen zwar nicht gegen Zahlung eines Preises bereitgestellt werden, der Verbraucher jedoch personenbezogene Daten bereitstellt, so sollte der Verbraucher das Recht haben, den Vertrag auch in Fällen einer geringfügigen Vertragswidrigkeit zu beenden, da ihm Abhilfe in Form einer Preisminderung nicht zur Verfügung steht (Erwägungsgrund 67); wenn er sowohl Entgelt zahlt als auch Daten bereitstellt, stehen dem Verbraucher alle Rechtsbehelfe zu.

Für während des ersten Jahres nach der Bereitstellung beziehungsweise während der Vertragslaufzeit auftretende Mängel gilt eine Beweislastumkehr. Den Verbraucher treffen allerdings Mitwirkungsobliegenheiten, um es dem Unternehmer zu ermöglichen, mögliche Ursachen in der digitalen Umgebung des Verbrauchers aufzudecken (Erwägungsgründe 60 und 61).

Wesentliche Änderung ist, dass ein Produkt nur vertragsgemäß ist, wenn es nicht nur dem Vereinbarten entspricht, sondern auch eine Reihe *objektiver* Leistungsmerkmale (z. B. Kompatibilität, Sicherheit) erfüllt, während das deutsche Recht bisher maßgeblich auf die vertraglich vereinbarte Beschaffenheit abstellt (§ 434 BGB). Der geschuldete Standard wird sich erst noch herausbilden beziehungsweise von der Rechtsprechung entwickelt werden, da der Verkäufer liefern muss, was der Verbraucher bei Gütern der jeweiligen Art „vernünftigerweise erwarten kann“. Erstmals wird der Verkäufer schließlich auch zur Bereitstellung von Updates verpflichtet (siehe auch unten die vergleichbaren Neuerungen bei der Richtlinie für den Warenhandel). Die objektiven Anforderungen kann der Unternehmer nicht im Wege der AGB abbedingen, sondern lediglich durch Beschreibung der Abweichung schon beim Vertragsschluss, der der Verbraucher ausdrücklich zustimmen muss (auch durch Anklicken eines Kästchens, Betätigung einer Schaltfläche oder Aktivierung einer ähnlichen Funktion möglich, siehe Erwägungsgrund 49). Die vertragliche Vereinbarung der Beschaffenheit kann also immerhin sozusagen subsidiär als (einzig) maßgebliche zum Tragen kommen.

Die Rechtsnatur von Verträgen über digitale Inhalte und Dienstleistungen richtet sich weiterhin nach dem nationalen Recht. Unberührt bleiben auch die nationalen Vorschriften über Zustandekommen, Wirksamkeit und Auswirkungen von Verträgen oder über die Rechtmäßigkeit des digitalen Inhalts. Das gilt auch dann, wenn die Gegenleistung des Verbrauchers in der Bereitstellung personenbezogener Daten besteht. Der Zeitraum, innerhalb dessen der Anbieter für Vertragswidrigkeiten haftbar gemacht werden kann, wird in der Richtlinie bewusst nicht geregelt; auch die Mitgliedstaaten sollen keinen solchen Zeitraum einführen (Erwägungsgrund 43). Möglich bleibt aber der Rückgriff auf nationale Verjährungsvorschriften.

2.5.1.2 Auswirkungen auf die rechtliche Behandlung von Daten als Gegenleistung

Lediglich implizit ist der Richtlinie zu entnehmen, dass personenbezogene Daten als geldwerte Gegenleistung anzusehen beziehungsweise dieser gleichzusetzen sind: Die Bestimmungen der Richtlinie sollen grundsätzlich unabhängig von der Art der Gegenleistung (Entgelt oder Daten) gelten (Erwägungsgrund 24).

Eine echte inhaltliche Auseinandersetzung mit der Frage, wie personenbezogene Daten kommerzialisiert und monetarisiert werden können, unterbleibt leider; der Hinweis, sie könnten „nichts als Ware betrachtet werden“, führt nicht weiter, zumal es hier ja auch nicht um einen Verkauf von Daten geht, sondern um deren Einsatz als Gegenleistung. Einstweilen bleibt das eine nach nationalem Recht (im Lichte der Richtlinie) zu beurteilende Frage.

Auch wenn das in der Richtlinie für digitale Inhalte nicht ausdrücklich geregelt ist, muss diese Einordnung bedeuten, dass der Anbieter/Unternehmer einen *Anspruch* auf Bereitstellung *vollständiger und wahrer* Daten als Gegenleistung erhält, der nicht durch einen pauschalen Verweis auf die informationelle Selbstbestimmung abgelehnt werden kann. Anderenfalls bestünde ein Anreiz, das Angebot so zu strukturieren, dass der Nutzer gar nicht aktiv Daten eingeben muss, dann allerdings auch keinerlei Recht beispielsweise in Gewährleistungskonstellationen erhielte. Entscheidend ist, was vertraglich (in der Regel in AGB) zu dieser Frage geregelt ist. Es würde regelmäßig den Vertragszweck gefährden, wenn der Verbraucher nach Vertragsschluss beliebige Daten zur Verfügung stellen könnte; er muss die vertraglich vereinbarten Daten liefern. Immerhin ist in der Richtlinie ausdrücklich auch die Konstellation vorgesehen, dass der Verbraucher die Bereitstellung personenbezogener Daten lediglich zusagt.

Es kann ferner davon ausgegangen werden, dass nun die Hingabe von Daten als Gegenleistung als entgeltlichen Vertrag zu qualifizieren beziehungsweise einem solchen gleichzustellen ist. Damit sind auch die Verbraucherschutzvorschriften der §§ 312 ff. BGB grundsätzlich anzuwenden.

AGB-Kontrolle

Vereinbarungen über die Datennutzung und die Zuordnung eines entstehenden Mehrwerts werden in der Regel in Allgemeinen Geschäftsbedingungen (AGB) getroffen. In Verträgen mit Verbrauchern (B2C) ist im Hinblick auf die strengen Kontrollmaßstäbe der Gerichte besonders darauf zu achten, keine zu weitgehenden Regelungen zu treffen (z. B. vollständiger Haftungsausschluss), um nicht eine Beurteilung als unangemessene Benachteiligung und damit die Unwirksamkeit der Klausel zu riskieren.

Eine im Vorfeld vielfach diskutierte Frage ist, inwieweit auch Daten, die sozusagen bei Gelegenheit der Nutzung des Dienstes übertragen werden, im Gegenseitigkeitsverhältnis stehen. Erwägungsgrund 14 gibt insoweit einen wichtigen Hinweis: „Im Hinblick auf digitale Inhalte, die nicht gegen Zahlung eines Preises, sondern gegen eine andere Leistung als Geld bereitgestellt werden, sollte diese Richtlinie nur für Verträge gelten, in deren Rahmen

der Anbieter vom Verbraucher Daten wie Name, E-Mail-Adresse oder Fotos verlangt und der Verbraucher dem Anbieter diese Daten beispielsweise im Wege einer individuellen Registrierung oder auf der Grundlage eines Vertrags, der den Zugang zu Fotos des Verbrauchers gestattet, aktiv zur Verfügung stellt. Die Richtlinie sollte nicht in Fällen gelten, in denen der Anbieter Daten verlangt, die er für die vertragsgemäße Funktionsweise digitaler Inhalte benötigt, beispielsweise Angaben zum geografischen Standort, die für das ordnungsgemäße Funktionieren einer mobilen Anwendung erforderlich sind. Ebenso wenig sollte die Richtlinie gelten in Fällen, in denen die Datenerhebung ausschließlich der Erfüllung rechtlicher Anforderungen dient, beispielsweise wenn die Registrierung des Verbrauchers zu Sicherheits- und Identifizierungszwecken gesetzlich vorgeschrieben ist. Diese Richtlinie sollte auch nicht in Fällen gelten, in denen der Anbieter Informationen einschließlich personenbezogener Daten wie z. B. die IP-Adresse oder sonstige automatisch generierte Informationen wie durch Cookies gesammelte und übermittelte Informationen erhebt, ohne dass der Verbraucher diese aktiv bereitstellt, wobei das Akzeptieren von Cookies durch den Verbraucher nicht als aktives Bereitstellen von Informationen zählt. Ebenso wenig sollte sie in Fällen gelten, in denen der Verbraucher ausschließlich zwecks Erlangung des Zugangs zu digitalen Inhalten Werbung ausgesetzt ist. Damit kann davon ausgegangen werden, dass diese Daten auch nicht im Gegenseitigkeitsverhältnis stehen. Der Anbieter hat keinen Anspruch darauf, solche zusätzlichen Daten zu erhalten, der Nutzer im Falle der Datenübermittlung aber selbstverständlich auch keinen Anspruch auf eine bestimmte Gegenleistung hierfür. Für den Spezialfall des pay as you drive-Tarifs in der Kfz-Versicherung dürfte danach die Richtlinie keine Anwendung finden, da die übermittelten Kundendaten (Fahrverhalten) für die Vertragserfüllung notwendig sind.

Werden die digitalen Inhalte nur während eines Teils der Vertragslaufzeit nicht vertragsgemäß bereitgestellt, soll der Vertrag im Ganzen beendet werden können. Hinsichtlich der personenbezogenen Daten treffen den Unternehmer die Verpflichtungen der Verordnung (EU) 2016/679. Auch sonstige Inhalte, die nicht personenbezogene Daten sind und die vom Verbraucher bereitgestellt oder erstellt wurden (digitale Bilder, Video- und Audiodateien oder auf mobilen Geräten erstellte Inhalte etc.) soll der Unternehmer nicht mehr nutzen dürfen, es sei denn, sie wurden mit anderen Daten aggregiert und könnten nur mit unverhältnismäßigem Aufwand wieder disaggregiert werden, oder sie wurden vom Verbraucher gemeinsam mit anderen erzeugt und können von diesen weiter genutzt werden (Erwägungsgrund 69).

Die Richtlinie klammert die Frage einer „gerechten“ Bezahlung für Verbraucherdaten aus, zumal personenbezogene Daten ja explizit keine „Ware“ sein sollen.

2.5.2 EU-Richtlinie für den Warenhandel

2.5.2.1 Anwendungsbereich und wesentliche Inhalte

Die *Richtlinie über vertragsrechtliche Aspekte des Warenhandels* (Richtlinie für den Warenhandel) erfasst alle Verkäufe von Waren, ob sie nun physisch (in Geschäften), online oder

im Fernabsatz erfolgen. Verträge über Waren, die noch hergestellt oder erzeugt werden müssen, gelten als Kaufverträge im Sinne der Richtlinie. Waren mit digitalen Elementen (beispielsweise automatisierte Fahrzeuge, intelligente Kühlschränke oder Smartwatches) werden von dieser Richtlinie erfasst, wenn sie digitale Inhalte oder digitale Dienstleistungen in einer Weise enthalten beziehungsweise damit verbunden sind, dass die Waren ihre Funktion ohne sie nicht erfüllen könnten. Das gilt unabhängig davon, ob diese digitalen Elemente vom Verkäufer oder einem Dritten bereitgestellt werden. Im Zweifel wird vermutet, dass die digitalen Inhalte oder Dienstleistungen (beispielsweise auch Software as a Service, die fortlaufende Bereitstellung von Verkehrsdaten in einem Navigationssystem) vom Kaufvertrag umfasst sind. Die Tatsache, dass der Verbraucher vor der Nutzung einer Lizenzvereinbarung mit einem Dritten zustimmen muss, soll für sich genommen diese Vermutungswirkung nicht beseitigen (Erwägungsgrund 21 der Richtlinie über digitale Inhalte).

Nicht erfasst sind dagegen körperliche Datenträger mit digitalen Inhalten, etwa eine CD, sowie (nicht im oben genannten Sinne mit der Ware verbundene) digitale Inhalte und Dienstleistungen. Hierfür gilt allein die Richtlinie über digitale Inhalte.

Die Neuregelung sieht eine Mindestgewährleistungsfrist von zwei Jahren vor (ab dem Zeitpunkt, an dem der Verbraucher die Ware erhalten hat), auch für Waren mit digitalen Elementen. Die Umkehr der Beweislast zugunsten der Verbraucher gilt für die Dauer eines Jahres. Für den digitalen Inhalt oder die digitale Dienstleistung, die fortlaufend geliefert werden, gilt die Beweislastumkehr über den gesamten Vertragszeitraum. Die Mitgliedstaaten können längere Fristen vorschreiben, um ihr derzeitiges Verbraucherschutzniveau aufrechtzuerhalten. Wie in der Richtlinie über digitale Inhalte sind auch hier objektive Anforderungen an die Vertragsmäßigkeit neben den subjektiven Anforderungen ausdrücklich vorgesehen.

Die Richtlinie über den Warenhandel führt ein sogenanntes *Update-Recht* ein: Käufer von Waren mit integrierten digitalen Elementen haben ein Recht darauf, vom Verkäufer innerhalb eines angemessenen Zeitraums über notwendige Updates informiert zu werden und diese zu erhalten. Stellt der Verkäufer etwa ein Sicherheits-Update nicht rechtzeitig zur Verfügung, so liegt darin ein Mangel. Das gilt bei fortlaufender Bereitstellung des digitalen Inhalts für die Dauer des Gewährleistungszeitraums (Vertragslaufzeit, mindestens aber zwei Jahre ab Lieferung, Art. 10), bei einmaliger Bereitstellung während des Zeitraums, „den der Verbraucher aufgrund der Art und des Zwecks der Waren und der digitalen Elemente und unter Berücksichtigung der Umstände und der Art des Vertrags vernünftigerweise erwarten kann“ (Art. 7). Der Verkäufer soll grundsätzlich auf andere verantwortliche Personen in der Vertragskette Rückgriff nehmen können; die Details regelt das nationale Recht (Erwägungsgrund 63, Artikel 18).

2.5.2.2 Auswirkungen (beider Richtlinien) auf das Haftungsrecht

Aufgrund des Regresses beziehungsweise möglicher gesamtschuldnerischer Konstellationen können sich Wertungen aus dem neuen digitalen Verbraucherrecht auch auf das Verhältnis zwischen Unternehmern auswirken.

Während bisher fraglich war, ob KI-Systeme überhaupt der Produkt- beziehungsweise Produzentenhaftung unterliegen können, ist das für die von den beiden Richtlinien adressierten Sachverhalte nunmehr jedenfalls im Ergebnis entschieden: Ohne, dass die KI (Software) selbst eine Sache sein müsste, greifen Rechtsbehelfe ein. Es ist davon auszugehen, dass diese Wertung – schon angesichts der zu erwartenden Regressansprüche in der Wertschöpfungskette – auch auf den B2B-Bereich übertragen wird. Auch im Hinblick auf den Anspruch auf Updates innerhalb eines angemessenen Zeitraums kann Ähnliches erwartet werden. Der objektivierte Fehlerbegriff könnte ebenfalls teilweise auf das B2B-Verhältnis durchschlagen, zum Beispiel dort wo es um die berechtigten Erwartungen an die Programmierung eines lernenden Systems geht.

2.5.3 Bewertung der vbw

Das Aufsplitten in zwei Richtlinien ist wenig glücklich, zumal die unterschiedlichen Wertungen (z. B. mit dem Gegenstand erworbene Software vs. später unabhängig vom Warenkauf aufgespielte Software) nicht erklärt werden. Im Ergebnis entsteht ein noch komplexeres Nebeneinander von Vorschriften an Stelle einer klaren und transparenten Systematik. Im Rahmen einer künftigen Überarbeitung sollte ein einheitliches Regelwerk erstellt werden, das unter anderem die Bereitstellung von Daten als Entgelt grundsätzlich adressiert und nicht nur beschränkt auf den Kontext einer einzelnen Richtlinie mit diversen Bereichsausnahmen.

Grundsätzlich zu begrüßen ist, dass die Richtlinien keine Vorgaben hinsichtlich der vertragsrechtlichen Einordnung machen – der damit verbundene Eingriff wäre jedenfalls im Hinblick auf das grundsätzlich offene und flexible BGB zu tief gewesen und die Folgen schwer abschätzbar. Die oben skizzierten offenen Fragen des nationalen Rechts werden aber gerade nicht gelöst. Ein Beispiel von vielen: Die Richtlinie soll ausdrücklich nicht die Folgen, für die von ihr erfassten Verträge regeln, die sich ergeben, wenn der Verbraucher die Einwilligung zur Verarbeitung seiner personenbezogenen Daten widerruft. Solche Folgen sollten weiterhin dem nationalen Recht unterliegen.

Generell werden Leistungspflichten des Verbrauchers und entsprechende Ansprüche des Anbieters nicht geregelt. Damit verfehlt die Richtlinie aber letztlich das Ziel einer Vereinfachung für Verbraucher und Unternehmen.

Auch der eindeutigen Auseinandersetzung mit der Problematik des auf Wirtschaftsbeziehungen nicht zugeschnittenen Datenschutzrechts weicht der europäische Gesetzgeber aus. Die DSGVO soll voll durchschlagen und im Zweifel Vorrang haben. Sachverhalte, die dazu führen, dass Anforderungen der DSGVO (z. B. Datensparsamkeit, Zweckbindungsgrundsatz) nicht eingehalten werden, können als Fehler im Sinne der Richtlinie zu sehen sein. Eine Überarbeitung der DSGVO auch unter dem Fokus Datenwirtschaft bleibt erforderlich.

Für die Umsetzung in deutsches Recht stehen verschiedene Alternativen zur Verfügung, unter anderem die punktuelle Anpassung der verschiedenen Vertragstypen im besonderen

Teil des BGB, die Schaffung neuer Vertragstypen für Verträge über digitale Güter oder die Aufnahme des Regelungsgehalts in den allgemeinen Teil des Schuldrechts. Die Frage bedarf noch weiterer Erörterung. Ziel muss in jedem Fall sein, das bewährte System soweit wie möglich zu erhalten und Systembrüche sowie neue Anwendungsschwierigkeiten zu vermeiden. Gegebenenfalls bietet sich dazu am ehesten die Schaffung (mehrerer) neuer Vertragstypen an. Es sollte auch klar geregelt werden, welche Pflichten den Verbraucher treffen, namentlich dann, wenn Daten als Gegenleistung geschuldet werden.

Die Befugnisse des nationalen Gesetzgebers, die Regelungen auf andere Vertragsverhältnisse auszudehnen – namentlich solche zwischen Unternehmen – macht die Lage noch unübersichtlicher. In Deutschland sollte davon nicht Gebrauch gemacht werden. Fragen wie diejenige nach der Ausgestaltung des Regresses, wenn der Verkäufer für die Software eines Dritten oder bereitzustellende Updates haftet, müssen allerdings auch im nationalen Recht zügig geklärt werden (siehe dazu schon oben 2.4.3).

Weiterführende Informationen

- *TechCheck 2019. Technologien für den Menschen.,* Zukunftsrat der Bayerischen Wirtschaft
- Leitfaden *IT-Sicherheit als Rechtspflicht*, bayme vbm/Heckmann 2020
- Leitfaden *Anonymisierung personenbezogener Daten*, BDI 2020
- Studie *Neue Wertschöpfung durch Digitalisierung*, vbw 2017
- *Neue Wertschöpfung durch Digitalisierung. Analyse und Handlungsempfehlungen.*, Zukunftsrat der Bayerischen Wirtschaft, vbw 2017
- Studie *Blockchain und Smart Contracts – Recht und Technik im Überblick*, Prof. Dirk Heckmann, vbw 2017
- Studie *Digitale Bezahlschraken – Profit- oder Problembringer?,* vbw, Hess/Berger/Rußell, 2019
- Studie *Big Data im Freistaat Bayern. Chancen und Herausforderungen.,* Prognos/Heckmann, vbw 2016
- B*ig Data im Freistaat Bayern – Analyse und Handlungsempfehlungen*., Zukunftsrat der Bayerischen Wirtschaft, 2016
- Positionspapier *Künstliche Intelligenz*, vbw 2019
- Studie *Digitalisierung der bayerischen Wirtschaft*, IW 2019
- Positionspapier *Automatisiertes Fahren – Datenschutz und Datensicherheit*, vbw 2018

3 Position unseres Standorts in der globalen Datenwirtschaft

Potenziale werden noch zu wenig genutzt

3.1 Standortbestimmung

Ebenso wenig, wie die Datenwirtschaft als solche präzise konturiert ist, kann die Positionierung im internationalen Vergleich an einer einzelnen Zahl oder einem Index festgemacht werden. Gleichzeitig zeigen wichtige Näherungswerte und Indizien etwa aus den beiden hier beispielhaft herausgegriffenen Bereichen Künstliche Intelligenz (KI) und Digitale Plattformen übereinstimmend, dass Europa, Deutschland und Bayern noch Luft nach oben haben.

Insgesamt lässt sich bisher ein Aufwärtstrend bei der Datennutzung beobachten, und das ist im Hinblick auf die damit verbundene Wertschöpfung ein positives Ergebnis. Erstmals 2017 und dann erneut 2019 haben wir den Digitalisierungsgrad der bayerischen und deutschen Wirtschaft erhoben. Höhere Reifegradstufen sind dabei mit einem höheren Grad an Datennutzung verbunden. Innerhalb von zwei Jahren ist der Anteil der Unternehmen auf den höchsten beiden Stufen um knapp drei Prozentpunkte gestiegen (siehe oben 1.2.3).

3.1.1 Künstliche Intelligenz

Ein wichtiges Beispiel ist der Anwendungsfall der Künstlichen Intelligenz. Bei den Weltklassepatenten in diesem Bereich liegen die USA sehr klar vorne; unter den TOP 10 befinden sich (auch nach dem Brexit) lediglich drei europäische Staaten. Bayern würde sich in diesem Staaten-Ranking auf Platz elf einreihen, zwischen Frankreich und den Niederlanden.

Weltklassepatente Künstliche Intelligenz 2018

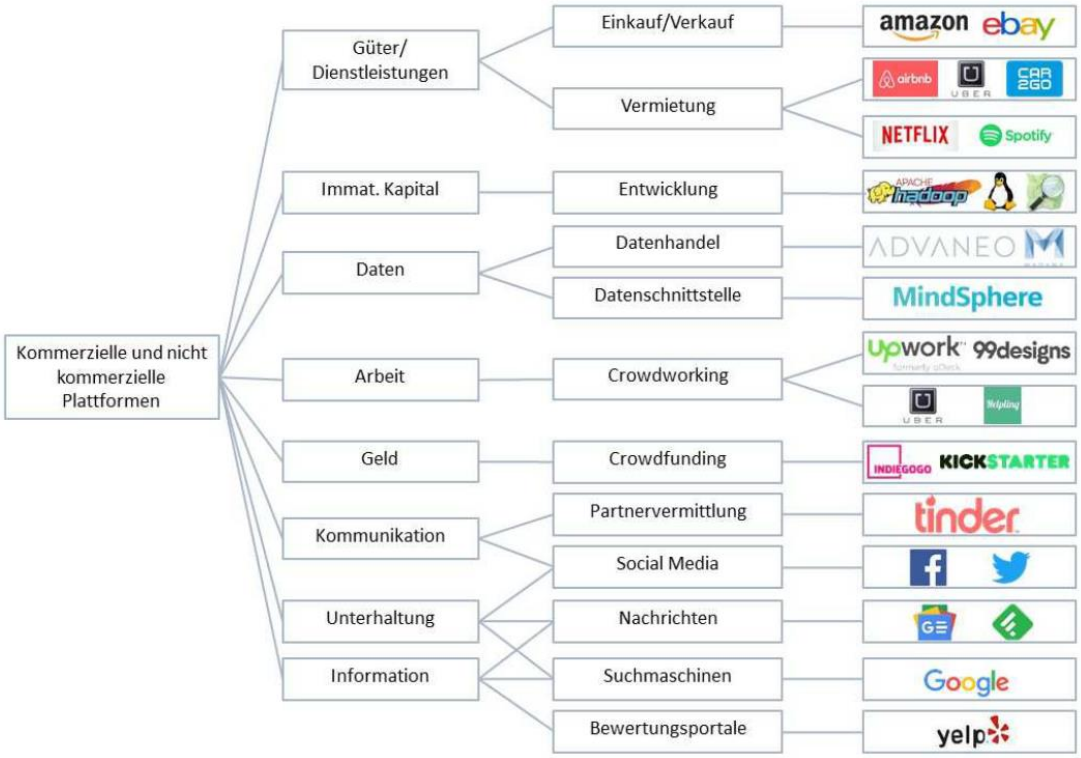
Quelle: vbw/EconSight 2019 für TechCheck 2019. Erfolgsfaktor Mensch.

Weltklassepatente sind besonders werthaltige Patente, gemessen an der subjektiven Einschätzung des Anmelders sowie an der Zitierung durch Dritte. Bei der Gesamtzahl der Patente liegt China vorne, was allerdings auch auf die extensive Patentpolitik des Landes zurückzuführen ist und das Bild insoweit etwas verzerrt. Gleichwohl ist das Wachstum von China in diesem Bereich in den letzten Jahren enorm (vgl. näher *TechCheck 2019. Erfolgsfaktor Mensch.* beziehungsweise die Dokumentation der Vorträge auf www.vbw-zukunftsrat.de).

3.1.2 Digitale Plattformen

Während die Patente im Bereich KI eher die Potenziale abbilden, geht es beim Beispiel der Plattformen um die konkrete Umsetzung. Plattformen haben eine zentrale Bedeutung als Infrastruktur der Digitalisierung und insbesondere der Datenwirtschaft. Dabei gibt es die verschiedensten Typen von Plattformen, wie in der Abbildung dargestellt.

Plattformmärkte nach Themen



Quelle: vbw/IW 2019

Die Nutzung ist nicht nur im Verbraucherbereich hoch. Rund 70 Prozent der deutschen Unternehmen aus den Bereichen der Industrie und der industrienahen Dienstleistungen nutzen oder betreiben Plattformen.

Knapp 15 Prozent der Wertschöpfung der Unternehmen, die Plattformen nutzen, sind davon heute substanziell abhängig. Bei den digital reifen Unternehmen ist dieser Anteil mit 27 Prozent deutlich höher. Bei einer gesamtwirtschaftlichen Betrachtung, die auch die Nichtnutzer einbezieht, sind 6,8 Prozent der Wertschöpfung substanziell von Plattformen abhängig. Bezogen auf die untersuchten Branchen der Industrie und der industrienahen Dienstleistungen entspricht das einer Bruttowertschöpfung von 112 Milliarden Euro. Die Unternehmen bewerten den Einfluss der Plattformen auf ihre Rentabilität insgesamt positiv oder zumindest neutral. Die Zahlen zeigen jedenfalls, dass stärker digitalisierte Unternehmen erfolgreicher sind. Bundesweit haben sie in den letzten drei Jahren ein deutlich höheres Wachstum bei Umsatz und Beschäftigung zu verzeichnen als die Gegengruppe der computerisierten Unternehmen. Auch die Produktivität ist bei den digitalisierten Unternehmen deutlich stärker gestiegen.

Bislang sind allerdings die datenzentrierten Plattformen eher eine Ausnahme, obwohl darin die größten Potenziale liegen. Bei den bisher genutzten Plattformen handelt es sich meistens um eher niedrigschwellige Lösungen wie eigene Webshops. Die befragten Unternehmen geben als wesentliche Hemmnisse für eine intensivere Nutzung, insbesondere datenzentrierter Plattformen, Datenschutzfragen, Rechtsunsicherheiten und fehlende Standards an (näher siehe vbw Studie *Plattformen – Infrastruktur der Digitalisierung*).

Bei den sogenannten „Einhörnern“ – also Unternehmen mit einem Marktwert von mindestens einer Milliarde Dollar auf Basis bisheriger Investitionsrunden – beruhte Anfang 2020 bei rund 29 Prozent beziehungsweise 135 Unternehmen das Geschäftsmodell auf einer Plattform. Noch höher ist der Anteil dieser Unternehmen an der Gesamtbewertung mit rund 43 Prozent. Zu diesen großen Unternehmen gehören Google, Facebook, Amazon, Microsoft, Alibaba, Airbnb oder eBay. Die Plattformen finden sich überwiegend im B2C-Geschäft, also im Bereich Internetdienste, E-Commerce oder Finanzdienstleistungen. Knapp zwei Drittel dieser Unternehmen stammen aus Asien (hauptsächlich China), etwa 30 Prozent aus Amerika und nur knapp fünf Prozent aus Europa.

Großes Potenzial besteht noch im Bereich der Industrieplattformen. Diverse deutsche Unternehmen und viele internationale Wettbewerber bieten hier eigene Lösungen an. Bisher konnte sich allerdings noch keine davon deutlich von den Mitbewerbern absetzen und in den Bereich echter Größenvorteile gelangen.

3.2 Position der vbw

3.2.1 Unternehmen: Chancen erkennen und nutzen

Die digitale Transformation macht es erforderlich, dass sich jedes Unternehmen – nicht nur diejenigen, die bereits intensiv digitale Technologien für ihr Geschäft einsetzen – eine Digitalisierungsstrategie überlegt, zu deren Kernelementen eine Daten- und eine Wissensstrategie gehören.

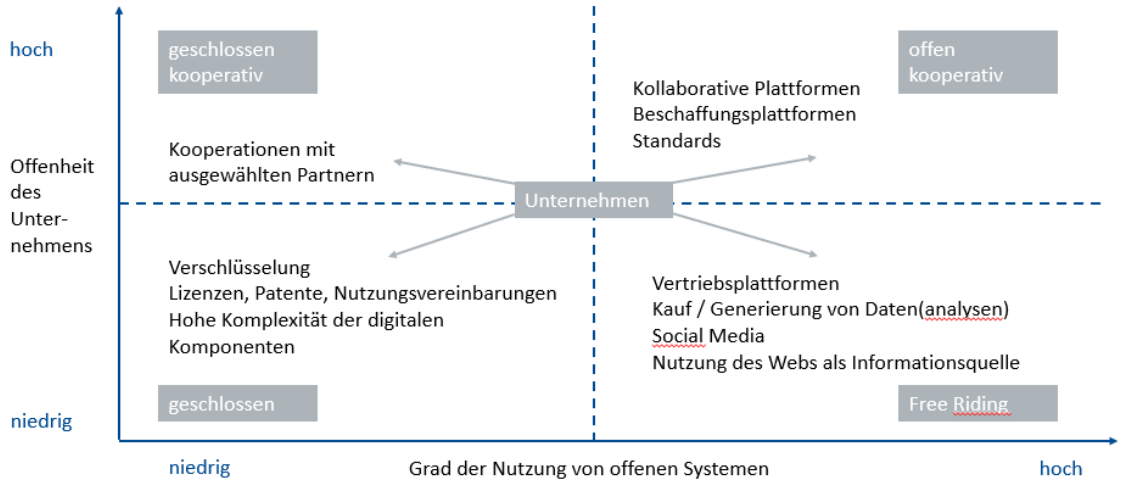
Jedes Unternehmen ist gefordert, seine Abläufe und Datenbestände beziehungsweise -zugriffsmöglichkeiten daraufhin zu analysieren, ob es noch relevante Potenziale brach liegen lässt. Speziell für die Herangehensweise im Bereich neuer (datengetriebener) Geschäftsmodelle enthalten die Handlungsempfehlungen des Zukunftsrats der Bayerischen Wirtschaft *TechCheck 2019. Technologien für den Menschen.* eine systematische Darstellung der zu beachtenden Aspekte – von der Analyse der Leistungsbeziehungen über mögliche Erlösmodelle bis zur Gestaltung des Angebots – und weiterführende Hinweise.

Erster Schritt ist dabei die systematische Erfassung der verfügbaren – eigenen und gegebenenfalls auch externen – Daten und Informationen. Das Vorgehen (Bestandsaufnahme, Potenzialabschätzung, Machbarkeitsanalyse sowie Erstellung eines darauf aufbauenden Konzepts) ist in *Zukunft digital – Big Data. Analyse und Handlungsempfehlungen.* näher beschrieben.

Für eine unternehmensinterne Ersteinschätzung der rechtlichen Risiken kann die Matrix Big Data und Recht dienen, die ebenfalls im Rahmen des Schwerpunktthemas *Big Data* des Zukunftsrats der Bayerischen Wirtschaft 2016 von Professor Dirk Heckmann entwickelt wurde und auch unter der DSGVO noch verwendet werden kann. Sie hat nicht alleine für Big Data-Anwendungen Gültigkeit, sondern ist auch für andere Fragen der Datennutzung von Interesse.

Darüber hinaus sollten Unternehmen auch prüfen, inwieweit das Teilen von Wissen (z. B. über Plattformlösungen, Open Innovation etc.) für sie von Vorteil sein kann.

Strategische Optionen im Hinblick auf das Teilen von Daten



Quelle: nach Twin Economics in vbw, Neue Wertschöpfung durch Digitalisierung, 2017

Im Hinblick auf die Nutzung offener Systeme und das Teilen eigener Daten gibt es kein pauschales Richtig oder Falsch. Die Vor- und Nachteile müssen individuell abgewogen werden. In *Neue Wertschöpfung durch Digitalisierung. Analyse und Handlungsempfehlungen.* ist das diesbezügliche Vorgehen näher beschrieben und die zugrundeliegende Studie enthält weitere Hinweise zur Bewertung von Wissen sowie zur Bestimmung des individuell passenden Grads an Offenheit.

3.2.2 Souverän agierende Verbraucher fördern

Verbraucher müssen sich mit der Bedeutung ihrer Daten und dem persönlich als richtig empfundenen Niveau an Transparenz oder Privatsphäre aktiv auseinandersetzen und Verantwortung für ihr Agieren in der digitalen Welt übernehmen. Die Stärkung dieser Souveränität beispielsweise mit entsprechenden Schulungen ist ein richtiger Ansatz.

Schutz vor Angriffen von außen und Systemsicherheit müssen bestmöglich gewährleistet werden, und missbräuchliches Verhalten von Unternehmen und Privatpersonen muss klar sanktioniert werden. Gleichzeitig muss sich jeder Beteiligte seiner Verantwortung bewusst sein. Die Regulierung zielt insgesamt zu sehr auf einzelne Unternehmen ab und scheint zu übersehen, dass es das typische „Machtgefälle“ zwischen Unternehmer und Verbraucher in der Datenwirtschaft nicht in gleicher Weise gibt: Auch der Einzelne hat eine beachtliches Macht- und Schädigungspotenzial. Fake News und Online-Bewertungen sind nur Beispiele dafür.

Teil dieser Verantwortung des Einzelnen ist auch die Einsicht, dass nicht alles, was ihm im Umgang mit Daten technisch *möglich* ist (Umgehung von Bezahlschranken, Download und Verbreitung urheberrechtlich geschützter Inhalte etc.), zugleich auch gesellschaftlich oder

rechtlich akzeptabel sein muss. Der Staat steht hier – namentlich über das Bildungssystem – vor der Aufgabe, den Bürgern das notwendige Rüstzeug für ein souveränes Handeln in der Datenwirtschaft an die Hand zu geben.

Gerade in den Anfangsjahren der massenhaften Nutzung des Internets erschien es vielen wie ein komplett rechtsfreier Raum. Das war noch nie richtig – wie beispielsweise im Fall der Musik-Tauschbörsen in der Folgezeit viele Gerichtsentscheidungen klargestellt haben – und das wird künftig nicht der Fall sein. Ein solcher rechtsfreier Raum ist auch nicht wünschenswert, wie sich am Beispiel der online vervielfältigten Raubkopien leicht nachvollziehen lässt: Wenn das nicht sanktioniert wird, fehlt es an einem Anreiz, hochwertige digitale (oder digitalisierbare) Inhalte überhaupt noch zu produzieren. Auch für die möglichen Folgen von (Be)Wertungen und Informationen in einer hochgradig vernetzten Welt muss möglichst frühzeitig sensibilisiert werden.

Während es in Teilen der Bevölkerung Misstrauen gegenüber der Datenwirtschaft und den darin agierenden Unternehmen gibt (siehe oben 1.5), ist ein – derzeit noch sehr kleiner – anderer Teil zu einem sehr viel weitgehenderen Einsatz der digitalen Version seiner persönlichen Daten bereit. Weltweit hat sich bereits eine sechsstellige Anzahl an Personen reiskorngroße Implantate einsetzen lassen, die beispielsweise für Zugangs- und Identifizierungsfunktionen im Rahmen von Smart-Home-Lösungen oder als Visitenkarte genutzt werden können. Auch wenn derartige *Smarte Implantate* in der Regel eine sehr geringe (Funk-)Reichweite haben und eine GPS-Ortung sehr aufwendig wäre, können grundsätzliche Sicherheitsbedenken und die Möglichkeit eines völligen Verlusts eines Teils der Privatsphäre nicht außer Acht gelassen werden. Hierüber gilt es ebenfalls aufzuklären, wenn der Markt weiter so rasant wächst.

Auf weitere Vorgaben zur Transparenz, insbesondere zusätzliche Informationspflichten, sollte nach Möglichkeit verzichtet werden. Es gibt Berechnungen, wonach die Lektüre jeder Datenschutzerklärung von allen besuchten Websites etwa 76 (Arbeits-)Tage à acht Stunden kosten würde. Tatsächlich führen immer umfangreichere Informationen im Ergebnis nur dazu, dass die meisten Verbraucher ungelesen Kenntnisnahme und Einverständnis bestätigen. Das ist auch nicht besonders unvernünftig – ähnlich wie generell im AGB-Recht ist das Schutzniveau derart hoch, dass sich der Verbraucher darauf verlassen kann, dass wirklich unangemessene beziehungsweise überraschende Klauseln ohnehin unwirksam wären.

Wenn in diesem Bereich neue Regulierung als notwendig erachtet würde, beispielsweise im Hinblick auf den Einsatz von KI, dann müsste umgekehrt darauf geachtet werden, die Informationspflichten so sehr auf das Wesentliche zu reduzieren, dass eine Kenntnisnahme und damit informierte Entscheidung des Verbrauchers realistisch ist.

Sehr zielführend wäre es, die Möglichkeiten der DSGVO (Art. 12 Abs. 7) auszuschöpfen und die relevanten Informationen (nach Art. 13 und 14 DSGVO) vorrangig über standardisierte Bildsymbole zu vermitteln. Damit lassen sich viele Informationspflichten erfüllen, beispielsweise hinsichtlich des Orts und Zwecks der Verarbeitung. Beispiele für eine grafische Umsetzung finden sich unter anderem im *PrimeLife* Projekt.

Piktografische Darstellung von Datenverarbeitungsoptionen

Under EC law
or equal protection

Not under EC law
or equal protection

Quelle: PrimeLife Projekt

Weiterführende Informationen

- Studie *Digitalisierung der bayerischen Wirtschaft*, vbw 2019
- Handlungsempfehlungen des Zukunftsrats *Resilienz. Schlussfolgerungen aus der Corona-Pandemie*., vbw, 2020
- Handlungsempfehlungen des Zukunftsrats *TechCheck 2019. Technologien für den Menschen.*, vbw 2019
- Studie *TechCheck 2019. Erfolgsfaktor Mensch.*, vbw 2019
- Studie *Neue Wertschöpfung durch Digitalisierung*, vbw 2017
- *Neue Wertschöpfung durch Digitalisierung. Analyse und Handlungsempfehlungen.*, Zukunftsrat der Bayerischen Wirtschaft, vbw 2017
- Studie *Daten als Wirtschaftsgut*, Prof. Dirk Heckmann, vbw 2018
- Studie *Plattformen – Infrastruktur der Digitalisierung*, vbw 2019
- Position *Künstliche Intelligenz*, vbw 2019

4 Rahmenbedingungen für die Datenwirtschaft

International wettbewerbsfähige Bedingungen für Spitzenleistungen

Die vorangehenden Ausführungen zeigen, dass die Chancen groß sind, die Lage allerdings vor allem im rechtlichen Bereich komplex ist. Der Vorsprung, den es auf die USA und Asien (namentlich China) aufzuholen gilt, ist jedenfalls im B2C-Bereich groß. Wir brauchen die richtigen Rahmenbedingungen am Standort, um eine weltweite Spitzenposition einnehmen und halten zu können.

4.1 Spezielle Rahmenbedingungen

4.1.1 Verfügbarkeit

4.1.1.1 Open Government Data

Open Data – insbesondere Open Government Data – ist ein wichtiger Katalysator für neue oder verbesserte Produkte und neue Geschäftsmodelle. Mit Steuergeldern erhobene Daten der öffentlichen Hand sind in aller Regel zu teilen und in einem zur Weiterverarbeitung geeigneten Format bereitzustellen. Dieser Grundsatz muss noch stärker in deutscher und europäischer Rechts- und Verwaltungspraxis verankert werden.

Auf der Grundidee von Open Data und Open Science basierende, von neutralen Intermediären (Staat, Wissenschaftseinrichtungen) gesteuerte Datenpools können gute Impulse setzen. Daneben muss es aber auch privatwirtschaftliche Angebote geben, die nicht von vornherein als weniger vertrauenswürdig etc. diskreditiert werden dürfen. Der Staat sollte sich deshalb auf besonders sensible Bereiche konzentrieren, etwa diejenigen, wo besonders intensiv personenbezogene oder personenbeziehbare Daten betroffen sind, wie im Bereich Gesundheit und Medizin (vgl. etwa den *Medical Data Space*).

4.1.1.2 Datenspenden

Mit dem Aufbau und der Förderung einer dezentralen Infrastruktur für freiwillig „gespendete“ (d. h. ohne konkrete Gegenleistung bereitgestellte) persönliche Daten würden Forschung und Wirtschaft in diesem Bereich gestärkt. Ein aktuelles Beispiel ist die Datenspende-App des Robert-Koch-Instituts (RKI): Wer ein Smartphone oder ein Fitnessarmband nutzt, kann bestimmte Daten – etwa zu Aktivität und Herzfrequenz sowie die eigene Postleitzahl – freiwillig mit dem RKI teilen. Eine Identifizierung der Person findet nicht statt. Algorithmen sollen Symptome erkennen, die mit einer Virusinfektion in Verbindung gebracht werden und den Wissenschaftlern zusätzliche Informationen zur Verbreitung des Virus liefern. Dem Nutzer selbst gibt diese App keine Rückmeldung. Den Erkenntnisgewinn

für die Wissenschaft könnte es noch einmal deutlich vergrößern und gegebenenfalls der Politik im Falle eines höheren Infektionsgeschehens ein zielgenaueres Eingreifen ermöglichen, wenn diese App auf freiwilliger Basis auch mit der Corona-Warn-App verknüpft werden könnte. Das ist aber nicht vorgesehen. Es sollte daher geprüft werden, ob nicht eine „Datenspende“ (z. B. für Studien zur Erforschung von Krankheitsbildern, Gesundheitsgefahren etc.) mit entsprechenden datenschutzrechtlichen Erleichterungen bei der späteren Nutzung der Daten (etwa für einen anderen als den ursprünglich angedachten Forschungszweck) als neuer Ansatz in die DSGVO eingeführt werden könnte.

4.1.2 Speicherung

4.1.2.1 Lokalisierung

Die im Mai 2018 in Kraft getretene DSGVO garantiert den freien Datenfluss personenbezogener Daten innerhalb des Binnenmarktes. Die Ende 2018 in Kraft getretene Verordnung über den freien Datenverkehr nicht-personenbezogener Daten (Free flow of data-Verordnung, (EU) 2018/1807) verpflichtet die Mitgliedstaaten zum Abbau von sogenannten Datenlokalisierungsauflagen. Das sind im Wesentlichen nationale Bestimmungen, die zur Verarbeitung nicht-personenbezogener Daten im Inland verpflichten und damit die Nutzung ausländischer Clouddienste verhindern. Echte Lokalisierungsauflagen gibt es ausweislich der dieser Regulierung zugrundeliegenden Untersuchung allerdings nur in sehr übersichtlicher Anzahl. Danach werden für Deutschland vier Stück aufgezählt, von denen gleich das erste Beispiel – Dokumentationspflichten nach der Musterberufsordnung für Ärzte – sich als fragwürdig erweist. Die MBO-Ä regelt nämlich in ihrem § 10 nur, dass Aufzeichnungen auf digitalen Speichermedien „besonderer Sicherungs- und Schutzmaßnahmen“ bedürfen, nicht aber, wo diese Speicherung zu erfolgen hat. Es geht bei der Dokumentation außerdem im Kern um Patientendaten, also personenbezogene Daten, auf die sich die Neuregelung gar nicht erstreckt. Ein Outsourcing, z. B. in eine Cloud, mag im Verhältnis Arzt-Patient rechtlich problematisch sein, aber aus anderen Gründen als den von der EU adressierten. Beispiele direkter Lokalisierungsauflagen werden nur ganz vereinzelt benannt, etwa für öffentliche Register in Kroatien, die nur in Datenzentren auf eigenem Staatsgebiet gespeichert werden dürfen. Die Umsetzung der Regelung wird also voraussichtlich aktuell keinen nennenswerten Effekt haben.

Bewertung der vbw

Trotzdem ist das Signal auch für die Zukunft richtig, wenn es im Rahmen der Vollendung des digitalen Binnenmarkts um die Schaffung eines Europäischen Datenraums auch als Gegengewicht zu großen internationalen Wettbewerbern geht. Weitreichende Lokalisierungsauflagen greifen etwa nach chinesischem Recht für in China gesammelte Daten. Hier kann das europäische Recht die Grundlage für entsprechende Reziprozitätsforderungen bilden.

4.1.2.2 Cloud-Lösungen

Die Bedeutung von Cloud-Lösungen wächst weltweit. Vorteile für Unternehmen bieten sie unter anderem durch die Vermeidung preisintensiver Managementtools, überflüssiger Hardwarestrukturen und überholter Vorgängersysteme sowie durch eine insgesamt deutlich höhere Flexibilität.

Bei den Cloud-Computing-Systemen, die mehrere Tausend bzw. Millionen Server miteinander zu einem Netzwerk verbinden und damit eine hohe Verfügbarkeit sowie Fehlertoleranz durch Redundanz gewährleisten, decken die drei großen Anbieter (sogenannte Hyperscaler) mit Amazon Web Services (AWS), Microsoft Azure und der Google Cloud Platform zusammen etwa 75 Prozent des Gesamtmarktes für Public Clouds ab. Viele insbesondere größere Unternehmen und öffentliche Einrichtungen nutzen mehrere davon. Marktführer mit rund 40 Prozent ist AWS, die inzwischen mehr als 90 verschiedene Dienste unter anderem aus den Bereichen Datenverarbeitung, Datenspeicherung, Künstliche Intelligenz und Internet der Dinge anbieten. In Deutschland ist Microsoft gerade im Mittelstand sehr stark vertreten.

Nicht zuletzt aufgrund der DSGVO haben die nationalen und europäischen Cloud-Angebote in letzter Zeit zugenommen.

- Die Bayerische Staatsregierung hat im Koalitionsvertrag zwischen CSU und Freien Wählern den Aufbau einer Bayern-Cloud angekündigt. Bisher ist daraus ein Forschungsvorhaben entstanden mit dem Ziel, zu ergründen, wie digitale Plattform-Ökosysteme gestaltet werden müssen, um kleine und mittelständische Unternehmen digital anzubinden und dabei mögliche Synergien zu heben. Im Rahmen des Projekts soll eine Referenzarchitektur entstehen; als Pilotdomäne dient die bayerische Tourismusindustrie.
- Der Bund betreibt unter anderem mit der mCloud eine eigene Lösung für Verkehrsdaten und will die Angebote im Bildungsbereich ausbauen. Die EU investiert ebenfalls in erheblichem Umfang in Cloud Computing-Technologien, rund 200 Millionen Euro seit 2014. Unter anderem wurde die Open Science Cloud aufgebaut, die es Forschern ermöglicht, Datensätze verschiedener in Europa tätiger Organisationen auszuwerten, um beispielsweise Umweltrisiken besser vorhersagen zu können.
- Seit 2016 bietet auch Microsoft den Cloud-Dienst *Azure* aus deutschen Rechenzentren an, die von der Telekom-Tochter T-Systems als Datentreuhänder verwaltet werden. Das Angebot soll vor allem Kunden aus Branchen mit besonders hohen Compliance-Anforderungen ansprechen, etwa den öffentlichen Sektor oder das Gesundheitswesen.

Bewertung vbw

Die staatlichen Ansätze sind sinnvoll, solange sie nicht auf Ausschließlichkeit setzen. Auch neue Lokalisierungstendenzen wären nicht sinnvoll. Es ist deshalb wichtig, dass Unternehmen und Verbrauchern grundsätzlich Wahlmöglichkeiten zur Verfügung stehen. „Regionalen“ Angebote sind auch deshalb grundsätzlich zu begrüßen, weil die Daten eben nicht nur körperlos in einer Wolke schweben, sondern auf Servern gespeichert sind, und damit im

physischen Einflussbereich eines Staates liegen und Rahmenbedingungen (z. B. Energieversorgung, Krisen etc.) ausgesetzt sind, auf die der Nutzer keinerlei Einfluss hat.

4.1.3 Europaweite Infrastruktur/GAIA-X

Mit GAIA-X soll nun der nächste große Schritt unternommen werden. Das Projekt wurde von der deutschen Bundesregierung unter Beteiligung von Vertretern aus Wirtschaft und Wissenschaft initiiert und soll dezentrale Infrastrukturdienste, insbesondere Cloud- und Edge-Instanzen, zu einem homogenen, nutzerfreundlichen System vernetzen. Die daraus entstehende Dateninfrastruktur soll sowohl die digitale Souveränität der Nachfrager von Cloud-Dienstleistungen als auch die Skalierungsfähigkeit und Wettbewerbsposition europäischer Cloud-Anbieter stärken. Ziele sind also eine europäische Cloud sowie der von Bundeswirtschaftsminister Altmeier angekündigte „KI-Airbus“. Bislang handelt es sich lediglich um ein Konzept, nicht um eine fertige Architektur.

GAIA-X: Vorgesehene technische Anforderungen laut BMWi/BMBF

- Datensouveränität im Sinne einer vollständigen Kontrolle über gespeicherte und verarbeitete Daten sowie die unabhängige Entscheidung darüber, wer darauf zugreifen darf.
- Einsatz nachvollziehbarer, sicherer, offener Technologien, unter anderem durch Einsatz von Open Source Grundsätzen, in einem offenen Ökosystem.
- Dezentrale beziehungsweise verteilte Datenverarbeitung über Multi-Edge, Multi-Cloud oder Edge-to-Cloud Verarbeitung für die Gewinnung von Verbundvorteilen.
- Interoperabilität sowohl hinsichtlich technischer und semantischer Standards als auch im Sinne einer Interkonnektivität auf Netzwerk-, Daten- und Dienstebene zwischen Edge- oder Cloudinstanzen.
- Unabhängige und automatisierbare Zertifizierung und Kontrahierung eines Teilnehmers am GAIA-X-Ökosystem bezüglich der Einhaltung des GAIA-X-Regelwerkes hinsichtlich IT-Sicherheit, Datensouveränität, Service Levels und Rahmenverträgen.
- Bereitstellung zentraler Dienste, die das Ökosystem für einen sicheren und anwendungsfreundlichen Betrieb benötigt (z. B. Authentifizierung).
- Selbstbeschreibende GAIA-X-Knoten zur Förderung der Transparenz, aber auch zur Schaffung neuer teilnehmerübergreifender Geschäfts- und Anwendungsmodelle (z. B. Daten- oder Dienstvermittlung).

Jeder Cloud-Anbieter könne mit der angedachten Technologie und einer geplanten Referenzarchitektur zum GAIA-X-Knoten werden. Diese Knoten sollen Rechenkapazitäten und Speicher bereitstellen, eindeutig identifizierbar sein sowie eine Selbstbeschreibung liefern (unter anderem Informationen zum angebotenen Dienst, Preismodell oder zertifizierten Schutzgraden). Ein zentraler Verzeichnisdienst soll Anwendern helfen, passende Anbieter und relevante Datenpools schnell und sicher zu identifizieren.

Für die Umsetzung wird eine zentrale, europäisch getragene Organisation als notwendig erachtet. Sie soll aus wirtschaftlicher, organisatorischer und technischer Sicht die neutrale Basis für eine vernetzte Dateninfrastruktur sein. Ihre Aufgabe wird sein, eine Referenzarchitektur zu entwickeln, Standards zu definieren sowie Kriterien für Zertifizierungen und Gütesiegel vorzugeben. Dabei könnte es sich um eine Europäische Genossenschaft (SCE) handeln, an der sich interessierte Partner beteiligen und einbringen. Ein Konkurrenzangebot zu den „Hyperscalern“ (siehe oben) wird ausdrücklich nicht angestrebt. Der Live-Betrieb soll noch im Jahr 2020 starten.

Bewertung der vbw

Es ist ein richtiger Ansatz, vorhandene Strukturen besser zu vernetzen und nutzbar zu machen. Das Vorgehen zielt aber stark darauf ab, den relativ einengenden Regularien in Europa noch größere Geltung zu verschaffen – europäischer Datenschutz wird gleich als erste Leitlinie genannt. Mindestens genauso wichtig wie eine europäische Infrastruktur ist aber ein innovationsfreundlicher europäischer Rechtsrahmen. Die mit dem Angebot angestrebte digitale Souveränität beschränkt sich im Wesentlichen darauf, die vollständige Kontrolle über die Daten und den Zugriff darauf zu erreichen. Das wird allerdings nicht ausreichen, da es nicht nur um eine „Lagerung“ oder eine Auslagerung von Verarbeitungsprozessen geht, sondern auch um die Anwendungen selbst, die den Unternehmen in der Cloud zur Verfügung stehen. So oder so ist auch angesichts des Vorsprungs der großen Anbieter wichtig, dass das System tatsächlich offen ist und international Partnerschaften statt neuen Konkurrenzsituationen aufzubauen versucht. Auf der Europäischen Ebene sollte sich mit der z. B. im Entwurf des *White Papers zur Künstlichen Intelligenz* geforderten Errichtung einer weltweit führenden Infrastruktur für KI und Daten auf Basis von vernetzten Höchstleistungsrechnern und Edge Computing (EuroHPC Joint Undertaking) ein passender Anknüpfungspunkt für GAIA-X ergeben.

Zentral ist bei der Umsetzung, dass das Angebot qualitativ am Markt bestehen kann und nicht hinter den heutigen Marktführern zurücksteht. Die noch zu errichtenden Strukturen müssen deshalb gewährleisten, dass agil nachgesteuert werden kann. Der Aufbau der entsprechenden Architektur muss in engster Zusammenarbeit mit der Wirtschaft erfolgen, um sowohl die erforderliche technische Expertise einzubinden als auch von Anfang an das System an den Bedürfnissen insbesondere der Industrie auszurichten.

Ein Start noch im laufenden Jahr erscheint sehr ambitioniert, da zahlreiche Fragen zu klären und technische Lösungen abzustimmen beziehungsweise zu entwickeln sind, beispielsweise zu Sicherheit, Support, Zugang und Finanzierung. Es erscheint angesichts des erheblichen Vorsprungs der US-amerikanischen Anbieter sinnvoll, sich zunächst auf einige besonders relevante Bereiche wie eine Infrastruktur für sensible Industriedaten zu fokussieren und sie unter Einbeziehung vorhandener Strukturen schnellstmöglich auf ein Level zu bringen, dass mit den Marktführern mithalten kann. Während wichtige Verbraucheranwendungen ohnehin auch künftig auf den US-amerikanischen Clouds stattfinden werden, weil von dort die relevantesten Angebote kommen, ist die Lage bei industriellen Anwendungen noch offener. So weist auch das Konzeptpapier darauf hin, dass

Industrieplattformen und neue B2B-Geschäftsmodelle gefördert werden müssen und GAIA-X hierfür eine Lösung anbieten soll, damit Unternehmen ihre Daten kontrolliert und vertrauensvoll teilen können.

Die Ausgestaltung muss auch auf die Bedürfnisse großer (Industrie)Unternehmen zugeschnitten werden. Die von den Autoren des Konzepts konstatierte Zurückhaltung des Mittelstands bei Cloud-Lösungen sollte nicht überbewertet werden und auch nicht dazu führen, sich speziell auf diese Zielgruppe auszurichten und größere beziehungsweise digital fortgeschrittenere Unternehmen außer Acht zu lassen, da die Architektur auch höchsten Ansprüchen entsprechen muss, wenn sie Bestand haben soll. Einer Umfrage von Ende 2018 zufolge nutzen bereits rund 20 Prozent der deutschen Mittelständler Cloud-Lösungen und 55 Prozent befanden sich in der Implementierungs- oder aktiven Vorbereitungsphase. Das ist nicht wenig, wenn man bedenkt, dass anspruchsvollere und insbesondere datenintensive Lösungen auch erst von wenig mehr als einem Fünftel aller deutschen Unternehmen eingesetzt werden (vgl. unter anderem die vbw Studie *Digitalisierung der bayerischen Wirtschaft*, Dezember 2019; auch unsere zweimal durchgeführten Umfragen bei bayme vbm zum Thema Big Data kommen zu ähnlichen Größenordnungen).

4.1.4 Übermittlung

Portabilität, Interoperabilität und entsprechende Standards sind wichtige Faktoren für das Gelingen einer datenbasierten Wirtschaft.

4.1.4.1 Portabilität

Wenn Daten nicht von einem Akteur auf den nächsten übertragen (Datenportabilität) beziehungsweise dort aus technischen Gründen nicht verarbeitet werden können (Kompatibilität), kann dies das ökonomische und gesellschaftliche Datenpotenzial empfindlich beeinträchtigen. Ein hohes Maß an Datenportabilität verhindert darüber hinaus Lock-In-Effekte und stimuliert den Wettbewerb zwischen digitalen Diensten.

Für den Bereich der personenbezogenen Daten enthält Art. 20 DSGVO bereits Vorschriften zugunsten der Verbraucher: Sie haben ein Recht auf Mitnahmebeziehungsweise direkter Übergabe ihrer personenbezogenen Daten von einem Anbieter auf einen anderen. Auch die Richtlinie für digitale Inhalte sieht so einen Anspruch vor.

Im Verhältnis zwischen Unternehmen beziehungsweise für reine Sachdaten ist gegenwärtig kein Bedarf an einer vergleichbaren Regelung erkennbar. Probleme, die jedenfalls in der Nähe eines Marktversagens gesehen werden können, wie sie im Bereich von Social Media (Lock-In-Effekte großer Plattformen wie Facebook) Grundlage des oben genannten gesetzgeberisches Handeln waren, sind im B2B-Bereich nicht ersichtlich. So ist etwa für Unternehmenskunden ein Wechsel des Cloud-Anbieters beziehungsweise die Mitnahme der dort gespeicherten Daten problemlos möglich und auch häufig Gegenstand der Cloud-Nutzung zugrundeliegenden Verträge.

4.1.4.2 Interoperabilität und Standards

Moderne IKT-Standards sind nicht nur auf klassische Computersysteme ausgerichtet, sondern bilden eine Referenzarchitektur für vernetzte Objekte. Es müssen hersteller- und gegebenenfalls auch industrieübergreifende Schnittstellenstandards – beispielsweise zwischen Werkzeug und Maschine – geschaffen werden, um die Kopplung verschiedener Systeme zu ermöglichen und die Datennutzung zu erleichtern beziehungsweise zur Verbesserung ihrer technischen und semantischen Auffindbarkeit (Strukturierung) und Interoperabilität beizutragen. Diese Aufgabe muss die Industrie in bewährter Weise übernehmen, wobei auch der Mittelstand einzubeziehen ist. Sinnvoll ist die Förderung entsprechender Forschungsprojekte durch die EU. In Deutschland ist zu prüfen, inwieweit die Asymmetrie der staatlichen Unterstützung bei der Normungsarbeit ausgeglichen werden sollte, die sich daraus ergibt, dass in Deutschland der Aufwand üblicherweise von den Unternehmen getragen wird, während sich dies im Ausland teilweise anders darstellt. Gerade eine Unterstützung des unternehmerischen Mittelstands bei der Normungsarbeit wäre sinnvoll.

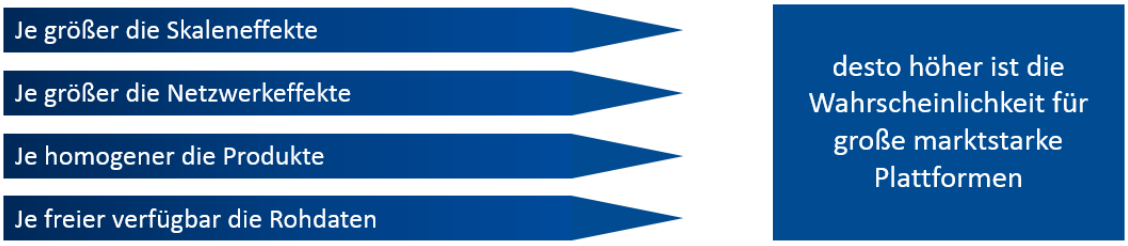
Standardisierungsvorhaben aus der Wirtschaft heraus müssen immer Vorrang haben. Nur ein Beispiel unter vielen ist der Bereich des automatisierten und autonomen Fahrens. Hier haben zahlreiche Unternehmen auf verschiedenen Ebenen der Wertschöpfungskette sich über Konzepte sowohl für den Zugang zu Daten und die entsprechenden Schnittstellen als auch über die zu gewährleistenden Sicherheitsanforderungen verständigt beziehungsweise arbeiten fortlaufend daran (*NEVADA*-Konzept, *Safety First For Automated Driving*). Diese Ansätze müssen der europäische und nationale Gesetzgeber flankieren, keinesfalls aber mit eigener Detailregulierung konterkarieren.

4.1.5 Entstehung und Nutzung von Plattformen fördern

Die zentrale Bedeutung wurde oben bereits skizziert, ebenso wie die noch ausbaufähige Nutzung und Schaffung eigener datenzentrierter Infrastrukturen.

Wichtig ist, dass die Rahmenbedingungen Wachstum von Plattformen grundsätzlich fördern und nicht behindern. Generell muss darauf geachtet werden, Plattformen nicht über einen Kamm zu scheren und insbesondere Industrieplattformen nicht „versehentlich“ mit zu regulieren. Hier ist schon die Informationsasymmetrie vollkommen unterschiedlich, ebenso das Schutzbedürfnis der Kunden. Die Sorge vor monopolartigen Strukturen darf gerade für Industrieplattformen keine überschießende Regulierung auslösen. In diesem komplexen, spezialisierten und wissensintensiven Umfeld ist das Entstehen von Monopolen und massiven Skaleneffekten eher nicht zu erwarten. Zudem befinden sich viele europäische Industrie-Plattformen noch in der Investitionsphase.

Erfolgsfaktoren von Plattformen



Beim Datenschutz ist darauf zu achten, dass durch einen zu restriktiven Schutz von personenbeziehbaren Daten im Umfeld von Maschinen- und Prozessdaten nicht die Digitalisierung in den Unternehmen gebremst wird. Die Maßstäbe für die Personenbeziehbarkeit müssen rechtssicher und praxisgerecht – das heißt vor allem nicht zu streng – ausgestaltet werden.

Auch Datenpools oder Datenkooperationen können unter das kartellrechtliche Kooperationsverbot fallen, wobei es nicht auf eine konkrete Vereinbarung oder eine direkte Abstimmung ankommt. Die Grenzen sind gegenwärtig zu unscharf formuliert, das Risiko für die Unternehmen – die das Vorliegen von Freistellungsvoraussetzungen nach europäischem wie nach nationalem Recht selbst einschätzen müssen – angesichts der drastischen Sanktionen bei Verstößen dementsprechend hoch. Schwierig ist unter anderem die Bestimmung des Adressatenkreises des Verbots, da sich Geschäftsmodelle im Rahmen der Datenwirtschaft teilweise schnell und relativ tiefgreifend ändern und bestehende Wettbewerbsverhältnisse nicht unbedingt ohne weiteres erkennbar sind. Das Risiko lässt sich zwar verringern, wenn die Daten um (potenziell) strategische Informationen bereinigt werden, das erhöht aber wiederum den Aufwand und senkt die Menge der zur Verfügung stehenden Daten. Um Kooperationen und das Teilen von Daten zwischen Unternehmen zu fördern, muss der Gesetzgeber durch klarstellende Regelungen im Kartellrecht größere Rechtssicherheit schaffen. Auch mit der 10. GWB-Novelle ist dieser Punkt noch nicht erledigt.

Auch im B2C-Bereich ist es wünschenswert, starke deutsche beziehungsweise europäische Plattformen zu unterstützen. Selbst wenn dabei vorübergehend eine Marktmacht entstehen würde, bleibt sie doch immer bestreitbar und unterliegt zugleich einer klaren Regulierung.

Am 12. Juli 2020 ist die *Verordnung (EU) 2019/1150 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten* (Platform-to-Business-Verordnung, P2B) in Kraft getreten. Erfasst werden Online-Marktplätze für den elektronischen Geschäftsverkehr, Online-Vertriebsplattformen für Software-Anwendungen, soziale Netzwerke und Suchmaschinen, also beispielsweise Google oder Booking ebenso wie Facebook und Ebay, sofern sie Vermittlungstätigkeiten innerhalb der EU durchführen, unabhängig von der geografischen Zuordnung der Plattform. Erfasst werden lediglich Plattformen, bei denen es um direkte Transaktionen zwischen gewerblichen Nutzern und Verbrauchern

geht, nicht aber reine Business-to-Business-Plattformen oder Peer-to-Peer-Vermittlungsdienste.

Kern des Entwurfs sind Transparenzpflichten, die von Plattform-Betreibern gegenüber ihren gewerblichen Nutzern einzuhalten sind. Diese sollen angesichts ihrer Abhängigkeit von den Plattformen vor möglichen schädlichen Handelspraktiken geschützt werden. Online-Vermittlungsdienste müssen, ebenso wie die Betreiber von Online-Suchmaschinen, insbesondere zukünftig die bestimmenden Hauptparameter ihrer Rankings offenlegen. Bieten die Online-Vermittlungsdienste auch eigene Waren und Dienstleistungen an, müssen sie darlegen, inwiefern sie eigene Angebote beziehungsweise Angebote der von ihnen beherrschten Unternehmen gegenüber Angeboten der Nutzer differenziert behandeln.

Gut ist, dass die EU hier auf Transparenz setzt, aber keine zusätzlichen einengenden Vorgaben zu zulässigen Geschäftspraktiken macht. An diesem Prinzip muss auch für weitere Regulierungsschritte festgehalten werden.

4.1.6 IT-Sicherheit

In den vergangenen Jahren haben sich die wirtschaftlichen Schäden aufgrund von IT-Sicherheitsvorfällen gehäuft. Tendenziell wächst mit der Bedeutung der Datenwirtschaft auch die Angriffsfläche, solange die Schutzvorrichtungen in den Unternehmen nicht (annähernd) mit der Entwicklung der internationalen Cyber-Kriminalität Schritt halten können. Das gesetzlich vorgesehene Sicherheitsniveau ist jedenfalls für die ausdrücklich erfassten Sektoren durchaus hoch, es sind aber neben regulativen Vorgaben auch konkrete Hilfestellungen notwendig, damit diesen Anforderungen auch in der Breite entsprochen werden kann.

4.1.6.1 Aktuelle Regulierungsbestrebungen

Wesentliche Normen sind auf europäischer Ebene die *Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union* und die *VO (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit*. Auf nationaler Ebene regelt seit 2015 das erste Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) die Gewährleistung von Cyber-Sicherheit. Ergänzt wurde es durch die BSI-Kritisverordnung und die Umsetzung der NIS-Richtlinie.

Die Kommission führt seit dem Sommer 2020 eine Konsultation zur Revision der NIS-Richtlinie durch. Das IT-Sicherheitsgesetz soll ebenfalls novelliert werden; im Mai 2020 hat das BMVI einen neuen Referentenentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetzes 2.0) vorgelegt.

Kernelemente des IT-Sicherheitsgesetzes 2.0

- deutliche Ausweitung der Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI), das unter anderem anlasslos alle IT-Produkte – auch noch in der Entwicklung befindliche – überprüfen dürfen und systematisch im Internet nach ungesicherten Computern suchen können soll, sowie gegenüber Providern in bestimmten Fällen Cyberabwehrmaßnahmen anordnen kann,
- Erweiterung des Kreises der Unternehmen mit besonderen Betreiberpflichten auf Rüstungs-, Raumfahrt- und IT-Sicherheitsunternehmen, Chemieunternehmen und Unternehmen, die „aufgrund ihrer volkswirtschaftlichen Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichen Interesse sind“,
- Regeln zur Verantwortung der Hersteller von IT-Produkten (freiwilliges IT-Sicherheitskennzeichen mit Überprüfung durch das BSI sowie Möglichkeit zur Überprüfung der Vertrauenswürdigkeit des Herstellers kritischer Komponenten und Untersagung des Einsatzes),
- signifikante Erhöhung von Bußgeldern auf bis zu 20 Millionen Euro oder vier Prozent vom weltweiten Jahresumsatz (bisher: 100.000 Euro).

4.1.6.2 Bewertung der vbw

IT-Sicherheit ist keine rein nationale Angelegenheit, und eine Harmonisierung im Binnenmarkt sowohl unter Sicherheits- als auch unter Wettbewerbsaspekten sinnvoll. Die Kommission führt seit dem Sommer 2020 eine Konsultation zur Revision der NIS-Richtlinie durch. In diesem Rahmen sollte die europaweite Harmonisierung von Anforderungen an die Wahrung und Stärkung der Cyberresilienz von Unternehmen, Produkten, Services und Infrastrukturen angestrebt werden. Nationale Alleingänge sollten vermieden und der Ausgang des europäischen Prozesses abgewartet werden, um einerseits Doppelregulierung zu vermeiden und andererseits nicht innerhalb kurzer Zeit die Anforderungen mehrfach anzupassen.

Die Überarbeitung des IT-Sicherheitsgesetzes sollte dann in erster Linie genutzt werden, um in Ergänzung zum EU-Rechtsrahmen den deutschen Unternehmen und namentlich der mittelständischen Industrie wirksame Hilfestellungen auf dem Weg zu einem höheren Schutzniveau zu bieten. Sinnvoll wäre ferner die Definition messbarer Sicherheitsziele und entsprechender Indikatoren, um die Lage der IT-Sicherheit in Deutschland fortlaufend zu evaluieren.

Auf die massive Erhöhung der nationalen Bußgelder sollte verzichtet werden, da anderenfalls eine Kumulierung von Bußgeldern droht, wenn Vorfälle zugleich DSGVO-relevant sind, und ohnehin schon finanziell betroffene Unternehmen massiv zusätzlich belastet werden könnten.

Insgesamt sollte eher ein kooperativer als ein repressiver Ansatz verfolgt werden, der auf die proaktive Unterstützung durch die Unternehmen setzt. Entsprechende Anreizelemente

fehlen jedoch im Entwurf des IT-Sicherheitsgesetz 2.0, etwa Haftungsreduzierungen für überdurchschnittliche Anstrengungen oder ein Rechtsrahmen für Selbstregulierung und Selbstkontrolle. Einziges Element ist das freiwillige Sicherheitskennzeichen – hier ist allerdings der vorgesehene Prozess sehr bürokratisch und es wurde bisher nicht deutlich, warum es neben dem freiwilligen europäischen Cybersicherheits-Zertifikat erforderlich ist.

IT-Sicherheit und Datenschutz müssen letztlich in ihrem Zusammenspiel betrachtet werden. Während nicht jede Verbesserung der IT-Sicherheit den Zielen des Datenschutzes entspricht, ist ohne IT-Sicherheit die Vertraulichkeit der Daten stark gefährdet. Auf europäischer Ebene soll dieser Konflikt dadurch gelöst werden, dass die ENISA die DSGVO mit einbezieht, die europäische Datenschutzbehörde bei deren Leitlinienerstellung berät, vor allem im Hinblick auf technische Details, und Meldungen zu Datenschutzverletzungen und Cybersicherheits-Attacken sowie Empfehlungen dazu bündelt. Ein solcher Gleichlauf muss dementsprechend auch national gewährleistet werden.

4.1.7 Fachkräftesicherung, Ausbildung

An den Hochschulen müssen Studiengänge wie Data Scientist oder Data Analyst weiter gestärkt werden. Die Maßnahmen der Hightech Agenda Bayern – unter anderem werden 100 Professuren für Künstliche Intelligenz eingerichtet – können hier einen wichtigen Beitrag leisten und sind zügig umzusetzen; bundesweit sind vergleichbare Schritte wünschenswert.

Auch in anderen Studiengängen, beispielsweise den Ingenieurswissenschaften, muss ein Grundwissen nicht nur über IT, sondern auch die Besonderheiten der Datenwirtschaft vermittelt werden, um eine Basis für mögliche neue Geschäftsmodelle zu legen, die physische Produkte und Daten verbinden.

4.1.8 Forschung und Entwicklung für die Datenwirtschaft

Das im Finanzpaket für das zukünftige EU-Forschungsrahmenprogramm Horizon Europe vorgesehene Gesamtbudget bleibt mit 80,9 Milliarden Euro für die Laufzeit 2021 bis 2027 deutlich hinter den Erwartungen zurück; notwendig wäre mindestens das Anderthalbfache dieser Summe. Hier muss dringend nachgebessert werden, um den Anschluss an die führenden Standorte (siehe Kapitel 3) nicht zu verlieren und die Konjunktur in den Mitgliedstaaten nachhaltig anzukurbeln. Gerade die Datenwirtschaft muss gefördert werden, weil Unternehmen jeder Größenordnung und Branche eine Beteiligung an digitaler Wertschöpfung und damit dem Wachstumsbereich schlechthin ermöglicht. Wichtig wären auch eine (temporäre) Erhöhung der Förderquoten, um der zu beobachtenden Reduktion der Forschungsbudgets entgegenzuwirken, sowie eine möglichst unbürokratische Antragsstellung.

Auf nationaler Ebene müssen vor allem die Rahmenbedingungen für Start-ups verbessert werden, die wichtige Treiber der Datenwirtschaft sind. Im Forschungsbereich sollte sich die Förderung auf die zentralen Digitalisierungstechnologien sowie die Schnittstellen zu

den sonstigen bayerischen beziehungsweise deutschen Zukunftstechnologien fokussieren und beispielsweise Technologiefelder wie Künstliche Intelligenz und Quantencomputing ebenso konsequent besetzen, wie autonome Mobilität und intelligente Stromnetze. Mindestens ebenso wichtig ist es speziell für die Förderung der Datenwirtschaft, etablierte und marktreife Technologien in die Breite zu tragen. Dafür ist in erster Linie das bestehende Instrumentarium zu nutzen und so weiterzuentwickeln, dass es für Unternehmen pragmatisch und unbürokratisch nutzbar wird.

Die Forschungsbudgets müssen sinnvollerweise durch Pilotprojekte ergänzt werden, auch um den Wissenstransfer in die Wirtschaft zu verbessern. Zwei Beispiel von vielen sind die Blockchain-Technologie und Projekte aus den Bereichen 3D-Visualisierung und 3D-Simulation. Das Potenzial ist unbestritten in beiden Fällen groß, aber die „Killer-Applikation“ als Anreiz für einen echten Breiteneinsatz fehlt, und vielen Unternehmen ist der konkrete Nutzen noch unklar. Der Freistaat Bayern verfolgt hier grundsätzlich den richtigen Ansatz, gerade auch mit der Prüfung von Einsatzgebieten in der öffentlichen Verwaltung für die Blockchain (z. B. Dokumentation der rechtlichen Gültigkeit digitaler Dokumente), allerdings mit einem zu bescheidenen Mitteleinsatz jedenfalls bei den 3D-Technologien.

4.1.9 Nachhaltigkeit

4.1.9.1 CDR und digitale Nachhaltigkeit

Über gesetzliche Anforderungen hinaus geht das Konzept der *Corporate Digital Responsibility* (CDR). Darunter versteht man die unternehmerische Verantwortung zum (ökonomisch, ökologisch und sozial) nachhaltigen Wirtschaften auch im digitalen Bereich. Abgeleitet ist der Begriff von dem bereits länger gebräuchlichen Corporate Social Responsibility (CSR). Inhaltlich geht es dabei um ungleich verteilte Chancen (etwa digitale Kompetenzen) und Risiken beispielsweise durch fehlende Kontrolle über die Nutzung von Daten sowie den ökologischen Fußabdruck digitaler Technologien.

Verwandt, aber nicht deckungsgleich ist das Konzept der digitalen Nachhaltigkeit, das sich mit der langfristig und auf die Maximierung des gesellschaftlichen Nutzens ausgerichteten Herstellung und Weiterentwicklung (immaterieller) digitaler Güter befasst.

Eigenschaften eines nachhaltigen digitalen Guts

- Qualitativ ausgereift (z. B. Software)
- Transparente Strukturen (z. B. offener Quellcode)
- Verknüpfung mit semantischen Daten für die maschinelle Weiterverarbeitung
- Speicherung an verschiedenen/verteilten Standorten
- Freie Lizenzen (z. B. Open Data, Open Access)
- Geteiltes Wissen (Know-how auf möglichst viele Menschen in unterschiedlichen Organisationen verteilt)

- Partizipationskultur bei der Erweiterung und Weiterentwicklung des digitalen Guts (wie beispielsweise Peer Review-Prozesse zur Qualitätssicherung)
- Faire Führungsstrukturen (Kontrolle liegt nicht bei einer einzelnen Person oder Organisation)
- Breit abgestützte Finanzierung der notwendigen Ressourcen (Infrastruktur wie Server, Personal etc.)
- Beitrag zur nachhaltigen Entwicklung (positive ökologische, soziale und ökonomische Wirkung, eingesetzte Ressourcen sind nachhaltig): Dieser Teilaspekt entspricht am ehesten der Idee von CDR.

Teilweise wird auch gefordert, dass sich staatliche Digitalisierungspolitik generell an diesen Vorstellungen ausrichten muss.

Bewertung der vbw

Vieles davon ist wünschenswert und es gibt eine Reihe von Vorbildern aus der digitalen Wirtschaft (z. B. Wikipedia, Linux). Das rechtfertigt aber noch keine Eingriffe in unternehmerische Freiheit und vermögenswerte Rechte; eine erzwungene Vergemeinschaftung darf es auch im digitalen Bereich nicht geben. CDR ist bereits vom Grundsatz her eine freiwillige Leistung des Unternehmens. Auch digitale Nachhaltigkeit kann aber nur auf Freiwilligkeit beruhen.

Verschiedene Aspekte der Nachhaltigkeit im oben genannten Sinn berücksichtigen Unternehmen schon im eigenen Interesse, beispielsweise um das Innovationspotenzial Dritter zu nutzen, Vertrauen in der Gesellschaft beziehungsweise beim Kunden aufzubauen und Risiken zu reduzieren. Auch abweichende Entscheidungen etwa zum Thema verteilte Kontrolle vs. Bündelung müssen aber gesellschaftlich akzeptiert werden. Die Diskussion über Verteilungsgerechtigkeit darf vor allem nicht außer Acht lassen, dass digitale Technologien per se einen erheblichen Beitrag zur sozialen Dimension der Nachhaltigkeit leisten. Ein wichtiges Beispiel ist der einfache und kostengünstige Zugang zu Wissen und Bildung: Eine Internetverbindung genügt heute, um von praktisch jedem Ort aus sofort auf wichtige Informationen zugreifen zu können, die noch vor gut zwei Jahrzehnten einem exklusiven Kreis an einem bestimmten Ort zugänglich waren. Ein weiterer wichtiger Effekt sind die Fortschritte, die in der Medizin durch den Einsatz digitaler Technologien möglich werden.

Nachhaltigkeit im oben genannten Sinn darf auch nicht zur Voraussetzung für Förderung oder Finanzierung gemacht werden (z. B. im Rahmen von Sustainable Finance). Wenn beispielsweise eine bestimmte Anwendung eine deutliche Reduktion des CO_2-Ausstoßes ermöglicht, wäre es mehr als kontraproduktiv, sie nicht zu nutzen, weil die Lizenzen kostenpflichtig sind. Das sollte vielmehr Ansporn sein, Vergleichbares oder Besseres den obigen Kriterien entsprechend als alternatives Angebot zu entwickeln. Plattformen für eine freiwillige Selbstverpflichtung beziehungsweise den entsprechenden Kompetenzaufbau bieten etwa die *Charta digitale Vernetzung* oder die Kompetenzplattform für

Nachhaltigkeit und Digitalisierung im Mittelstand nachhaltig.digital. Auch die Themenplattform Verbraucherbelange in der Digitalisierung des Zentrum Digitalisierung.Bayern (mittlerweile bei der Bayern Innovativ GmbH) arbeitet an entsprechenden Angeboten.

4.1.9.2 Position der vbw: Potenziale der Digitalisierung für Nachhaltigkeit heben

Die Potenziale digitaler Technologien im Bereich der Nachhaltigkeit – insbesondere in ihrer ökologischen Dimension – müssen umfassend gehoben werden. Digitale Technologien können erhebliche positive ökologische Effekte auslösen. Allgemein erhöhen digitale Tools die Effizienz von Prozessen, quer durch alle Branchen, und helfen damit, Ressourcen zu sparen. Eine intelligente Datennutzung in Kombination mit der Vernetzung und Automatisierung von Prozessen ermöglicht beispielsweise eine bessere Steuerung und Auslastung von Produktionsanlagen sowie die deutliche Reduzierung von Ausschuss. In der Logistik können Wege optimiert werden, in der Landwirtschaft sind ein höchst präziser Einsatz von Düngemitteln und die laufende Überwachung der Bodenqualität möglich.

Beispiel Energie und Klima

Digitale Technologien als „Enabler“ energietechnischer Innovationen können auch für den Klimaschutz nutzbar gemacht werden. Die Etablierung von intelligenten Messsystemen (Smart Meter) und damit einhergehende Transparenz und Steuerungsmöglichkeiten, die stärkere Synchronisation von Verbrauch und Erzeugung vor allem bei industriellen Stromnutzern oder die intelligente Verknüpfung von Sektoren können sich sehr positiv auf eine effiziente Nutzung von Energie und damit eine Verringerung der CO_2-Emissionen auswirken. Eine Studie („Smarter 2030“) der Global e-Sustainability Initiative (GeSI) geht davon aus, dass IKT-Technologien die globalen CO_2-Emissionen bis 2030 gegenüber jetzigen Prognosen um 20 Prozent senken.

Gleichzeitig sind viele IT-Prozesse sehr energieintensiv. Der Energieverbrauch für eine einzelne Bitcoin-Transaktion (die heute schon in etwa dem monatlichen Strombedarf eines Durchschnittshaushalts entspricht) mag für die meisten Verbraucher ein exotisches Beispiel sein – für die Kühlung der großen Server, auf denen unsere alltäglichen Anwendungen laufen, und den Strom für unsere Smartphones arbeiten aber in jedem entwickelten Staat viele Großkraftwerke. Mit zunehmendem Einsatz von Industrie- und Servicerobotern gewinnt das Thema weiter an Bedeutung. Unter dem Stichwort Green IT wird daher diskutiert, wie IKT-Technologien ressourcen- und klimaschonend eingesetzt werden können. Forschung und Entwicklung muss deshalb Energieeffizienz und Nachhaltigkeit von Anfang an mitbedenken. Der Staat muss auf allen Ebenen – EU, Bund, Land – seine Förderprogramme darauf ausrichten. Spezifische Programme zu Nachhaltigkeit beziehungsweise Klimaschutz durch Digitalisierungstechnologien sind bisher nicht vorgesehen. Das wäre insbesondere für die Agentur für Sprunginnovationen eine sinnvolle Mission. Immerhin wurde dort inzwischen ein Pilotinitiativwettbewerb zum Thema energieeffizientes

KI-System durchgeführt, und das Projekt „Analogrechner auf einem Chip“ adressiert das Problem der Energieeffizienz.

Im Rahmen des diesjährigen Schwerpunktthemas des Zukunftsrats der Bayerischen Wirtschaft *Klima 2030. Nachhaltige Innovationen.* werden diese Aspekte weiter vertieft.

Weiterführende Informationen

- Handlungsempfehlungen des Zukunftsrats *Resilienz. Schlussfolgerungen aus der Corona-Pandemie*., vbw, 2020
- Handlungsempfehlungen des Zukunftsrats *TechCheck 2019. Technologien für den Menschen.*, vbw 2019
- Studie *TechCheck 2019. Erfolgsfaktor Mensch.*, vbw 2019
- Studie *Neue Wertschöpfung durch Digitalisierung*, vbw 2017
- *Neue Wertschöpfung durch Digitalisierung. Analyse und Handlungsempfehlungen.*, Zukunftsrat der Bayerischen Wirtschaft, vbw 2017
- Studie *Daten als Wirtschaftsgut*, Prof. Dirk Heckmann, vbw 2018
- Studie *Plattformen – Infrastruktur der Digitalisierung*, vbw 2019
- Position *Künstliche Intelligenz*, vbw 2019

4.2 Allgemeine Rahmenbedingungen

Neben den spezifischen Anforderungen für eine funktionierende Datenwirtschaft müssen auch diverse weitere Rahmenbedingungen für die digitale Transformation insgesamt, wie auch für jedes erfolgreiches Wirtschaften am Standort stimmen.

Sie werden bereits in verschiedenen anderen Papieren der vbw vertieft, so dass sie hier nur aufgezählt werden sollen:

- leistungsfähige, flächendeckende Breitbandverbindungen,
- Forschungsförderung mit besonderem Fokus auf digitale Zukunftstechnologien einschließlich der dafür notwendigen Infrastruktur (Kapazitätsentwicklung in Bereichen wie Rechenzentren, Hochleistungsrechnern und Edge Computing),
- Wissenstransfer in die Wirtschaft, vor allem Vermittlung von Handlungskompetenz und Informationen über konkrete Einsatzmöglichkeiten
- Gründerförderung einschließlich eines besseren Zugangs zu Wagnis- und Wachtumskapital,
- Unterstützung von Unternehmen in der digitalen Transformation,
- Fachkräftesicherung, Qualifizierung und digitale Bildung,
- modernes Arbeitsrecht für die Arbeitswelt 4.0,
- E-Government, digitale Verwaltungsleistungen und Open Data,
- stabile und bezahlbare Energieversorgung,

– eine Flexibilisierung des beihilfe- und förderrechtlichen Rahmens auf der EU-Ebene, jedenfalls zeitlich befristet zur Überwindung der Wirtschaftskrise
– keine nationale oder europäische Digitalsteuer,
– innovationsfreundliches Steuerrecht.

Weiterführende Informationen

– *Studie Breitbandbedarf leitungsgebunden und mobil der bayerischen Unternehmen 2020, vbw 2020*
– Studie *Versorgungsgrad der digitalen Infrastruktur 2020 in Bayern*, vbw 2020
– Positionspapier *Digitale Netze: Ausbauerfolge und weiter notwendige Impulse, vbw 2019*
– Positionspapier *Der Mensch in der Digitalen Arbeitswelt*, vbw 2019
– Studie *8. Monitoring der Energiewende*, Prognos 2020
– Positionspapier *Digitalisierung in der Energiewirtschaft*, vbw 2018
– Information *Horizon Europe – das neue Forschungsrahmenprogramm der EU*, vbw 2020
– Studie Gesundheit und Medizin, vbw 2018
– Position Steuerpolitik – Gerecht, für Wachstum und Chancen, vbw 2019
– Position Klimapolitik, vbw 2020
– Handlungsempfehlungen des Zukunftsrats *TechCheck 2019. Technologien für den Menschen.*, vbw 2019
– Studie *TechCheck 2019. Erfolgsfaktor Mensch.*, vbw 2019
– Handlungsempfehlungen des Zukunftsrats *Resilienz. Schlussfolgerungen aus der Corona-Pandemie.,* vbw, 2020

5 Fazit zu den aktuellen Datenstrategien Bund und EU

Bewertung im Lichte der vorstehenden Überlegungen

Die Europäische Kommission hat im Januar 2017 eine Mitteilung zum Aufbau einer europäischen Datenwirtschaft veröffentlicht. Die Initiative ist Teil der Strategie für einen Digitalen Binnenmarkt und umfasst eine Reihe von Maßnahmen, um die Verfügbarkeit und Nutzbarkeit von Daten im Binnenmarkt zu steigern. Darunter fallen auch der freie Datenverkehr nicht-personenbezogener Daten sowie der Ausbau von offen zugänglichen Datenquellen (Open Data). Ziel der EU ist es, das gesamt-gesellschaftliche und ökonomische Potenzial von Datennutzung auszuschöpfen.

Am 19. Februar 2020 hat die EU ein White Paper zur Künstlichen Intelligenz und den Entwurf einer Datenstrategie vorgelegt. Begleitend hat die EU ihre Digitalstrategie („Gestaltung der digitalen Zukunft Europas“) noch einmal verdichtet dargestellt.

Der Bund hat bereits im November 2019 Eckpunkte einer Datenstrategie formuliert und diese Ende Februar 2020 zur Konsultation gestellt. Bis zum Sommer sollte daraus eine Datenstrategie entwickelt werden. Zum Zeitpunkt der Erstellung dieses Dokument liegt sie noch nicht vor.

5.1 EU

Die Digitalstrategie benennt drei große Aktionsbereiche:

- Technologie im Dienste des Menschen: unter anderem digitale Kompetenzen in der Gesellschaft, Schutz vor Cyber-Gefahren, Ausbau von Breitband und Hochleistungsrechenkapazitäten.
  Hier ist auch die KI-Strategie verankert.
- Eine faire und wettbewerbsfähige digitale Wirtschaft: unter anderem Förderung von Start-ups und KMU.
  Hier sind die Datenstrategie und weitere mögliche Regulierungsansätze (Rechtsakt über digitale Dienste etc.) verankert.
- Eine offene, demokratische und nachhaltige Gesellschaft: unter anderem Nutzung digitaler Technologien für das Erreichen der Klimaziele, Stärkung der Handlungsfähigkeit der Bürger bei Kontrolle/Schutz ihrer Daten.

Das Weißbuch zur Künstlichen Intelligenz und die Europäische Datenstrategie sind aus Sicht der Kommission die ersten Säulen dieser neuen Digitalstrategie.

5.1.1 Datenstrategie

Das Ziel der Strategie besteht in der Schaffung eines echten Binnenmarkts für Daten, in dem personenbezogene und andere Daten sicher sind, und Unternehmen und Behörden leicht auf große Datenmengen von hoher Qualität zugreifen können, um kreativ und innovativ tätig zu werden. Die bestehenden Datenschutzvorschriften (DSGVO) sollen uneingeschränkt weitergelten und eingehalten werden. Behörden sollen noch deutlich mehr Daten zur Verfügung stellen (Open Data), aber auch Unternehmen. Einerseits betont die Kommission, dass Unternehmen gemeinsame Normen und klare Regeln dafür benötigen, wie Daten weitergegeben werden, andererseits sollen die Unternehmen frei darüber entscheiden können, wem und unter welchen Bedingungen Zugang zu ihren nicht personenbezogenen Daten gewährt wird. Geplant sind auch Investitionen in neue Technologien und Infrastruktur.

5.1.2 Weißbuch KI

KI-Systeme „mit hohem Risiko“ sollen künftig zertifiziert, erprobt und kontrolliert werden. Der risikobasierte Ansatz soll so ausgestaltet werden, dass einerseits bestimmte Sektoren legal definiert werden (z. B. Verkehr, Gesundheit), die als risikoträchtig gelten, und andererseits innerhalb dieser Sektoren nur solche Anwendungsszenarien erfasst werden, bei denen mit erheblichen Risiken zu rechnen ist. Denkbar sind daneben auch noch sektorunabhängige „riskante“ Einsatzszenarien. Für andere KI-Systeme schlägt die Kommission eine freiwillige Kennzeichnung vor. Daneben steht die – zutreffende – Feststellung, dass KI-Systeme insgesamt vom geltenden Rechtsrahmen erfasst werden; die Kommission betont, dass diese Regelungen (z. B. zum Verbraucherschutz) auch künftig weitergelten sollen. Neben dem (künftigen) regulativen Rahmen sieht das Papier auch höhere Investitionen in KI vor. Unter anderem soll eine neue öffentlich-private Partnerschaft für KI und Robotik aufgebaut werden, nationale Exzellenzzentren für KI-Forschung sollen gestärkt und vernetzt werden und mithilfe des Europäischen Investitionsfonds soll mehr Beteiligungskapital für die Entwicklung und Nutzung von KI bereitgestellt werden.

5.1.3 Investitionen

Die erforderlichen Investitionen sollen aus dem Programm *Digitales Europa* (DEP), der Fazilität *Connecting Europe 2* und *Horizon Europe* kommen. Für das künftige Forschungsrahmenprogramm Horizon Europe hat die Kommission Investitionen in Höhe von 15 Milliarden Euro für das Cluster „Digitalisierung, Industrie und Weltraum“ vorgeschlagen; KI ist dabei eine der zu unterstützenden Hauptaktivitäten. Im Rahmen des DEP hat die Europäische Kommission die Investition von fast 2,5 Milliarden Euro in den Aufbau von Datenplattformen und KI-Anwendungen vorgeschlagen. Davon könnten zwei Milliarden Euro in ein europäisches High-Impact-Projekt zu europäischen Datenräumen fließen, das auch vertrauenswürdige und energieeffiziente Infrastruktur für Cloud-Dienste und die gemeinsame Nutzung von Daten umfasst. Über das DEP werden ferner einzelstaatliche

Behörden dabei unterstützt, hochwertige Datensätze für die Weiterverwendung in verschiedenen gemeinsamen Datenräumen zur Verfügung zu stellen.

5.1.4 Weitere Schritte

Die Kommission kündigt bereits an, im Laufe des Jahres weitere Maßnahmen vorzulegen. Dazu zählen: Ein Rechtsakt über digitale Dienste (Digital Services Act) zur Verantwortung von Online-Plattformen bis Ende 2020, eine sichere elektronische Identifizierung und die Zusammenarbeit im Rahmen einer gemeinsamen „Cyber-Stelle“ für den Schutz kritischer europäischer Infrastrukturen. Relevant werden kann ferner die ebenfalls im Laufe der Legislaturperiode vorgesehene Überprüfung der Wettbewerbsregeln, z. B. im Hinblick auf die Definition des Markts.

5.1.5 Bewertung vbw

Positiv ist, dass Vorteile der Datennutzung betont werden und ein Wille, KI in der EU zu fördern, klar erkennbar ist. Auch der Bedarf an höheren Mitteln – für Forschung, Infrastruktur, Finanzierung für innovative Unternehmen – wird gesehen. Viel wird davon abhängen, ob und in welchem Umfang tatsächlich bei der Mittelausstattung von Horizon Europe noch einmal nachgebessert werden kann siehe oben 4.1.8). Die im Programm “Digitales Europa” vorgesehenen Mittel für Hochleistungsrechner, Künstliche Intelligenz, Cybersicherheit und 6G-Netze dürfen nicht gekürzt werden, denn sie sind von entscheidender Bedeutung für die künftige Wettbewerbsfähigkeit Europas.

Insbesondere bei der KI besteht die Gefahr einer Überregulierung, verbunden mit dem Risiko eines Ausbremsens von Wirtschaftsaktivitäten. Es bleibt klares Ziel, neue Regelungen zu erlassen, obwohl der spezifische Regulierungsbedarf nicht dargelegt ist. Etliche Fragen hängen nicht vom Einsatz Künstlicher Intelligenz ab, wie beispielsweise Risiken durch Cyber-Angriffe oder aufgrund von Unterbrechungen der Datenverbindung. Auch die Veränderung von Produkten und Systemen während ihres Lebenszyklus ist kein KI-Phänomen, sondern tritt insbesondere überall dort auf, wo Software-Updates vorgenommen werden. Sofern hier – beispielsweise im Hinblick auf Haftungsfragen in der Wertschöpfungskette – Regelungslücken bestehen, dann wäre es nicht angebracht, nur Produkte und Dienstleistung mit KI zu regulieren. Notwendig wäre in diesem Fall eine horizontale Regulierung. Auch der begleitend vorgelegte Bericht über die Auswirkungen von Künstlicher Intelligenz, des Internets der Dinge und der Robotik auf Sicherheits- und Haftungsfragen liefert insoweit allerdings noch kein eindeutiges Ergebnis, bezüglich des gesetzgeberischen Handlungsbedarfs.

Angesichts unseres bereits bestehenden Rückstands im Vergleich zu den USA und Asien, den unter anderem die Analysen im Rahmen der Studie *TechCheck 2019. Erfolgsfaktor Mensch.* aufgezeigt haben, dürfen wir nicht ohne Not neue Hürden aufstellen (vgl. oben). Eine solche wäre es aber, wenn bestimmte KI-Anwendungen nur noch nach vorheriger

Zertifizierung und Prüfung eingesetzt werden dürften, obwohl entsprechende Verfahren gar nicht zur Verfügung stehen.

Kritisch zu sehen ist ferner, dass die Kommission Datennutzung regeln will, ohne die bestehende Datenschutzregulierung zu hinterfragen. Schwächen der DSGVO (z. B. weiterhin bestehende Rechtsunsicherheiten bei der Anonymisierung, teilweise sehr weitgehendes Verständnis des EuGHs von der Personenbeziehbarkeit bei Sachdaten, bürokratischer Aufwand) auszuräumen sollte der erste Schritt sein, um neue datenbasierte Anwendungen zu erleichtern.

Ein weiterer wichtiger Ansatzpunkt für die auch von der Kommission anstrebte Erhöhung der Menge an verfügbaren Daten wären (freiwillige) Vertragsmuster für typische Anwendungsfälle mit (potenziell) grenzüberschreitendem Bezug, die unter anderem eine Einhaltung der DSGVO gewährleisten, gegebenenfalls aber auch zur Konkretisierung der schon 2018 vorgelegten Prinzipien für nicht-personenbezogene Daten (Towards a common european data space, COM 2018, 232). Damit könnten auch auf Seiten der Unternehmen die Transaktionskosten deutlich gesenkt werden.

Die Überlegungen einerseits zum Einsatz digitaler Technologien für den Klimaschutz und andererseits zur Reduktion der durch sie selbst verursachten Emissionen (Green IT, Green AI) bleiben vollkommen vage. Hier muss die Kommission – die Green Deal und KI zu ihren Leuchtturmprojekten macht – zügig überzeugende Konzepte vorlegen.

Die Datenstrategie und namentlich die beabsichtigte Schaffung von Data Spaces für Unternehmen muss zum Anlass genommen werden, kartellrechtliche Unsicherheiten zu beseitigen – auch jenseits der gegebenenfalls staatlich geförderten beziehungsweise bereitgestellten Infrastrukturen. Kein Handlungsbedarf besteht dagegen im Hinblick auf die Maßstäbe zur Feststellung der Marktmacht (Missbrauchsverbot, Art. 102), wie die Monopolkommission in ihrem aktuellen Hauptgutachten zutreffend ausführt.

Speziell zum *Digital Services Act* kann nur noch einmal wiederholt werden, dass Plattformen in der EU nicht überreguliert werden dürfen. Für B2B- und Industrie-Plattformen muss es eine Bereichsausnahme geben. Am Grundsatz der Haftungsprivilegierung für Host-Provider muss festgehalten werden, ebenso wie an den weiteren bewährten Prinzipien der E-Commerce-Richtlinie und der wettbewerbsrechtlichen Missbrauchskontrolle.

5.2 Bund

Die KI-Strategie wurde bereits in der entsprechenden vbw-Position bewertet. Viele Aspekte gehen in die richtige Richtung, es fehlt allerdings nach wie vor an einer entschlossenen Umsetzung, auch mit Blick auf die notwendigen Investitionen. Letztere kommen in der Datenstrategie bisher gar nicht erst konkret vor.

5.2.1 Eckpunkte Datenstrategie

Ziel ist es, die verantwortungsvolle Bereitstellung und Nutzung von Daten durch alle Akteure in Deutschland signifikant zu steigern, keine neuen Datenmonopole entstehen zu lassen, eine gerechte Teilhabe zu sichern und zugleich Datenmissbrauch konsequent zu begegnen.

Die Menschen sollen durch wirksame technische Maßnahmen geschützt und souverän (selbstbestimmt und kompetent, unabhängig und sicher) agieren können. Der Bund selbst will bei der verstärkten verantwortungsvollen Datennutzung und Datenbereitstellung Vorreiter sein.

Dementsprechend adressiert die Datenstrategie die folgenden vier Handlungsfelder:
– Datenbereitstellung verbessern und Datenzugang sichern
– Verantwortungsvolle Datennutzung befördern und Innovationpotenziale heben
– Datenkompetenz erhöhen und Datenkultur etablieren
– Den Staat zum Vorreiter machen

5.2.2 Bewertung vbw

Sehr zu begrüßen ist, dass der Bund im Gegensatz zur EU grundsätzlich bereit scheint, das geltende Recht – etwa Fragen der rechtlichen Anforderungen an die Anonymisierung – zu hinterfragen. Dafür werden allerdings die bestehenden Umsetzungsspielräume nicht ausreichen; letztlich erscheinen Korrekturen auf der europäischen Ebene unausweichlich. Offen bleibt, ob eine moderate Öffnung der DSGVO angestrebt wird, um die Einwilligung in die Nutzung von Daten auch für noch nicht vollständig eingrenzbare Zwecke zu erleichtern, wie regelmäßig bei Big Data-Anwendungen der Fall.

Richtig ist auch, dass ein Bedarf an infrastrukturellen Maßnahmen und Hardware gesehen wird (Breitbandverbindungen, Rechnerkapazitäten etc.), ebenso wie unterstützende Maßnahmen im Bereich Software (Bereitstellung, Zertifizierung) und Standardisierung. Insbesondere kleinere Unternehmen und Unternehmen mit einem geringeren digitalen Reifegrad können vertrauenswürdige Produkte „von der Stange“ helfen. Ebenso wichtig wären allerdings eine Information über den konkreten Nutzen bestimmter digitaler Technologien, praktische Handreichungen für die ersten Schritte und Best Practice Beispiele, was hier noch fehlt.

Das Bekenntnis zu Open (Government) Data ist richtig. Für das Teilen von Unternehmensdaten setzt der Bund grundsätzlich auf Freiwilligkeit und passende Anreize; angedacht sind unter anderem Datenräume und Datentreuhänder sowie genossenschaftlich organisierte Systeme. Gerade in industriellen Prozessen liegt im Datenaustausch und Datenpooling ein großes wirtschaftliches Potenzial. Kartellrechtliche Zweifel müssen daher ausgeräumt werden, wie bereits in der KI-Strategie des Bundes angelegt.

Gut ist, dass der Bund vorrangig auf untergesetzliche Maßnahmen setzt, um den verantwortungsvollen Umgang mit Daten unter anderem im Bereich einer Cloud-Infrastruktur zu fördern. Dabei soll allerdings aus Sicht des Bundes nicht nur der aktuelle Standard im Bereich Sozial- und Beschäftigtendatenschutz gewährt, sondern auch eine Stärkung der institutionellen Umsetzung und Verankerung geprüft werden. Das ginge angesichts der bereits sehr weitreichenden bestehenden Rechte in die falsche Richtung (siehe oben).

Die Überlegungen zu einem „Datenökosystem“ bleiben relativ blutleer. Es wird schon nicht klar, ob hier an ein bestimmtes Vorbild gedacht wird, beispielsweise aus einer Branche, oder ob es sich eher um branchenübergreifende Lösungen handeln soll. Am Reißbrett wird sich ein solches Ökosystem ohnehin nicht entwerfen lassen. Sinnvoller wären strategische Überlegungen zum Grad der technologischen Souveränität auch im Hardware-Bereich (z. B. Prozessoren, Chips) und die Definition bestimmter Schlüsselanwendungen (z. B. aus dem Robotik-Bereich). Insoweit ist eine Verzahnung mit der Industriestrategie erforderlich, und in jedem Fall eine schlüssige Systematik zur Bestimmung der in diesem Sinne strategisch relevanten Bereiche. Auf die Arbeit des Zukunftsrats der Bayerischen Wirtschaft kann insoweit zurückgegriffen werden. Zum Thema GAIA-X vgl. die Ausführungen oben unter 4.1.3.

Kritisch ist, dass „Anforderungen lokaler Datenspeicherung für bestimmte Datentypen“ als mögliche wettbewerbsfördernde Maßnahme aufgeführt werden. Nationale Lokalisierungsauflagen sind schon im Hinblick auf Gemeinschaftsrecht sehr fragwürdig (vgl. oben), aber auch auf der europäischen Ebene kann sich das als zusätzliches Hemmnis erweisen: Unternehmen sollten grundsätzlich die aus ihrer Sicht beste verfügbare Lösung wählen können; Ausnahmen sind sehr sorgfältig zu begründen. Sinnvoller wäre es beispielsweise, hier mit einer höheren Transparenz zu arbeiten.

Die Erhöhung der „Datenkompetenz“ („Data Literacy“) auf allen Ebenen des Bildungssystems und die Handlungssicherheit in der Bevölkerung zu stärken, sind hehre Ziele. Eine positive Darstellung des unter dem Regime der DSGVO Erlaubten (z.B. mit Leitfäden, Praxisbeispielen) wäre sinnvoll. Die Überlegungen für staatliche Umsetzungsmaßnahmen im Bereich Datenkompetenz gehen allerdings über Fragen des Datenschutzes kaum hinaus, während ebenso wichtige Themen (etwa Grundlagen der Nutzungsmöglichkeiten, Verständnis für die Funktionsweise datengetriebener Geschäftsmodelle, realistische Sicht auf den Wert von Daten etc.) keine Erwähnung finden. Zu eng ist der Ansatz auch insoweit, als der Bund besonders auf gemeinwohlorientierte Unternehmen abzielen will. Der Wissenstransfer muss Unternehmen jeder Größenordnung und jeder inhaltlichen Ausrichtung offenstehen.

Wichtige Bereiche werden weder in den Eckpunkten noch in der Konsultation adressiert. Dazu zählen
- die Ermittlung des Werts von Daten und die Zuordnung entstehenden Mehrwerts,
- zahlreiche weitere Forschungsthemen über die wenigen ausdrücklich Genannten (z. B. Anonymisierung) hinaus, auch in digitalen Schlüsseltechnologien,
- Kompetenz im Umgang mit Sachdaten (genannt werden nur personenbezogene),

– mögliche Risiken für Unternehmen z. B. im Hinblick auf Preisgabe oder Verlust strategisch wichtiger beziehungsweise wettbewerbsrelevanter Daten,
– Rechte der Unternehmen gegenüber Verbrauchern, die Dienstleistungen mit Daten „bezahlen“.

Es fehlt schließlich auch eine Querverbindung zur „Agentur für Sprunginnovationen“ (am 16. Dezember 2019 als "SprinD GmbH" in Leipzig gegründet), wo datenintensive Innovationen eine bedeutende Rolle spielen müssten.

Diese Felder müssen in der Datenstrategie berücksichtigt werden. Sehr sinnvoll wäre darüber hinaus auch eine klare Verknüpfung mit übergreifenden Anliegen wie dem Klimaschutz oder der Akzeptanzsteigerung für Infrastrukturvorhaben über einen intelligenten Einsatz digitaler Werkzeuge.

Ansprechpartner/Impressum

Christine Völzow
Geschäftsführerin
Leiterin der Abteilung Wirtschaftspolitik

Telefon 089-551 78-251
Telefax 089-551 78-249
christine.voelzow@vbw-bayern.de

Impressum
Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

Herausgeber

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de