

Rechtliche Rahmenbedingungen von Industrie 4.0

Stellungnahme

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Thomas Kriesel | Bereichsleiter Steuern, Unternehmensrecht und -finanzierung
T 030 27576-146 | t.kriesel@bitkom.org

Copyright

Bitkom 2016

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom.

Zusammenfassung

Die durchgehende Vernetzung von Wertschöpfungsketten in der Industrie über Digitalisierungs-, Kommunikations- und Automatisierungstechniken wird in Deutschland unter dem Stichwort Industrie 4.0 diskutiert und vielfach auch bereits umgesetzt.

Industrie 4.0 wirft viele, teilweise neuartige Rechtsfragen auf. Allerdings machen nicht alle dieser Rechtsfragen Aktivitäten des Gesetzgebers erforderlich.

Rechtsetzungsbedarf sieht Bitkom derzeit nur in wenigen Rechtsbereichen, so im AGB-Recht, im Vertragsrecht, im Datenschutzrecht und beim Schutz von Knowhow. Dabei sind teilweise nur Änderungen, teilweise die Ausfüllung bestehender Rahmenvorschriften und teilweise auch nur untergesetzliche Normen erforderlich.

Ganz überwiegend hält Bitkom die geltende Rechtslage für ausreichend, um die Herausforderungen von Industrie 4.0 in den Griff zu bekommen, ohne die weitere Entwicklung der Digitalisierung in der Wirtschaft zu beeinträchtigen.

Inhaltsverzeichnis

1	Einführung	5
2	Allgemeine Anmerkungen	6
3	Datenhoheit	7
3.1	Ausgangslage	7
3.2	Bitkom-Position	7
4	Datenschutz	9
4.1	Ausgangslage	9
4.2	Bitkom-Position	10
5	Allgemeines Vertragsrecht	12
5.1	Ausgangslage	12
5.2	Bitkom-Position	12
6	Allgemeine Geschäftsbedingungen	13
6.1	Ausgangslage	13
6.2	Bitkom-Position	14
7	IT-Sicherheit	15
7.1	Ausgangslage	15
7.2	Bitkom-Position	15
8	Verantwortlichkeit	16
8.1	Ausgangslage	16
8.2	Bitkom-Position	16
9	Arbeitsrecht	17
9.1	Ausgangslage	17
9.2	Bitkom-Position	17
10	Urheberrecht	18
10.1	Ausgangslage	18
10.2	Bitkom-Position	18
11	Knowhow-Schutz	19
11.1	Ausgangslage	19
11.2	Bitkom-Position	19

1 Einführung

Industrie 4.0 erfordert von den daran beteiligten Unternehmen nicht unerhebliche Investitionen, um Produktions- und Wertschöpfungsprozesse auf eine neue Qualitätsstufe zu heben. Unternehmen sind bestrebt, die Grundlage für diese Investitionen, insbesondere die rechtlichen Grundlagen, so weit wie möglich abzusichern. Rechtssicherheit ist eine der wichtigsten Voraussetzungen für Investitionen in Projekte der Industrie 4.0. Rechtssicherheit bedeutet zum einen, dass rechtliche Hindernisse möglichst beseitigt werden, andererseits aber auch, dass sich der bekannte und für eine Investitionsplanung zugrunde gelegte Rechtsrahmen möglichst wenig ändert. Denn jede Änderung rechtlicher Grundlagen erzeugt auch Anwendungsunsicherheit bei den Unternehmen und die Notwendigkeit, zeit- und kostenaufwändige Anpassungsprozesse durchzuführen.

Dieses Positionspapier untersucht und formuliert einen etwaigen Anpassungsbedarf der rechtlichen Rahmenbedingungen in Rechtsgebieten, die für Industrie 4.0 von besonderer Bedeutung sind. Dabei wird unter Industrie 4.0 die Vernetzung von Systemen und Gegenständen in Produktions- und Vertriebsprozessen verstanden, die durch automatisierten Datenaustausch kommunizieren, sowie darauf aufbauende datenbasierte Dienstleistungen. Eine Besonderheit von Industrie 4.0 liegt darin, dass die Verfügbarkeit von Daten eine besondere Bedeutung gewinnt und freie Datenströme unverzichtbarer Bestandteil der Geschäftsbeziehungen werden. Ein Nutzen liegt aber meist nicht schon in den Datenströmen selbst, sondern entsteht erst nach besonderer Auswertung und Verarbeitung der Daten.

Kennzeichnend für Industrie 4.0 ist daneben, dass die vernetzten Kommunikationsprozesse nicht mehr einzeln von Menschen angestoßen werden. Die Vernetzung kann sich auf den Herrschaftsbereich eines einzelnen Unternehmens beschränken (z. B. innerhalb einer Fabrik, in der lediglich die verschiedenen Produktionsprozesse miteinander vernetzt sind). Die Vernetzung kann aber auch mehrere Unternehmen bzw. deren Systeme umfassen. Diese Stellungnahme schließt daher Aspekte unternehmensübergreifend vernetzter Produktions- und Dienstleistungsprozesse und deren rechtliche Rahmenbedingungen ein. Verbraucherschutzbelange und Smart-Home-Anwendungen bleiben dagegen in dieser Stellungnahme genauso außer Betrachtung wie verkehrsrechtliche Fragen des vernetzten und automatisierten Fahrens. Zu den bereichsspezifischen Rechtsfragen von Vernetzung und Datenfluss zwischen den Beteiligten in diesen Bereichen sowie zu weiteren Fragen im Umfeld von Industrie 4.0 (z. B. im Wettbewerbs- und Kartellrecht) wird Bitkom ggf. in gesonderten Positionspapieren Stellung nehmen. Dies gilt auch für Ausführungen zu patenrechtlichen Fragen, insbesondere zu standardessentiellen Patenten, deren Darstellung aufgrund ihrer Komplexität den Rahmen dieses Positionspapiers sprengen würde.

2 Allgemeine Anmerkungen

Die Herausforderungen der Industrie 4.0 lassen sich im Wesentlichen mit den Instrumenten des geltenden Rechts bewältigen. Daher besteht lediglich stellenweise Regelungsbedarf, vor allem im nationalen Recht. Der europäische Gesetzgeber sollte von weiterer Regulierung derzeit Abstand nehmen und nur bisher offene Ausführungsbestimmungen zu bereits erlassenen Rahmenvorschriften treffen. Bei einer Umgestaltung des Rechtsrahmens für Industrie 4.0 sollte der Gesetzgeber behutsam vorgehen. Es gilt vor allem, vorschnellen Aktionismus, wenig hilfreiche Überregulierung und zu ausgefeilte Detailregelungen zu vermeiden. Zu granulare Regelungen oder ein zu starker Regelungsimpuls lassen befürchten, dass die Entwicklung von Industrie 4.0 behindert anstatt gefördert wird.

Wurde – nach genauer vorheriger Analyse – ein Regelungsbedarf identifiziert, darf nicht versucht werden, aufgrund der Erfahrungen in der Vergangenheit noch unklare Herausforderungen der Zukunft zu regeln. Vielmehr sollte der Wirtschaft auch Spielraum eingeräumt werden, um Geschäftsmodelle und ihre Skalierbarkeit zu testen. Nicht umsonst sind datenbasierte Geschäftsmodelle mit Weltbedeutung vor allem in den USA entstanden, wo zum einen ein großer Markt vorhanden ist, zum anderen aber auch eine relativ zurückhaltende staatliche Regulierung herrscht. Der Gesetzgeber muss schließlich die bestehenden Möglichkeiten zur Selbstregulierung von Unternehmen der Industrie 4.0 intakt lassen und stellenweise erweitern.

Soweit schnell wachsende neue Geschäftsmodelle zu einer Monopolisierung und zu Marktungleichgewichten führen, ist dem mit dem Kartell- und Wettbewerbsrecht und durch ausgewogene Geltung und Anwendung bestehender Marktregulierungen zu begegnen. Ein ausgewogener Wettbewerb kann dagegen nicht durch das allgemeine Zivilrecht hergestellt werden. Insgesamt sollte das Recht nicht etablierte Geschäftsmodelle gegen die Verdrängung durch neue Geschäftsmodelle in Schutz nehmen und damit Innovation verhindern.

3 Datenhoheit

3.1 Ausgangslage

In der Industrie 4.0 spielt die Erhebung, Auswertung, Analyse, Bearbeitung und Nutzung von Daten eine zentrale Rolle. Für die Betrachtung rechtlicher Aspekte des Datenverkehrs ist zu unterscheiden zwischen »personenbezogenen Daten« und sonstigen Daten ohne Bezug zu einer konkreten natürlichen Person (»Produkt- und Maschinendaten«). Der Umgang mit personenbezogenen Daten unterliegt den besonderen Anforderungen des Datenschutzrechts (vgl. dazu unten). Aber auch Produkt- und Maschinendaten sind für die Industrie 4.0 von großer Bedeutung und stellen für die Unternehmen einen eigenen Wert dar. Denn solche Daten sind Grundlage für die Entwicklung von neuen oder die Verbesserung von vorhandenen Produkten, Dienstleistungen und Geschäftsmodellen, für Effizienzsteigerungen im Produktionsprozess und für die bessere Befriedigung von Kundenbedürfnissen. Für Zwecke der Industrie 4.0 sind Unternehmen daher auf den Zugang zu Daten angewiesen.

Im geltenden Zivilrecht ist eine ausdrückliche Erlaubnis für die Erhebung, Sammlung, Nutzung oder Auswertung von Produkt- und Maschinendaten derzeit nicht vorhanden. Eigentumsrechte des BGB sind nicht auf Daten anwendbar, da diese Rechte für Sachen konzipiert wurden. Auch das Recht des geistigen Eigentums lässt sich nicht allgemein auf Daten anwenden, sondern höchstens auf Investitionen zur Erzeugung, Auswertung oder Zusammenstellung von Daten. Andererseits ist die Erhebung, Vervielfältigung, Sammlung und Nutzung von Produkt- und Maschinendaten durch Unternehmen im geltenden Zivilrecht auch nicht generell verboten. Denn anders als für eine Datenerhebung zu staatlichen Zwecken oder für die Erhebung personenbezogener Daten ist für die Erhebung von Produkt- und Maschinendaten im Privatrechtsverkehr eine gesetzliche Ermächtigungsgrundlage nicht erforderlich.

Auch wenn das geltende Recht umfassende eigentumsähnliche Rechte an Produkt- oder Maschinendaten nicht vorsieht, erkennt es doch teilweise den Schutz von Maschinendaten an. Immaterialgüterrecht, Wettbewerbsrecht, Zivilrecht und Strafrecht sanktionieren unbefugte Datenzugriffe sowie Veränderungen, Löschungen, Nachahmungen oder Manipulationen von geschützten Datenbeständen und die Überwindung von Sicherungsvorrichtungen für Daten. Wenn also ein Unternehmen technische Schutzvorrichtungen (z. B. Passwortschutz) gegen unbefugten Datenzugriff installiert, gewährt ihm dies eine gewisse faktische Ausschließlichkeit, die Abwehrrechte gegen den Zugriff Dritter auf die Daten begründen können.

3.2 Bitkom-Position

Das geltende Recht enthält einerseits kein generelles Verbot, Produkt- und Maschinendaten zu erheben und auszuwerten, gewährt andererseits jedoch die Möglichkeit, einen Datenzugang auf abgegrenzte Datenbestände auszuschließen und diesen Zugangsausschluss auch rechtlich abzusichern. Zur Umsetzung von Industrie 4.0 ist die Schaffung eines umfassenden Zugriffsrechts von Anbietern und Herstellern auf Produkt- und Maschinendaten (also auf Daten, die nicht vom besonderen Schutz für personenbezogene Daten erfasst sind) nicht erforderlich und

nicht wünschenswert. Ein Bedürfnis an zusätzlichen Schutzrechten an Daten wird derzeit nicht gesehen. Die bestehende Rechtslage lässt den Unternehmen ausreichende Spielräume, Zugang zu und Nutzung von Maschinendaten vertraglich zu begründen bzw. abzusichern und entsprechend den Interessen der Vertragspartner auszugestalten. Es ist darauf zu achten, dass solche vertraglichen Regelungen zum Datenaustausch im Geschäftsverkehr zwischen Unternehmen nicht an den Anforderungen des AGB-Rechts (§§ 305 ff. BGB) zum isolierten Nachteil der deutschen Marktteilnehmer scheitern. Allerdings wird zukünftig zu beobachten sein, ob ein fehlendes Zugriffsrecht an Daten die Entstehung neuer Geschäftsmodelle verhindert und die Nachteile von Datenmonopolen durch das Kartellrecht ausreichend berücksichtigt werden. Erst dann, wenn dazu belastbare Erkenntnisse vorliegen, kann ein Handeln des Gesetzgebers in Betracht kommen.

Eine etwas andere Bewertung gilt für Daten des Staates, also Daten, die Körperschaften des öffentlichen Rechts im Rahmen ihrer hoheitlichen Aufgabenerfüllung und steuerfinanziert erheben, sammeln, auswerten, verarbeiten oder zur Kenntnis erhalten. Der Staat und öffentliche Verwaltungsträger sollten ihnen vorliegende und zugängliche Informationen (z. B. Verkehrsdaten, Klimadaten, Topographiedaten) ggf. in anonymisierter Form und in auswertbaren Formaten zur Verfügung stellen. Öffentliche Daten müssen zu Open Data werden. Wenn diese Informationen öffentlich bereitstehen und nutzbar sind, können neue Anwendungen, Dienstleistungen mit Mehrwert und neue Geschäftsmodelle entstehen. Offene Daten der öffentlichen Verwaltung sind somit die Basis für Innovationen.

Entsprechende Selbstverpflichtungen der Bundesregierung liegen auch bereits vor. So heißt es z. B. auf S. 107 des [Koalitionsvertrages für die 18. Legislaturperiode im Abschnitt »Moderne Verwaltung«](#): »Die Bundesverwaltung muss auf der Basis eines Gesetzes mit allen ihren Behörden Vorreiter für die Bereitstellung offener Daten in einheitlichen maschinenlesbaren Formaten und unter freien Lizenzbedingungen sein. Wir wollen für Bund, Länder und Kommunen ein Open-Data-Portal bereitstellen.« Der Umsetzungsstatus dieser Pläne ist aber auf den verschiedenen Verwaltungsebenen noch sehr uneinheitlich. Zurzeit entscheidet jedes Bundesland und jede Kommune eigenständig, welche Daten herausgegeben werden. Viele Verwaltungen betrachten Daten immer noch als ihr Eigentum, nicht jedoch als frei zugänglichen Informationspool und als Grundlage für neue Wertschöpfungsmöglichkeiten. Die Bundesregierung muss ihre Open Data Strategie für die öffentliche Verwaltung konsequent weiterverfolgen und auf eine gesetzliche Basis stellen. Der Zugang zu öffentlichen Daten darf nur vom Datenschutz und von besonderen, gesondert zu begründenden Geheimhaltungsinteressen begrenzt werden. Ein solches besonderes Geheimhaltungsinteresse kann z. B. für Kooperationen zwischen Wirtschaftsunternehmen und Hochschulen im Bereich Forschung und Entwicklung bestehen. Denn solche Kooperationen werden nicht zustande kommen, wenn eine gewisse Exklusivität der Ergebnisse und ihrer Nutzung nicht gewährleistet ist.

4 Datenschutz

4.1 Ausgangslage

Das Datenschutzrecht ist auf personenbezogene Daten anwendbar. Bei Industrie 4.0 stehen nicht vorrangig personenbezogene Daten, sondern Produkt- und Maschinendaten (vgl. oben Ziffer 3) im Fokus des Interesses. Diese fallen nicht in den Anwendungsbereich des Datenschutzes, selbst wenn sie teilweise mit ähnlichen Kennungssystemen arbeiten (z. B. IP-Adressen für Geräte).

Sowohl unter dem aktuellen Bundesdatenschutzgesetz als auch unter der ab Mai 2018 zur Anwendung kommenden Datenschutz-Grundverordnung (DS-GVO) stellt die exakte Abgrenzung von personenbezogenen Daten einerseits und Produkt- und Maschinendaten andererseits in der Praxis eine Herausforderung dar. Bei jeglichem Personenbezug, sei er direkt oder nur indirekt, gelten die strengen Anforderungen des Datenschutzes. In einer stark vernetzten Umwelt kann es allerdings durch die Kombination großer Datenmengen aus verschiedenen Quellen auch zufällig dazu kommen, dass ein Personenbezug wieder hergestellt werden könnte, auch wenn jedes einzelne Datum für sich alleine dies nicht zulassen würde. Daher muss unterschieden werden, für welche Marktteilnehmer welche Daten zugänglich sind. Daraus leitet sich ab, ob es sich um anonyme oder um personenbezogene Daten handelt, die ggf. unter Verwendung von Pseudonymen verarbeitet werden dürfen, und welche Anforderungen die Datenverarbeitung erfüllen muss.

Neben den klassischen Szenarien existieren aber auch Anwendungen in der Industrie 4.0, bei denen bewusst personenbezogene Daten verarbeitet werden. Hier ist selbstverständlich das Datenschutzrecht vollumfänglich anwendbar (z. B. bei Auswertungen des Kundenverhaltens). Die DS-GVO hat für solche Fälle vor allem im Bereich der Harmonisierung des europäischen Datenschutzrechts große Vorteile, aber auch teilweise neue Verpflichtungen gebracht. So sind die Informationsanforderungen von Seiten der Unternehmen gegenüber den Kunden deutlich umfassender als zuvor. Für einige Datenkategorien gibt es zudem verschärfte Regelungen, was die Verarbeitung angeht. Positiv für die Industrie 4.0 sind vor allem die Regeln zur vereinfachten Verarbeitung von Daten zu statistischen Zwecken.

Da sich die wesentlichen Konflikte mit dem Datenschutzrecht vor allem auf den Graubereich zwischen klar personenbezogenen Daten und Produkt- und Maschinendaten beziehen, müssen hier klare Regeln geschaffen werden. Zum einen gilt es, durch technisch-organisatorische Schutzmaßnahmen das potentielle Risiko für Individuen bei falscher oder unabsichtlicher Verarbeitung personenbezogener Daten zu reduzieren. Zum anderen müssen Streitfragen schnell und effizient geklärt werden können.

4.2 Bitkom-Position

Bei der Verarbeitung von personenbezogenen Daten bietet die Pseudonymisierung eine Möglichkeit, diese Daten weiter zu verarbeiten und gleichzeitig ein hohes Schutzniveau für das betroffene Individuum zu ermöglichen. In der DS-GVO hat der europäische Gesetzgeber bereits in Artikel 6 Abs. 4 deutlich gemacht, dass er die Verarbeitung pseudonymer Daten (insbesondere auch bei Auswertungen von Big Data) privilegieren und inzentivieren möchte. Die Kriterien für die Pseudonymisierung und die konkreten Anforderungen an die Zulässigkeit der Verarbeitung pseudonymisierter Daten müssen aber noch vom neu geschaffenen Europäischen Datenschutzausschuss in Zusammenarbeit mit der Industrie entwickelt werden. Hier ist zu wünschen, dass nicht erst bis zum Inkrafttreten der DS-GVO gewartet wird. Industrie 4.0 benötigt Handlungsspielräume, zumal die Verarbeitung personenbezogener Daten in vielen Fällen von Industrie 4.0 nicht im Zentrum der Wertschöpfung steht, sondern allenfalls als unerwünschte Nebenfolge von Prozessabläufen auftritt. Für die Annahme eines Zugangs zu personenbezogenen Daten darf – entgegen der möglichen Auffassung des EuGH in der Rechtssache Breyer – eine lediglich abstrakte und rein theoretische Zugriffsmöglichkeit nicht ausreichen. Die von der Politik vielfach propagierte flächendeckende Einholung von Einwilligungen der Betroffenen ist dagegen keine für Industrie 4.0 praktikable Möglichkeit, den Anforderungen des Datenschutzes nachzukommen. Dies betrifft insbesondere die weitergehende Nutzung bereits vorhandener Daten für innovative Anwendungen (außerhalb der Werbung), die von der ursprünglichen Einwilligung aufgrund eng ausgelegter Zweckbindung nicht umfasst waren.

Da in der Industrie 4.0 typischerweise mehrere verantwortliche Stellen Daten untereinander austauschen und nutzen, muss die Frage geklärt werden, ab wann ein Datum für eine verantwortliche Stelle als pseudonym und ab wann als anonym gilt (und damit nicht unter das Datenschutzrecht fällt). Da für eine verantwortliche Stelle, die keine Möglichkeit besitzt, Daten in ihrem Bestand wieder zu repersonalisieren, diese Daten faktisch anonymisiert sind, müssen diese auch zwingend so behandelt werden. Vor diesem Hintergrund ist es wünschenswert, die Anforderungen an eine rechtlich wirksame Anonymisierung für Anwendungsszenarien der Industrie 4.0 weiter zu definieren und Leitlinien zu schaffen.

Grenzfälle, ab wann ein Datum als personenbeziehbar gilt, kann der Europäische Datenschutzausschuss in Abstimmung mit der Industrie bewerten. Dazu sollte die Form einer Black List (Verbotsliste) gewählt werden, die ständig erneuert wird und bestimmt, welche Daten in welchen Verarbeitungszusammenhängen als eindeutig personenbeziehbar gelten. Aus Sicht des Bitkom muss es EU-weit einheitliche Auslegungen der DS-GVO geben. Der deutsche Gesetzgeber ist aufgefordert, die Mitwirkung und Unterstützung der deutschen Behörden im Europäischen Datenschutzausschuss effizient zu organisieren.

Zudem bietet die DS-GVO das Instrument der genehmigten Verhaltensregeln sowie das Instrument der Zertifizierung als Möglichkeiten, die Einhaltung der datenschutzrechtlichen Vorgaben auch in der Industrie 4.0 zu erleichtern und den Unternehmen Rechtssicherheit zu geben. Dazu müssten Zertifikate als Nachweis für die Erfüllung datenschutzrechtlicher Anforderungen auch in der Praxis sicher anerkannt werden.

Aufsichtsbehörden, Datenschutzausschuss und die Kommission sind angehalten, datenschutzspezifische Zertifizierungsverfahren und Datenschutzsiegel insbesondere auf Unionsebene zu fördern, wobei sich die Wirtschaft im konkreten Fall aktiv einbringen wird. Zur Förderung datenschutzkonformer Verhaltensregeln stellt der auf europäischer Ebene von der Europäischen Kommission, der Art. 29-Gruppe und Industrievertretern erarbeitete »Data Protection Code of Conduct for Cloud Service Providers« bereits ein nützliches Regelwerk dar, auf das im Rahmen der Industrie 4.0 zurückgegriffen werden kann.

In anderen Bereichen (z. B. bei Informationsverpflichtungen) setzt sich der Bitkom für ein vorrangiges Tätigwerden selbstregulierender Initiativen ein, die durch die DS-GVO gestärkt wurden.

Insgesamt sollte die Bundesregierung bei der Umsetzung der DS-GVO darauf achten, dass die erreichte Harmonisierung beim Datenschutz in der EU nicht durch weitgehende nationale Sonderregelungen aufgeweicht wird. Denn die DS-GVO sieht zahlreiche Öffnungsklauseln vor, die es Mitgliedsstaaten erlauben, eigene nationale Regelungen zu erlassen. Von solchen Wahlrechten sollten alle EU-Mitgliedstaaten möglichst zurückhaltend Gebrauch machen, um eine erneute Rechtszersplitterung in der EU und die daraus resultierende Rechtsunsicherheit für die Unternehmen zu vermeiden. Soweit Deutschland von einem Mitgliedstaatenwahlrecht Gebrauch macht, sollte die daraufhin gewählte Regelung im Sinne der Industrie 4.0 einfach administrierbar sein und innovative Geschäftsmodelle fördern, z. B. im Bereich der Zweckänderung (Art. 6 Abs. 4 DS-GVO) sowie der wissenschaftlichen und statistischen Auswertungen (Art. 89 Abs. 2 DS-GVO). Gerade für die Industrie 4.0 ist eine grenzübergreifende Vernetzung von großer Bedeutung. Spezifische Regelungen in jedem Mitgliedsstaat führen zu neuen Hürden für den grenzüberschreitenden Datenfluss, die wenig zusätzlichen Schutz für Nutzer bringen.

5 Allgemeines Vertragsrecht

5.1 Ausgangslage

Das geltende deutsche Zivilrecht geht im Grundsatz davon aus, dass rechtlich relevante (Willens-) Erklärungen stets durch natürliche Personen gegenüber anderen natürlichen Personen abgegeben werden. Die Erklärung wird zunächst dem Erklärenden selbst zugerechnet und kann unter den jeweiligen Voraussetzungen der Stellvertretung oder Botenschaft Rechtswirkungen für andere natürliche oder juristische Personen begründen. In der Industrie 4.0 kommunizieren allerdings vielfach Maschinen autonom miteinander. Diese Kommunikation schließt regelmäßig auch Vorgänge ein, die eine rechtliche Wirkung auslösen sollen (z. B. Bestellvorgänge). Erfolgt diese Kommunikation zwischen Maschinen, die in Eigentum oder Besitz unterschiedlicher natürlicher oder juristischer Personen stehen (z. B. zwischen Betreiber einer Produktionsanlage, Hersteller der Produktionsanlage, mehreren Lieferanten in der Lieferkette), stellt sich die Frage nach den rechtlichen Wirkungen dieser Kommunikation. Dabei ist zu beachten, dass die konkreten Inhalte, Ablauf und Zeitpunkte einer solchen Kommunikation bei selbstlernenden oder selbstoptimierenden Maschinen immer weniger für deren Betreiber vorhersehbar sind. Dies gilt erst recht in selbstoptimierenden Produktionsketten und -netzwerken. Gleichzeitig kann eine ausbleibende oder inhaltlich unrichtige Kommunikation zwischen den beteiligten Maschinen erhebliche wirtschaftliche Nachteile bewirken (etwa Produktionsausfälle oder Lagerkosten).

5.2 Bitkom-Position

Das allgemeine Vertragsrecht einschließlich des Rechts der Willenserklärungen ist grundsätzlich auch anwendbar, wenn im Rahmen des sog. Internet der Dinge Maschinenerklärungen ausgetauscht werden. Denn diese Maschinenerklärungen können denjenigen natürlichen oder juristischen Personen zugerechnet werden, die eine »erklärende Maschine« für ihre Zwecke einsetzen und dadurch in den Rechtsverkehr einbringen. Die Maschine hat insoweit lediglich die Funktion einer (technischen) Empfangs- oder Erklärungsvorrichtung. Auch eine über eine Maschine geäußerte Willenserklärung muss daher Rechtswirkungen auslösen können.

Damit in diesem Zusammenhang keine Irritationen oder Rechtsunsicherheiten aufkommen, wäre jedoch eine Klarstellung im Gesetz wünschenswert. Der Gesetzgeber sollte deutlich machen, dass die Vorschriften der Willenserklärungen (§§ 116 ff. BGB) auch Anwendung finden, wenn Erklärungen durch Maschinen abgegeben und empfangen werden. In diesen Fällen treten die rechtlichen Wirkungen für denjenigen ein, der Maschinen für seine Zwecke zum Austausch rechtswirksamer Erklärungen nutzt.

6 Allgemeine Geschäftsbedingungen

6.1 Ausgangslage

Vertragliche Regelungen können im heutigen Geschäftsverkehr, der auf standardmäßige Abwicklung von Geschäftsbeziehungen ausgelegt ist, nur noch im Ausnahmefall individuell vereinbart werden. Standardisierte Vertragsvorgaben stoßen aber auch im Geschäftsverkehr zwischen Unternehmen (B2B) zunehmend an die Einschränkungen des AGB-Rechts. Die Grundausrichtung des Gesetzes, Verträge zwischen Unternehmen nur in begründeten Ausnahmefällen einer AGB-Kontrolle zu unterziehen, findet in der Rechtsprechungspraxis immer weniger Beachtung. Stattdessen überträgt die Rechtsprechung über die Generalklausel des § 307 Abs. 2 BGB Wertungen für die Beurteilung von Verbraucherverträgen (B2C) auf die Beurteilung von Verträgen zwischen Unternehmen (B2B). In der Folge kann z. B. eine angemessene Risikoverteilung zwischen den Vertragspartnern der Industrie 4.0 über AGB nicht mehr hergestellt werden, da die entsprechenden Vertragsklauseln den Wertungen der Rechtsprechung zuwiderlaufen. So können z. B. Anbieter Haftungsrisiken auch dann nicht der Höhe nach nennenswert begrenzen, wenn die Vergütung der vertragsgegenständlichen Leistung vergleichsweise gering ist und zum Haftungsrisiko des Anbieters in keinem angemessenen Verhältnis steht. Die Einschränkungen der Inhaltskontrolle für AGB im Geschäftsverkehr zwischen Unternehmen nach § 310 Abs. 1 BGB finden dagegen in der Rechtsprechung immer weniger Beachtung.

Da die Rechtsprechung nicht immer konsistent und belastbar ist, treten außerdem Rechtsunsicherheiten auf. Dies betrifft z. B. die Bestimmung von Kategorien wie »Kardinalpflichten« und »vorhersehbare Schäden«, die durch die Rechtsprechung eingeführt wurden. Insbesondere für Verträge über Datendienste sind Reichweite und Konsequenz dieser Konzepte unklar. Die Unsicherheiten werden in die Inhaltskontrolle von AGB übertragen, da nach § 307 Abs. 2 BGB die Wirksamkeit von AGB an den wesentlichen Grundgedanken der gesetzlichen Regelung für den zugrundeliegenden Vertragstyp zu messen ist. Die gesetzlichen Vertragstypen und ihre Ausformungen im BGB entsprechen aber immer weniger den Anforderungen einer zunehmend digitalisierten Wirtschaft.

Es ist davon auszugehen, dass die Verwendung formularmäßiger Standardverträge in den vernetzten Wertschöpfungsketten der Industrie 4.0 noch deutlich an Bedeutung gewinnen wird. Gleichzeitig können die Vertragspartner in einer internationalisierten Welt das anwendbare Recht frei wählen. Ausufernde Restriktionen für AGB im deutschen Recht bedeuten einen Unsicherheitsfaktor für die Verlässlichkeit des deutschen Zivilrechts, der sich gerade für innovative Geschäftsmodelle der Industrie 4.0 nachteilig auswirkt. Um den Unsicherheiten und Restriktionen zu entgehen, sind viele Unternehmen bereits dazu übergegangen, für ihre Vertragsbeziehungen in internationalen Geschäftsbeziehungen die Geltung einer Rechtsordnung außerhalb Deutschlands zu vereinbaren.

6.2 Bitkom-Position

Viele wichtige rechtliche Aspekte in Geschäftsbeziehungen der Industrie 4.0 können und müssen durch vertragliche Regelungen adressiert werden, da spezifische gesetzliche Bestimmungen fehlen. Die ausufernde Anwendung von AGB-rechtlichen Restriktionen im B2B-Bereich verhindert aber vielfach eine belastbare vertragliche Grundlage. Insbesondere die ausufernde Anwendung von Rechtsgedanken aus Verbraucherverträgen in B2B-Geschäftsbeziehungen durch die Rechtsprechung muss beendet werden. Über kurz oder lang werden sie zu deutlichen Wertungswidersprüchen führen. So würde z. B. eine Übertragung der Wertung in § 309 Nr. 13 BGB neu (Schriftform darf in AGB nicht mehr vorgegeben werden) auf den B2B-Geschäftsverkehr bestehenden Dokumentationsanforderungen zuwiderlaufen (z. B. kann der Nachweis über den Abschluss eines Lizenzvertrages nach BGH-Urteil vom 21.10.2015 – I ZR 173/14 nur durch Vorlage einer schriftlichen Dokumentation des Vertragsschlusses erbracht werden).

Nahezu unerfüllbar sind auch die Anforderungen der Rechtsprechung an die Individualisierung von Vertragsabsprachen. Individualisierte Vertragsabsprachen, die nicht von den Restriktionen des AGB-Rechts betroffen sind, müssen ausgehandelt werden. Nach der Rechtsprechung kann von einem Aushandeln nur dann gesprochen werden, »wenn der Verwender zunächst den in seinen Allgemeinen Geschäftsbedingungen enthaltenen gesetzesfremden Kerngehalt, also die den wesentlichen Inhalt der gesetzlichen Regelung ändernden oder ergänzenden Bestimmungen, inhaltlich ernsthaft zur Disposition stellt und dem Verhandlungspartner Gestaltungsfreiheit zur Wahrung eigener Interessen einräumt mit zumindest der realen Möglichkeit, die inhaltliche Ausgestaltung der Vertragsbedingungen zu beeinflussen. ... Der allgemeine Hinweis, alle Vertragsbedingungen hätten zur Disposition gestanden, enthält nicht die notwendige Konkretisierung hinsichtlich der Kerngehalte der einzelnen Klauseln.« (BGH, Urteil vom 20. März 2014, VII ZR 248/13). Um dieses »Zur-Disposition-Stellen« nachzuweisen, muss es zukünftig wieder ausreichen, dass die Verhandlungen der Parteien zu einer Vertragsabsprache dokumentiert werden.

Im Umfeld von Industrie 4.0 sollte dem Grundsatz der Vertragsfreiheit wieder ein breiterer Raum gewährt werden, sodass B2B-Geschäftsbeziehungen der Industrie 4.0 auf einer belastbaren vertraglichen Grundlage abgewickelt werden können. Der Gesetzgeber sollte dem gesetzlichen Grundsatz in § 310 Abs. 1 BGB wieder zu mehr Durchschlagskraft verhelfen. So könnte z. B. § 310 Abs. 1 BGB um eine Passage ergänzt werden, wonach für die Inhaltskontrolle von Allgemeinen Geschäftsbedingungen, die gegenüber einem Unternehmer, einer juristischen Person des öffentlichen Rechts oder einem öffentlich-rechtlichen Sondervermögen verwendet werden, Wertungen aus der Inhaltskontrolle von Verbraucherverträgen nicht zu übernehmen sind.

Ein anderer denkbarer Weg zur Korrektur übermäßiger Restriktionen durch AGB-Kontrolle wäre eine gesetzliche Anerkennung von Industriestandardverträgen bzw. einer darin gefundenen fairen Risikoverteilung.

Keinesfalls dürfen über das AGB-Recht neue Wertungen zu Datenzugriff und Datenaustausch zwischen Unternehmen in B2B-Geschäftsbeziehungen der Industrie 4.0 eingeführt werden.

7 IT-Sicherheit

7.1 Ausgangslage

Vernetzte Anlagen müssen eine gewisse Sicherheit bieten (Integrität, Vertraulichkeit, Verfügbarkeit der Systeme). Aus rechtlicher Sicht ist zwischen einer ordnungsrechtlichen Seite und einer zivilrechtlichen Seite der IT-Sicherheit zu unterscheiden. Das Ordnungsrecht (z. B. IT-Sicherheitsgesetz, TMG, BDSG) verpflichtet Betreiber von Datennetzen und datenverarbeitende Stellen dazu, ein bestimmtes Mindestniveau an Datensicherheit zu gewährleisten. Bei Nichtbeachtung dieser Vorgaben drohen Bußgelder oder sogar Strafen. Das Zivilrecht legt Haftungsfolgen fest, wenn Lücken der IT-Sicherheit zu Schäden führen, und gewährt dem Geschädigten Ersatzansprüche (z. B. Produkt- und Produzentenhaftung).

7.2 Bitkom-Position

Die rechtlichen Folgen für Verstöße gegen Anforderungen der IT-Sicherheit sind festgelegt und bedürfen derzeit keiner Änderung. Dagegen sind die technischen Standards, die Grundlage für die rechtlichen Vorgaben bilden (z. B. bei der Konkretisierung des Verschuldensmaßstabs für eine Haftungsnorm), noch uneinheitlich. Standards werden von der Industrie in verschiedenen Gremien erarbeitet, um allen Beteiligten die Entwicklung marktreifer Produkte zu ermöglichen und die Wettbewerbsfähigkeit der Industrie 4.0 zu steigern. Die Politik sollte diese Initiativen der Wirtschaft unterstützen.

Nicht in jedem Fall ist jedoch eine Zertifizierung der angemessene Weg zu mehr IT-Sicherheit. Denn die Anforderungen an die IT-Sicherheit sind nicht in allen Unternehmen und für alle Datenverarbeitungsprozesse der Industrie 4.0 gleich. So kann das hohe Sicherheitsniveau einer BSI-Zertifizierung überdimensioniert sein und ist auch nicht von allen Unternehmen erfüllbar. Andererseits können auch die höchsten Standards keinen hundertprozentigen Schutz von IT-Systemen vor unberechtigtem Zugriff gewährleisten. Hinzu kommt, dass Zertifizierungsprozesse meist sehr langwierig sind und noch nicht für alle kritischen Produkte angemessene Zertifizierungsparameter vorliegen, während die Produktionszyklen von Produkten der IT-Sicherheit angesichts der vielfältigen und ständig wechselnden Bedrohungen aber sehr kurz sein müssen. Daher sollten auch Verfahren der Selbstregulierung in der Wirtschaft und wirtschafts-eigenen Zertifizierungsverfahren (z. B. PCI-Zertifizierung) anerkannt werden.

8 Verantwortlichkeit

8.1 Ausgangslage

Kennzeichnend für Industrie 4.0 ist eine hohe technische Komplexität sowie das Streben nach möglichst weitgehender Automatisierung und Selbststeuerung der vernetzten Systeme. Das Risiko eines möglichen Fehlverhaltens der eingesetzten Systeme und hierdurch verursachter Schäden wird gerade in der Anfangsphase nicht gänzlich auszuschließen sein. Bei der Verantwortlichkeit für Schäden kann grob differenziert werden zwischen der Haftung des Systembetreibers (beruht weitgehend auf verschuldensabhängiger Haftung für Pflichtverletzungen) und der Haftung des Systemherstellers (beruht weitgehend auf verschuldensunabhängiger Produkthaftung). Darüber hinaus kennt das geltende Recht eine Gefährdungshaftung für begrenzte Anwendungsbereiche wie die Tierhalterhaftung oder die Haftung des KfZ-Halters.

Nach aktueller Rechtslage setzt die Haftung des Systembetreibers für einen eingetretenen Schaden voraus, dass der Schaden von ihm verursacht und verschuldet wurde. Bei Handlungen voll-autonom und selbstlernender Systeme kann es jedoch schwierig sein, einen Schadensfall einem Systembetreiber kausal zuzurechnen. Fehlen Möglichkeiten, in automatisierte Abläufe einzugreifen und diese nachzusteuern, wird auch ein pflichtwidriges Verhalten und somit ein Verschulden des Systembetreibers kaum zu begründen sein. Die Komplexität kann sich noch erhöhen, wenn in den Schadensfall autonom interagierende Systeme diverser Beteiligter der Wertschöpfungskette involviert sind. Es ist anzunehmen, dass im Falle eines Rechtsstreits über den Schadensfall zeitaufwendige und kostenintensive Sachverständigengutachten zur Klärung der Verursachungs- und Verschuldensfrage erforderlich werden. Lässt sich nicht hinreichend ermitteln, welcher Beteiligte den Schaden verursacht hat, kommt es aufgrund der Regelung des § 830 Abs. 1 S.2 BGB zu einer gesamtschuldnerischen Haftung aller in Betracht kommender Verursacher.

8.2 Bitkom-Position

Auch wenn möglicherweise Kausalitätsketten in der Industrie 4.0 weniger überschaubar werden, so werden doch mögliche Schadensursachen eher reduziert. Denn zum einen sind viele Abläufe in der Industrie 4.0 genau darauf ausgerichtet und zum anderen wird menschliches Fehlverhalten als potenzielle Fehlerursache und Gefahrenquelle vielfach ausgeschaltet. Vor diesem Hintergrund erscheinen die Haftungsgrundlagen des geltenden Rechts ausgewogen und ausreichend. Eine Änderung oder gar Ausweitung der deliktischen Haftungsregeln ist also für Industrie 4.0 nicht veranlasst. Zu große Haftungsrisiken der Unternehmen könnten für die weitere Entwicklung von Industrie 4.0 auch hinderlich sein. Allerdings sollte die weitere Entwicklung beobachtet werden, um eventuell auftretende Haftungslücken zeitnah zu adressieren.

9 Arbeitsrecht

9.1 Ausgangslage

Neue Prozesse und Technologien verändern nicht nur die Industrie, sondern auch das Arbeitsleben. Die Industrie 4.0 wird vom Arbeiten 4.0 begleitet. Das betrifft Arbeitsformen, Arbeitsinhalte und Berufsbilder. Mit der Industrie 4.0 verändern sich auch die Anforderungen an Arbeitnehmer. Zukünftig wird auf dem Arbeitsmarkt nur derjenige bestehen, der über digitale Kompetenzen verfügt und der rasanten technologischen Entwicklungen Schritt halten kann. Zudem werden körperlich anstrengende, eintönige oder gefahrgeneigte Arbeiten zukünftig noch weiter reduziert werden können. Durch neue Technologien und Arbeitsmodelle lassen sich auch familiäre, private und berufliche Belange wesentlich besser vereinbaren.

Relevante Handlungsfelder liegen vor allem in den Bereichen allgemeine Bildung und Weiterbildung, Fachkräftesicherung und Arbeitsrecht, einschließlich Regelungen zur Vereinbarkeit von Familie und Beruf. Dabei muss folgendes bedacht werden: Die Weichen, die wir heute stellen, werden maßgeblich über die Attraktivität und Wettbewerbsfähigkeit des Standorts Deutschland entscheiden.

9.2 Bitkom-Position

Die Industrie 4.0 muss grundsätzlich von den Einschränkungen bei Arbeitnehmerüberlassung und Werkverträgen ausgenommen werden. Vielmehr sollte sich die Arbeitsmarktregulierung auf jene Branchen konzentrieren, in denen tatsächlich prekäre Arbeitsverhältnisse vorherrschen. Das Arbeitszeitgesetz muss flexibler ausgestaltet werden. Die gesetzlich vorgeschriebene elfstündige Ruhepause ist beispielsweise nicht mehr zeitgemäß und steht dem Wunsch nach flexiblen Arbeitszeiten entgegen. Auch die Arbeitsstättenverordnung und die betriebliche Mitbestimmung müssen der Entgrenzung von Arbeit Rechnung tragen und entsprechend angepasst werden. Flexible Arbeitsplätze können nicht nach den gleichen Maßstäben beurteilt werden wie der Arbeitsplatz in den Räumlichkeiten eines Arbeitgebers. Die umfassende Bitkom-Position zu arbeitsrechtlichen Anforderungen bei Industrie 4.0, auch zu Themen wie Aus- und Weiterbildung, Qualifizierung und Fachkräftesicherung, finden sich im Bitkom-Positionspapier »Arbeit 4.0 – Die deutsche Arbeitswelt zukunftsfähig gestalten«.

10 Urheberrecht

10.1 Ausgangslage

Eine bedeutende technische Neuerung der Industrie 4.0 stellt der 3D-Druck dar. Für den 3D-Druck wird eine Druckvorlage in Form einer CAD-Datei erstellt, die alle technischen Informationen für den Druckvorgang enthält. Die CAD-Datei wiederum kann am Computer mit Hilfe eines Konstruktionsprogramms oder mit Hilfe eines Scans des zu vervielfältigenden Objekts erzeugt werden. 3D-Drucker können Objekte herstellen, die immaterialgüterrechtlichen Schutz genießen. Fraglich ist, ob sich hier rechtliche Lücken auftun, die ein Handeln des Gesetzgebers erforderlich machen.

10.2 Bitkom-Position

Die derzeit geltenden Regelungen zum Immaterialgüterrecht wie Design-, Marken-, Patent-, Gebrauchsmuster- und Urheberrecht schützen ausreichend sowohl die für den 3D-Druck notwendige CAD-Datei, als auch das kopierte Objekt gegen Verletzungen. Dabei bietet das Urheberrecht den am weitesten reichenden Schutz gegen unbefugte Vervielfältigung. Eine gesonderte Regulierung erscheint momentan nicht erforderlich. Ein falscher Weg wäre in diesem Kontext die Anwendung von Urheberrechtsabgaben auf 3D-Drucker. Dies würde bisher ungelöste Rechtsprobleme und große Rechtsunsicherheit in den Anwendungsbereich von Industrie 4.0 einführen.

11 Knowhow-Schutz

11.1 Ausgangslage

Die [EU-Richtlinie 2016/943](#) vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung gewährt nach ihrem Art. 2 einen Rechtsschutz gegen unbefugten Zugriff auf Geschäftsgeheimnisse nur dann, wenn diese Geschäftsgeheimnisse vom Berechtigten durch »angemessene Geheimhaltungsmaßnahmen« vor Zugriff geschützt sind. Nur wenn der Berechtigte »angemessene Geheimhaltungsmaßnahmen« ergreift, nimmt die Richtlinie für die so abgeschirmten Informationen überhaupt erst von einem rechtlich schützenswerten Geschäftsgeheimnis aus. Diese Anforderungen laufen den Abläufen der Industrie 4.0 bis zu einem gewissen Grad zuwider, da Industrie 4.0 gerade einen blockadefreien Datenfluss zwischen vernetzten Unternehmen voraussetzt. Dennoch sind Unternehmen der Industrie 4.0 auf den rechtlichen Schutz ihres Knowhows besonders angewiesen, um ihre Marktposition bei Industrie 4.0 halten zu können.

11.2 Bitkom-Position

Bei der Umsetzung der EU-Richtlinie 2016/943 in deutsches Recht dürfen die Anforderungen an die »geeigneten Geheimhaltungsmaßnahmen« nicht zu hoch geschraubt werden, um einerseits den notwendigen Knowhow-Schutz bei Industrie 4.0 zu gewährleisten, andererseits aber keine Hindernisse für den für Industrie 4.0 ebenfalls essentiellen Datenaustausch aufzubauen. So müssen sowohl einfache faktische Schutzmaßnahmen (z. B. Einrichtung von Zugriffsbeschränkungen oder Verschlüsselungen) als auch juristische Vorsichtsmaßnahmen (z. B. Abschluss von Vertraulichkeitsvereinbarungen) jeweils isoliert für sich bereits als »geeignete Geheimhaltungsmaßnahme« ausreichen.

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 79 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, weitere 9 Prozent kommen aus Europa, 8 Prozent aus den USA. 4 Prozent stammen aus Asien, davon die meisten aus Japan. Bitkom fördert die digitale Transformation der deutschen Wirtschaft und setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

**Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.**

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom