# Rechtliche Aspekte von Industrie 4.0

Leitfaden (Vorabfassung)
Stand: 1. April 2016

www.bitkom.org

bitkom

**Herausgeber**

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

**Ansprechpartner:**

Thomas Kriesel | Bitkom e. V.
T 030 27576-146 | t.kriesel@bitkom.org

# Inhaltsverzeichnis

# Danksagung

Der vorliegende Leitfaden zu rechtlichen Aspekten von Industrie 4.0 ist eine gemeinsame Publikation von Rechtsexperten der Bitkom-Mitgliedsunternehmen, die sich in ihrer beruflichen Tätigkeit intensiv mit den rechtlichen Rahmenbedingungen digitaler Geschäftsmodelle befassen. Die Erstellung dieses Leitfadens beruht jedoch weitgehend auf ihrem persönlichen und ehrenamtlichen Engagement.

Wir danken herzlich folgenden Personen für ihre Beiträge:

- Dr. Katharina Garbers-von Boehm, CMS Hasche Sigle
- Dr. Philipp Haas, Bosch Innovation Software GmbH
- Björn Helwig, DLA Piper UK LLP
- Nils Hullen, IBM Deutschland GmbH
- Martin Schweinoch, SKW Schwarz Rechtsanwälte
- Olaf Vogel, Deutsche Telekom AG
- Peter Zang, Siemens AG
- Wolfgang Zeiler, Siemens AG
- David Ziegelmayer, CMS Hasche Sigle

# 1 Einführung

# 1 Einführung

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. Die Nutzung der in diesen Prozessen erzeugten Daten (z. B. Anwender-, Mess- und Produktionsdaten) und der Umgang mit diesen Daten werfen besondere rechtliche Fragestellungen auf, die bisher nicht abschließend geklärt sind. Auch stellen sich Fragen der rechtlichen Zurechnung, der Haftung und des gewerblichen Rechtsschutzes, die im Rahmen von Industrie 4.0 beantwortet werden müssen.

Diese Publikation extrapoliert die rechtlichen Fragestellungen entlang den Wertschöpfungsketten der Industrie 4.0 und versucht, Antworten und Praxishinweise zu geben. Sie wendet sich an Entscheidungsträger in der Industrie und in IT-Unternehmen. Die Darstellung soll sowohl die Fertigungsseite (Produktionsprozess) als auch die Kundenseite (Services) umfassen.

Dabei wird von der Prämisse ausgegangen, dass sich die rechtlichen Fragen der Industrie 4.0 in verschiedenen Zusammenhängen unterschiedlich stellen und auch nicht immer gleich zu beantworten sind. Entsprechend werden die rechtlichen Fragestellungen anhand einzelner Anwendungsbeispiele bzw. Anwendungsszenarien untersucht.

Zu beachten ist, dass diese Publikation lediglich eine Vorabfassung eines geplanten umfangreicheren Bitkom-Leitfadens zu Rechtsfragen der Industrie 4.0 darstellt. In der für Herbst 2016 zur Veröffentlichung vorgesehenen Endfassung des Leitfadens wird die Betrachtung auf weitere Rechtsgebiete ausgeweitet und die Darstellung der juristischen Zusammenhänge vertieft. Bei möglichen Abweichungen sind die Aussagen in der Endfassung des Leitfadens zugrunde zu legen. Diese Vorabfassung soll Denkanstöße setzen, kann aber keine endgültigen und umfassenden Lösungen präsentieren.

# 2 Begriffsbestimmung

# 2 Begriffsbestimmung

Diese Publikation versteht für Zwecke der hier vorgenommenen rechtlichen Betrachtung unter Industrie 4.0 die Vernetzung kommunikationsfähiger und einzeln identifizierbarer Systeme und Gegenstände in Produktions- und Vertriebsprozessen, die durch automatisierten Datenaustausch kommunizieren sowie darauf aufbauende datenbasierte Dienstleistungen. Kennzeichnend ist dabei, dass die 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. Die automatisierte Kommunikation wird zur Optimierung von Produktions-, Logistik-, Vertriebs- und Dienstleistungsprozessen oder zu sonstigen Steuerungsprozessen eingesetzt.

Weitere Ziele von Industrie 4.0 sind die exakt auf Wünsche und Anforderungen des Kunden zugeschnittene Herstellung von Maß-Produkten (z. B. individualisierte Implantate) sowie die Herstellung von Maschinen und Anlagen, die – zumindest in beschränktem Rahmen – eigenständig auf Umwelteinflüsse und deren Änderung reagieren können (z. B. Windräder, die sich auf die Windrichtung einstellen). Angestrebt wird auch die Parallelisierung von Entwicklungs- und Produktionsschritten im Rahmen einer Zusammenarbeit mehrerer Partner.

Industrie 4.0 ist durch zunehmende Digitalisierung und durch Entstehung von großen Datenmengen gekennzeichnet (Big Data), die zu erfassen und mit Mehrwert zu verarbeiten sind (Generierung von Smart Data). Diese Datenmengen werden vielfach in Clouds vorgehalten.

Im internationalen Kontext finden sich Begriffe wie »internet of things« oder »digitalisation«. Diese sind jedoch mit dem hier zugrunde gelegten Begriffsverständnis von Industrie 4.0 nicht deckungsgleich, sondern schließen weitere Bereiche (z. B. Smart home-Anwendungen oder Wearables) mit ein.

# 3 Anwendungsbeispiele für Industrie 4.0

# 3 Anwendungsbeispiele für Industrie 4.0

## 3.1 Vernetzte Fabrik (Smart Factory)

In einer Smart Factory werden dem im Produktionsprozess befindlichen Produkt die Informationen für die weiteren Stufen der Fertigstellung mitgegeben. Das Produkt kommuniziert (z. B. über RFID-Chips) mit Mess-, Prüfungs- und Fertigungsmaschinen und steuert seinen Fertigungsprozess damit weitgehend selbst. Der gesamte Produktionsablauf wird ebenfalls gesteuert und überwacht, die Bereitstellung benötigter Einzelteile und deren Beschaffung erfolgen durch M2M-Kommunikation und teilweise unternehmensübergreifend in der Zuliefererkette.

## 3.2 Vernetzte Logistik

Die Logistik organisiert die Versorgung mit Gütern und Waren sowohl für Verbraucher als auch im Produktionsprozess (supply chain). Insbesondere für die Zulieferung von Rohstoffen, Vorfabrikaten und Montageteilen im Produktionsprozess spielen Kosten- und Zeiteffizienz (Zulieferung »just in time«) eine überragende Rolle. Das jeweils richtige Gut muss entsprechend den Bedarfsanforderungen des Empfängers in der richtigen Menge und Sorte im richtigen Zustand, in der richtigen Zeit und am richtigen Ort geliefert werden. An diesem Zulieferprozess sind in der Regel mehrere Akteure beteiligt. Entsprechend hoch sind die Anforderungen an Organisation und Lenkung von Logistikketten. Die Vernetzung der Beteiligten erleichtert diese Lenkung und schafft weitere Effizienzgewinne. Durch Bereitstellung von Informationen in Echtzeit können Leerläufe und Missverständnisse vermieden und beschränkte Kapazitäten optimal genutzt werden.

## 3.3 Vernetzte Fernwartung (Predictive Maintenance)

Durch kontinuierliche Messung und Kontrolle von Betriebs- und Produktionsdaten kann per Ferndiagnose ein Wartungsbedarf wartungsintensiver Geräte sehr früh erkannt werden. Die Wartung kann vorgenommen werden, bevor eine Störung oder ein Schaden des Gerätes auftritt. Dadurch werden Wartungskosten und Betriebsunterbrechungen des Gerätes minimiert. Anwendungsbeispiele hierfür sind Aufzüge oder Rolltreppen. Dabei liefern Sensoren an den Fahrstühlen zum Beispiel Schwingungs-, Geschwindigkeits- oder Temperaturdaten, die über ein M2M-System über das Internet der Dinge an eine zentrale Connectivity-Management-Plattform gesendet werden. So kann Wartungsbedarf oder ein bevorstehender Ausfall frühzeitig bemerkt und beim Hersteller angezeigt werden. Ein Servicetechniker kann auf den Weg geschickt werden, bevor es zum Ausfall kommt.

Da er bereits durch Vorabanalyse weiß, welche Störungen drohen, kann er die benötigten Ersatzteile schon mitbringen. Kernstücke der Technologie bilden ein digitaler Werkzeugkoffer für die Techniker im Außendienst – basierend auf Apple iPhones und iPads – sowie das M2M-System für Generierung und Übertragung der Messdaten an den Fahrstühlen.[1]

## 3.4 Vernetzte Mobilität (Connected car und automatisiertes Fahren)

Ein Kraftfahrzeug kann in vielerlei Hinsicht vernetzt sein. Mit dem Internet verbundene Bordcomputer können zur Unterhaltung der Insassen und als Orientierungshilfe dienen. Die Ausrüstung mit Sensoren und Messgeräten erlaubt es, die Daten z. B. zu Temperatur, Geschwindigkeit, Straßenverhältnissen, Reifendruck, Fahrverhalten, Motorzustand zu ermitteln und an den Fahrer sowie an den Hersteller weiterzuleiten. Der Hersteller kann die Daten zur Produktverbesserung, für Wartungszwecke oder zur Prüfung von Gewährleistungsansprüchen verwenden oder sie an Dritte (z. B. Arbeitgeber, Behörden, Versicherungen, Diensteanbieter zur Abrechnung von Dienstreisen, Klärung von Unfallursachen bzw. Konzeption neuer Versicherungstarife oder Dienstangebote) weiterreichen.

Davon zu unterscheiden ist das automatisierte Fahren. Nach dem Konzept des automatisierten Fahrens übernehmen vernetzte Systeme Hilfsfunktionen für den Fahrer bis hin zu selbständigen, fahrerunabhängigen Fahr-, Brems- und Steuerungsfunktionen. Die Bandbreite reicht dabei von der Verfeinerung bereits heute genutzter Funktionen (z. B. Einparkhilfen, Optimierung des Kraftstoffverbrauchs oder Navigationsunterstützung zur Reaktion auf Verkehrs- und Wetterunregelmäßigkeiten), bis hin zum vollautomatisierten Fahren, das ein Eingreifen des Fahrers nicht mehr erfordert.[2]

Neben verkehrsrechtlichen Voraussetzungen sind Fragen hinsichtlich der Daten zu klären, die für die vernetzte Mobilität gesammelt, ausgewertet und verarbeitet werden. Wem sind die Daten über ein Fahrzeug, seinen Standort, das Fahrverhalten des Fahrers oder den Kraftstoffverbrauch zuzuordnen? Wer darf diese Daten erfassen und für welche Zwecke? Wer schützt die Kommunikation zwischen Fahrsystem und Infrastruktur- bzw. Fahrleitsystemen gegen unberechtigten Zugriff? Wer ist für Sicherheitslücken in diesem Bereich verantwortlich? Können diese Daten auch von Dritten für neue Geschäftsmodelle genutzt werden und ggf. unter welchen Bedingungen (z. B. von Kfz-Versicherungen als Kalkulationsgrundlage für neue Versicherungstarife)?[3]

1 Vgl. die Beispielbeschreibung unter: http://cases.t-systems.de/maschinenbau/use-case-schindler/das-internet-der-dinge-fuehrt-hoch-hinaus-42624.

2 Vgl. zu den verschiedenen Abstufungen des automatisierten Fahrens die ↗ Übersicht des Bundeskanzleramtes.

3 Zu den rechtlichen Fragen beim automatisierten Fahren vgl. auch die ↗ Überlegungen von Bundesjustizminister Heiko Maas.

# 4 Werkzeuge der Industrie 4.0

# 4 Werkzeuge der Industrie 4.0

## 4.1 Big Data-Analysen

Big Data-Analysen ermöglichen die gezielte Auswertung großer Datenmengen. Unternehmen verwenden Big Data-Analysen z. B. zur Berechnung der Kreditwürdigkeit, zur Bestimmung des Konsumverhaltens oder zur Verfeinerung medizinischer Behandlungen. Inzwischen benötigen Analyse-Tools für Big Data keine strukturierten Daten mehr, sondern können auch unstrukturierte Daten auswerten. Damit lassen sich Daten sogar in Echtzeit auswerten, die aus ganz unterschiedlichen Quellen stammen. Erst solche Analysewerkzeuge und Suchalgorithmen generieren aus unstrukturierten Datenhaufen (»Big Data«) »Smart Data«, also Datensätze, denen neue Erkenntnisse und ein wirtschaftlicher Wert innewohnen. Die Big Data-Analyse ist ein wichtiges Hilfsinstrument von Industrie 4.0, aber weder für Industrie 4.0 allein kennzeichnend noch in ihrer Anwendung auf Industrie 4.0 beschränkt. Die Anwendung dieses Werkzeugs setzt voraus, dass auf Daten zugegriffen werden kann, die zunächst erhoben und gesammelt, wenn auch nicht strukturiert werden müssen. Vorhandene Daten wecken die Begehrlichkeit, sie für andere Zwecke auszuwerten als ursprünglich beabsichtigt, z. B. könnten Bewegungs- und Verhaltensprofile für Überwachung und Strafverfolgung eingesetzt werden. Fraglich ist, ob und inwieweit Big Data-Analysen eine rechtliche Grundlage benötigen und wo ihre rechtlichen Grenzen verlaufen.

## 4.2 Cyber-Physical-Systems

Cyber-Physical-Systems verbinden Bauteile und Maschinen in einem Informationsnetz, das sich selbst steuert und überwacht. Solche Systeme sind mit eingebetteter Software ausgestattet und stellen Wechselbeziehungen zwischen realer Außenwelt und Diensten im Internet her. Mithilfe von Sensoren und Kameras verarbeiten die Systeme Daten aus der physikalischen Welt, geben sie über das Internet weiter und machen sie für netzbasierte Dienste verfügbar. Über Aktoren (Antriebselemente) wirken sie auf Vorgänge in der physikalischen Welt ein. Zu den typischen Anwendungsfeldern zählen Smart Grids in der Energieversorgung, Smart eHealth, Smart Home, Smart Mobility, und Smart Logistics. Im Produktionsumfeld von Industrie 4.0 spricht man bei einer Vernetzung von Cyber-Physical-Systems von Smart Factory.

## 4.3 3D-Druck

Der 3D-Druck eröffnet viele neue Anwendungsbereiche. Für Industrie 4.0 besteht der Wert des 3D-Drucks vor allem darin, schwer erhältliche Ersatzteile in niedrigen Stückzahlen oder sogar Einzelteile produzieren zu können. Dem Druckvorgang geht entweder ein 3D-Scan eines physischen Objekts oder die Konstruktion des zu druckenden Objekts mit Hilfe von CAD-Software (computer aided design) voraus. Die Druckinformationen aus der Scan-Datei oder der CAD-Konstruktion werden dann durch eine besondere Software in Druckerbefehle übersetzt.[4] Neben gewerblichen Schutzrechten für die 3D-Drucker selbst und ihre Komponenten sind insbesondere die Schutzrechte an den Objekten von rechtlicher Relevanz, die als Druckvorlage dienen. z. B. stellt sich die Frage, wie ein Hersteller eines solchen Objekts seine Patent-, Urheber- und Designrechte an dem Objekt durchsetzen und wirksam vermarkten kann sowie wo und wie der Betreiber eines 3D-Druckers und dessen Auftraggeber Lizenzen für den Nachdruck erwerben können.

## 4.4 Cloud Computing

Im Rahmen der Industrie 4.0 fallen riesige Datenmengen an. Um diese zu speichern und für Auswertungen verfügbar zu halten, wird vielfach auf Cloud Computing zurückgegriffen. In diesem Zusammenhang werden Fragen zur Exklusivität des Datenzugriffs, Datensicherheit und Geheimnisschutz relevant. Daher werden insoweit vor allem Private Clouds eingesetzt, Hybrid und Public Clouds finden jedoch zunehmend Berücksichtigung.

4 Vgl. zu Technik, Einsatzmöglichkeiten, Potenzial und Rechtsfragen des 3D-Drucks auch Bechtold, Stefan für World Intelectual Property Organization, Economic Research Working Paper No. 28 »3D printing and the intellectual property system«.

# 5 Rechtssphären und Interessen

# 5 Rechtssphären und Interessen

Im Rahmen von Industrie 4.0 fällt eine große Menge von Daten an: Produktionsdaten und Mitarbeiterdaten aus dem Produktionsprozess, Daten, die bei der Nutzung eines Produkts entstehen (reine Produktdaten, aber auch Daten über das Verhalten des Nutzers) und Daten, die aus der Zusammenarbeit mehrerer Unternehmen bei der Forschung oder im Wertschöpfungsprozess entstehen. An der Entstehung dieser Daten sind viele Personen beteiligt: z. B. Hersteller, Kunden, Kooperationspartner, Anbieter von Zusatzleistungen, Verbraucher. Sie können dabei ganz eigene, teilweise gegenläufige Interessen am Umgang mit diesen Daten haben. Auf der Seite der Anbieter eines Produkts oder einer Dienstleistung geht es um Zugriff auf Daten und die Möglichkeit zur Auswertung von Datenbeständen für neue Geschäftsmodelle, um Leistungsschutz für Investitionen zur Erhebung und Verarbeitung bestimmter Daten, um Verhinderung von Datenverlust, um gewerbliche Schutzrechte an den Erkenntnissen aus Datenauswertungen und um den wirtschaftlichen Wert von Datenbeständen.

Andererseits werden Unternehmen bestrebt sein, wichtige Datenbestände und damit ihre Betriebs- und Geschäftsgeheimnisse vor Zugriff durch Dritte zu schützen. Privatpersonen werden vielfach bestrebt sein, ihr Selbstbestimmungsrecht über ihre persönlichen Daten zu erhalten und nicht sämtliche Informationen über sich preiszugeben. Dabei können sie sich auf das Datenschutzrecht berufen und insbesondere die Auswertung ihrer persönlichen Daten verhindern. Schließlich werden Personen und Unternehmen, die an einem Vorgang zur Datenerzeugung oder Datenauswertung beteiligt sind, regelmäßig ein Interesse haben zu erfahren, für welche Zwecke und auf welche Weise die Daten genutzt und an wen sie weitergeleitet werden.

Aus volkswirtschaftlicher Sicht kann es in gewissem Umfang wünschenswert sein, dass Daten und Informationen offen für alle zugänglich (gemeinfrei) sind, damit sich der Innovationswettbewerb frei entfalten kann. Wenn Produkthersteller nicht über Ausschließlichkeitsrechte an Daten verfügen, lässt sich die Entstehung von Monopolen für Geschäftsmodelle auf dieser Datengrundlage leichter verhindern. Auch kann dann ein Kunde seinen Anbieter, der auf einer bestehenden Datengrundlage aufsetzen muss, leichter wechseln.

Jedoch müssen die Interessen von Anbietern und Nutzern der Industrie 4.0 nicht gegenläufig sein. So können z. B. Verkehrsunternehmen ein Interesse daran haben, Informationen über ihre Verkehrsmittel anderen Unternehmen zur Verfügung zu stellen, damit diese Mittel und Wege finden, um die Angebote des Verkehrsunternehmens zu verbessern. Und Verbraucher wie Unternehmen können ein Interesse an Produkten haben, die auf Grundlage umfangreicher Datenauswertungen speziell auf ihre Bedürfnisse zugeschnitten sind, ohne dass sie entsprechende Bedürfnisse artikulieren müssen.

Es obliegt der Rechtsordnung, die verschiedenen Interessen angemessen zum Ausgleich zu bringen. Das geltende Gesetzesrecht stellt in Teilbereichen Vorschriften zur Verfügung, die für die Datenströme und Anwendungsszenarien in der Industrie 4.0 Regelungen enthalten. Denn Industrie 4.0 stellt noch eine relativ neue Entwicklung dar. Solange aber die geltende Rechtsordnung für den Umgang mit Daten und die Beurteilung von Anwendungsszenarien in der Industrie 4.0 ausreichend ist, sind keine spezifischen Vorgaben des Gesetzgebers erforderlich.

# 6 Rechte an Daten

# 6 Rechte an Daten

## 6.1 Themenaufriss

Für die Betrachtung rechtlicher Aspekte des Datenverkehrs ist zu unterscheiden zwischen »personenbezogenen Daten« (§ 3 Abs. 1 BDSG) und sonstigen Daten ohne Bezug zu einer konkreten natürlichen Person (reine »Maschinendaten«).[5] Der Umgang mit personenbezogenen Daten unterliegt den besonderen Anforderungen des Datenschutzrechts (vgl. dazu unten Kapitel 7). Aber auch sonstige Daten aus der Sphäre ihrer Kunden und aus betrieblichen Wertschöpfungsprozessen können für viele Unternehmen sehr wichtig sein und einen eigenen wirtschaftlichen Wert darstellen. Aggregierte (d. h. nicht mehr auf einzelne Individuen rückführbare) und ausgewertete Datenbestände über das Verhalten von Unternehmenskunden, Verbrauchern oder Nutzern technischer Geräte oder Betriebsdaten einer laufenden Maschine können Grundlage für die Entwicklung von neuen oder die Verbesserung von vorhandenen Produkten, Dienstleistungen und Geschäftsmodellen sein. Die Erfassung solcher Daten ist jedoch vielfach mit dem Eindringen in die Sphäre einer anderen Person verbunden, die an der Datenerzeugung zumindest beteiligt ist. Fraglich ist, ob dies rechtliche Bedenken auslöst, ob für eine Erhebung und Auswertung von Daten in diesen Fällen eine besondere Befugnis nötig ist und wie eine solche Befugnis ggf. erlangt werden könnte. Zudem erfolgt die Auswertung großer Datenmengen häufig nicht durch das Unternehmen, welches die Daten erzeugt oder sammelt, sondern durch einen externen Dienstleister für die Aufbereitung und Analyse.

Für Zwecke der Industrie 4.0 sind Unternehmen auf den Zugang zu Daten angewiesen, um weitere Geschäftsmodelle, Produktverbesserungen, Effizienzsteigerungen und eine bessere Bedienung von Kundenwünschen realisieren zu können. Neben einem Zugangsrecht sind aber weitere Rechte an Maschinendaten denkbar. Rechte an Daten können als (exklusive) Zuordnung zu einem Dateninhaber, als gemeinsames oder ausschließliches Nutzungsrecht, als Abwehrrecht gegen Zugriffe Dritter auf einen Datenbestand, als Recht der wirtschaftlichen Verwertung, als Schadensersatzanspruch oder als Auskunftsanspruch ausgestaltet sein. Diese Rechte können in verschiedenen Konstellationen auch in Konflikt geraten. Wenn sich ein Akteur der Industrie 4.0 kein Zugriffsrecht auf benötigte Daten sichern kann, fehlt eine rechtssichere Grundlage für die Auswertung und Verwertung dieser Daten. Die Datennutzung könnte schlimmstenfalls durch andere Berechtigte untersagt und unterbunden werden.

5 Relevante »Maschinendaten« im Rahmen von Industrie 4.0 wären z. B. Informationen über das Verhalten von Maschinen oder einzelnen Maschinenteilen unter bestimmten Umweltbedingungen (z. B. Temperatur, Druck, Verschleiß) oder Informationen über den Ablauf von Fertigungsprozessen.

## 6.2 Rechtliche Fragestellungen

Inwieweit sind Daten und die Verfügungsbefugnis darüber nach geltendem Recht geschützt oder begrenzt? Gibt es ein Ausschließlichkeitsrecht an Daten oder sind Daten »Allgemeingut« und für jeden Interessierten zugänglich? Ist eine Zustimmung zur Nutzung der Daten durch den Datenurheber erforderlich oder kann er die Nutzung von ihm (mit-)generierter Daten verbieten? Ist diese Zustimmung ggf. begrenzt oder kann sie wirksam begrenzt werden auf bestimmte Datennutzer? Besteht ein Anspruch des Kunden auf Auskunft, welche Daten der Hersteller des von ihm genutzten Produkts sammelt? Besteht ein Anspruch des Herstellers auf Herausgabe von Daten, die ein Kunde mit einem Produkt dieses Herstellers erzeugt? Welche Datennutzung ist erlaubt bzw. bedarf einer besonderen Erlaubnis durch den Datenerzeuger?

## 6.3 Antworten und Handlungsempfehlungen

- **Kein Anspruch auf Datenzugriff und -verwertung im geltenden Zivilrecht:**
  Eine allgemeine Erlaubnis für die Erhebung, Sammlung, Nutzung oder Auswertung von »Maschinendaten« der Industrie 4.0 für private oder unternehmerische Zwecke ist im deutschen Recht derzeit nicht vorhanden. Eigentumsrechte des BGB sind nicht auf Einzeldaten anwendbar, da diese Rechte für Sachen konzipiert wurden. Auch das Recht des geistigen Eigentums lässt sich nicht auf Einzeldaten anwenden. Denn es schützt nur entweder Investitionen oder eine geistige Schöpfung von gewisser Schöpfungshöhe. Maschinell erzeugten Daten liegt gerade kein persönlicher geistiger Schöpfungsakt zugrunde, und ein rechtlicher Investitionsschutz umfasst regelmäßig nicht einzelne maschinell erzeugte Daten selbst, sondern höchstens Investitionen zur Erzeugung solcher Daten. Das geltende Recht gewährt auch keinen allgemeinen Auskunftsanspruch des Nutzers eines Produkts oder einer Maschine über die bei der jeweiligen Nutzung entstehenden Maschinendaten und deren Verwendung. Einen solchen Anspruch kennt nur das Datenschutzrecht für personenbezogene Daten (§§ 19, 34 BDSG). Andererseits ist die Erhebung, Vervielfältigung, Sammlung und Nutzung von Maschinendaten durch Unternehmen im geltenden Zivilrecht auch nicht generell verboten. Denn anders als für eine Datenerhebung zu staatlichen Zwecken ist für die Erhebung von Maschinendaten im Privatrechtsverkehr eine gesetzliche Ermächtigungsgrundlage nicht erforderlich.

- **Geltendes Recht sanktioniert Datenzugriff und -verwertung durch Unbefugte:**
  Auch wenn das geltende Recht umfassende eigentumsähnliche Rechte an Maschinendaten nicht vorsieht, erkennt es doch teilweise den Schutz von Maschinendaten an. Entsprechend gewährt es demjenigen, der Datenbestände gespeichert hat (Dateninhaber), gewisse Abwehransprüche, die z. B. mit Abmahnungen und Unterlassungsverfügungen durchgesetzt werden können. Immaterialgüterrecht, Wettbewerbsrecht und Strafrecht sanktionieren unbefugte Datenzugriffe sowie Veränderungen, Löschungen, Nachahmungen oder Manipulationen von geschützten Datenbeständen und die Überwindung von Sicherungsvorrichtungen für Daten. Hieraus können im Weiteren auch Schadensersatzansprüche des rechtmäßigen Dateninhabers gegen den unberechtigten Dritten resultieren. Wenn also ein Unternehmen technische Schutzvorrichtungen (z. B. Passwortschutz) gegen unbefugten Datenzugriff installiert, gewährt ihm dies eine gewisse faktische Ausschließlichkeit und Abwehrrechte gegen den Zugriff Dritter auf die Daten. Der rechtliche Schutz ist jedoch nicht lückenlos und bezieht sich nicht bei allen Vorschriften auf die Einzeldaten selbst. Insoweit wird immer eine Betrachtung des Einzelfalls nötig sein, um zu beurteilen, ob und inwieweit einer konkret beabsichtigten Datennutzung Rechte Dritter entgegenstehen.

- **Verträge zur Absicherung der Datenverwertung:**
  Da das gegenwärtig geltende Zivilrecht keine Zugriffs- und Verwertungsrechte für Maschinendaten gewährt, jedoch Abwehrrechte gegen Datenzugriffe zu beachten sind, die Rechtsentwicklung in diesem Bereich noch nicht abgeschlossen ist und es noch keine Rechtsprechung zu diesen Fragen gibt, empfiehlt sich, Nutzungs- und Zugriffsbefugnisse auf Maschinendaten, die in der Sphäre eines anderen Rechtssubjekts erzeugt werden (Datenerzeuger), vertraglich zu begründen bzw. abzusichern. In der jeweiligen vertraglichen Vereinbarung sollten insbesondere Nutzungsbefugnisse an Daten auch nach Vertragsende geregelt und damit mögliche Herausgabe- bzw. Löschungsansprüche des Datenerzeugers abbedungen werden. Dabei sollte eindeutig festgelegt werden, welcher Vertragspartner welche Daten erhält, wie er sie auswerten und verwenden darf und welche Verwendungen explizit ausgeschlossen sind, insbesondere, ob und mit welchen Dritten die Daten geteilt werden dürfen. Da aber faktisch nicht alle aktuell oder zukünftig denkbaren Verwendungen vertraglich erfasst werden können, sollte der Vertrag eine grundsätzliche Aussage darüber treffen, welcher der Vertragsparteien im Innenverhältnis die Rechte an den Daten zugeordnet sein sollen. Dabei ist das AGB-Recht der §§ 305 ff. BGB zu beachten. Das AGB-Recht sieht zunehmend auch für den Geschäftsverkehr zwischen Unternehmen Einschränkungen der vertraglichen Gestaltungsmöglichkeiten vor.

- **Datenmanagement einrichten:**
  Die Bestimmung und Abgrenzung von Rechten an Daten ist schwierig und hängt teilweise von der Art der Daten selbst ab (von wem wurden sie erzeugt, welche Informationen enthalten sie, bestehen an ihnen Abwehrrechte gegen Datenzugriff). Daher ist es sinnvoll, dass ein Unternehmen seine Datenbestände entsprechend daran bestehender Rechte kategorisiert und kontrolliert. Mit Applikationen, die aus der IT-Verwaltung von Mobilgeräten bekannt sind, können Unternehmen sichere, kontrollier- und verschlüsselbare Bereiche (»Datencontainer«) in einer IT-Umgebung schaffen. Die Zugriffsmöglichkeiten können dann auf einzelne Container beschränkt und von anderen Daten auf dem Speichermedium isoliert werden. Für erhöhte Datensicherheit ist es zudem möglich, die Kommunikation mit den Containern über einen privaten Kommunikationskanal zu betreiben, der jegliche Verbindung verschlüsselt und authentifiziert. Dieser Ansatz schirmt das Netzwerk gegen Angriffe, Malware und befallene Geräte ab, da sich nur der gesicherte Container mit dem Unternehmensnetz eines externen Dritten verbindet.

# 7 Vorgaben des Datenschutzrechts

# 7 Vorgaben des Datenschutzrechts

## 7.1 Themenaufriss

Datenschutz gilt nur für personenbezogene Daten im Sinne von § 3 des Bundesdatenschutzgesetzes (BDSG). Die Bestimmung personenbezogener Daten und die Abgrenzung zu nicht dem Datenschutz unterliegenden Daten ist schwierig und umstritten. So hat z. B. der BGH mit Beschluss vom 28.10.2014 (Az.: VI ZR 135/13) dem EuGH erneut die Frage vorgelegt, ob auch personenbeziehbare Daten, z. B. IP-Adressen als personenbezogene Daten anzusehen sind, obwohl der EuGH hierzu bereits eine Entscheidung getroffen hatte (vgl. Urteil vom 24.11.2011 in der Rs. C 70/10, Rz. 51). Die Frage der Personenbeziehbarkeit durch IP-Adressen ist auch für die Industrie 4.0 relevant, weil Daten in der Industrie 4.0 vielfach über das Internet übermittelt werden. Personenbeziehbare Daten lassen lediglich indirekte Rückschlüsse auf eine Person und ihr Verhalten zu, z. B. über die Auswertung von Geschwindigkeits- und Bremsdaten auf das Fahrverhalten.

Das Datenschutzrecht folgt dem Prinzip des Verbots mit Erlaubnisvorbehalt. Das bedeutet, dass die Erhebung, Sammlung und Verarbeitung von personenbezogenen Daten untersagt ist, wenn nicht ein Gesetz die Datenverarbeitung erlaubt. Soweit eine besondere Ermächtigungsgrundlage für Erhebung und Verarbeitung personenbezogener Daten fehlt, ist die Einwilligung des Betroffenen (= Zuordnungssubjekt personenbezogener Daten) einzuholen.

## 7.2 Rechtliche Fragestellungen

Unternehmen der Industrie 4.0 werden bestrebt sein, die hohen Anforderungen des BDSG an den Umgang mit personenbezogenen Daten zu vermeiden, wenn es nicht gerade auf die Auswertung solcher Daten ankommt. Wie aber sind personenbezogene Daten von nicht personenbezogenen Daten rechtssicher abzugrenzen? Und wie kann die Anwendung des BDSG zulässigerweise vermieden werden?

Eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Industrie 4.0 enthält das geltende Recht nicht. Bestehende Erlaubnistatbestände gelten immer nur für einzelne, abgegrenzte Anwendungsfelder. Inwieweit aber nutzen diese Erlaubnistatbestände für Industrie 4.0 und wie weit reichen sie? Und welche Anforderungen stellt das BDSG an eine wirksame Einwilligung, falls keine sonstige Erlaubnisgrundlage nutzbar gemacht werden kann?

Schließlich ist für die betroffenen Unternehmen von Interesse, welche Sanktionen für Verstöße gegen das Datenschutzrecht drohen.

## 7.3 Antworten und Handlungsempfehlungen

- **Anwendungsbereich des Datenschutzrechts:**
  Unternehmen, die personenbezogene Daten erheben, verarbeiten oder nutzen wollen, haben als verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG die Vorgaben des BDSG zu beachten. Zwar enthält § 3 Abs. 1 BDSG eine Definition personenbezogener Daten, diese ist jedoch nicht eindeutig und in der Praxis schwer zu handhaben. Insbesondere verursacht das Kriterium der »Personenbeziehbarkeit« Anwendungsunsicherheiten. Aufgrund dieser Unsicherheiten können in einen auszuwertenden Datenbestand unbeabsichtigt Daten geraten, die dem Datenschutz unterliegen und die Verwertung der Ergebnisse aus der Datenauswertung beeinträchtigen. Wegen der begrifflichen Unklarheiten kann die Grenze zwischen personenbezogenen Daten einerseits und reinen Maschinen- oder Umweltdaten andererseits nicht abstrakt, sondern nur im konkreten Anwendungsfall bestimmt werden. Für den Personenbezug kommt es in jeder Situation darauf an, welche Daten von wem für welchen Zweck mit welchen Zusatzinformationen erhoben und gespeichert werden und wem die verantwortliche Stelle die von ihr gesammelten Daten zugänglich macht. Werden z. B. im Connected Car Daten über Straßen- und Wetterverhältnisse und das Verkehrsaufkommen verarbeitet, ist damit noch kein Personenbezug hergestellt. Werden diese Daten jedoch mit Informationen z. B. über Aufenthaltsort des Fahrzeugs, über Fahr- und Bremsverhalten und zurückgelegte Strecken angereichert und evtl. an den Arbeitgeber des Fahrers weitergeleitet, lassen sich Rückschlüsse auf das Verhalten des Fahrers ziehen. Daher könnte die Erfassung dieser Daten durch den Fahrzeughersteller oder durch Dritte die Einwilligung des Kfz-Halters und des Fahrers erfordern. Die bei der Kfz-Nutzung anfallenden Daten sollen dann personenbezogen im Sinne des BDSG sein, wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz- Kennzeichen gegeben ist.[6] Letztlich muss zumindest von einer Personenbeziehbarkeit von Daten ausgegangen werden, wenn sie nicht sicher ausgeschlossen werden kann.

- **Abschichtung von Datenbeständen:**
  Da die Verarbeitung personenbezogener Daten besonderen Anforderungen und Einschränkungen des Datenschutzrechts unterliegt, sollten pPersonenbezogene Daten müssen als solche identifiziert, gekennzeichnet, klassifiziert und abgeschichtet werden. Dies entspricht dem datenschutzrechtlichen Trennungsgebot, wonach personenbezogene Daten, die zu unterschiedlichen Zwecken oder von unterschiedlichen verantwortlichen Stellen erhoben wurden, getrennt verarbeitet und genutzt werden müssen. Insgesamt sollte die Verarbeitung personenbezogener Daten in der Industrie 4.0 möglichst weitgehend reduziert werden, d. h. Daten mit Personenbezug sollten entweder möglichst nicht erfasst werden oder ein vorhandener Personenbezug sollte vor der Verarbeitung entfernt werden. Dies entspricht auch dem Grundsatz der Datensparsamkeit, den das geltende Datenschutzrecht zugrunde legt. Es sollten nur die tatsächlich benötigten Daten und nur nach strengen, vorab rechtlich geprüften Kriterien erhoben und weitergeleitet werden.

6 Vgl. ↗ Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) unter 1.

- **Datenschutz by Design:**
  Bereits bei Konzeption und Konstruktion neuer Geräte und Produkte sollten Datenschutz und Datensicherheit berücksichtigt und einbezogen werden. So könnten z. B. bei Datenentstehung, Datensammlung und Datenverarbeitung verschiedene Sphären voneinander abgegrenzt werden, sodass Daten bereits dort verarbeitet werden, wo sie anfallen (Konstruktion von »Datenkapseln«). Außerdem können dem regelmäßig nicht versierten Endnutzer Sperr- bzw. manuelle Einstellungsmöglichkeiten an die Hand gegeben werden, mit denen er die Datenerhebung unterbinden kann (»Opt-Out«). Noch weiter geht der Ansatz »Privacy by Default«. Diese Methode zur Verringerung des Gefahrenpotentials für die informationelle Selbstbestimmung durch proaktive Technikgestaltung verhindert in der Ausgangsstellung, dass Daten erhoben bzw. gespeichert werden, bevor der Nutzer dies nicht ausdrücklich erlaubt (»Opt-In«).

- **Anonymisierung:**
  Die Anwendung des BDSG scheidet aus, wenn lediglich anonymisierte Daten verarbeitet werden. Nach § 3 Abs. 6 BDSG sind Daten als anonymisiert anzusehen, wenn sie nicht oder nur mit unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft zu einer konkreten Person rückverfolgt werden können. Eine Anonymisierung entsteht aber nicht oder wird wieder aufgehoben, wenn sich durch die gleichzeitige Verarbeitung zusätzlicher Daten und die Kombination von Daten innerhalb eines Datenpools ein Personenbezug wieder herstellen lässt.

- **Pseudonymisierung:**
  Bei der Pseudonomysierung nach § 3 Abs. 6a BDSG und § 15 Abs. 3 TMG werden der Name oder andere Identifikationsmerkmale durch ein Kennzeichen ersetzt, damit die Bestimmung des Betroffenen ausgeschlossen oder wesentlich erschwert ist. Dies kann z. B. durch Verschlüsselung erfolgen. Im Gegensatz zur Anonymisierung kann bei der Pseudonymisierung die Identitätsverschleierung wieder rückgängig gemacht werden. Pseudonymisierte Daten sind grundsätzlich vom Anwendungsbereich des BDSG erfasst, ihre Verarbeitung ist aber unter bestimmten Umständen und für bestimmte Zwecke durch Gesetz gestattet (z. B. § 15 Abs. 3 TMG).

- **Einwilligung in die Datenverarbeitung:**
  Wenn sich die Verarbeitung personenbezogener Daten nicht vermeiden lässt und kein gesetzlicher Erlaubnistatbestand passt, benötigt die verantwortliche Stelle die Einwilligung der betroffen Personen. Nach § 4 Abs. 1 BDSG ist die Einwilligung des Betroffenen in die Erhebung, Verarbeitung und Nutzung der auf ihn bezogenen Daten erforderlich, soweit keine sonstige gesetzliche Vorschrift diese Tätigkeiten erlaubt. Zur Erhebung und Verarbeitung zählt das BDSG z. B. auch das Sperren, Speichern, Verändern und Löschen von Daten (vgl. § 3 Abs. 3 und Abs. 4 BDSG). Irrelevant sind dabei Anlass der Datenbeschaffung, ihr Zweck und die beabsichtigte oder tatsächliche Verwendung der erhaltenen Informationen. Insbesondere sind dDie gesetzlichen Vorschriften sind auch dann zu beachten, wenn eine Absicht fehlt, die Informationen personenbezogen zu verwenden. Nach dem geltenden Datenschutzrecht gilt der Grundsatz der informierten Einwilligung (§§ 4, 4 a BDSG).
  Dem Betroffenen muss die beabsichtigte Verarbeitung seiner Daten transparent gemacht werden und er muss die Tragweite seiner Entscheidung absehen können. Die Person, die personenbezogene Daten erhebt, muss ihre Identität, den Zweck der Datenerhebung und Empfänger der erhobenen Daten gegenüber dem Betroffenen offen legen (§ 4 Abs. 3 BDSG).
  Eine Einwilligung des Betroffenen für die Verarbeitung seiner personenbezogenen Daten gilt nur für den Zweck, der dem Betroffenen bei Einholung der Einwilligung zur Kenntnis gegeben wurde. Eine Zweckänderung bedarf wiederum einer gesetzlichen Erlaubnis oder einer erneuten Einwilligung.

- **Sanktionen:**
  Verstöße gegen die Vorgaben des BDSG können mit Bußgeldern bis zu 300.0000 Euro, bei Vorliegen einer Bereicherungs- oder Schädigungsabsicht sogar mit Freiheitsstrafe geahndet werden (§§ 43, 44 BDSG). Nach der auf EU-Ebene bereits beschlossenen Daten-schutz-Grundverordnung werden die Bußgelder erheblich erhöht (auf bis zu 20 Mio. Euro oder 4% des weltweiten Jahresumsatzes für einen Verstoß).

# 8 IT-Sicherheit als rechtliche Herausforderung von Industrie 4.0

# 8 IT-Sicherheit als rechtliche Herausforderung von Industrie 4.0

## 8.1 Themenaufriss

Der IT-Sicherheit kommt in der Industrie 4.0 eine besondere Relevanz zu. Vernetzte Anlagen müssen eine gewisse Sicherheit bieten (Integrität, Vertraulichkeit, Verfügbarkeit der Systeme). Viele IT-Angriffe von außen lassen sich jedoch bereits durch die Umsetzung von Standard-sicherheitsmaßnahmen in vernetzten Anlagen abwehren (z. B. zeitnahes Einspielen aktueller Sicherheits-Updates, Virenscan, Firewall). Aus rechtlicher Sicht ist zwischen einer ordnungs-rechtlichen 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).

Selbst wenn nur ein einziges Unternehmen eine vernetzte Fabrik betreibt, bieten die Vernetzungen einzelner Komponenten des Produktionsprozesses, wie über RFID-Chips oder QR-Codes, Einfallstore für Angriffe. Diese Angriffe müssen entdeckt und abgewehrt werden können, damit Produktion und Qualität der Produkte nicht gefährdet werden.

## 8.2 Rechtsfragen

Fraglich ist, wie Mängel der IT-Sicherheit in das zivilrechtliche Haftungsregime einzuordnen sind, eventuell als zusätzliche Kategorie von Produktsicherheit und Produkthaftung? Fraglich ist in diesem Zusammenhang auch, wie der jeweils maßgebliche Stand der Technik zu ermitteln ist, dessen Unterschreitung eine Haftung nach sich ziehen kann. Fraglich ist des Weiteren, welche Pflichten den Betreiber einer vernetzten Anlage treffen können. Besteht ggf. insoweit ein Unterschied bei der rechtlichen Bewertung vor und nach einer Cyberattacke, d. h. erhöhen sich die Sorgfaltspflichten nach einer Cyberattacke?

Schließlich: Gibt es gesetzliche Anforderungen für Produkte der IT-Sicherheit (z. B. im Produkt-sicherheitsgesetz oder im Produkthaftungsgesetz)? In wieweit ist die Berücksichtigung von IT-Sicherheit bei der Konzeption von Software, Produkten und Systemen (»Security by Design«) verpflichtend?

## 8.3 Antworten und Handlungsempfehlungen

- **Wenige zwingende Rechtsvorgaben:**
  Zwar gibt es keine allgemeingültige Vorgabe für die Einführung eines bestimmten Niveaus der IT-Sicherheit im Unternehmen. Das Gesetz definiert aber durchaus Daten, die als besonders

sensibel gelten und nach der Konzeption des Gesetzes besonders geschützt werden müssen (z. B. § 203 StGB, § 3 Nr. 9 BDSG). Daraus ergeben sich besondere, erhöhte Sorgfaltsanforderungen und Verantwortlichkeiten für diejenigen, die mit diesen Daten umgehen. Werden personenbezogene Daten verarbeitet, müssen die Schutzmaßnahmen zur IT-Sicherheit zumindest den Anforderungen des Datenschutzes nach § 9 BDSG entsprechen. Wird der vom Gesetz verlangte Sorgfaltsmaßstab nicht beachtet, drohen Strafen und Bußgelder. Zur Einhaltung eines bestimmten IT-Sicherheitsniveaus gesetzlich verpflichtet sind auch Unternehmen, die kritische Infrastrukturen betreiben, und Anbieter von Telemedien (z. B. Plattformbetreiber).

- **Anpassung der IT-Sicherheit an Unternehmensbedürfnisse:**
  Allgemein ist zu empfehlen, dass Sicherheitsmaßnahmen und –prozesse auf den jeweiligen Bedarf im Unternehmen angepasst, klar festgelegt, transparent dokumentiert und regemäßig aktualisiert werden. Dabei sollte auf den Datenaustausch mit Dritten besonderes Augenmerk gelegt werden. Insoweit ist auf Zugangssicherheit (Authentifizierung und Berechtigungskonzepte) und Übertragungssicherheit (sichere Kommunikationsprozesse durch Verschlüsselung) zu achten. Ein Daten- oder Systemzugriff von außerhalb des Unternehmens sollte beschränkt werden auf Informationen und Anwendungen, die innerhalb einer Kooperation tatsächlich benötigt werden. Zugriffe sollten auf jeden Fall protokolliert werden.

- **Zertifizierung für sensible IT-Systeme:**
  Ob IT-Systeme aktuellen Anforderungen der IT-Sicherheit genügen, kann in einem Zertifizierungsverfahren ermittelt und dokumentiert werden. Allerdings fehlt gegenwärtig eine angemessene und anerkannte Beschreibung der Soll-Beschaffenheit eines IT-Systems, sodass es kaum Zertifizierungsstandards gibt. Der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist für den Regelanwendungsfall von Unternehmen in der Industrie 4.0 zu überdimensioniert, der Aufwand unverhältnismäßig hoch. Die ISO/IEC-Reihe 27000 z. B. enthält zwar Empfehlungen für das Management von Informationssicherheit, aber überwiegend für organisatorische Maßnahmen im Unternehmen und nur im Anhang A des Standards 27001 auch Ausführungen zur technischen Umsetzung. Gegenstand eines Zertifizierungsverfahrens können auch die technischen und organisatorischen Maßnahmen sein, die nach § 9 BDSG einzurichten sind.

- **IT-Sicherheit beim Produktdesign:**
  Verfügbarkeit, Integrität der Systeme und (verschlüsselte) Verbindungen sowie die Sabotagefestigkeit (Resilienz) bei Produktion und Produkten nehmen einen fundamentalen Stellenwert ein. Deshalb sollte schon beim Entwicklungs- und Konstruktionsvorgang oder weitergehend für den gesamten Lebenszyklus eines Produkts der IT-Sicherheit Beachtung geschenkt werden. Rechtlich zwingende Anforderungen an die Sicherheit von einzelnen Produkten und Dienstleistungen lassen sich vereinzelt aus IT-Sicherheitsgesetz und Produktsicherheitsgesetz ableiten.

- **Kein absoluter Schutz:**
  Trotz aller Sicherheitsmaßnahmen kann es bei einer übergreifenden Vernetzung mehrerer Akteure in der Industrie 4.0 einen absoluten Schutz vor unberechtigtem Datenzugriff, vor Datenmanipulationen und Cyberattacken nicht geben.

# 9 Schutz des geistigen Eigentums (Intellectual Property)

# 9 Schutz des geistigen Eigentums (Intellectual Property)

## 9.1 Themenaufriss

Zum Schutz ihrer Investitionen und ihrer Stellung im Geschäftsverkehr können sich Unternehmen auf den gewerblichen Rechtsschutz und das Urheberrecht berufen (Rechtsschutz des geistigen Eigentums). Der Schutz setzt zunächst die Schutzfähigkeit der durchgeführten Investition voraus. Einzeldaten als solche sind nicht Gegenstand eines gewerblichen Schutzrechtes (vgl. 6.). Jedoch kann eine besondere Zusammenstellung von Daten, eine durch ein geschütztes Datenerzeugungsverfahren hervorgebrachte Datenfolge oder der Aufbau von Schutzvorrichtungen gegen den unbefugten Zugriff auf die Daten einen rechtlichen Schutz begründen (Datenbankschutz, Patentschutz, Strafrechtsschutz). Insoweit schützt das Recht Investitionen, die im Hinblick auf eine Datenerzeugung oder einen Datenbestand vorgenommen werden.

Weiterhin kann in Projekten der Industrie 4.0 Knowhow zum Einsatz kommen, das zwar keinen eigenen Schutzrechten zugänglich ist, jedoch über entsprechende Geheimhaltungsvereinbarungen und über das Wettbewerbsrecht (§ 17 UWG) rechtlich geschützt sein kann. Fraglich ist, wie weit der Rechtsschutz jeweils reicht und ob er für Zwecke der Industrie 4.0 ausreicht. Denn die einschlägigen Schutzrechte untersagen in der Regel nur die Nutzung des geschützten Knowhows selbst, nicht die Nutzung von Daten, die mithilfe des Knowhows erzeugt wurden.

In einer vernetzten Produktion, an der mehrere Unternehmen beteiligt sind, stellt sich darüber hinaus regelmäßig die Frage, welcher der Beteiligten die Verwertungsrechte und Nutzungsbefugnisse an den Arbeitsergebnissen bzw. an den Ergebnissen vorgelagerter Forschung erhält und wer die Verantwortung für etwaige Schutzrechtsverletzungen trägt.

## 9.2 Rechtsfragen

Inwieweit und unter welchen Voraussetzungen besteht Rechtsschutz für Knowhow, Instrumente und Neuerungen der Industrie 4.0 (z. B. für softwarebezogene Erfindungen, Datenanalysewerkzeuge oder Algorithmen) und welche Restriktionen sind dabei zu beachten?

Wann liegt eine Verletzung von Schutzrechten vor, schon bei einer unbefugten Entschlüsselung von Datenströmen oder erst bei der unbefugten Nutzung von Informationen aus diesen Datenströmen? Ist die Erstellung einer Druckvorlage für den 3D-Druck eines rechtlich geschützten Design-Objekts bereits eine Schutzrechtsverletzung? Liegt die Schutzrechtsverletzung in der vom Berechtigten nicht gestatteten Veräußerung der Druckvorlage oder erst im unbefugten Ausdrucken des Druckobjekts?

Welche Konsequenzen hat die Verletzung eines Schutzrechtes? Wer trägt die Verantwortung für Schutzrechtsverletzungen? Wie kann der Inhaber von Schutzrechten die Verletzung seiner Rechte auch in unternehmens- und grenzüberschreitenden Kooperationen effektiv verfolgen? Wie können Erkenntnisse und Forschungsergebnisse, die in Zusammenarbeit mehrerer Unternehmen entstanden sind, rechtskonform verwertet werden?

## 9.3 Antworten und Handlungsempfehlungen

- **Know-how-Schutz im geltenden Recht:**
  Das geltende Recht ist für die Herausforderungen durch etwaige Verletzungen von IP-Rechten im Rahmen von Industrie 4.0 (z.B. durch den Gebrauch von 3D-Druckern) grundsätzlich gut gerüstet. Der Schutz des Urheberrechts reicht dabei oftmals am weitesten. Denn anders als die gewerblichen Schutzrechte bietet es auch Rechtsschutz gegen private Verletzungshandlungen. Im gewerblichen Umfeld bietet aber auch das Wettbewerbsrecht weitreichenden Schutz. Ein Schutz über das Patent-, Gebrauchsmuster- oder Designrecht ist von Bedeutung für technische Lösungen und Designs, die faktisch nicht geheim gehalten werden können (z. B. bei Verkörperung in einem Produkt oder beim Einsatz in unternehmensübergreifenden Produktions-, Logistik oder Serviceprozessen). Die bei Industrie 4.0 zum Einsatz kommenden internetbasierten Prozesse und Systeme werden häufig grenzüberschreitend sein und somit einen möglichst internationalen Rechtsschutz erfordern. Hierbei ist aber das Territorialitätsprinzip bei den gewerblichen Schutzrechten zu beachten, wonach nationale Schutzrechte nur in dem Land verletzt werden, in dem sie gewährt worden sind. Bei grenzüberschreitenden Prozessen und Systemen können sich hierdurch im Patentrecht Probleme bei der Durchsetzung der Schutzrechte ergeben. Auf europäischer Ebene wird hierfür das kommende EU-Patent (offizieller Name: Europäisches Patent mit einheitlicher Wirkung) eine Erleichterung darstellen, da es für den größten Teil der EU relativ kostengünstig einen einheitlichen Patentschutz und einen einheitlichen Rechtsraum für ein Vorgehen gegen Schutzrechtsverletzungen bieten wird.

- **Investitionsschutz:**
  Erhebt ein Unternehmen Daten, stellt sie nach bestimmten Gesichtspunkten zusammen und leistet dafür einen gewissen wirtschaftlichen Aufwand, so kann ihm für den Schutz des wirtschaftlichen Aufwands ein Leistungsschutzrecht zustehen (z. B. Datenbankschutz nach UrhG).

- **Urheberrechtsschutz:**
  Wenn das Urheberrecht mangels Vorliegens eines urheberrechtlich geschützten Werks oder infolge einer nur schwer nachweisbaren Rechteinhaberschaft keinen hinreichenden Schutz bietet, so kann beispielsweise das Design- oder Markenrecht Abhilfe verschaffen. Hinsichtlich des Designrechts sollten Rechteinhaber sicherstellen, dass sie über eine hinreichende Zahl registrierter deutscher oder europäischer Designs verfügen, um so von der maximalen Schutzdauer von 25 Jahren profitieren zu können. Darüber hinaus empfiehlt es sich, beispielsweise in den USA und Japan auf entsprechende Schutzsysteme zurückzugreifen.

- **Vertragliche Absicherung des Know-how-Schutzes:**
  Soweit der gesetzlich vorgesehene Schutz für eine konkrete Geschäftsbeziehung nicht ausreichend erscheint, oder es um Gegenstände geht, die gewerblichen Schutzrechten nicht zugänglich sind (z. B. nicht patentfähiges Know-how), empfiehlt sich, eine Vertraulichkeitsklausel in den Vertrag über die Geschäftsbeziehung aufzunehmen oder ein besonderes Non-Disclosure-Agreement (NDA) – möglichst flankiert durch eine Vertragsstrafe bei Verstoß – abzuschließen.

- **Faktischer Know-how-Schutz:**
  Zu einem effektiven Schutz von Geschäfts- und Betriebsgeheimnissen sowie von vertraulichen Daten gehören auch technische Zugangsbarrieren, z. B. die restriktive Vergabe von Zugangsrechten zu bestimmten Informationen sowie die umsichtige Löschung von Daten, wenn ihre Speicherung nicht mehr notwendig ist. Zu schützendes Know-how ist zu identifizieren und ggf. als »geheim« oder »vertraulich« zu kennzeichnen; die Mitarbeiter, die Zugang zu dem Know-how (auf need-to-know Basis) erhalten sollen, sind ebenfalls zu identifizieren.

- **Strategie zum Schutz von Know-how:**
  Insbesondere im Umfeld von Industrie 4.0 kommt dem Schutz von Know-how entscheidende Bedeutung zu, weil einerseits im Know-how Wettbewerbsvorteile und letztlich die Existenzsicherung eines Unternehmens stecken und sich andererseits durch die zunehmende Vernetzung die Risiken für die Aufdeckung von Geschäfts- und Betriebsgeheimnissen erhöhen. Daher sollte jedes Unternehmen eine Strategie entwickeln, wie es auf der Basis der vorhandenen gewerblichen Schutzrechte sein Know-how, seine Produkte und damit seine Investitionen schützen kann.
  Zur Umsetzung einer solchen Strategie gehören der Abschluss von Vertraulichkeitsvereinbarungen (NDA), die Sensibilisierung von Mitarbeitern für den Umgang mit Know-how und die Einrichtung technischer Maßnahmen (z. B. Mailverschlüsselung) und der Erwerb gewerblicher Schutzrechte. Bei Verletzungen von Rechten sollten Ansprüche schnell im einstweiligen Verfügungsverfahren geltend gemacht werden. Ob eine Abmahnung sinnvoll ist oder bei noch notwendiger Beweissicherung der Überraschungseffekt eines unangekündigten Vorgehens ausgenutzt werden sollte, ist Frage des Einzelfalls.

# 10 Vertragsrechtliche Zurechnung von »Maschinenerklärungen«

# 10 Vertragsrechtliche Zurechnung von »Maschinenerklärungen«

## 10.1 Themenaufriss

In der Industrie 4.0 kommunizieren Maschinen autonom miteinander. 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 und 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).

Das deutsche Zivilrecht geht im Grundsatz davon aus, dass rechtlich relevante (Willens-) Erklärungen stets durch natürliche Personen gegenüber anderen natürlichen Personen abgegeben werden. Mit anderen Worten: Ein Mensch gibt eine (Willens-) Erklärung gegenüber einem anderen Menschen ab. Diese Erklärung wird zunächst dem Erklärenden selbst zugerechnet und kann unter den jeweiligen Voraussetzungen der Stellvertretung einer anderen natürlichen Person oder einer juristischen Person zugerechnet werden.

## 10.2 Rechtliche Fragestellungen

Zu klären ist, ob und wie autonome »Maschinenerklärungen« rechtlich relevante (Willens-) Erklärungen darstellen können und wem sie ggf. zuzurechnen sind. Wie kann die Abgabe einer »Maschinenerklärung« wirksam erfolgen und wann ist diese der anderen Maschine zugegangen? Können hierfür die Vorschriften des Allgemeinen Vertragsrechts im BGB Anwendung finden? Wann und in welchem Umfang sind Inhalte einer »Maschinenerklärung« dem Eigentümer, Besitzer oder Betreiber der »erklärenden« Maschine zuzurechnen? Treffen den Erklärungsempfänger etwaige Prüfungs- oder Mitteilungspflichten bei »unerwarteten« Nachrichten von einer Maschine gegenüber deren Eigentümer, Besitzer oder Betreiber? Kann der Eigentümer, Besitzer oder Betreiber von seiner Maschine ausgehende unerwünschte oder unrichtige Erklärungen widerrufen oder deren Wirkung beseitigen? Welche Rechtsfolgen hätte ein solcher Widerruf?

## 10.3 Antworten und Handlungsempfehlungen

- **Zurechnung:**
  Inhalte einer »Maschinenerklärung« sind für den Betreiber der Maschine, dem die Erklärung als deren Absender zugerechnet wird, auch dann verbindlich, wenn er diese Inhalte nicht näher voraussehen konnte (Ausnahme: für Empfänger klar erkennbar fehlerhafte Erklärungsinhalte). Für den Inhalt einer Erklärung und deren Verbindlichkeit kommt es darauf an, wie der Empfänger die Erklärung unter Berücksichtigung der gegebenen Umstände verstehen kann (Empfängerhorizont). Es können vorab durch Vertrag Parameter festgelegt werden, nach denen einer Maschinenreaktion ein rechtlicher Gehalt beigemessen wird oder nicht. Auf diese Weise programmiert der Maschinenbesitzer ein Erklärungsverhalten vor, das ihm dann auch zugerechnet werden kann.

- **Verantwortlichkeit:**
  Verantwortlich im rechtlichen Sinne für eine Erklärung bleibt derjenige, aus dessen Sphäre die Erklärung kommt. Auf Industrie 4.0 übertragen, heißt das, dass eine Maschinenerklärung der Partei zuzurechnen ist, die sich beim Vertragsabschluss eines autonomen Systems bedient bzw. ein autonomes System in die Vertragsdurchführung einbringt.

- **Fehlerhafte Erklärungen:**
  Auch für fehlerhafte Erklärungen bleibt derjenige verantwortlich, dem die Erklärung zuzurechnen ist. Erklärungswirkungen können nur nach allgemeinen Regeln beseitigt werden (etwa durch Anfechtung). Für maschinengenerierte Erklärungen, deren Verbindlichkeit der Absender nicht mehr beseitigen kann, deren Inhalt er aber später so nicht mehr will, hat der Absender – unter den notwendigen Voraussetzungen – nur Ansprüche gegen Dritte (Schadensersatz gegen Maschinenhersteller).

- **Empfang von Maschinenerklärungen:**
  Sinnvoll sind Vereinbarungen im Vertrag, wonach der Empfänger den Zugang einer Nachricht bestätigt und auf ungewöhnliche Nachrichteninhalte hinweisen muss.

# 11 Verantwortung und Haftung

# 11 Verantwortung und Haftung

## 11.1 Themenaufriss

Im deutschen Recht gilt der Grundsatz, dass nur natürliche Personen im rechtlichen Sinn verantwortlich sein können. Eine Haftung setzt im Regelfall ein persönlich vorwerfbares Verhalten einer natürlichen Person voraus (Haftung nur bei Verschulden). Da das Charakteristikum von Industrie 4.0 gerade darin besteht, dass Maschinen miteinander kommunizieren und Prozesse automatisiert ablaufen, sind natürliche Personen als Auslöser und Urheber einer Handlung teilweise schwer zu identifizieren. Noch schwieriger kann es sein, aus einem Maschinenfehler einen persönlichen Vorwurf abzuleiten.

Des Weiteren werden Eingriffsmöglichkeiten in automatisch ablaufende Prozesse der Industrie 4.0 bewusst limitiert und ein menschliches Handeln ist meist nicht mehr vorgesehen. Auch in den Datenaustausch von Abläufen der Industrie 4.0 kann sich der Anwender im Regelfall nicht einschalten. Insoweit verliert er in gewisser Weise an Selbstbestimmtheit und Steuerungsmacht. Aus juristischer Sicht schließt sich daran die Frage nach den passenden Haftungskategorien an: Soll an der vorherrschenden Verschuldenshaftung festgehalten werden oder sollte möglicherweise verstärkt auf verschuldensunabhängige Produkt-, Gefährdungs- oder Betreiberhaftung abzustellen sein?

Durch gezielte Big Data-Auswertungen teilweise nur beiläufig generierter Daten können Produkt- und Serviceverbesserungen erreicht oder das kundenspezifische Marketing durch individuelle Ansprache optimiert werden. Aber auch hier können Schadensursachen liegen, z. B., wenn eine betriebliche Optimierung fehlschlägt, Investitionen ins Leere laufen oder der Marktangang eines Unternehmens nicht in optimaler Weise gelingt. Eine Haftung erscheint jedoch mit Blick auf die nur schwer nachzuvollziehenden Kausalverläufe in Folge von Big Data-Analysen eher schwer begründbar. Daten können nicht unter denselben Umständen erneut erhoben werden, um deren Richtigkeit zu überprüfen. Sollte die Ursache nicht bei den erhobenen Daten zu finden sein, sondern nachweisbar in einer ungeeigneten oder fehlerhaften Analysemethodik liegen, kommt hinzu, dass die Anforderungen an die Qualität des insoweit zu erbringenden Ergebnisses häufig nur schwer zu bestimmen sind, weil es eher um unscharfe Trendanalysen oder sonstige Prognosen geht.

## 11.2 Rechtliche Fragen

Das Zusammenwirken unterschiedlicher vernetzter Systeme und die neue massenhafte Verbreitung von Smart Products durch die Industrie 4.0 erhöht grundsätzlich die Möglichkeit von Schäden.

Fraglich ist, ob dies auch zu neuen haftungsrechtlichen Grundsätzen führen muss. Zur Klärung einer möglichen Haftung im Rahmen von Industrie 4.0 ist zunächst zu untersuchen, welche Art von technischen Störungen naheliegende Auslöser möglicher Schadensereignisse sein können.

In Betracht kommen insoweit:

- Verbindungsunterbrechungen in der M2M- Kommunikation (und in der Folge z. B. Produktionsunterbrechung durch Störungen der Logistik, Verlust von Waren bei der elektronischen Verfolgung etc.);
- Fehlfunktionen der »künstlichen Intelligenz« in Smart Products (z. B. fehlerhafte Steuerung im Smart Home führt zu Frost- oder gar Brandschäden);
- Fehlerhafte Erhebung oder Interpretation von Big Data (z. B. Personenschäden in Krankenhäusern wegen mangelnder Medikamentenverfügbarkeit).

Des Weiteren gilt es, verschiedene Haftungsregime auseinanderzuhalten: vertragsrechtliche Gewährleistungshaftung, verschuldensabhängige Deliktshaftung, verschuldensabhängige Produzentenhaftung, verschuldensunabhängige Produkthaftung und Gefährdungshaftung. Fraglich ist, ob sich im Rahmen von Industrie 4.0 gesteigerte Anforderungen an die Haftung und an die Qualitätssicherung von Herstellern und Nutzern ergeben, die die kommerziellen Vorteile der Technologie aufzehren können.

Im Falle von »kooperierenden« Systemen, die neben- oder hintereinandergeschaltet sind, stellt sich die Frage, wie die Verantwortung den einzelnen Nutzern von Technologien der Industrie 4.0 zugerechnet wird. Gleiches gilt mit Blick auf die gemeinsame Verantwortung von Herstellern und Nutzern der Technologie im Verhältnis zum geschädigten Dritten. Wäre hier ggf. eine neue Kategorie der Produkthaftung für autonome Systeme zu schaffen?

Schließlich ist es für Unternehmen der Industrie 4.0 wichtig, mögliche Haftungsrisiken abzusichern. Daraus ergibt sich die Frage, inwieweit sich Haftungsrisiken der Industrie 4.0 quantifizieren und durch Versicherungen abdecken lassen?

## 11.3 Antworten und Handlungsempfehlungen

- **Geltendes Recht bietet ausreichende Grundlagen:**
  Die einzelnen Techniken der Industrie 4.0 sind nicht neu und konnten bisher mit den vorhandenen rechtlichen Instrumentarien bewertet und eingeordnet werden. Im Wesentlichen können erhöhte Haftungsrisiken durch Produktmängel und Fehlverhalten im Rahmen der Industrie 4.0 mit den Kategorien des geltenden Haftungsrechts erfasst werden. In digitalen Prozessen, die in der Industrie 4.0 vorherrschen, lassen sich – eine entsprechende Datensammlung vorausgesetzt – Systemzugänge, Daten- und Prozessveränderungen meist gut protokollieren und nachvollziehen. Entsprechend ist auch überprüfbar, welche Partei in welchem Umfang Schadensursachen gesetzt hat und für daraus entstandene Schäden verantwortlich ist. Um solche Überprüfungen durchführen zu können, sollten sich die Vertragspartner jedoch entsprechende Auditrechte und einen Zugang zum Datenpool, auch zu den Daten anderer Projektpartner gegenseitig zusichern.

- **Zurechnung von Schadensursachen:**
  Selbst wenn im konkreten Fall ein Schadensverursacher nicht sofort greifbar ist, gibt es immer jemanden, der eine fehlerhafte Software programmiert, ein fehlerhaftes Produkt in den Verkehr gebracht oder eine fehlerhafte Anlage aufgestellt hat. Zu dieser Person lässt sich jedenfalls theoretisch immer ein Kausalbezug im Sinne einer conditio sine qua non herstellen. Da nur menschliches Handeln als Anknüpfungspunkt für eine Haftung in Betracht kommt, muss als Zurechnungskriterium auf die Entscheidung zur Herstellung bzw. die tatsächliche Verwendung einer Technologie abgestellt werden. Der Haftungsvorwurf wird dabei auf das schuldhafte Inverkehrbringen oder die Entscheidung zur Nutzung verlagert. Dadurch kommt es nicht mehr auf eine spätere ggf. autarke Entscheidung der Maschine an, die den Schadenshergang ausgelöst hat. Ein entscheidendes Kriterium der Haftung ist somit die Vorhersehbarkeit der schädigenden Kausalität aus Sicht des Herstellers bzw. des späteren Verwenders. Dazu gehören auch die Möglichkeit einer zutreffenden Prognostizierung der Gefahrneigung und die Erkennbarkeit etwaiger Gegenmaßnahmen. Dieser Ansatz erscheint sachgerecht, weil letztendlich trotz »Autonomie« der Maschinen alle Vorgänge in der Logik der jeweiligen Steuersoftware angelegt sind. In der Regel wird es danach bei demjenigen, der lediglich eine Maschine entsprechend den Herstellervorgaben einsetzt, an der Vorhersehbarkeit fehlen.

- **Haftung bei unklaren Kausalbeziehungen:**
  Bei Kooperation mehrerer Unternehmen in einem Projekt der Industrie 4.0 oder bei Zusammenwirken mehrerer autonomer Systeme kann es allerdings schwierig werden, einen einzelnen Verursacher für Fehler zu identifizieren und ihm ein Verschulden nachzuweisen. Hierfür enthält § 830 Abs. 1 S. 2 BGB eine Vorschrift, wonach in diesen Fällen alle in Betracht kommenden Verursacher als Gesamtschuldner haften. Diese Vorschrift gilt jedoch nur für die deliktische, d. h. außervertragliche Haftung. Es empfiehlt sich, bei unklaren Verursachungsbeiträgen für eine vertragliche Haftung vorab festzulegen, wie die Verteilung der Haftungsbeiträge intern ausgestaltet werden soll, z. B. nach Wertschöpfungsanteilen, nach statistischen Verursachungsbeiträgen, nach Beteiligung am Auftragswert.

- **Qualitätssicherung zunehmend wichtig:**
  Da Produkthaftung gesetzlich festgelegt und nicht beschränkbar ist, sollte der Qualitätssicherung ein hoher Stellenwert eingeräumt werden. Die Qualitätssicherung eigener Prozesse muss die IT-Sicherheit mit umfassen, sie sollte regelmäßige Funktionstests und Audits durch Dritte einbeziehen.

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 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, 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. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom 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