IP/IT/Medien

August 2017

„Die allgegenwärtige Vernetzung von Personen, Dingen und Maschinen wird ganz neue Produktionsumgebungen hervorbringen, so eine Vision der Fertigung der Zukunft. In Deutschland arbeiten Industrie, Forschung und Politik unter dem Schlagwort „Industrie 4.0" an der Umsetzung dieser Vision." (Siemens)[1]

„Industrie 4.0 hat hohes Nutzenpotenzial für deutsche Unternehmen. Unternehmen wollen kräftig in Lösungen zu Industrie 4.0 investieren. 2020 sollen bereits 80 Prozent der Wertschöpfungsketten einen hohen Digitalisierungsgrad aufweisen. Das ermöglicht Datenaustausch entlang der gesamten Wertschöpfungskette in Echtzeit." (PWC)[2]

„Industrie 4.0 ist längst Realität: Maschinen werden von den Produkten selbst dynamisch gesteuert, individuelle Kleinst-Serien-Fertigungen auf ein und derselben Produktionsanlage sind möglich. Produkte erkennen im Voraus einen möglichen Defekt und leiten Wartungsarbeiten in die Wege. Die richtige Software macht es möglich." (Bernd Leukert, Mitglied des Vorstands der SAP)[3]

Inhalt

Industrie 4.0

Ein Überblick zu den rechtsgebietsübergreifenden Herausforderungen

1. Einleitung

Industrie 4.0 ist spätestens seit der CeBIT und Hannover Messe 2015 als Schlagwort in aller Munde. Der vorliegende Newsletter soll einen Überblick über die damit in Zusammenhang stehenden rechtlichen Herausforderungen geben. Diese wurden bisher nur wenig beleuchtet, die Diskussion kommt gerade in Gang. Der vorliegende Newsletter ist daher eine Momentaufnahme des derzeitigen Diskussionsstandes.

1.1 Industrie 4.0 ist ein Kunstbegriff zur Beschreibung der umfassenden Digitalisierung und Vernetzung der Industrie (-produktion)

Industrie 4.0 vereint damit vier Themenfelder, die in jüngerer und jüngster Zeit diskutiert werden.

- **Internet of Things:**

  Der Begriff Internet of Things bzw. Internet der Dinge bezeichnet die **Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer erledigen können**[4].

  Ein Beispiel aus dem häuslichen Umfeld könnte ein intelligenter Kühlschrank sein, der selbstständig Milch nachbestellt, sobald diese zur Neige geht. Ein Beispiel aus dem Automotive-Bereich kann das in der Produktion befindliche Auto sein, das nach Kundenwünschen konfiguriert die Maschinen an der Produktionslinie wie auch die technischen Agenten des Zulieferers über Bearbeitungs- und Materialwünsche informiert.

  Die Gegenstände im Internet der Dinge erfassen, speichern, tauschen untereinander und sammeln auch Daten über ihre Nutzer und Anwender. Hier ist die Wahrung der Souveränität der Nutzer und Anwender über ihr Persönlichkeits- und Kundenprofil ein entscheidendes Anliegen des Datenschutzes.[5] Im Übrigen stehen die Themen „Vertragsbeziehungen" und „Haftungsrisiken" im Zentrum des juristischen Interesses.

- **Cloud Computing:**

  „Cloud Computing ist ein Modell, das es erlaubt, **bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen** (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Management-Aufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."[6] Die Mehrzahl und die wichtigsten Anbieter von Cloud Computing-Lösungen und Ressourcen haben ihren **Sitz in den USA bzw. betreiben ein Rechenzentrum in EU-Drittstaaten**.

[1] Homepage Siemens, online im Internet (http://www.siemens.com/innovation/de/home/pictures-of-the-future/industrie-und-automatisierung/digitale-fabrik-industrie-4-0.html).
[2] Homepage PWC, online im Internet (http://www.pwc.de/de/digitale-transformation/pwc-studie-industrie-4-0-steht-vor-dem-durchbruch.html).
[3] Computerwoche, Artikel Bernd Leukert vom 13.01.2015 (http://www.computerwoche.de/a/industrie-4-0-software-macht-den-unterschied,3091777).
[4] SpringerGabler Verlag (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Internet der Dinge, online im Internet (http://wirtschaftslexikon.gabler.de/Archiv/1057741/internet-der-dinge-v4.html).
[5] Wikipedia, Internet der Dinge, Datengewinnung (http://de.wikipedia.org/wiki/Internet_der_Dinge).
[6] Bundesamt für Sicherheit in der Informationstechnik, Cloud Computing-Grundlagen, Zitat der Definition der US-amerikanischen Standardisierungsstelle NIST sowie der ENISA (https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/CloudComputing-Grundlagen.html).

- **Big Data:**

  Big Data bezeichnet den Einsatz großer Datenmengen aus vielfältigen Quellen mit einer hohen Verarbeitungsgeschwindigkeit zur Erzeugung wirtschaftlichen Nutzens[7]. Ein Beispiel kann die Gasturbine von Siemens sein, die ca. 1.500 Sensoren enthält, die permanent eine Unmenge an Daten über den Betriebszustand liefern und durch systematische Analyse dieser Big Data genaue Vorhersagen über Verschleiß, Wartungsbedarf und Ausfallrisiken ermöglicht.

  Aus juristischer Sicht stehen bei Big Data vor allem Fragen des **Datenschutzes** und des **Data Ownership** im Zentrum des Interesses.

- **Smart Factory:**

  Der Begriff Smart Factory bzw. auch Smart Production wird im Rahmen hochmoderner, roboterbasierter Fahrzeugproduktion verwendet. Es handelt sich bei Smart Factory um einen Begriff aus der Forschung im Bereich Fertigungstechnik, der auch zur Hightech-Strategie der Deutschen Bundesregierung als Teil des Zukunftsprojekts Industrie 4.0 gehört[8].

1.2 Rechtliche Themenfelder

Bei Industrie 4.0 stehen daher aus juristischer Sicht jedenfalls die Themen Datenschutz, Datensicherheit, veränderte Vertragsbeziehungen und die damit zusammenhängenden Probleme bei der Konfliktlösung im Zentrum des Interesses. Die aus technischer und betriebswirtschaftlicher Sicht diskutierte Notwendigkeit von Normierungen und Standardisierungen hat ebenfalls rechtliche Konsequenzen.

2. Datenschutz und Datensicherheit

2.1 Arbeitnehmerdatenschutz

Die datenschutzrechtlichen Aspekte – insbesondere, aber nicht nur im Hinblick auf Arbeitnehmerdatenschutz – bewegen sich beim Thema Industrie 4.0 insbesondere im Spannungsfeld der damit verbundenen Neuerungen der 4. industriellen Revolution in der Produktion und sind eng verknüpft mit der Thematik Big Data einerseits sowie Cloud Computing andererseits.

Die für datenschutzrechtliche Aspekte besonders relevanten Gesetze – das Bundesdatenschutzgesetz (BDSG), das Telemediengesetz (TMG), das Telekommunikationsgesetz (TKG) sowie ab 25. Mai 2018 die Datenschutz-Grundverordnung – sind durchgängig von vergleichsweise restriktiven Regelungen für den Umgang mit Mitarbeiter- wie auch Kundendaten geprägt.

Das Datenschutzrecht geht insgesamt von dem Grundsatz der Datensparsamkeit aus, das in einem Spannungsverhältnis mit der Grundidee von Big Data steht. Nun ist dieses Gebot der Datensparsamkeit wenig mehr als Wunschdenken der Datenschützer. Juristisch viel relevanter ist, dass im deutschen Datenschutzrecht ein sog. Verbot mit Erlaubnisvorbehalt im Hinblick auf jegliche Datenverarbeitung gilt. Darunter ist zu verstehen, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (vgl. § 4 Abs. 1 BDSG).

Damit datenschutzrechtliche Vorschriften überhaupt zur Anwendung kommen, ist Voraussetzung, dass es sich bei den betreffenden Daten um **personenbezogene** Daten handelt.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person – vom Gesetz „Betroffener" genannt (vgl. § 3 Abs. 1 BDSG).

Bei den Anwendungsfällen im Kontext Industrie 4.0 steht in aller Regel die Verarbeitung technischer Daten im Vordergrund. Beispielhaft seien hier wiederum die eingangs erwähnten Gasturbinen genannt. Doch auch diese **technischen Daten können zu personenbezogenen Daten werden, sobald es Verknüpfungsmöglichkeiten gibt und die Daten mit einem nicht unverhältnismäßig großen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können**. Insbesondere für dynamische IP-Adressen hat der EuGH mittlerweile klargestellt, dass diese personenbezogene Daten sein können, wenn der Webseitenbetreiber mit rechtlichen Mitteln an die nötigen Zusatzinformationen gelangen kann, um den Nutzer einer bestimmten dynamischen IP-Adresse zu identifizieren (EuGH, Urteil v. 19.10.2016 - C 582/14).

Industrie 4.0 und Big Data sind dadurch charakterisiert, dass besonders große Datenmengen gesammelt werden, laufend neue und ergänzende Datenquellen hinzukommen können, und neue automatisierte Analysen und Analysemöglichkeiten zugänglich und entwickelt werden. In solchen Szenarien ist es zum einen denkbar und zum anderen möglicherweise nicht von Beginn an erkennbar, dass sich durch das Hinzufügen weiterer Datenquellen, die Kombination von Daten und die Variation derer Analyse neue Zusammenhänge ergeben, die einen Personenbezug herstellen. Die weite Definition persönlicher oder sachlicher Verhältnisse einer bestimmten oder bestimmbaren Person lässt auf diese Weise in der Hauptsache technische Daten im Ergebnis zu personenbezogenen Daten werden.

Ein Beispiel für die Verknüpfungsmöglichkeit, wie vorbeschrieben, kann die Identifizierung der eine Maschine bedienenden Person sein; beispielsweise, weil aus den Datenbeständen des Unternehmens ersichtlich ist, wann welche Person welches Gerät bedient hat und dadurch mit verhältnismäßigem Aufwand eine Zuordnung der vom Gerät erhobenen, an sich technischen Informationen zu der Person des Bedienenden ermöglicht wird.

Lösungsansätze: Vor diesem Hintergrund kann es von Bedeutung sein, Arbeitsprozesse so zu gestalten, dass eine Verknüpfung mit

[7] bitkom Leitfaden Big Data Technologien – Wissen für Entscheider, 2014, Seite 12 (https://www.bitkom.org/noindex/Publikationen/2014/Leitfaden/Big-Data-Technologien-Wissen-fuer-Entscheider/140228-Big-Data-Technologien-Wissen-fuer-Entscheider.pdf).

[8] Wikipedia, Stichwort Smart Factory (http://de.wikipedia.org/wiki/Smart_Factory).

personenbezogenen Daten gerade vermieden wird. Eine solche Anonymisierung kann beispielsweise darin bestehen, dass vorgesehen wird, die Änderung von Betriebsparametern nur von Endgeräten aus zu ermöglichen, die eine Vielzahl von Personen im Betrieb nutzen. **Im Grundsatz ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können** (vgl. § 3 Abs. 6 BDSG). Anonymisierte Daten sind also keine personenbezogenen Daten; für diese ist der datenschutzgesetzliche Anwendungsbereich nicht eröffnet.

Als weiterer Lösungsansatz ist die Nutzung gesetzlicher Erlaubnistatbestände denkbar, insbesondere § 32 BDSG, soweit Mitarbeiterdaten betroffen sind. Demnach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Der Anwendungsbereich dieses Erlaubnistatbestandes ist also stets mit einer Interessenabwägung nach dem Grundsatz der Verhältnismäßigkeit („**erforderlich**") verknüpft.

Insbesondere im Bereich der Personalplanung und Regelbeurteilung lassen sich tendenziell weitere Spielräume nutzen.

Die Einwilligung der Betroffenen wäre im Bereich des Datenschutzrechts ein klassischer Lösungsansatz. Im Bereich des Arbeitnehmerdatenschutzes erweist sich dieses Instrument aber als schwieriger im Vergleich mit anderen Bereichen. Die Einwilligung von Mitarbeitern in die Verarbeitung ihrer personenbezogenen Daten wird regelmäßig kritisch gesehen, insbesondere weil die für eine wirksame Einwilligung erforderliche **Freiwilligkeit** fraglich sein kann. Ein Vehikel kann hier aber die Nutzung von **Betriebsvereinbarungen** darstellen, soweit Beteiligungsrechte der Interessenvertretungen (und entsprechende Interessenvertretungen selbst) bestehen. Namentlich betrifft das den jeweiligen Betriebsrat. **Mitbestimmungsrechte bestehen insbesondere im Bereich datenschutzrelevanter Regelungen der betrieblichen Ordnung und des Verhaltens sowie des Einsatzes technischer Überwachungseinrichtungen. Die Zustimmung des Betriebsrats ist dann Rechtmäßigkeits- und Wirksamkeitsvoraussetzung der jeweiligen Maßnahme, Anweisung etc.**

Soweit im Rahmen der Leistungserbringung für einen Kunden personenbezogene Daten von dessen Mitarbeitern verarbeitet werden sollen, ist jedenfalls zu überlegen, diesen vertraglich zur Einholung rechtlich wirksamer Einwilligungen der betroffenen Mitarbeiter zu verpflichten.

Falls personenbezogene Daten von Mitarbeitern verarbeitet werden und dabei externe Dienstleister oder sonstige Vertragspartner wie auch andere Konzernunternehmen eingebunden werden, bedarf es für eine Datenübermittlung in diesem Verhältnis stets auch einer **Rechtfertigung oder Einwilligung**. Anders verhält es sich, wenn der **Dritte im Auftrag der verantwortlichen Stelle** tätig wird. In diesem Fall handelt es sich bereits gar nicht um eine Übermittlung von personenbezogenen Daten, sondern der Auftragserbringer wird gerade nicht als Dritter betrachtet. Im Rahmen einer solchen Auftragsdatenverarbeitung bedarf es dann zwar einer entsprechenden schriftlichen Vereinbarung, eine andere Rechtfertigung oder Einwilligung zum Transfer der Daten an den Dritten bzw. Zugriff auf die Daten durch den Dritten ist jedoch nicht erforderlich.

2.2 Datentransfers in Drittstaaten

Im Zusammenhang mit Industrie 4.0 kann es zur Übermittlung von Daten ins Ausland kommen, beispielsweise im Rahmen der grenzüberschreitenden Zusammenarbeit, durch Datenanalysen im Ausland oder bei der Speicherung von Daten in der Cloud. Insbesondere wenn es sich dabei um personenbezogene Daten handelt, kann dies zu einer weiteren Komplexitätsstufe führen.

Die Übermittlung von personenbezogenen Daten **an Dritte** bedarf, wie erwähnt, grundsätzlich einer separaten gesetzlichen Rechtfertigung oder Einwilligung des Betroffenen (erste Prüfungsstufe).

Wie bereits dargestellt, gilt im Datenschutzrecht der Grundsatz des Verbots mit Einwilligungsvorbehalt, d. h. die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (vgl. § 4 Abs. 1 BDSG). Unter den Begriff des Verarbeitens fällt u. a. auch das Übermitteln personenbezogener Daten (vgl. § 3 Abs. 4 Satz 1 BDSG). Übermitteln ist dabei das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereit gehaltene Daten einsieht oder abruft (vgl. § 3 Abs. 4 Ziff. 3 BDSG).

Hinzu kommt, dass es im Datenschutzrecht **kein Konzernprivileg** gibt, d. h. jede Gesellschaft innerhalb eines Konzerns gilt stets als eigene verantwortliche Stelle und eine Übermittlung von personenbezogenen Daten von einer Konzerngesellschaft zu einer anderen unterliegt den allgemeinen datenschutzrechtlichen Bestimmungen.

Auf einer zweiten Prüfungsstufe ist zudem bei Datentransfers nach außerhalb der EU bzw. des EWR erforderlich, ein **angemessenes Datenschutzniveau** im Zielland sicherzustellen – denn die **Übermittlung hat zu unterbleiben, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn beim Datenempfänger ein angemessenes Datenschutzniveau nicht gewährleistet ist** (vgl. § 4b BDSG).

Soweit nicht die **EU-Kommission für das entsprechende Zielland ein angemessenes Datenschutzniveau festgestellt** hat, kann dies durch den Einsatz und die Vereinbarung der **EU-Standardvertragsklauseln erfolgen**, die sog. „Model Contracts for the transfer of personal data to third countries". Es ist darüber hinaus gegebenenfalls zu empfehlen, den Auftragsdatenverarbeiter ergänzend einem Standardvertrag zur Auftragsdatenverarbeitung gem. § 11 BDSG zu unterwerfen, soweit dessen Inhalte nicht bereits Bestandteil der Standardvertragsklauseln sind.

Als eine weitere und in der Vergangenheit von einigen Unternehmen genutzte Möglichkeit zur legalen Datenübermittlung in die USA existierte **Safe Harbor**. Safe Harbor ist an sich eine Entscheidung der Europäischen Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (2000/520/EG) – wurde regelmäßig aber wegen der Abstimmung und Vereinbarung mit den USA auch als **Safe Harbor-Abkommen** bezeichnet.

Im Rahmen des Safe Harbor-Verfahrens konnten US-Unternehmen sich auf einer Liste des US-Handelsministeriums eintragen lassen. Voraussetzung war, dass sie sich den Prinzipien von Safe Harbor unterwarfen und diese beachteten.

Angesichts der Enthüllungen über die weitreichenden Aktivitäten der US-amerikanischen National Security Agency (NSA) und insbesondere deren Programm PRISM wurde das Safe Harbor-Konzept zunehmend kritisch betrachtet. Schließlich entschied der EuGH, dass das Safe-Harbor-Abkommen nicht geeignet ist, Datentransfer in die USA zu legitimieren (Urteil v. 6.10.2015 – C-362/14).

Nach der Nichtigkeitserklärung von Safe-Harbor durch den EuGH haben die Europäische Kommission und die U.S.-Regierung am 2. Februar 2016 eine politische Einigung zu neuen Rahmenbedingungen für den transatlantischen Austausch personenbezogener Daten zu kommerziellen Zwecken erzielt, den sog. **EU-US Privacy Shield**. Seit dem 1. August 2016 können sich US-Unternehmen, die personenbezogene Daten aus der EU übermittelt bekommen und das Übereinkommen nutzen wollen, nach den neuen EU-US Privacy Shield-Richtlinien beim US-Handelsministerium zertifizieren lassen. In der EU ansässige Unterneh-men, die Daten an U.S.-Firmen übermitteln und dies nach den Regeln des EU-US Privacy Shield tun möchten, sollten bei ihren amerikanischen Geschäftspartnern eine solche Zertifizierung anregen.

Datenschutzaktivisten und EU-Datenschutzbehörden bezweifeln jedoch, dass der EU-US Privacy Shield die vom EuGH im Urteil vom 6. Oktober 2015 festgelegten Voraussetzungen erfüllt, aufgrund derer bereits die früheren Safe-Harbor-Grundsätze für ungültig erklärt wurden. Es ist daher zu erwarten, dass Aktivisten den Datentransfer auf Grundlage des EU-US Privacy Shields gerichtlich angreifen und die Gerichte der Mitgliedsstaaten diese Fälle erneut an den EuGH verweisen werden, um insoweit eine endgültige europaweite Klärung herbeizuführen.

Wie bereits erläutert, bietet sich als Lösungsansatz für internationale Auftragsdatenverarbeitung an, die hierfür vorgesehenen EU-Standardvertragsklauseln einzusetzen. Alternativ ist im Einzelfall auch die Einführung von sog. Binding Corporate Rules denkbar. Dabei handelt es sich um verbindliche unternehmensweit geltende Richtlinien, die unter Verpflichtung auf das europäische Datenschutzrecht einen Transfer von personenbezogenen Daten innerhalb einer Unternehmensgruppe über die EU-Grenzen hinaus ermöglichen sollen. In der Regel ist die Erstellung und Einführung von **Binding Corporate Rules** vergleichsweise aufwändig, da in der Regel **alle Aufsichtsbehörden der betroffenen Länder** einzubeziehen sind sowie die Rechtslage aller betroffenen Länder entsprechend abgebildet werden muss. Daneben besteht als „charmante" Variante der Verzicht auf die Übermittlung personenbezogener Daten, insbesondere durch **Anonymisierung von Datenbeständen**.

2.3 Datensicherheit

Durch die engmaschige und vielfältige Datensammlung über Prozesse, Maschinenzustände und Ähnliches im Rahmen des Einsatzes von Industrie 4.0-Technologien werden für Hacker, Konkurrenten und andere Dritte besonders attraktive Angriffsziele geschaffen.

Gleichzeitig ergibt sich durch die umfassende und allgegenwärtige Digitalisierung und Vernetzung quer durch alle Wertschöpfungsprozesse eine enorm vergrößerte Angriffsfläche. Ist erst einmal jede einzelne Maschine, jedes Produkt etc. über das Internet direkt oder indirekt erreichbar, multipliziert sich hierdurch naturgemäß die Anzahl potentieller Angriffspunkte.

Nicht nur in den Fokus der Öffentlichkeit und Medienberichtserstattung, auch in den der Politik ist das Thema Datensicherheit mittlerweile gerückt. Die Einführung des **IT-Sicherheitsgesetzes** (**„Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme"** vom 17. Juli 2015, BGBl. I, S. 1324) dürfte insoweit nur der Anfang sein. Nach der Regelung, welchen Anforderungen die Sicherheit bestimmter kritischer Infrastrukturen genügen muss, werden sich aller Voraussicht nach und vor dem Hintergrund der immer wieder und immer häufiger bekannt werdenden „Hacks" und sonstiger Cyberangriffe auf Unternehmen und damit auch auf deren Kunden- und Mitarbeiterdaten weitere gesetzgeberische Aktivitäten auf Themen der IT- und Datensicherheit konzentrieren.

Der **Datensicherheit dienende technische und organisatorische Maßnahmen** sind aber ohnehin schon nach geltendem Recht vorgeschrieben, soweit personenbezogene Daten verarbeitet werden (vgl. § 9 BDSG). Diese werden im eigenen Interesse der Verantwortlichen und Dateneigentümer ohnehin eine sinnvolle **Minimalabsicherung** widerspiegeln.

2.4 Data Ownership

Ein weiteres Thema ist die Frage, inwieweit gesetzlicher Schutz für im Rahmen von Industrie 4.0 und Big Data gesammelte und verwendete Daten besteht.

Ein **Eigentumsschutz** für Daten wird mangels Körperlichkeit derselben ausscheiden. Insoweit ist auch keine Regelungslücke ersichtlich, selbst wenn dies in Fachkreisen diskutiert wird.

Ggf. kommt ein urheberrechtlicher Schutz in Betracht. An den unstrukturierten „Rohdaten" wird mangels einer persönlichen geistigen Schöpfung im Sinne des Urheberrechts kein entsprechender Schutz bestehen können.

Auch ein **Datenbankurheberrecht** gem. § 4 Abs. 2 UrhG wird wohl ausscheiden, weil es in der Regel an der schutzbegründenden, schöpferischen Eigenart bei der Auswahl und Anordnung der Daten fehlt. Deren Gewinnung wie auch Auswahl und Anordnung stellt bei Big Data-Anwendungen stets nur die Vorstufe dar. Je nach Einzelfall kann zwar u. U. ein Datenbankurheberrecht angenommen werden, die Regel wird es aber nicht sein.

Dagegen kann allerdings ein **Datenbankherstellerrecht** gem. §§ 87 a ff. UrhG entstehen. Eine schutzfähige Datenbank in diesem Sinne ist eine **Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet** und einzeln **mit Hilfe elektronischer Mittel** oder auf andere Weise zugänglich sind und deren **Beschaffung, Überprüfung oder Darstellung** eine nach Art oder Umfang **wesentliche Investition** erfordert.

Da die Daten ohne Bezug zu einem bestimmten Prozess bzw. zu einer bestimmten Maschine etc. an sich ohne Wert sind, wird man davon ausgehen müssen, dass gerade eine systematische oder methodische Anordnung, wie in der Definition der Datenbank im Sinne § 87 a Abs. 1 UrhG verlangt, gegeben ist. Auch dürften die für Speicherung und Verarbeitung anfallenden Kosten in der Regel als durchaus wesentlich anzusehen sein. Allerdings werden die allermeisten Anwender entsprechende **Dienstleister** einschalten, die die Industrie 4.0- / Big Data-Anwendungen unterstützen bzw. die Dienste hierfür übernehmen. In solchen Konstellationen wird der Datenbankhersteller dann regelmäßig der Dienstleister sein. Um letztlich nicht auf den „Umweg" der Geltendmachung von Geschäfts- und Betriebsgeheimnissen, Herausgabepflichten von Beauftragten etc. verwiesen zu sein, empfiehlt es sich daher dringend, in den Verträgen mit diesen Dienstleistern entsprechende Regelungen zur „Data Ownership" zu treffen.

3. Vertragsrecht

Im Zuge der immer weiter fortschreitenden Digitalisierung des Produktionsprozesses im Rahmen von Industrie 4.0 werden sich die **Entwicklungen verstärken, die in den letzten Jahren im Bereich Software stattgefunden haben**. Natürlich spielen Softwarekomponenten bereits heute auch in der Produktion eine wichtige Rolle. Diese wird sich weiter verstärken. Die **Bedeutung der Auswertung von Daten wird steigen**. Ein zentrales Element von Industrie 4.0 ist aber auch die Vernetzung der einzelnen Anlagen im Produktionsprozess. Dies muss vertraglich abgebildet werden. Die einzelnen Maschinen arbeiten nicht mehr allein – entsprechend müssen gemeinsame Standards dauerhaft eingehalten werden.

3.1 „Machines as a Service" in der Vertragswirklichkeit

Das Schlagwort „Software as a Service" dürfte allgemein bekannt sein. Der Kauf von Software ist heute zwar immer noch gängig, verliert aber ständig an Bedeutung. Eine ähnliche Entwicklung ist auch in der Industrieproduktion zu erwarten: **„Machines as a Service"**.

Dies wird auch Auswirkungen auf die Vertragsbeziehungen haben.

Mit zunehmender Bedeutung der digitalen Komponenten in den Maschinen werden sich die vertraglichen Beziehungen auch immer weiter vom bisherigen Leitbild des Kaufvertrages über eine Maschine entfernen. Die Maschine wird nicht mehr nur physisch gewartet, vielmehr gewinnen Wartung und Pflege der Software an Bedeutung. Softwareupdates werden notwendig sein, damit die Maschine weiter einsetzbar bleibt und weiterhin mit anderen Maschinen kommunizieren kann. Man denke an eine Fortentwicklung von Kommunikations- und Sicherheitsstandards und das Schließen von Sicherheitslücken durch Softwareupdates.

Eine Finanzierung über die Jahre im Rahmen von Wartungs- und Pflegeverträgen wird vermehrt neben die Finanzierung durch den Kaufpreis treten und an Bedeutung gewinnen. Denkbar sind die verschiedensten **Erlös- und Vergütungsmodelle**. Statt der Maschine kann deren Leistung gekauft werden, vergütet beispielsweise nach **Stückzahl oder Effizienzgewinnen**.

In anderen Bereichen ist es längst üblich, dass beispielsweise **Hardware** günstig abgegeben wird, um später Einnahmen mit Zusatzprodukten zu erzielen. Wir kennen das nicht nur aus dem Bereich von Videospielkonsolen, in dem die Einnahmen durch Softwareverkäufe wichtig sind, sondern beispielsweise auch im Bereich von Kaffeemaschinen, in dem es deshalb zu einem Streit um die Patentierbarkeit von Kapseln kam. Auch Software selbst wird teilweise kostenlos angeboten, um Nachfolgegeschäft generieren zu können. All diese Entwicklungen werden wir in ähnlicher Form im Bereich von Industrie 4.0 künftig sehen.

Auch bei Einzelanfertigungen nach Kundenwünschen wird nicht mehr Kaufvertragsrecht zur Anwendung kommen, sondern das Recht des Werkliefervertrages.

3.2 Maschinen suchen sich ihre Kapazitäten selbst

Die Maschinen der „smart factory" suchen sich selbst Kapazitäten bei Zulieferern oder bedienen sich entsprechender Plattformen zum Auffinden von freien Kapazitäten bei den Zulieferern. Dies zieht sich durch die gesamte Lieferkette.

Wie das aussehen könnte, zeigt ein Blick auf den Handel mit Medien. Früher verhandelten beispielsweise Handelsvertreter und Buchhändler über abzunehmende Stückzahlen und ggf. Retourenrechte. Heute setzen viele auf das von Amazon angebotene Programm „Advantage". Dies bedeutet: Der Algorithmus von Amazon gibt die Taktung vor und entscheidet aufgrund einer aufwendigen Auswertung des Nutzerverhaltens, welche Medien in welcher Stückzahl von Amazon bestellt und dem Verleger / Publisher geliefert werden.

Übertragen auf die Automotive-Industrie könnte dies in Zukunft bedeuten: Aufträge werden künftig vom Autohersteller (OEM) an die Zulieferer auf verschiedenen Stufen (zunächst zu Tier 1, von dort zu Tier 2) durch standardisierte Prozesse ohne weitere Verhandlungen elektronisch abgeschlossen. In diesem Rahmen wird der (jeweilige) Lieferant Kapazitäten mitteilen, der Abnehmer wird Produkte abrufen. Dabei ist durchaus denkbar, dass der jeweilige Lieferant be-

stimmte Kapazitäten und Reaktionszeiten garantieren muss, ohne dass der Abnehmer zu einer Abnahme verpflichtet ist. Der gesamte Prozess wird in Echtzeit ablaufen und durch Algorithmen gesteuert.

Die Entwicklung wird in Richtung „künstliche Intelligenz" gehen. Daher ist die Rede davon, dass digitale Stellvertreter der einzelnen Beteiligten, sog. Agenten, weitgehend autonom handeln. Es stellt sich daher die Frage, ob bzw. wie diese automatisiert erzeugten Erklärungen einer natürlichen oder (eher) juristischen Person zuzurechnen sind. Teilweise wird diskutiert, hierauf das Stellvertreterrecht anzuwenden. Tatsächlich führt u. E. nach geltender Rechtslage kein Weg daran vorbei, derartige Erklärungen dem Nutzer / Eigentümer des „Agenten" zuzurechnen, sofern es sich überhaupt um rechtsgeschäftliche Erklärungen handelt. Etwaigen Unsicherheiten bei steigender Autonomie wäre durch technische Begrenzungen zu begegnen, beispielsweise durch sog. Attributzertifikate, die eine Überschreitung der „Vertretungsmacht" technisch unmöglich machen.

3.3 Vertragliche Absicherung der Datenqualität

Der durch eine solche Vernetzung erhoffte Effizienzvorteil steht und fällt mit der Qualität der erhobenen Daten und der darauf aufbauenden Prognosen.

Wenn wir unterstellen, dass die Automobilbauer ähnlich effiziente Prozesse und Datenanalysen einführen wie Amazon, dann wird schon beispielsweise anhand von Zugriffszahlen auf die Webseiten, Besuchen in Autohäusern und Probefahrten der künftige Kundenwunsch antizipiert werden – und die Produktion eines maßgeschneiderten Autos beginnt, bevor es der Kunde überhaupt bestellt hat.

Dies muss vertraglich abgebildet werden, insbesondere durch Absicherung der Datenqualität, beispielsweise über „Data Quality Level Agreements".

3.4 F & E: Annäherung an IT-Projektverträge

Zu erwarten ist auch im Bereich der Forschung und Entwicklung eine weitere Annäherung an IT-Entwicklungsverträge. Ein Schlagwort im Bereich Softwareentwicklung ist die sog. agile Softwareentwicklung, deren Erkenntnisse bei Industrie 4.0 zu diskutieren sein werden.

Als Leitsatz der agilen Programmierung gilt: **Je mehr nach Plan gearbeitet wird – d. h. nach der klassischen „Wasserfallmethode" – desto eher wird das Ergebnis der Planung entsprechen, aber nicht dem, was tatsächlich benötigt wird**.

Als Jurist muss hier natürlich hinzugefügt werden: auch wenn die Zusammenarbeit mit dem Kunden wichtiger ist als Vertragsverhandlungen, muss auch eine agile Entwicklung auf einer soliden vertraglichen Basis stehen. Selbst wenn von Verfechtern der agilen Programmierung die Zusammenarbeit mit dem Kunden höher bewertet wird als robuste Verträge: Verträge müssen dennoch so gestaltet sein, dass eine agile Entwicklung ermöglicht wird – wenn eine solche denn gewollt ist.

Festzuhalten bleibt:

Neue Geschäfts- und Erlösmodelle erfordern neue Vertragsmodelle.

Dazu die Thesen:

- Projektverträge werden sich den Verträgen für komplexe IT-Projekte weiter annähern.
- Neue Vertragsarten und gemischt typische Verträge werden eingeführt, ggf. inspiriert durch IT-Verträge.

Für die auftretenden vertraglichen Herausforderungen zeichnen sich die folgenden Lösungsansätze ab:

- Hersteller von Maschinen werden über Garantien und SLAs (Service-Level-Agreements) die Einsetzbarkeit und Übereinstimmung mit Normen und Standards sicherstellen müssen.
- Wartungsverträge und Serviceverträge enthalten zusätzliche Komponenten für Updates im Rahmen des vorgesehenen Life-Cycles – SLAs müssen in diesem Zusammenhang auch (geplante) Updates berücksichtigen, die im Extremfall zu einem Bandstillstand führen können.
- Bei Unternehmenskaufverträgen muss die entsprechende vertragliche Dokumentation die Kompatibilität der Maschinen und Sicherung der Daten vorsehen.

4. Kooperationen über Unternehmensgrenzen hinweg

Industrie 4.0 bedeutet auch **Kooperationen über Unternehmengrenzen** hinweg. Einerseits in Form von Kooperationen zwischen dem produzierenden Gewerbe und IT-Unternehmen, insbesondere solchen aus den Bereichen Big Data und Cloud Computing. Dies bedeutet aber auch eine horizontale Kooperation, beispielsweise gesteuert durch den Abnehmer, der sich – wie bereits erwähnt – softwaregesteuert freie Kapazitäten bei den Zulieferern sucht.

In Bezug auf **Big Data** bedeutet dies: **Auftragnehmer mit spezialisiertem Know-how übernehmen oder unterstützen bei der Datenerhebung und Analyse**. Denkbar ist auch eine Weiterverwertung der erhobenen und analysierten Daten. Der **Verkauf von Daten** kann (sekundärer oder sogar primärer) Umsatzbringer sein. Dies erfordert vertragliche Absicherungen, bei denen Datenschutzfragen und Datensicherheitsfragen eine zentrale Rolle spielen.

Ein zentraler Verhandlungspunkt in diesem Zusammenhang wird die **Data Ownership** sein. Wie erwähnt, bestehen keine klassischen Eigentumsrechte an Daten. Geistige Eigentumsrechte sind eher fernliegend, am ehesten ist an das Recht des Datenbankherstellers zu denken. Abweichende vertragliche Regelungen sind denkbar und aus Sicht des produzierenden Gewerbes empfehlenswert.

Bei der Kooperation über Unternehmensgrenzen hinweg sind regelmäßig kartellrechtliche Vorgaben zu beachten.

Vertragstechnisch gehen wir von folgenden Lösungsansätzen aus:

- Datenschutz-Compliance wird eine Grundvoraussetzung sein;
- klare vertragliche Regelungen zur Abgrenzung von Verantwortlichkeiten und Festlegung von Data Ownership sind essenziell;
- das Instrument Auftragsdatenverarbeitung wird (auch verhandlungstaktisch) genutzt werden;
- spezifische Geheimhaltungs- und Vertraulichkeitsvereinbarungen bekommen einen hohen Stellenwert.

5. Haftung und Konfliktlösung

Das neue Set-up führt auch zu neuen Verantwortlichkeiten und neuen Herausforderungen im Bereich der **Haftung und Konfliktlösung**.

Diskutiert werden im Zusammenhang mit dem Internet der Dinge (smart products) zahlreiche **haftungsrechtliche Fragen**, u.a. eine Ausdehnung der Gefährdungshaftung. Dies würde aber eine gesetzgeberische Entscheidung verlangen. Daher ist, zumindest derzeit, die Frage auf Ebene des (Organisations-) Verschuldens zu lösen.

Bandstillstand und Serienschäden sind als konfliktträchtige Szenarien bekannt und werden es bleiben. Die Herausarbeitung des Verursachungsbeitrags wird aber schwieriger.

Die Systeme werden komplexer, was nicht zuletzt eine vertragstechnische Herausforderung darstellt. Verträge müssen selbstverständlich in der Praxis gelebt werden, um juristisch durchsetzbar zu bleiben – angesichts der Komplexität der Systeme werden aber **Beweislastregeln** enorm wichtig werden. Im Bereich von IT-Projekten lässt sich dies jetzt schon beobachten. Beweislastfragen sind häufig streitentscheidend. Zur Sicherstellung eines Minimums an Sachkunde werden sehr häufig **Schiedsklauseln** vereinbart.

Je stärker die Produktion vernetzt ist und je eher sie datengesteuert ist, desto stärker rückt auch die Datenqualität als möglicher Schadenverursacher in den Mittelpunkt des Interesses. Zu denken ist hier beispielsweise an die Nutzung von fehlerhaften Daten Dritter oder Fehler bei der Datenübertragung.

Die vertraglichen Lösungsansätze:

- klare vertragliche Verteilung von Rollen und Verantwortlichkeiten;
- Data Quality Level Agreements;
- ggf. Variation der Beweislastverteilung, z.B. durch die Vereinbarung von Hinweispflichten eines Dienstleisters auf fehlerhafte Daten des Anwenders – natürlich gepaart mit den entsprechenden Rechtsfolgen bei Unterlassen eines entsprechenden Hinweises.

6. Standardisierungen, Normierungen

Als zentrales Thema im Zusammenhang mit Industrie 4.0 wird auch immer wieder das Thema Normen, Zertifizierungen und Standards genannt. In Bezug auf technische Normen dürften die „üblichen Verdächtigen" aus dem Bereich der Normierung relevant sein bzw. werden, beispielsweise DIN und ISO.

Zu verweisen ist jedoch auch auf das BMBF „Zukunftsprojekt" bzw. die „Plattform" Industrie 4.0 mit einer Referenzarchitektur.

Wo **Standards durch Schutzrechte, insbesondere Patente,** abgesichert sind, stellt sich die Frage nach der Lizenzerteilung an Dritte. Hier wird es auch an der Industrie selbst liegen, ob die Standardisierung durch eine **Institution der wichtigsten Marktteilnehmer** vorangetrieben wird, die **(kostenlose) Cross-Lizenzierung vorsieht**, oder ob die **einzelnen Marktteilnehmer ihre eigenen Schutzrechte** haben und durch Lizenzen verwerten. Bei der letztgenannten Variante ist eine lebhafte Prozesstätigkeit nicht selten, wo es typischerweise um die Vergabe von Lizenzen und deren entsprechenden Bedingungen geht. Dies lässt sich seit einiger Zeit besonders gut im Mobilfunkbereich beobachten, in dem regelmäßig um die Erteilung von Lizenzen und deren Bedingungen gestritten wird. Bisher ging man davon aus, dass der Inhaber eines sog. standardessenziellen Patentes automatisch eine marktbeherrschende Stellung innehat – mit den entsprechenden kartellrechtlichen Folgen, insbesondere also Lizenzen zu diskriminierungsfreien Bedingungen erteilen muss. Tut er dies nicht, kann er sich gegenüber dem Unternehmen, das sich um eine Lizenz bemüht, nicht auf sein Schutzrecht berufen (Zwangslizenzeinwand). Dieser Grundsatz gerät nun zunehmend ins Wanken. Das Landgericht Düsseldorf ging kürzlich in einem Verfahren davon aus, dass die Frage der marktbeherrschenden Stellung auch bei standardessenziellen Patenten einer Einzelfallprüfung unterliegt (France Brevets gegen HTC, Az. 4b O 140/13).

Dr. Andreas Lober,
Rechtsanwalt,
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Frankfurt am Main

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin
für Informationstechnologierecht
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Frankfurt am Main

Hinweise

Diese Veröffentlichung stellt keine Rechtsberatung dar.

Wenn Sie diesen Newsletter nicht mehr erhalten möchten, können Sie jederzeit per E-Mail (bitte E-Mail mit Betreff „Abbestellen" an **Melanie.Jost@bblaw.com**) oder sonst gegenüber BEITEN BURKHARDT widersprechen.

Impressum

BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
(Herausgeber)
Ganghoferstraße 33, D-80339 München
AG München HR B 155350/USt.-Idnr: DE-811218811

Weitere Informationen (Impressumsangaben) unter:
https://www.beiten-burkhardt.com/de/hinweise/impressum

Redaktion (verantwortlich)

Dr. Andreas Lober, Rechtsanwalt

Ihre Ansprechpartner

Berlin • Kurfürstenstraße 72-74 • 10787 Berlin
Tilmann Lührig, Rechtsanwalt
Tel.: +49 30 26471-0 • Tilmann.Luehrig@bblaw.com

Düsseldorf • Cecilienallee 7 • 40474 Düsseldorf
Mathias Zimmer-Goertz, Rechtsanwalt
Tel.: +49 211 518989-0 • Mathias.Zimmer-Goertz@bblaw.com

Frankfurt am Main • Mainzer Landstraße 36
60325 Frankfurt am Main
Dr. Andreas Lober, Rechtsanwalt
Tel.: +49 69 756095-0 • Andreas.Lober@bblaw.com

München • Ganghoferstraße 33 • 80339 München
Matthias W. Stecher, Rechtsanwalt
Tel.: +49 89 35065-0 • Matthias.Stecher@bblaw.com

Weitere interessante Themen und Informationen zu unserer Expertise finden Sie in unserem Onlinebereich.