PLATTFORM INDUSTRIE 4.0

ERGEBNISPAPIER

Industrie 4.0 – wie das Recht Schritt hält

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
Oktober 2016

Druck
MKL Druck GmbH & Co. KG, Ostbevern

Bildnachweis
Getty Images/Ralf Hiemisch (Titel); fotogestoeber – Fotolia (S. 4); vege – Fotolia (S. 5); Nonwarit – Fotolia (S. 6); vectorfusionart – Fotolia (S. 9); iconimage – Fotolia (S. 10); bluebay2014 – Fotolia (S. 13); cunaplus – Fotolia (S. 15); sebra – Fotolia (S. 17); Maksim Kabakou – Fotolia (S. 18); deepagopi2011 – Fotolia (S. 23); industrieblick – Fotolia (S. 25); Syda Productions – Fotolia (S. 27); contrastwerkstatt – Fotolia (S. 29)

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Einführung

Die Arbeitsgruppe 4 „Rechtliche Rahmenbedingungen“ (AG 4) hat in den vergangenen Monaten eine systematische Identifizierung und Bearbeitung der aus ihrer Sicht wichtigsten rechtlichen Themen von Industrie 4.0-Prozessen vorgenommen. Nachdem zunächst die Abstimmung über die erkennbaren Problemaufrisse im Vordergrund stand, befassten sich die gut 30 Unternehmens-/Verbandsjuristen und Anwälte im Anschluss mit der Analyse der durch die technischen Arbeitsgruppen der Plattform Industrie 4.0 entwickelten Anwendungsszenarien. Durch den so gewonnenen Einblick in die heutigen und zukünftigen technischen Möglichkeiten von Industrie 4.0-Anwendungsszenarien wurden die inhaltlichen Schwerpunkte der AG 4 in 17 Themenkomplexen strukturiert.

Zu jedem Themenkomplex wurde zunächst ein Steckbrief (Teil A) erstellt, der kurz den inhaltlichen Fokus und die sich ergebenden Fragen sowie Handlungsfelder mit Bezug auf Industrie 4.0-Prozesse skizziert.

An die Steckbriefe schließt sich Teil B mit der juristischen Einschätzung der Themenkomplexe an. Diese umfasst die Zusammenstellung und Prüfung der relevanten existierenden rechtlichen Grundlagen hinsichtlich der aufgeworfenen Fragen bzw. Handlungsfelder.

Im letzten Teil C werden zu jedem Themenkomplex mögliche Handlungsoptionen für den Gesetzgeber aufgezeigt sowie konkrete Handlungsempfehlungen aus Sicht der Arbeitsgruppe „Rechtliche Rahmenbedingungen“ gegeben.

Themenübersicht

Zivilrecht und Zivilprozessrecht

Vertragsfreiheit

A: Steckbrief

Worum geht es:

Die Umsetzung der Chancen und die Nutzung der Potenziale von Industrie 4.0 erfordern innovative Geschäftsprozesse und Geschäftsmodelle für neuartige Leistungen.

Für wichtige Aspekte innovativer Geschäftsmodelle können aufgrund des Neuheitsgrades naturgemäß keine spezifischen gesetzlichen Regelungen vorhanden sein (etwa für „automatisierte Willenserklärungen", Leistungsinhalte und Risikoverteilungen). Wichtige Aspekte und Faktoren können und müssen daher durch vertragliche Regelungen gelöst werden.

Um innovative Geschäftsprozesse und Geschäftsmodelle auch für neuartige Leistungen wirtschaftlich umzusetzen, sind belastbare vertragliche Regelungen unabdingbar notwendig. Die ausufernde Anwendung von AGB-rechtlichen Restriktionen im B2B-Bereich verhindert aber nach deutschem Recht eine belastbare vertragliche Grundlage.

Damit wird der Business-Case für innovative Geschäftsmodelle und notwendige Investitionen grundlegend in Frage gestellt.

Sich ergebende Fragen und Handlungsfelder:

- Inwieweit ist eine Anwendung von Verbraucherschutzregelungen des deutschen AGB-Rechts im B2B-Bereich gerechtfertigt? Prüfung einer Flexibilisierung des AGB-Rechts für B2B-Verträge über innovative Geschäftsmodelle.
- Wie kann die notwendige und klar prognostizierbare Belastbarkeit vertraglicher Vereinbarungen im B2B-Bereich (wieder) erreicht werden?
- Wie können Investitionshemmnisse für innovative Geschäftsprozesse und Geschäftsmodelle durch Unsicherheiten über die Wirksamkeit getroffener Vereinbarungen beseitigt werden? Prüfung der Steigerung internationaler Wettbewerbsfähigkeit für innovative Vertragsmodelle.
- Wie kann die notwendige Kalkulationsfähigkeit für innovative Geschäftsmodelle und neuartige Leistungen durch belastbare Vereinbarungen sichergestellt werden (etwa Wirksamkeit vereinbarter Leistungszusagen, Risikoverteilungen, Haftungsdefinitionen und -zuordnungen)?
- Prüfung vertraglicher Absicherungsmöglichkeiten im internationalen Kontext.

B: Juristische Einschätzung

Der rechtliche Status wird dargestellt durch die §§ 305 ff. BGB. Die Rechtsprechung wendet zunehmend ausufernd die Klauselverbote für Verbrauchergeschäfte (§§ 308, 309 BGB) über die Generalklausel des § 307 Abs. 2 BGB auch im unternehmerischen Geschäftsverkehr an. Der Gesetzesvorschlag zur Novelle des Bauvertragsrechts sieht in den Regelungen für den Geschäftsverkehr mit Verbrauchern sogar ausdrücklich Indizwirkungen für den Geschäftsverkehr mit Unternehmern im Sinne des AGB-Rechts. Die Regelung des § 310 Abs. 1 Satz 2 BGB, wonach bei einer Anwendung im unternehmerischen Geschäftsverkehr auf die im Handel geltenden Gewohnheiten und Gebräuche angemessen Rücksicht zu nehmen ist, ist in der Praxis und in der Rechtsprechung fast völlig bedeutungslos.

Die rechtsvergleichende Studie von Prof. Leuschner, Universität Osnabrück, im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz (veröffentlicht im Februar 2015) kommt in rechtstatsächlicher Hinsicht zu dem Ergebnis, das deutsche AGB-Recht stelle einen Standortnachteil dar und bedürfe einer Reform. Dieser Trend verstärkt sich noch durch die neueren Gesetzesinitiativen (etwa Bauvertragsrecht), die eine weiter ausufernde Anwendung von Verbraucherschutzvorschriften des AGB-Rechts auch im unternehmerischen Geschäftsverkehr fördern.

Dieser Standortnachteil zeigt sich auch im Vergleich mit angrenzenden europäischen Rechtsordnungen. Im ausländischen Recht international übliche Standardregelungen können oft nicht in Deutschland verwendet werden.

Für Unternehmen führt dies zu verstärkten Anreizen oder sogar einem faktischen Zwang zur Flucht aus deutschem Recht. Da weder das Internet noch die Industrie 4.0 nationale Landesgrenzen kennen, besteht die entsprechende örtliche Flexibilität. Sie ermöglicht es auch, die notwendige Voraussetzung für eine nach deutschem AGB-Recht zulässige Rechtswahl zugunsten eines ausländischen Rechts zu schaffen.

Gerade für kleine und mittlere Unternehmen ist die Flucht in ein ausländisches Recht mit einem erhöhten Aufwand und erhöhten Unsicherheiten verbunden, was den Standortnachteil für KMU noch verstärkt. Dies gilt umso mehr bei Start-ups: Zum einen erfolgt deren Ansiedlung möglicherweise gleich im Ausland. Zum anderen kann eine rechtliche Unterstützung in Form geeigneter Erklärungs- und Vertragsmuster nach geltendem AGB-Recht auch im unternehmerischen Geschäftsverkehr kaum mit sicher prognostizierbarer Wirksamkeit entsprechender Regelungen erfolgen. Vor diesem Problem stehen auch mögliche Konditionenempfehlungen für Regelungen in der Industrie 4.0.

C: Handlungsoptionen und Handlungsempfehlungen

Ziel und Voraussetzung für eine erfolgreiche Umsetzung von Industrie 4.0 in Deutschland muss es sein, die Belastbarkeit rechtlicher Regelungen für innovative Geschäftsmodelle hinreichend sicher prognostizierbar zu machen.

Elemente für denkbare Lösungen könnten sein:

- Haupt- und Nebenpflichten müssen in Verträgen wieder ohne weitgehende Einschränkungen durch eine AGB-Kontrolle wirksam definierbar sein. Lösungselemente wären realistisch im unternehmerischen Geschäftsverkehr umsetzbare Anforderungen an die Möglichkeit eines „Aushandelns“ im Sinne des § 305 Abs. 1 S. 2 BGB und die Abschaffung der Indizwirkung der §§ 308 und 309 BGB im Rahmen der Unangemessenheitsprüfung des § 307 Abs. 2 BGB einschließlich der Berücksichtigung innovativer Geschäftsmodelle, die nicht identisch einem Vertragstyp des BGB von 1900 entsprechen.

- Das Erfordernis hinreichender Transparenz soll zum Schutz von KMU gewahrt bleiben.

- Der Schutz von KMU gegen den Missbrauch von Marktmacht ist weiterhin Kernaufgabe des Kartell- und Wettbewerbsrechts, nicht jedoch des Vertragsrechts. Für das Kartellrecht liegt eine entsprechende Novelle (9. GWB-Novelle) zur besseren Berücksichtigung digitaler Geschäftsabläufe bereits als Entwurf vor.

Um Industrie 4.0 auf rechtlich belastbarer Basis in Deutschland möglich zu machen, muss das AGB-Recht entsprechend flexibilisiert werden. Ziel ist nicht eine vollständige Abschaffung der Schutzfunktion des AGB-Rechts für tatsächlich schutzbedürftige Unternehmen, insbesondere KMU, vor unangemessenen Klauseln.

Denkansätze für mögliche Änderungen finden sich auch in den Vorschlägen der AGB-Initiative von VDMA und ZVEI für § 305 BGB und § 310 BGB.

Zu einem solchen gesetzgeberischen Handeln bestehen aus Sicht der Plattform Industrie 4.0 keine Alternativen. Die unveränderte Beibehaltung der bestehenden Regelungen würde anhand der langfristigen Entwicklung der Rechtsprechung zu einer weiteren Verstärkung der Nachteile und Restriktionen für die Industrie 4.0 in Deutschland führen. Auch eine Lösung auf europäischer Ebene wäre nicht zielführend, da es sich um einen isolierten Regelungsnachteil des nationalen deutschen Rechts handelt.

Das zukunftsorientierte Handeln am Markt erfordert insbesondere die Verlässlichkeit vereinbarter Regelungen für innovative Geschäftsmodelle. Dafür ist die notwendige vertragliche Handlungsfreiheit wieder zu schaffen.

Willenserklärungen und Vertragsabschluss

A: Steckbrief

Worum geht es:

Ein wesentlicher Innovationsschritt der Industrie 4.0 ist die automatische Steuerung und Optimierung von Geschäftsprozessen und Produktionsabläufen durch unternehmensübergreifende Vernetzung von Maschinen und IT-Systemen. Nur so lassen sich Effizienz- und Kostenvorteile nutzen und die Leistungserbringung flexibilisieren.

Dafür müssen durch direkt miteinander kommunizierende Maschinen rechtlich wirksame Erklärungen ausgetauscht und bindende Vereinbarungen abgeschlossen werden. Die gesetzlichen Regelungen sind aber nur auf Erklärungen und Vereinbarungen zwischen Menschen ausgerichtet, nicht zwischen Maschinen (Maschinenerklärungen).

Ohne verbindliche Erklärungen und Vereinbarungen durch Maschinen werden Geschäftsprozesse und Produktionsabläufe der Industrie 4.0 grundlegend in Frage gestellt.

Sich ergebende Fragen und Handlungsfelder:

Unter welchen Voraussetzungen sind Maschinenerklärungen rechtlich wirksam?

- Welchen Parteien werden Maschinenerklärungen zugerechnet? Betrachtung der sachgerechten Risikosphären für die Zurechenbarkeit und Wirksamkeit von Maschinenerklärungen.
- Sind Maschinenerklärungen auch dann verbindlich, wenn der Inhalt für den Betreiber der Maschine nicht klar vorhersehbar war? Einordnung von eigenständigen Willenserklärungen durch KI-Systeme.
- Wie können Wirkungen einer „unrichtigen" Maschinenerklärung beseitigt werden?
- Wie können Maschinenerklärungen überwacht und überprüft werden?
- Wie kann ein verbindlicher Vertragsabschluss zwischen Maschinen erfolgen? Abgrenzung der Rollen von schlichten Maschinenerklärungen (als technisches/r Mittel/Bote/Vertreter) zu eigenständigen Erklärungen von Systemen mit künstlicher Intelligenz (kurz: KI-System).
- Welche Sorgfaltspflichten haben Absender und Empfänger von Maschinenerklärungen?

B: Juristische Einschätzung

Das BGB kennt keine ausdrücklich auf Maschinenkommunikation anwendbaren Regelungen. Die Rechtsprechung wendet derzeit die Regelungen des BGB für menschliche Willenserklärungen teilweise auch auf digitale Kommunikation unter Verwendung von Maschinen an.

Die Anwendung der Regelungen für menschliche Willenserklärungen auch auf Maschinenerklärungen ergibt aus Sicht der Arbeitsgruppe folgendes Bild:

- Erklärungen (auch „intelligenter" Maschinen) sind stets dem Absender zuzurechnen, wenn sie tatsächlich aus seiner Sphäre stammen. „Absender" ist die Partei, die für den Empfänger erkennbar die Erklärung mit Wirkung für sich oder einen Dritten abgeben will. Das wird regelmäßig die Partei sein, die die Maschine für ihre Zwecke einsetzt oder einsetzen lässt, jedoch nicht zwingend der technische Versender der digitalen Nachricht.
- Erklärungsinhalte sind auch dann für den Absender verbindlich, wenn er diese Inhalte nicht näher voraussehen konnte (Ausnahme: für Empfänger klar erkennbar fehlerhafte Erklärungsinhalte).
- Erklärungswirkungen können nur nach allgemeinen Regeln beseitigt werden (etwa Anfechtung).
- Für verbindliche „fehlerhafte" Erklärungsinhalte hat der Absender – unter den notwendigen Voraussetzungen – nur Ansprüche gegen Dritte.

C: Handlungsoptionen und Handlungsempfehlungen

Man könnte an die Schaffung spezieller gesetzlicher Regelungen für Maschinenerklärungen denken. Dadurch wäre jedoch keinerlei Verbesserung gegenüber den bestehenden Regelungen für Willenserklärungen zu erwarten. Auch deswegen besteht keine Veranlassung für spezifische Regelungen.

Um die Anwendung der Regelungen für menschliche Willenserklärungen auch auf Maschinenkommunikation sicher umzusetzen und Unsicherheiten oder gegensätzlichen Auffassungen in Literatur oder Rechtsprechung vorzubeugen, empfiehlt sich allerdings eine Klarstellung der gesetzlichen Regelungen:

> *„Die Vorschriften für Willenserklärungen und Vertragsabschlüsse gelten auch dann, wenn diese unter Verwendung von Maschinen erfolgen."*

Schon aus Gründen der Rechtssicherheit, insbesondere für den jeweiligen Erklärungsempfänger, besteht zur Anwendung dieser gesetzlich verankerten Grundsätze keine sinnvolle Alternative. Denn der Erklärungsempfänger wird regelmäßig nicht erkennen und nicht erkennen können, auf welche Weise die Erklärung bei deren Absender zustande gekommen ist. Daher sollte diese Klarstellung auch unabhängig davon erfolgen, in welcher Rolle die Maschinen eingesetzt werden, insbesondere unabhängig von einer rechtlichen Qualifizierung etwa als Bote oder Vertreter.

Weitere Klarstellungen oder Ergänzungen sind indes derzeit nicht veranlasst. Gleichwohl sollte die praktische Umsetzung kontinuierlich beobachtet und analysiert werden, um etwaigen Präzisierungs- und Regelungsbedarf für Industrie 4.0 zu evaluieren.

IT- und Datenschutzrecht

IT-Sicherheit

A: Steckbrief

Worum geht es:

Die Gewährleistung von IT-Sicherheit ist eines der Kernthemen der digitalisierten Wirtschaft in Gänze und damit aber nicht ein reines Phänomen im Bereich Industrie 4.0. Eine fortschreitende Vernetzung von Systemen und Produktionsanlagen sowie die zunehmende Autonomisierung von Produktionsprozessen führen aber in Summe zu einer signifikanten Erhöhung der Angriffs- und Bedrohungspotenziale im Cyber-Raum. Zudem erfolgen Cyber-Angriffe zunehmend zielgerichteter und mit technologisch ausgereifteren Mitteln. Auch dieser Umstand erhöht die Bedrohungslage. Angesichts dieser wachsenden Bedeutung des Cyber-Raums und informationstechnischer Systeme ist es wichtig, Risiken und Bedrohungen der Netz- und Informationssicherheit zu minimieren.

Die Gewährung von IT-Sicherheit beinhaltet zwei nebeneinanderstehende Stoßrichtungen:

1. Schutz von Menschen und Umgebung vor IT-Systemen
2. Schutz von Anlagen und Produkten vor unbefugtem Zugriff

Allgemein geht es bei der Umsetzung der IT-Sicherheit um fünf anerkannte Grundwerte:

1. Schutz der Verfügbarkeit: Gewährleistung der Funktionalität von IT-Systemen
2. Integrität: Verhinderung von Manipulationen an Informationen
3. Vertraulichkeit: Zugang zu Daten und Informationen nur für entsprechend Befugte
4. Authentizität: Sicherstellung der Quelle
5. Qualität: Fortlaufende Überprüfung der sachgerechten Umsetzung von Sicherheitsmaßnahmen

IT-Sicherheit betreffende Regelungen finden sich in einer Vielzahl gesetzlicher Regelungen und betreffen nur einzelne, meist besonders schützenswerte Teilbereiche der deutschen Wirtschaft oder besonders schützenswerte Daten. So legt das IT-Sicherheitsgesetz den Fokus nur auf den Schutz kritischer Infrastrukturen, nicht aber auf die Stärkung der Vertraulichkeit oder Sicherung der Integrität informationstechnischer Systeme insgesamt. Mit Blick auf Industrie 4.0-Anwendungen muss aber beachtet werden, dass etwaige regulatorische Anpassungen auch immer einen Eingriff in die Geschäfts- und Vertragsautonomie der Unternehmen darstellen.

Sich ergebende Fragen:

- In welchem Maße sind Industrie 4.0-Anwendungen allgemeinwohlorientiert?
- Wie ist die Verortung im unternehmerischen Eigeninteresse zu bewerten?
- Sind die Haftungsregeln von IT-Herstellern und Anbietern von IT-Diensten für Datenschutz- und IT-Sicherheitsmängel ausreichend geregelt?
- Gibt es einen Anpassungsbedarf bei grenzüberschreitenden Kooperationen?

B: Juristische Einschätzung

Die Aspekte der Betriebssicherheit produktionstechnischer Anlagen und damit die Schutzkategorie „Mensch und Umgebung“ (Safety) sind gelernte Bereiche und bereits heute durch vielfältige Normen und Standards abgebildet. Exemplarisch genannt für diese Regelungen sind die euro-

päische Maschinenrichtlinie 2006/42/EG und die deutsche Implementierung im Rahmen der neunten Verordnung zum Produktsicherheitsgesetz, 9. ProdSV. Einschätzungen der einschlägigen Literatur folgend[1], besteht ein akuterer Handlungsbedarf beim Schutz von IT-Systemen und Produktionsanlagen vor Eingriffen von außen. Dies betrifft sowohl i. S. der Industrie 4.0 vernetzte Produktionsstätten als auch solche bekannten Typs (Industrie 3.0; Zusammenspiel von Informatik, Elektronik und Mechanik) und umfasst die unter A dargestellten Grundwerte.

1. Gemeinwohlorientierung

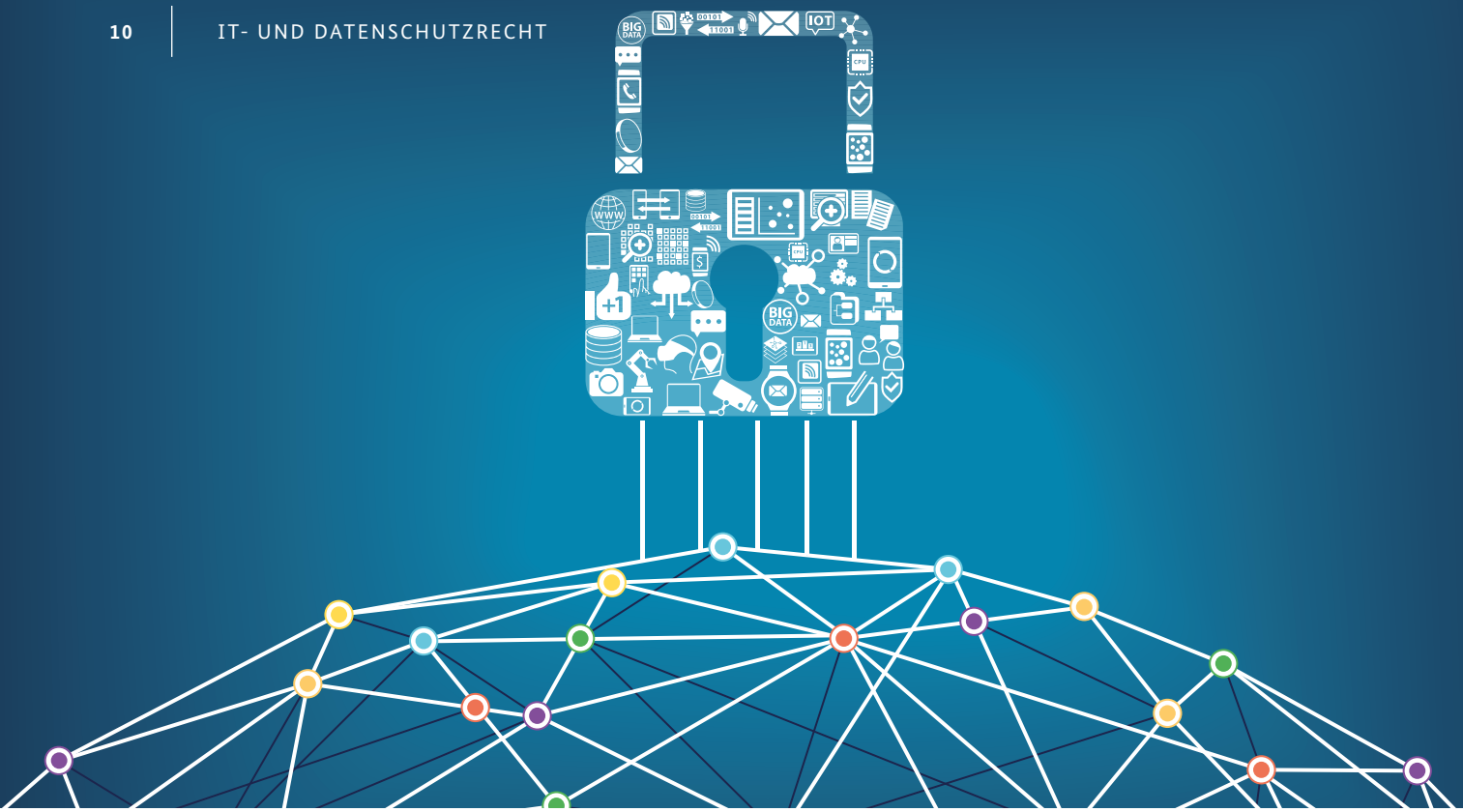
Die bisher ergriffenen gesetzgeberischen Maßnahmen, allen voran das IT-Sicherheitsgesetz und die europäische Richtlinie zur Steigerung der Netz- und Informationssicherheit, zielen nicht auf eine Erhöhung des Security-Niveaus im Allgemeinen, sondern „nur“ auf den Erhalt der Funktionsfähigkeit des Internets als kritische Infrastruktur sowie auf den Schutz verschiedener Bereiche kritischer Infrastrukturen, wie Energie, Verkehr und Gesundheit, ab. Diese Maßnahmen bauen auf einem verfassungsstaatlichen Gemeinwohlverständnis auf und regeln somit nur solche Bereiche (kritische Infrastrukturen), die die Gemeinwohlinteressen tangieren. Der Rechtsrahmen des IT-SiG findet nur dann im Industrie 4.0-Kontext Anwendung, wenn Teile der vernetzten Systeme auf kritischen Infrastrukturen aufbauen bzw. selbst Teil einer kritischen Infrastruktur sind. Auch mit der NIS-Richtlinie wird sich diese Fokussierung im Kontext von Industrie 4.0 nur marginal verschieben. Die Gemeinwohlorientierung stellt auch i. S. der besonderen Systemrelevanz kein ausreichendes Ordnungskriterium dar, um a) zu einer grundlegenden Zuordnung von Industrie 4.0-Anwendungen in den Bereich kritischer Infrastrukturen zu führen und damit b) eine Erhöhung der Cyber-Sicherheit über alle Anwendungsszenarien hinweg zu erzielen.

2. Eigeninteresse

Daher ist es erforderlich, den Blick stärker auf die unternehmerischen Eigeninteressen zu lenken. Allgemein gesprochen obliegt Unternehmen die Pflicht, eine ordnungsgemäße Geschäftsorganisation sicherzustellen, zu der auch angemessene Schutzvorkehrungen zur Gewährleistung der IT-Sicherheit zählen.[2] In § 91 Abs. 2 Aktiengesetz findet dies im Rahmen der Vorstandspflichten eine allgemeine Verankerung, soweit es um Frühwarn- bzw. „Überwachungssysteme geht, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen erkannt werden“. Daraus lassen sich zwar keine klar definierten Sicherheitsstandards ableiten. Zudem betreffen solche Frühwarnsysteme den Fortbestand eines Unternehmens als solchem, dagegen nicht notwendigerweise die Gefährdungen oder Beeinträchtigungen des laufenden Geschäftsbetriebs. Es könnte aber durchaus zu überlegen sein, im Rahmen des § 91 Abs. 2 AktG eine stärkere Verankerung bzw. Klarstellung einzupflegen, dass zu den „Überwachungssystemen“ auch in besonderer Weise Schutzmechanismen gegen Cyber-Gefahren gehören.

Unter dem Begriff der IT-Sicherheit wird primär die funktionale Sicherheit als Bestandteil der Betriebssicherheit verstanden und weniger der Komplex der Angriffssicherheit[3]. „Allgemein ist zu empfehlen, dass Sicherheitsmaß-

1. Vgl. u. a. Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 50, BDI, Digitalisierte Wirtschaft/Industrie 4.0, November 2015, S. 108.
2. Vgl. BDI, Digitalisierte Wirtschaft/Industrie 4.0, November 2015, S. 109.



nahmen und -prozesse auf den jeweiligen Bedarf im Unternehmen angepasst [...] werden."[4] Das Eigeninteresse zur Herstellung eines hohen IT-Sicherheitsniveaus u. a. auch in vernetzten Cyber-physischen Systemen wird im Kern aus anderen Motiven ableitbar. Im Vordergrund des unternehmerischen Schutzinteresses steht der Schutz des Prozess-Know-hows und der Intellectual Property Rights (IPR). Das heißt aber auch, mit Blick auf die Handlungsbedarfe, dass aus Gründen der Eigenmotivation kein gesetzgeberischer Handlungsbedarf erwächst. Mit Blick auf IT-Sicherheit zur Vermeidung von Industriespionage bzw. dem Schutz von IPR sind aus juristischer Sicht keine besonderen Aspekte der Industrie 4.0 im Vergleich zu bisherigen Prozessen erkennbar, außer, dass durch die zunehmende Vernetzung der Systeme die „Einbruchs- und Missbrauchsmöglichkeiten" zunehmen und insoweit Zugriffskontrollen und Verschlüsselungsmethoden weiter verbessert werden müssen. Nach derzeitigem Stand bleibt es letztendlich dem Nachfrageverhalten der Anwender – bzw. in vernetzten Industrie 4.0-Strukturen den miteinander vernetzten Unternehmen in einem ggf. konsortialen Ansatz – überlassen, ob diese individuell ein höheres Sicherheitsniveau als den Mindeststandard implementieren.

3. Haftung

Aufgrund der Schwierigkeit, standardisierte Sicherheitsnormen zu definieren, kommt den Haftungsfragen auch im Kontext der Gewährung eines hohen Maßes an IT-Sicherheit eine durchaus gewichtige Bedeutung zu. Allerdings, so auch die Erfahrungen im Rahmen des IT-SiG, ist es hinlänglich schwierig, ein konkretes IT-Sicherheitsniveau vom Gesetzgeber vorzugeben. Eine gesetzliche Regelung des technischen Sicherheitsniveaus würde regelmäßig an den langwierigen Gesetzgebungsverfahren scheitern, sodass die Beschreibung des „Standes der Technik" ein fortwährender Parallelprozess wäre. Auch in diesem Fall können vertragliche Regelungen besser auf die speziellen Erfordernisse der jeweiligen Situation und der geforderten Sicherheitsaspekte eingehen und so den jeweiligen Schutzinteressen adäquater Rechnung tragen.

Im Rahmen der Produkthaftung zeichnet sich ein Spannungsverhältnis ab, ob und in welchem Umfang nach dem Stand der Technik die Einhaltung spezifischer IT-Sicherheitsstandards ohne zusätzliche vertragliche Grundlage einzufordern ist. Eine nähere Auseinandersetzung mit diesem Themenkomplex erfolgte im Rahmen der Unterarbeitsgruppe 3 (Produkthaftung).

4. Grenzüberschreitende Kooperationen

Nach der Logik der Netzarchitektur, wonach die Netzinfrastruktur nicht nationalstaatlich organisiert ist, ist davon auszugehen, dass mit zunehmender Vernetzung auch die grenzüberschreitende Kooperation zunehmen wird, was bei einer gesetzlichen Normierung auch zu erheblichen Friktionen und Diskussionen führen könnte. Allgemein ist dazu festzustellen, dass innerhalb der EU ein ausreichendes Maß an Rechtssicherheit und Harmonisierung vorliegt und auch außerhalb der EU eine Vielzahl bilateraler und internationaler Abkommen zu Datenschutz und -sicherheit

3. BITKOM, Rechtliche Aspekte von Industrie 4.0, April 2016, S. 28.

(bspw. im Rahmen von Adäquanzentscheidungen zum internationalen Datentransfer) u.Ä. existieren. Entscheidend für die Anforderungen an die IT-Sicherheit ist letztlich die konkrete gesetzliche Situation in dem jeweiligen Land, in dem das Produkt in den Verkehr gebracht wird oder die Industrie 4.0-Technologie genutzt wird. Auch hinsichtlich einer grenzüberschreitenden Kooperation besteht insoweit auch im Industrie 4.0-Kontext ein eindeutiger Rechtsrahmen (vgl. u.a. Richtlinie 85/374/EWG), bei dem gegenwärtig keine Anpassungsbedarfe erkennbar sind.

C: Handlungsoptionen und Handlungsempfehlungen

Die Regelungen zur IT-Sicherheit sind größtenteils generischer Natur, wodurch vor allem für betroffene Unternehmen stets Unsicherheiten entstehen, welche konkreten Maßnahmen im konkreten Fall zu ergreifen sind. Daher muss sich jede Debatte um eine juristische Handlungsoption auch der Frage stellen, ob dadurch das IT-Sicherheitsniveau im Allgemeinen und bei den betroffenen Akteuren im Speziellen erhöht wird. Dies trifft in einem noch gravierenderen Maße auf kleine und mittelständische Unternehmen zu. „Zwar kann der Gesetzgeber ihnen – theoretisch – die Pflicht auferlegen, entsprechende Vorkehrungen zu treffen, doch ob dies allein zu volkswirtschaftlich und im Sinne der Unternehmen gewünschte Lösungen führt, ist mit einem großen Fragezeichen zu versehen.“[5] Zudem dürfte bspw. eine Ausdehnung der Meldepflichten nach § 8b Abs. 4 BSIG alle Beteiligten vor die Herausforderung der schieren Masse an Meldungen stellen, ohne einen signifikanten Sicherheitsmehrwert zu erzielen. Zielführender sind Ansätze, die, flankiert durch politische Maßnahmen, Unternehmen allgemein in die Lage versetzen, ein hohes Maß an IT-Sicherheit sicherzustellen. Jenseits der Unternehmen, die als kritische Infrastrukturen eine Relevanz für das Gemeinwohl besitzen, sollte die Gewährleistung von IT-Sicherheit vorrangig im Eigeninteresse der Unternehmen liegen – Anbieter wie Anwender – und daher keiner „gesetzlichen Anreize“ bedürfen. Eine zukunftsweisende Stärkung der IT-Sicherheit sollte hier ansetzen und praktische Maßnahmen wie Verschlüsselung oder „Security by Design“, ggf. auf der Basis zu entwickelnder branchenüblicher Standards (vgl. § 8a Abs. 2 BSIG) und Zertifizierungen (bspw. ISO), fördern.

Datenschutzrecht

A: Steckbrief

Worum geht es:

Bei Industrie 4.0-Szenarien spielt der Datenschutz immer dann eine Rolle, wenn die erhobenen Daten einen Personenbezug aufweisen. Das kann etwa der Fall sein:

1. In der Mensch-Maschine-Interaktion, insbesondere im Rahmen betrieblicher Abläufe (Beispiel: halbautomatisierte Roboterbedienung etc.), in denen dann die Schnittstelle von Datenschutz und Verhaltenskontrolle (Mitbestimmungsrecht) berührt wird;

2. Im Rahmen der eigentlichen Anwendung, wenn die Herstellung des Personenbezugs unmittelbar oder retrospektiv möglich ist bzw. erfolgt (Beispiel: Sensordaten eines Fahrzeugmotors, die im Falle eines Unfalls zur Ermittlung des Unfallhergangs und damit des Fahrerverhaltens herangezogen werden);

3. Durch die Verknüpfung von Sensordaten mit anderen Datenquellen bei Big-Data-Verfahren, wenn sich daraus Personenprofile herausbilden lassen.

Das Datenschutzrecht als Ausdruck des Grundrechts auf informationelle Selbstbestimmung stellt an die Erhebung und Verarbeitung personenbezogener Daten hohe Anforderungen. Grundsätzlich bedarf es der vorherigen Einwilligung der Betroffenen oder einer anderen gesetzlichen Ermächtigungsgrundlage. Zudem ist die Verarbeitung nur im Rahmen eines vorher festzulegenden, legitimen Zwecks gestattet. Eine Verwendung für andere Zwecke oder gar die Weitergabe der Daten an Dritte ist grundsätzlich an die Zustimmung der Betroffenen oder einen gesetzlichen Erlaubnistatbestand geknüpft. Sollen Daten außerhalb der EU und des EWR verarbeitet werden, muss ein angemessenes Datenschutzniveau gewährleistet sein.

Die Möglichkeiten einer Verarbeitung von personenbezogenen Daten sind also beschränkt. Das hat auch Einfluss auf die wirtschaftliche Wertschöpfung von Industrie 4.0-Szenarien.

4. BDI, Digitalisierte Wirtschaft/Industrie 4.0, November 2015, S. 112.

Sich ergebende Fragen:

- Wann haben Daten Personenbezug? Und wo sind die Grenzen? Gilt ein absoluter oder relativer Begriff des Personenbezugs?

- Wie lassen sich verlässliche und allgemein verbindliche Kriterien zur Anonymisierung, Pseudonymisierung, Verschlüsselung von Daten mit Personenbezug entwickeln und zeitnah umsetzen? Wie kann hierbei ein risikobasierter Ansatz integriert werden?

- Wie lässt sich der Grundsatz der Datenminimierung zeitgemäß umsetzen? Genügen Maßnahmen wie Anonymisierung, Pseudonymisierung oder Verschlüsselung als hinreichendes Steuerungsmittel oder muss über einen Regelungsrahmen für weitergehende Modelle nachgedacht werden (Beispiel: Datentreuhändermodelle für Industrie 4.0-Konsortien)?

- In welchem Verhältnis stehen die Datenschutzrechte der Betroffenen zu anderen Rechten an den Daten, etwa der Datengeneratoren, sowie deren wirtschaftlichen Interessen?

- Unter welchen Voraussetzungen ist eine Erhebung, Verarbeitung und Weitergabe von Daten mit Personenbezug in Industrie 4.0-Szenarien gestattet? Diese Voraussetzungen müssen je nach Risiko für den Betroffenen differenziert erfolgen (siehe das unterschiedliche Risiko in den Eingangsbeispielen).

- Was ist bei grenzüberschreitenden Datenverarbeitungsszenarien (mit Personenbezug) zu beachten?

- Gibt es spezifische Anforderungen an Plattformbetreiber, Datenaggregatoren und Intermediäre, die besser als durch das Mittel der Auftragsdatenverarbeitung abzubilden sind? Wie lässt sich Transparenz über die Verantwortlichkeiten über die gesamte Prozesskette herstellen?

B: Juristische Einschätzung

1. Weiter Schutzbereich, Einwilligung und Zweckbindung

Das geltende Datenschutzrecht wie auch die künftige Datenschutzgrundverordnung (DSGVO) definieren den Begriff des personenbezogenen Datums sehr weit. Darunter fällt jede Information „über eine bestimmte oder bestimmbare natürliche Person". Damit kann prinzipiell jedes Datum zum personenbezogenen Datum werden, wenn und sobald es mit einer Person in Beziehung gesetzt werden kann. Das gilt auch für rein technische Informationen, wie z. B. Maschinendaten oder GPS-Koordinaten, etwa wenn sie als Aufenthaltsort einer Person erhoben werden bzw. in sonstiger Weise zugeordnet werden können.

Werden personenbezogene Daten zu geschäftlichen oder zu Forschungszwecken verarbeitet, wie dies bei Industrie 4.0-Szenarien regelmäßig der Fall sein dürfte, ist der Anwendungsbereich des Datenschutzrechts sachlich eröffnet. Eine Verarbeitung ist dann nur zulässig, wenn und soweit die betroffenen Personen zuvor eingewilligt haben oder eine andere gesetzliche Rechtfertigung vorliegt. Die Einwilligung dient nur insoweit als tragfähige Rechtsgrundlage, wie Zweck und Reichweite der Verarbeitung zuvor festgelegt sind. Für Industrie 4.0-Szenarien, in denen Verwendungszwecke und Umfang der Verarbeitung nicht vollständig vorab definiert werden können, scheidet die Einwilligung entsprechend aus. Zudem können Betroffene ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Damit ist das „Damoklesschwert des Widerrufs" als Planungsfaktor zu berücksichtigen; entsprechend scheidet die Einwilligung in der Praxis in vielen Fällen als Gestaltungsmittel aus.

Liegen die Voraussetzungen einer zulässigen Verarbeitung nicht vor, kann jeder Betroffene die Verarbeitung der auf ihn beziehbaren Daten untersagen. Ferner können Aufsichtsbehörden und nunmehr auch Interessenverbände gegen eine unzulässige Verarbeitung vorgehen.

Die sonstigen in Frage kommenden gesetzlichen Verarbeitungsgrundlagen stehen unter dem Vorbehalt einer Abwägung mit den Interessen der Betroffenen, die in bestimmten Fällen einer Verarbeitung dann auch widersprechen können. Es besteht das Risiko, dass in bestimmten Fällen die Persönlichkeitsrechte Betroffener den wirtschaftlichen Interessen der Datenverarbeiter vorgehen. Mithin schränkt die Personenbeziehbarkeit eines Datums die Möglichkeiten der Verarbeitung und damit oft genug die wirtschaftliche Wertschöpfung ein.

Zulässigerweise erhobene Daten dürfen im Rahmen des definierten Zwecks oder auf gesetzlicher Grundlage verarbeitet werden. Die Zweckbindung erfordert die Verarbeitung ausschließlich im Rahmen der – mehr oder minder eng oder weit gefassten – Verarbeitungszwecke; erhobene Daten sind nach Zweckerreichung grundsätzlich sofort zu löschen. Die Verwendung für weitere Zwecke ist nur unter engen Voraussetzungen möglich. In vielen Industrie 4.0-Szenarien stehen Zweckbindung und Datenminimierung mit dem Aufbau umfangreicher Datenbestände und deren flexibler Verarbeitung in einem Spannungsverhältnis, das insbesondere mit den Handlungsebenen Datenreichtum, Datenvielfalt und Zweitverarbeitung in Balance zu bringen ist. In der Praxis benötigen Unternehmen (auch durch entsprechende Guidelines etc.) Maßgaben, um diesen Anforderungen durch intelligente „Privacy by Design"-Modelle und hochskalierbare technische und organisatorische Schutz-

maßnahmen, z. B. Pseudonymisierung, Verschlüsselung und Berechtigungskonzepte, gerecht zu werden.

Handlungsempfehlung: Der Grundsatz der Datenminimierung ist durch nähere Maßgaben für sichere Anonymisierungs- und Pseudonymisierungstechnologien auszutarieren, damit Datenvielfalt, Datenreichtum und Zweitverarbeitung im Bereich Industrie 4.0 zur flexiblen Wertschöpfung genutzt werden können.

2. Anonymisierung und Pseudonymisierung

Da für den Anwendungsbereich des Datenschutzrechts die Personenbeziehbarkeit von Daten konstitutiv wirkt, kommt der Anonymisierung von Daten in Industrie 4.0-Szenarien erhöhte Bedeutung zu. Die Anforderungen an eine erfolgreiche Anonymisierung sind sehr hoch. Hier aber liegt eines der wesentlichen Probleme. Einige europäische Datenschutzbehörden vertreten, dass es nicht nur auf den Horizont des Datenverarbeiters ankomme, sondern alle denkbaren Umstände (einschließlich einer möglichen De-Anonymisierung durch Dritte) einzubeziehen seien, unter denen der Personenbezug hergestellt werden könnte. Die Datenschutzbehörden anderer EU-Mitgliedstaaten stellen darauf ab, ob das Herstellen des Personenbezugs durch den jeweiligen Verarbeiter hinreichend wahrscheinlich ist oder überhaupt rechtmäßig erfolgen darf. Zudem kann bei für sich genommenen anonymen Daten in Kombination mit anderen Daten oder Hintergrundwissen ein Personenbezug entstehen bzw. sich dynamisch über die Zeit ergeben. Es besteht das Risiko des Fehlschlagens der Anonymisierung bzw. der zunächst nicht absehbaren De-Anonymisierung. Werden in gutem Glauben auf den Erfolg der Anonymisierung keine weiteren datenschutzrechtlichen Maßnahmen ergriffen, kommt es unter Umständen zu einer unzulässigen Verarbeitung personenbezogener Daten, mit entsprechenden rechtlichen **Handlungsempfehlungen**: Vor diesem Hintergrund ist es wünschenswert, die Anforderungen an eine rechtlich wirksame Anonymisierung für Industrie 4.0-Szenarien weiter zu definieren und Leitlinien und Zertifizierungsmechanismen zu schaffen. Ferner ist zu überlegen, ob eine verantwortliche Stelle, die eine Anonymisierung ggf. nach Vorgaben durchführt, datenschutzrechtlich nicht weiter verantwortlich ist, wenn die De-Anonymisierung später durch Dritte möglich wird.

Dasselbe gilt für andere Maßnahmen, insbesondere die Pseudonymisierung und die Verschlüsselung. Mit ihnen entfällt zwar nicht der Personenbezug, aber die Verarbeitung wird erheblich erleichtert bei gleichzeitiger Wahrung der Persönlichkeitsrechte der Betroffenen. Nach derzeitigem Recht sind die Regelungen zum Umgang mit pseudonymisierten Daten unterentwickelt. Aus den Erwägungsgründen 26 und 28 sowie Artikel 6 (4(e)) DSGVO wird deutlich, dass der europäische Gesetzgeber die Verarbeitung pseudonymer Daten (insbesondere auch in Big-Data-Lösungen) klar privilegieren und inzentivieren möchte. Die Kriterien für die Pseudonymisierung und die konkreten Anforderungen an die Zulässigkeit der Verarbeitung pseudonymisierter Daten müssen aber noch entwickelt werden. Hier ist zu wünschen, dass nicht erst bis zum Inkrafttreten der DSGVO gewartet wird. Industrie 4.0 benötigt Handlungsspielräume, zumal die Verarbeitung personenbezogener Daten in vielen Fällen von Industrie 4.0 nicht im Zentrum der Wertschöpfung steht, sondern sich allenfalls als ungewünschte Nebenfolge der Prozessketten erweist. Verlässliche und allgemeinverbindliche Regeln zur Pseudonymisierung – einschließlich mittels Verschlüsselung – sind eine besonders wichtige Hilfestellung, um Industrie 4.0 zum Erfolg zu verhelfen.

C: Handlungsoptionen und Handlungsempfehlungen

1. Interessenabwägung bzw. Folgenabschätzung anhand von Kriterien der Eingriffsintensität

Um Industrie 4.0 – überall dort, wo Anonymisierung oder Pseudonymisierung an ihre Grenzen stoßen bzw. nicht greifen – voranzubringen, haben geeignete Kriterien und Verfahren zur vereinfachten Interessenabwägung bzw. nach der DSGVO in Zukunft geforderten Folgenabschätzung („Privacy Impact Assessment“) erhebliche Bedeutung.

Dazu sind vorrangig die Aufsichtsbehörden bzw. nach der DSGVO in Zukunft der Europäische Datenschutzausschuss („European Data Protection Board", „EDPB") aufgefordert, Regelungen und Maßstäbe zu entwickeln. Als „Leitmotiv" sollte dabei ein risikobasierter Ansatz gelten, der auf die Eingriffsintensität der Datenverarbeitung abstellt. Unter Wahrung der Betroffenenrechte auf Auskunft, Berichtigung und Löschung sowie der Schutzziele ist größere Klarheit erforderlich, in welchen Fällen die Interessenabwägung im Zweifel grundsätzlich zugunsten klar bestimmter Industrie 4.0-Szenarien ausfallen kann.

2. Grenzüberschreitende Datenübermittlungen

Vernetzung und Virtualisierung sind Wesensmerkmale der digitalen Transformation und damit auch von Industrie 4.0. Dabei kommt der Cloud-Technologie besondere Bedeutung zu. Damit sich die deutsche Wirtschaft und Industrie nicht von globalen Lieferketten und Technologieangeboten abkoppelt, ist ein sicherer Rechtsrahmen für den grenzüberschreitenden (d. h. ex-EU / EWR-) Datentransfer unerlässlich. Neben der (möglichst) gerichtsfesten Ausgestaltung des EU-US Privacy Shield, der Aufrechterhaltung der Standardvertragsklauseln und Binding Corporate Rules kommt Zertifikaten und Gütesiegeln hohe Bedeutung zu. Der europäische Verordnungsgeber hat wichtige Voraussetzungen geschaffen, durch die Zertifizierung von Datenverarbeitungsvorgängen ein angemessenes Schutzniveau für Datentransfers in Drittländer sicherzustellen (Art. 24, 42, 43, 44 DSGVO). Die Erfahrungen aus der Pilotzertifizierung nach dem TCDP-Standard (siehe www.trusted-cloud.de) und die Entwicklung eines entsprechenden Marktumfeldes sind wichtige Beiträge, um bereits vor Inkrafttreten der DSGVO die entsprechende Rechtspraxis vorzubereiten.

3. Plattformbetreiber, Aggregatoren und Intermediäre

Nach hergebrachtem Datenschutzrecht vollziehen sich sämtliche Verarbeitungsvorgänge zwischen verantwortlichen Stellen („data controller") und ggf. von ihnen beauftragten weisungsgebundenen handelnden Datenverarbeitern („data processor"). Nach deutschem Recht wird das Rechtsverhältnis für einen „controller-to-processor"-Transfer („C2P") durch die Vereinbarung der Datenverarbeitung im Auftrag („ADV") bestimmt und unterliegt den im Einzelnen aufwendigen Anforderungen des § 11 BDSG. Soweit es hingegen zu Funktionsübertragungen kommt, scheidet die ADV aus; es gelten dann die Maßstäbe einer Übermittlung an eine neue verantwortliche Stelle („controller-to-controller", „C2C"). Dieses System wird unter der DSGVO beibehalten und begründet einen eigenen Pflichtenkatalog für Auftragsverarbeiter (Artikel 28). Für eine Vielzahl von Verarbeitungsvorgängen gerade im Bereich Industrie 4.0 stellt dies die Beteiligten vor besondere Herausforderungen.

Mit dem Aufbau nichtlinearer Wertschöpfungsketten bzw. Eco-Systeme, die durch einen multilateralen Austausch von Daten gekennzeichnet sind, werden die Konturen – wer „Controller" und wer „Processor" ist oder sein könnte – zunehmend schwer erkennbar. Teilweise wird daher gefordert, die Unterscheidung zwischen „Controller" und „Processor" aufzugeben und am Prinzip der Verantwortlichkeit nicht länger festzuhalten. Die Annahme und konkrete Ausgestaltung von Weisungsbefugnissen stoße an praktische Grenzen, der jeder praktische Bezug fehle. Andere Autoren erkennen zwar gewisse Zuordnungsprobleme an, ziehen daraus aber die Konsequenz, dass die jeweiligen Verantwortlichkeiten über die gesamte Prozesskette umso transparenter und verständlicher dargestellt werden müssten. Auch sei in der Datenökonomie – gerade im Bereich Industrie 4.0 – absehbar, dass Plattformbetreiber, Datenaggregatoren und Intermediäre benötigt werden, um den effizienten und sicheren Austausch von Daten zwischen den verschiedenen Beteiligten zu ermöglichen. Daher bedürfe es einer klaren und transparenten Zuordnung der Aufgaben und des datenschutzrechtlichen Pflichtenkatalogs.

In diesem Zusammenhang gewinnen gerade für Plattformbetreiber, Aggregatoren und Intermediäre die Schutzziele Verarbeitungstransparenz, Datensicherheit (Authentizität, Integrität), Mandantenfähigkeit und Portabilität und deren Absicherung durch Zertifikate erhöhte oder sogar zentrale Bedeutung. Sie unterstützen die Ausübung der datenschutzrechtlichen Kontrolle der verantwortlichen Stelle und die Wahrung der Betroffenenrechte weitaus stärker, als dies die Fixierung abstrakter und konkreter Weisungsbefugnisse vermag – die die verantwortliche Stelle bzw. der Betroffene beim Bezug komplexer Technologiedienste ohnehin kaum oder gar nicht ausüben wird.

Handlungsempfehlung: Hier würde es sich anbieten, die datenschutzrechtliche Compliance von – gesetzlich noch näher zu definierenden – Plattformbetreibern, Aggregatoren und Intermediären durch eine Rahmenregelung zu stärken, die unter Verzicht auf das überkommene Konstrukt der ADV die Schutzziele der Verarbeitungstransparenz, Datensicherheit und Portabilität als zentrale Verantwortungselemente durch entsprechende Zertifikate absichert.

Produkthaftungsrecht

Rechtsgutverletzung durch Industrie 4.0-mäßig gefertigtes (fehlerhaftes) Produkt

A: Steckbrief

Worum geht es:

Dieser Themenkomplex befasst sich mit Fragen, die sich mit den Ergebnissen einer Industrie 4.0-Fertigung beschäftigen: Die smart, ggf. customized, hergestellten Produkte aus dem Industrie 4.0-Produktionsumfeld gelangen anschließend bestimmungsgemäß in den Wirtschaftskreislauf und damit in das Feld der Benutzer. Fehler am Produkt, die sich aus dem Fertigungsprozess ergeben, setzen sich dann als Fehler in der Produktnutzung fort, und das mit möglichen Sicherheitsrisiken.

Sich ergebende Fragen und Handlungsfelder:

- Wer haftet, wenn (auch beweisrechtlich) der Schaden während der Benutzung klar auf einen alleinigen Fehler des Produkts zurückzuführen ist?
- Wer haftet, wenn unklar bleibt, ob das Schadensbild durch das Produkt selbst oder einen Fehler im Einsatzumfeld (z. B. durch eine „intelligente Peripherie“) verursacht wurde?

B: Juristische Einschätzung

- *Wer haftet, wenn (auch beweisrechtlich) der Schaden während der Benutzung klar auf einen alleinigen Fehler des Produkts zurückzuführen ist?*

  Hier kommen vertragliche wie außervertragliche Ansprüche in Betracht. Die Unterarbeitsgruppe wirft ihren Blick naturgemäß vorrangig auf außervertragliche Ansprüche. Haftungsbegründend können hier die Vorschriften der §§ 823 ff. BGB[6] sowie des § 1 ProdHaftG genannt werden.[7]

  Eine Regelungslücke ist hier nicht erkennbar.

  Vertragsrechtliche Schadensersatzansprüche kommen jedenfalls dem Grunde nach dann in Betracht, wenn der Benutzer zugleich im vertragsrechtlichen Sinne auch der Käufer des Produkts ist. Für Schadensersatzansprüche nach § 280 BGB wird es dann im Übrigen (auch beweisrechtlich) auf ein Verschulden zum Zeitpunkt der Übergabe mit den bekannten Problemen der verschuldens-

5. Vgl. zu Problemen des Deliktsrechts in der Rechtsanwendung: Bräutigam/Klindt, NJW 2015, 1137 (1139); Rempe, InTeR 2016, 17 (18).
6. Vgl. zur Anwendbarkeit des ProdHaftG: Littbarski in Kilian/Heussen, Computerrechts-Handbuch, Teil 18, Rn. 24, 116, sowie zur Produkteigenschaft von Software nach dem ProdHaftG: Wagner in § 2 ProdHaftG, MüKo, 6. Aufl. 2013, Rn. 13, 15.

abhängigen Schadensersatzhaftung ankommen. Je nach Vertragsausgestaltung (z. B. unter Anwendung des UN-Kaufrechts) kann dies zu unterschiedlichen Ergebnissen führen.

- *Wer haftet, wenn unklar bleibt, ob das Schadensbild durch das Produkt selbst oder einen Fehler im Einsatzumfeld (z. B. durch eine „intelligente Peripherie") verursacht wurde?*

  Die außervertraglichen, namentlich deliktischen Anspruchsgrundlagen bleiben identisch, soweit es um den Hersteller geht. Sonstige störende Einflussfaktoren können prinzipiell unter das Tatbestandsmerkmal des rechtswidrigen Eingriffs i. S. d. § 823 BGB, ggf. auch in Verbindung mit einem öffentlich-rechtlichen Schutzgesetz nach § 823 Abs. 2 BGB, subsumiert werden. Dies wird in jedem Einzelfall Tatfrage sein.

  Bleibt indes der technische Root Cause unaufklärbar, ergeben sich für den Geschädigten unter Umständen Schwierigkeiten bei der Identifizierung des Anspruchsgegners. Dies unterscheidet die unter Industrie 4.0 diskutierte Situation strukturell indes nicht vom Rechtsrisiko sonstiger Situationen nicht aufklärbaren Verursachungshergangs.

C: Handlungsoptionen und Handlungsempfehlungen

Ist der Schaden während der Benutzung klar auf einen alleinigen Fehler des Produkts zurückzuführen, ergeben sich nach aktueller Rechtslage keine Regelungslücken. Für außervertragliche Ansprüche eignen sich sowohl das Deliktsrecht, als auch das ProdHaftG zur Lösung von Thematiken im Zusammenhang mit Industrie 4.0.[8]

Der Nachweis schuldhaften Handelns im Fall von vertraglichen Ansprüchen stellt hingegen eine der deutschen Rechtsordnung systemimmanente Hürde dar. Gleiches gilt für den Nachweis eines Verursachungsbeitrags des Produkts zum Schadensbild.

Falls dies rechtspolitisch als Regelungslücke empfunden würde, müsste ohne jeden Bezug auf ein Verschulden oder auf einen Verursachungsbeitrag der Gedanke einer reinen Gefährdungshaftung eines/mehrerer Teilnehmer aus dem diffusen Peripherieumfeld diskutiert werden. Die Unterarbeitsgruppe sieht jedenfalls derzeit noch keinen Handlungsbedarf in Richtung einer reinen Gefährdungshaftung.

Die weitere Entwicklung sollte jedoch aufmerksam beobachtet werden: Zumindest in Bezug auf den Einsatz autonomer bzw. selbstlernender Produkte oder sofern der Nachweis schuldhaften Handelns aufgrund der Eigenart der Industrie 4.0-Fertigung nicht möglich sein sollte, könnte sich die rechtspolitische Frage nach einer gesetzlichen Regelung der Gefährdungshaftung (z. B. ähnlich der Halterhaftung im Straßenverkehr) mittelbar stellen.

Rechtsgutverletzung innerhalb der Industrie 4.0-Fertigungsstätte

A: Steckbrief

Worum geht es:

Dieser Themenkomplex befasst sich mit Fragen der Unfallfolgenhaftung, die durch Vorfälle innerhalb einer Fabrikation nach Industrie 4.0-Maßstäben aufgerufen werden. Es geht mithin um Arbeitsunfälle (oder um Sachbeschädigungen), die innerhalb der vernetzten Fabrik erfolgen, in der es indes keinerlei Auswirkungen auf das zu erstellende Produkt im Außenbezug gibt.

Sich ergebende Fragen und Handlungsfelder:

- Wer haftet, wenn dieser Unfall durch eine Cyber-Attacke von außen provoziert wurde, die schädigend etwa in einzelne Prozessschritte eingegriffen hat?

- Wer haftet, wenn ohne Einflussnahme von außen der Schadensfall auftrat, indes ein klarer Ursachenpfad auf einen isolierbaren Prozessschritt-Beteiligten nicht erkennbar ist?

B: Juristische Einschätzung

- *Wer haftet, wenn ein Unfall durch eine Cyber-Attacke von außen provoziert wurde, die schädigend etwa in einzelne Prozessschritte eingegriffen hat?*

  Die Cyber-Attacke wird als vorsätzlicher und ohnehin rechtswidriger Eingriff im Sinne des § 823 Abs. 1 BGB mühelos zu subsumieren sein. Die Attacke schädigt im Grunde wie jede Form des Vandalismus. Der identifizierte Angreifer kann daher nach § 823 Abs. 1 (im Übrigen auch nach § 823 Abs. 2 BGB) in Anspruch genommen werden.[9]

7. Vgl. Spindler, MMR 2008, 7 (12).
8. Vgl. zu einer umfassenden Behandlung haftungsrechtlicher Fragen bei Cyber-Attacken: Mehrbrey/Schreibauer, MMR 2016, 75 (76).

- *Wer haftet, wenn ohne Einflussnahme von außen der Schadensfall auftrat, indes ein klarer Ursachenpfad auf einen isolierbaren Prozessschritt-Beteiligten nicht erkennbar ist?*

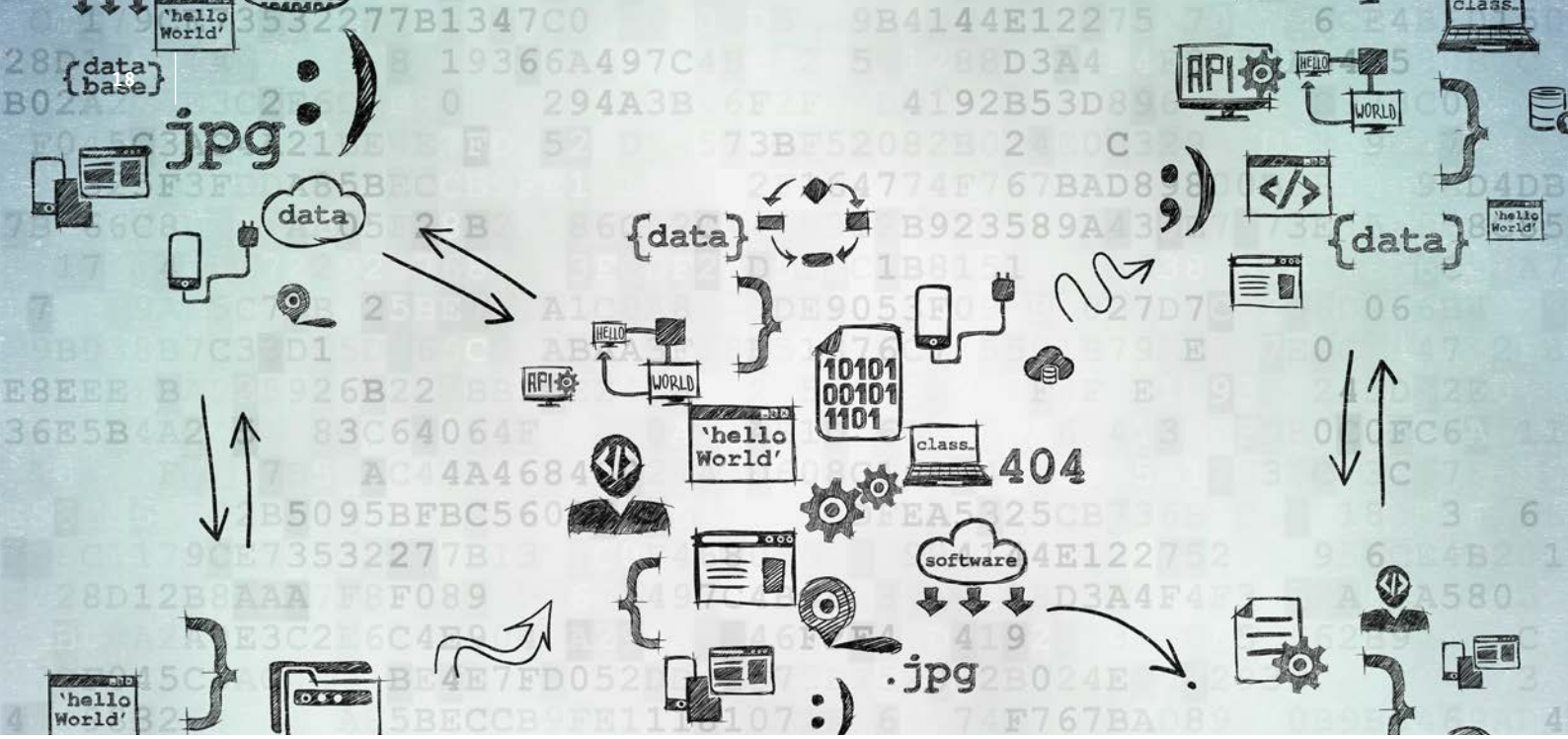
  Bezieht sich der erwähnte Schadensfall auf eine Arbeitnehmerverletzung (Arbeitsunfall/Gesundheitsverletzung), so greift jedenfalls in Deutschland das berufsgenossenschaftliche Sozialversicherungssystem. Ob die BG ihrerseits regressrechtlich auf einen Passivlegitimierten zurückgreifen kann, scheint fraglich. Die Frage suggeriert ja gerade die Nicht-Identifizierung eines konkreten Verursachers.

  Bei Sachschäden oder sonstigen Personenschäden, die nicht Arbeitnehmer betreffen (z. B. Kunden im Rahmen eines Audits), greift ersichtlich das berufsgenossenschaftliche System hingegen nicht. In solchen Fällen kann die aktuelle Rechtsordnung „an ihre Grenzen“ gelangen.

C: Handlungsoptionen und Handlungsempfehlungen

Die zivilrechtliche Beurteilung von betriebsfremden Cyber-Attacken kann bereits mittels des vorhandenen deliktsrechtlichen Instrumentariums erfolgen. Einer Fortentwicklung der Rechtsordnung bedarf es insoweit nicht.

Anders mag dies bei Schadensfällen im Zusammenhang mit dem Produktionsprozess aussehen, die sich ohne feststellbaren Verursachungsbeitrag eines daran Beteiligten ereignen. Wer jenseits des berufsgenossenschaftlichen Sicherungssystems für Betriebsangehörige eine Regelungslücke für sonstige Schäden jeder Art sieht, wird über eine behutsame Weiterentwicklung des Haftpflichtgesetzes nachzudenken haben.



IP-Recht und Datenhoheit

Schutz von Know-how

A: Steckbrief

Worum geht es:

Der Themenkomplex „Schutz von Know-how“ befasst sich mit Fragen, die sich aufgrund einer immer komplexeren, u. U. automatisierten Schaffung und Nutzung sowie Auswertung von Unternehmens- und Maschinendaten stellen. Dies ist insbesondere aufgrund der unternehmensübergreifenden Vernetzung, etwa bei der Nutzung von Cloudservices, Predictive Maintenance, Condition Monitoring, Big-Data-Analysen durch Dritte im Auftrag oder auch bei dem einfachen Betrieb von Maschinen, relevant.

Sich ergebende Fragen und Handlungsfelder:

- Große Bereiche von Produktionsdaten sind zzt. nicht durch vorhandene gesetzliche Rechtsinstitute bestimmten Inhabern zugewiesen oder geschützt. Können diese Daten als „Know-how“ bzw. vertrauliche Geschäftsinformationen (Geschäftsgeheimnisse) ausreichend geschützt werden?

- Welche Maßnahmen sind notwendig, um ggf. einen Schutz als Betriebsgeheimnis annehmen zu können (etwa: vertragliche Vereinbarungen und tatsächliche Geheimhaltung)?

B: Juristische Einschätzung

In der EU gibt es sehr unterschiedliche nationale Regelungen zum Schutz von Betriebs- und Geschäftsgeheimnissen. Häufig sind sie zivilrechtlich ausgeprägt. Im nationalen deutschen Recht sind Betriebs- und Geschäftsgeheimnisse in erster Linie über § 17 UWG geschützt. Dabei handelt es sich um eine Strafrechtsnorm im Lauterkeitsrecht. Zivilrechtliche Anspruchsgrundlagen ergeben sich über § 3a UWG bzw. § 823 Abs. 2/§ 1004 BGB. Den von Anfang an international geprägten Märkten der Datenwirtschaft wird diese national zerklüftete Rechtslandschaft in Europa nicht gerecht.

Daher wird sehr begrüßt, dass mit der EU-Richtlinie zur Harmonisierung des Know-how-Schutzes wenigstens eine Vereinheitlichung in Form von Mindeststandards auf EU-Ebene stattfindet. Als Geschäftsgeheimnisse (damit können Know-how, Geschäftsinformationen und technologische Informationen gemeint sein, Erwägungsgrund 14 der Richtlinie) gelten danach Informationen, die (1) geheim sind, die (2) einen kommerziellen Wert haben, weil sie geheim sind, und die (3) Gegenstand angemessener Geheimhaltungsmaßnahmen sind. Die nationalen Rechtsordnungen in der EU waren bisher zum erforderlichen Grad der Geheimhaltungsmaßnahmen sehr unterschiedlich ausgeprägt. Da es sich bei der Richtlinie um einen Mindeststandard handelt, könnten die EU-Mitgliedsländer bei der Umsetzung der Richtlinie in nationales Recht den erforderlichen

Grad an Geheimhaltungsmaßnahmen immer noch sehr unterschiedlich ausprägen. In allen Rechtsordnungen haben Maßnahmen der Geheimhaltung vertraglichen oder rein tatsächlichen Charakter:

- Die Geheimhaltung ist rechtlich von den Wirtschaftsakteuren durch Verträge (z. B. bilateral, multilateral oder durch Pools/Communities etwa in Form von Vertraulichkeitsvereinbarungen oder in Nutzungsverträgen/Verwertungsgemeinschaften) zu regeln.

- Geheimhaltungsschutz muss aber auch rein tatsächlich etwa durch physische Trennung von Netzwerken und Serverstrukturen sowie durch Cyber-Sicherheitsmaßnahmen (Firewalls, regelmäßige Softwareupdates, Datenverschlüsselung etc.) und den Einsatz von hybriden oder privaten Clouds gewährleistet werden. Dabei müssen je nach Sensibilität der betroffenen Informationen unterschiedliche Schutzgrade und -konzepte angestrebt werden. Ein entsprechendes Vorgehen zur Klassifizierung der Informationen wird in der Publikation „Technischer Überblick: Sichere unternehmensübergreifende Kommunikation“ der Plattform Industrie 4.0 beschrieben.

C: Handlungsoptionen und Handlungsempfehlungen

Die Arbeitsgruppe sieht bei folgenden Schwerpunkten einen Handlungsbedarf des Gesetzgebers bzw. eine Notwendigkeit zur gesetzgeberischen Zurückhaltung, um die grundsätzlich bestehende Vertragsfreiheit zur Entfaltung kommen zu lassen:

- Die EU-Richtlinie zum Know-how-Schutz sollte schnellstmöglich national umgesetzt werden. Dabei sollte möglichst auf die Einheitlichkeit der Umsetzung in den verschiedenen nationalen Rechtsordnungen geachtet werden, um einheitliche Bedingungen für die digitale Transformation der Wirtschaft und Industrie 4.0 in Europa zu schaffen. Allerdings sollten bei der Umsetzung keine zu hohen Anforderungen an die „angemessenen Geheimhaltungsmaßnahmen“ gestellt werden, deren Einrichtung nach der EU-Richtlinie Voraussetzung für einen rechtlichen Know-how-Schutz ist. Insoweit sollte z. B. der Abschluss von Vertraulichkeitsvereinbarungen zwischen zwei Partnern der Industrie 4.0 bereits ausreichen.

- Daneben sollten durch die Wirtschaft zu definierende Cyber-Sicherheitsstandards auch auf europäischer Ebene schnell zur Verfügung stehen. Diese sind nicht rechtlich verpflichtend im Sinne „angemessener Schutzmaßnahmen“ der Know-how-Richtlinie einzuordnen, vielmehr dienen sie als Grundlage freiwilliger flankierender Maßnahmen der Cyber-Sicherheit dem Schutz von Informationen im Kontext der Industrie 4.0. Einheitliche Standards beschleunigen zudem die Entwicklung von Cyber-Sicherheitsprodukten und -dienstleistungen (sowohl durch große Unternehmen als auch durch KMU), fördern den Export und tragen dazu bei, mit Cyber-Sicherheitslösungen am Weltmarkt erfolgreich zu sein. In diesem Zusammenhang sollte auch die Exportkontrolle zu Produkten, die Cyber-Sicherheit durch Verschlüsselungstechnologien bietet, differenziert gestaltet werden und europaweit möglichst einheitlich gehandhabt werden.

- Der Gesetzgeber sollte nach heutigem Stand nicht in die Vertragsfreiheit zur Gestaltung der Geheimhaltung eingreifen. Dadurch können die Vertragspartner weiterhin selbst bilateral oder multilateral definieren, was sie wie schützen möchten.

Mitinhaberschaft bzw. „Rechteketten“

A: Steckbrief

Worum geht es:

Industrie 4.0 fördert das verstärkte Zusammenwirken zwischen Beteiligten verschiedener Produktionsstufen über die Grenzen klassischer Wertschöpfungsketten hinweg. Gerade aus diesem Zusammenwirken werden immer neue Erkenntnisse entstehen, die Gegenstand von Schutzrechten, insbes. von Patenten, sein können. Das Zusammenwirken lässt künftig also vermehrt Situationen erwarten, in denen sich die Beteiligten die Schutzrechte an gemeinsamen Ergebnissen teilen (Mitinhaberschaft). Nach derzeitiger Rechtslage ist unklar, inwieweit und in welchen Fällen sich Mitinhaber untereinander die Verwertung, insbes. die Lizenzierung an Dritte, untersagen, und sich damit gegenseitig am Markt blockieren können. Eine solche Blockade ist spätestens dann untragbar, wenn allein die formale Rechtsstellung einen Mitinhaber in die Lage versetzt, ein Geschäftsmodell oder Marktsegmente zu blockieren, in denen er keine eigenen Interessen verfolgt.

Da das vorbeschriebene Problem in der Praxis, insbesondere im Patentbereich, bereits aus der Vergangenheit hinreichend bekannt ist, wird hierfür im Rahmen von Industrie 4.0 ein umso stärkerer Neuregelungsbedarf gesehen.

Sich ergebende Fragen und Handlungsfelder:

- Lässt sich für oben skizzierte Konstellationen eine Liberalisierung erreichen, die zumindest verhindert, dass sich Teilnehmer unterschiedlicher Marktstufen/Interessenlagen künftig gegenseitig blockieren?

- Darüber hinaus wird die Frage aufgeworfen, ob gleichartiger Handlungsbedarf auch im Hinblick auf andere, klassische Schutzrechtsarten besteht, z. B. im Urheber- oder Datenbankrecht. Diese Frage stellt sich weiterhin dann, wenn neue Leistungsschutzrechte auf Dateninhalte angedacht werden, wie dies im Rahmen der Industrie 4.0-Diskussion teilweise angeregt wurde.

B: Juristische Einschätzung

Im **deutschen Recht zum geistigen Eigentum** werden auf das Verhältnis von Mitinhabern eines gemeinschaftlichen Schutzrechts untereinander mangels Vorliegens abweichender Vereinbarung bislang häufig die allgemeinen BGB-Regelungen angewandt (so beispielsweise im Patentrecht die Regelungen zur Bruchteilsgemeinschaft, s. nur BGH GRUR 2005, 663, 664 – Gummielastische Masse II). Dies kann – nach allerdings nicht unumstrittener Meinung – zur Folge haben, dass ein Mitinhaber im Zweifel für sich allein nicht das Recht hat, Dritten Lizenzen an dem gemeinsamen Recht zu vergeben (vgl. beispielsweise für das Patentrecht nur Benkard/Melullis, Patentgesetz, 11. Aufl. 2015, § 6, Rz. 67 m. weit. Verw.). Verweigert ein Mitinhaber die Zustimmung zur Lizenzvergabe, entsteht in Anbetracht gegebener Rechtsunsicherheit in jedem Fall eine faktische Blockade. Dem Betroffenen bleibt zwar im Streitfall der Ausweg, Aufhebung der Gemeinschaft mitsamt Versteigerung des zugrunde liegenden Schutzrechts zu verlangen (vgl. zum Patentrecht Benkard/Melullis, aaO, Rz. 69). Damit aber fällt ein Patent möglicherweise in Dritthände, womit der Betroffene im Hinblick auf die beabsichtigte Patentverwertung sich nicht bessersteht.

Die befasste Arbeitsgruppe hat zu diesem Thema am Beispiel des Patentrechts einen Blick in andere Rechtsordnungen geworfen. Ohne hierzu Anspruch auf Vollständigkeit zu erheben, ergab sich dabei folgendes Spektrum:

- Am liberalsten stellt sich die **U.S.-Lösung** dar, wo in konsequenter Fortführung des Grundsatzes „gleicher und ungeteilter Anteil am gesamten Patent“ („equal and undivided interest in the entire patent“) jeder Mitinhaber in der Patentverwertung und insbesondere auch bei der Lizenzvergabe an Dritte grundsätzlich frei ist, ohne dass für die beabsichtigte Verwertung die Zustimmung anderer Mitinhaber erforderlich ist. Eine Ausnahme hiervon gilt lediglich für ausschließliche Lizenzen. Der erwähnte Grundsatz führt im Übrigen auch nicht zur etwaigen Verpflichtung, anderen Mitinhabern monetären Ausgleich an den Patentverwertungs-Erlösen zu leisten. Zumindest im letzten Punkt allerdings läuft das deutsche Recht seit der BGH-Entscheidung „Gummielastische Masse II“ (vorstehend zitiert) bereits in diese Richtung.

- Einen Kompromiss bietet das **englische Recht**: Dieses geht zwar grundsätzlich davon aus, dass Mitinhaber an einem Patent in Ermangelung abweichender Vereinbarung nicht befugt sind, ohne Zustimmung der anderen Drittlizenzen zu vergeben. Es besteht jedoch ein Rechtsmittel zum sog. „comptroller“ (Präsident des britischen Patentamts), der bei Auftreten von Blockadesituationen zwischen Mitinhabern die Lizenzvergabe an Dritte genehmigen kann. Der „comptroller“ hat dabei weites Ermessen im Sinne einer vernünftigen, angemessenen und verhältnismäßigen Entscheidung, unter Berücksichtigung aller Umstände des Einzelfalles, und mit dem Ziel, eine ausgewogene wirtschaftliche Lösung zu finden, falls sich die Mitinhaber nicht einigen können. Als Referenzfall wird die Berufungsentscheidung Hughes v Paxman [2006] EWCA Civ 818; [2007] RPC 2 zitiert, bei der im Ergebnis dann allerdings keine Blockadesituation festgestellt und daher keine Lizenzeinräumung angeordnet wurde (s. BL O/217/08).

- Vergleichsweise komplex stellt sich der **französische Weg** dar: Dort darf zwar jeder Mitinhaber zu seinem eigenen Nutzen nicht-ausschließliche Lizenzen an Dritte vergeben, jedoch unter dem Vorbehalt, angemessenen Ausgleich an die anderen Mitinhaber zu leisten, die die Erfindung selbst nicht verwerten bzw. selbst keine Lizenzen vergeben haben. Dazu kommt, dass der Lizenzvertragsentwurf den anderen Mitinhabern zu übermitteln ist, begleitet von einem Angebot auf Abtretung des betreffenden Mitinhaber-Anteils zu einem definierten Preis. Sodann können die anderen Mitinhaber, falls die Lizenzeinräumung ihren eigenen Marktinteressen entgegensteht, dieser binnen 3-Monats-Frist widersprechen, unter der Bedingung, dass sie den betreffenden Mitinhaber-Anteil erwerben.

- Schließlich geht auch das **chinesische Recht** vom Prinzip aus, dass mangels abweichender Vereinbarungen jeder Mitinhaber nicht-ausschließliche Drittlizenzen vergeben darf, ohne dazu einer Zustimmung der anderen Mitinhaber zu bedürfen. Allerdings geht dies einher mit der Verpflichtung, die „Lizenzgebühren“ mit den anderen Mitinhabern gemäß gesetzlich getroffener Regelung zu „teilen“.

C: Handlungsoptionen und Handlungsempfehlungen

- Speziell zum Themenkomplex „Mitinhaberschaft/Rechteketten“ erscheint es empfehlenswert, sich im deutschen Patentrecht an einem liberaleren Modell zu orientieren. Nach dieser Orientierung wären Mitinhaber an (angemeldeten bzw. erteilten) Patenten künftig – soweit nicht vertraglich etwas anderes vereinbart wurde – grundsätzlich ungehindert, Dritten ohne Zustimmungserfordernis seitens anderer Mitinhaber nicht-ausschließliche Lizenzen an dem gemeinsamen Recht zu vergeben; dies ggf. im Rahmen anderer noch zu eruierender Grenzen (unter Billigkeitsgesichtspunkten sollten ggf. auch Ausgleichsleistungen nicht ausgeschlossenen werden, welche dann aber von der Rechtsprechung nötigenfalls im Nachhinein zu bestimmen wären). Die Details einer hierzu nach Möglichkeit gesetzlich zutreffenden Lösung sollten zeitnah angegangen werden, um andernfalls im Rahmen von Industrie 4.0 verstärkt zu erwartende Blockadesituationen am deutschen Industriestandort nicht entstehen zu lassen.

- Auch allen anderen, vorstehend unter B. skizzierten Rechtsordnungen ist gemeinsam, dass sie zu diesem Themenkomplex einen liberaleren Ansatz als das deutsche Recht aufweisen; diese anderen Rechtsordnungen sind aber entweder mit prozessualen Unsicherheiten behaftet (so etwa das englische Recht) oder mit zwingenden materiellen Ausgleichsansprüchen (so etwa das französische oder das chinesische Recht), wie sie sowohl im U.S.-Recht als auch soweit bereits nach deutscher Rechtsprechung zu Recht überwunden sind.

- Die vorstehenden Handlungsempfehlungen wurden bewusst mit Fokus auf das Patentrecht ermittelt. Soweit Gleiches auch im Bereich anderer klassischer Schutzrechte zutrifft, sollte die Frage ebenfalls, etwa im Urheber- und Datenbankrecht, nicht aus den Augen verloren werden.

- In Bezug auf eine Diskussion um neue Leistungsschutzrechte auf Dateninhalte, mit eigentumsähnlicher Zuordnung von Maschinendaten, ergeben sich die hier beleuchteten Fragestellungen nicht, solange derartige, mit korrelierenden Unterlassungsverfügungen ausgestattete Leistungsschutzrechte nicht bestehen. Sollten derartige Leistungsschutzrechte angedacht werden, ist bereits im Ansatz gründlich zu überprüfen, ob nicht durch deren Schaffung die Komplexität potenzieller Mitinhaberschaften/Rechteketten und damit einhergehende Blockaden auf ein derart unüberschaubares Maß intensiviert würden, dass selbst eine Regelung wie die hier im Patentrecht vorgeschlagene keine Rechtssicherheit mehr schaffen könnte.

Daten im Kontext von Industrie 4.0

A: Steckbrief

Worum geht es:

Für Anwendungen der Industrie 4.0 sind Daten unentbehrlich und entscheidende Faktoren für die Erhöhung der Wettbewerbsfähigkeit. Dabei geht es um eine Vielfalt von Daten ganz unterschiedlichen Ursprungs und Aussagegehalts. Daten über die Maschine (z. B. aus ihrer Parametrisierung) können genauso nützlich sein wie Daten, die bei der Nutzung der Maschine anfallen. In vielen Fällen wird sich ein Mehrwert erst durch die Korrelation verschiedener Datensätze erweisen (Big Data Analytics). Die systematische Auswertung verspricht neue Produktionserkenntnisse und Vorsprung im Wettbewerb. Für die Betrachtung rechtlicher Aspekte des Datenverkehrs ist zu unterscheiden zwischen „personenbezogenen Daten“ im Sinne des § 3 Abs. 1 BDSG und sonstigen Daten ohne Bezug zu einer konkreten natürlichen Person (reine „Maschinendaten“). Der Umgang mit personenbezogenen Daten unterliegt den besonderen Anforderungen des Datenschutzrechts.

In der Analyse und Auswertung von Maschinendaten liegen – zum Teil noch unbekannte – Geschäftsmodelle der Zukunft. Maschinendaten können insoweit wesentliche wirtschaftliche Werte darstellen und im Zentrum veränderter Wertschöpfung stehen. Es stellt sich daher die Frage nach der Notwendigkeit und den Möglichkeiten rechtlicher Absicherung der entsprechenden Daten. Gegenwärtig bestehen für die Zuweisung von Maschinendaten zu einem bestimmten Rechtsträger (Datenhoheit) keine spezifischen gesetzlichen Vorschriften.

In Anwendungsszenarien, in denen die nutzungsbezogenen Daten einen Personenbezug aufweisen, ist die Einhaltung des gültigen Datenschutzrechtes zudem eine notwendige, nicht Industrie 4.0-spezifische, Bedingung.

Sich ergebende Fragen:

- Schützt das Gesetz Maschinendaten in vernetzten Wertschöpfungsketten ausreichend vor Eingriffen Dritter?
- Müssen etwaige rechtliche Schutzlücken für Maschinendaten geschlossen werden?
- Welches Schicksal nehmen werthaltige Bestände von Maschinendaten in der Insolvenz?
- Wäre ein neues Gesetz wünschenswert, welches bestimmte Maschinendaten bestimmten Marktteilnehmern in eigentumsähnlicher Weise zuordnet?
- Wie können personenbezogene Daten geschützt und gleichzeitig nutzbar gemacht werden?

B: Juristische Einschätzung

Datenhoheit

1.1 Situation im geltenden Recht

Das geltende Recht kennt kein umfassendes, absolutes Recht an jedwedem Datum an sich. Je nach ihrer Ausprägung sind bestimmte Konstellationen von bzw. an Daten jedoch heute bereits – vielfach indirekt – durch ein Netz verschiedener nationaler und internationaler Gesetze geschützt (Urheberrecht, Patentrecht, Datenbankrecht, Betriebs- und Geschäftsgeheimnisse, Datenschutzrecht, Strafrecht etc.).

Auffallend ist, dass gesetzliche Bestimmungen einem Einzeldatum häufig erst über seine Bedeutungsebene einen schützenswerten Gehalt beimessen. So ist das einzelne zusammenhangslose Sensordatum „18 Grad Celsius“ als naturgegebenes Faktum an sich nicht geschützt. Wird jedoch ein Temperaturverlauf mit Uhrzeiten gespeichert und mit einem Messpunkt in einer bestimmten Anlage verknüpft, erhalten diese Daten einen Aussagegehalt, der bspw. ein Geschäfts- und Betriebsgeheimnis darstellen kann. Welcher Schutz für Maschinendaten greift, hängt also in der Regel vom jeweiligen Kontext ab.

1.2 Möglicher Regelungsbedarf

Vor diesem Hintergrund hat sich die Arbeitsgruppe mit der Frage auseinandergesetzt, ob ein neues Gesetz notwendig wäre, das bestimmte Maschinendaten ggf. klar bestimmten Marktteilnehmern in eigentumsähnlicher Weise zuordnet (die dann wiederum über diese Daten verfügen können).

Nach ganz überwiegender Sicht der Teilnehmer der AG Rechtliche Rahmenbedingungen sollte der Gesetzgeber über den bisherigen Rechtsrahmen hinaus zurückhaltend und entweder gar nicht oder jedenfalls nicht übereilt agieren. Es erscheint darüber hinaus zweifelhaft, dass sich die unzähligen Konstellationen im Zusammenhang mit der Zuordnung von Daten dauerhaft zufriedenstellend in abstrakten Gesetzesvorschriften lösen lassen.

Zudem zeichnet sich als wichtiger Schwerpunkt der Themenbereich Datenzugang, Zugriffsrechte und Portierbarkeit von Daten vor dem Hintergrund wettbewerbsrechtlicher Konstellationen in verschiedensten Sektoren und regulierten Bereichen ab. Dieser steht beim Aufbau der Datenökonomie im Rahmen einer offenen, innovationsorientierten Rechtskultur mit der Frage etwaiger Datenhoheit bzw. dem Schutz von Datendomänen in einer Wechselwirkung. Die vorschnelle Festlegung auf Eigentums- und eigentumsähnliche Ausschließlichkeitsrechte am Einzeldatum könnte dem zuwiderlaufen.

Die Diskussion in der Rechtswissenschaft zu schützenswerten Interessen an Daten ist mithin im Fluss und wird durch die Entwicklung heute ungeahnter Möglichkeiten und heute unbekannter Geschäftsmodelle dynamisch bleiben. Vorschnelle statische Zuordnungen mit der Folge des Schutzes bestimmter Interessen könnten innovationshemmend wirken und eine Fragmentierung der globalen Märkte begünstigen.

Eine Zuordnung von Daten über die bisherigen Rechtsinstitute hinaus durch Eingreifen des Gesetzgebers zugunsten bestimmter „data stakeholder“ könnte zudem die Gefahr der automatischen Beeinträchtigung der wirtschaftlichen Entfaltungsfreiheit und Chancengleichheit für andere „Stakeholder“ in sich bergen. Dadurch könnte einerseits die Entwicklung neuer Geschäftsmodelle in Europa verhindert werden, von denen man sich möglicherweise gerade das gewünschte Wachstum und die Wettbewerbsfähigkeit gegenüber anderen Weltregionen verspricht, z. B. im Bereich Datenanalyse. Andererseits könnten ohne adäquate rechtliche Absicherung von Zugriffsrechten, faktischen Datendomänen und Know-how solche Unternehmen, die entsprechende Geschäftsmodelle betreiben, unbillig getroffen werden.

Das Handeln von Gesetzgeber und Verwaltung sollte davon geleitet sein, eine interessengerechte Bewertung der unterschiedlichen Positionen vorzunehmen. Dies bedeutet, Innovationen Raum zu geben und Fehlentwicklungen nur dann gezielt entgegenzutreten, wenn bestimmte Schutzinteressen und Chancengleichheit der Marktteilnehmer insbesondere auf fairen Wettbewerb („level playing field") systematisch verletzt werden oder eine solche Verletzung droht.

Sollte sich zu einem späteren Zeitpunkt eine Monopolisierung von Märkten zugunsten einiger weniger „Datenmonopole oder Datenoligopole" abzeichnen, wäre dem ggf. über das Wettbewerbsrecht zu begegnen. Eine solche Machtkonzentration durch Datenexklusivität ist in der Industrie aber noch nicht nicht absehbar. Im Unterschied zum Verbrauchergeschäft gibt es in der Industrie nicht „den einen schutzbedürftigen" Marktteilnehmer.

Die Industrie verfügt über eine ausgeprägte Sensibilität im Umgang mit betrieblich relevanten Daten. Vor diesem Hintergrund hat die Vereinbarung von Geheimhaltungs- und Nutzungsbeschränkungsvereinbarungen in der Industrie über die letzten Jahrzehnte nicht nur einen hohen Grad an inhaltlicher Standardisierung erreicht, sondern auch eine sehr hohe Marktdurchsetzung. Das sind gute Voraussetzungen für eine Selbstregulierung des Marktes im Hinblick auf die Weiterentwicklung nachhaltiger Daten-Nutzungsvereinbarungen, auch im Rahmen von Eco-Systemen in der Industrie 4.0. Im Umgang mit Maschinendaten werden die am Datenaustausch beteiligten Unternehmen daher Daten-Nutzungsvereinbarungen schließen bzw. in ihre Verträge aufnehmen. Diese vertragliche Lösung ist auch ohne eine eigentumsähnliche gesetzliche Zuordnung von Maschinendaten möglich.

2. Schutz personenbezogener Daten in innovativen Geschäftsmodellen

Wo immer möglich, sollte der Gesetzgeber auf eine internationale Harmonisierung des Regelungsrahmens hinwirken.

Wenn Daten einen mittelbaren oder unmittelbaren Personenbezug aufweisen, wird auch die EU-Datenschutzgrundverordnung für Anwendungen der Industrie 4.0 Relevanz erlangen. Daher ist es im Interesse der Entwicklung von innovativen Anwendungen in der Industrie 4.0, dass die Verordnung in allen EU-Mitgliedstaaten möglichst einheitlich angewendet wird. Dabei muss das Potenzial technischer Lösungen wie Anonymisierung und Pseudonymisierung zum Schutz personenbezogener Daten, bei gleichzeitiger Ermöglichung von Big Data Analytics Services, gehoben werden. Hier ist perspektivisch das European Data Protection Board verantwortlich, welches unter Beteiligung der Industrie – ggf. auch branchenspezifische – Richtlinien erarbeiten bzw. bestätigen und genehmigen sollte, die es der Wirtschaft ermöglichen, auf rechtssicherer Grundlage entsprechende Dienste anzubieten.

Wahl des deutschen Rechtsrahmens bei Formularverträgen

Statt Dateneigentums- und Datenzugriffsrechte durch gesetzliche Maßnahmen bestimmten Kategorien von Marktteilnehmern starr zuzuordnen, sollten die Unternehmen besser in die Lage versetzt werden, die jeweiligen Rechte vertraglich untereinander festzulegen. Um die Vertragsfreiheit im B2B-Geschäftsverkehr zu stärken, sollten die bestehenden Rechtsunsicherheiten im deutschen AGB-Vertragsrecht daher vom Gesetzgeber beseitigt werden. Es ist davon auszugehen, dass die Verwendung formularmäßiger Standardverträge in den vernetzten Wertschöpfungsketten einer Industrie 4.0 noch deutlich an Bedeutung gewinnen werden. Gleichzeitig können die Vertragspartner in einer internationalisierten Welt das anwendbare Recht frei wählen. Die ausufernde Anwendung von Restriktionen für Allgemeine Geschäftsbedingungen im deutschen Recht (AGB-Recht) auf Verträge zwischen Unternehmen stellt einen Unsicherheitsfaktor für die Verlässlichkeit des deutschen Zivilrechts dar, der sich gerade für Vertragsregelungen in innovativen Industrie 4.0-Geschäftsmodellen nachteilig auswirkt. Um im internationalen Wettbewerb bestehen zu können, sollte der Gesetzgeber diesen Standortnachteil, soweit sinnvoll, möglichst beseitigen.

Arbeitsrecht

Arbeitszeit in einer digitalisierten Industrie

A: Steckbrief

Worum geht es:

Die Dauer und Lage der Arbeitszeit ist durch europäische und nationale Regeln determiniert. Das europäische Recht gibt vor, dass in der Woche die Arbeitszeit regelmäßig 48 Stunden nicht übersteigen darf. Zudem werden Ruhezeiten vorgegeben, die zwischen Arbeitseinsätzen eingehalten werden müssen. Der nationale Gesetzgeber hat im Arbeitszeitgesetz zudem festgelegt, dass die Arbeitszeit 10 Stunden täglich nicht überschreiten darf. Für bestimmte Situationen gibt es eng begrenzte Ausnahmen. In einer digitalisierten Arbeitswelt wird es einerseits weiter „traditionelle Arbeitsplätze“ geben, andererseits aber der Bedarf nach eigenverantwortlich gestalteter Arbeitszeitplanung zunehmen. Weiterhin ist damit zu rechnen, dass der Bedarf an Flexibilität steigt und die Gestaltung der Arbeitszeit nicht immer autonom vom Vertragsarbeitgeber vorgegeben wird, sondern externe Faktoren bestimmend werden, wie beispielsweise bei einer endkundengesteuerten Auftragserteilung, die unmittelbar einen Beschaffungs- und Produktionsprozess auslöst.

Sich ergebende Fragen und Handlungsfelder:

- Reichen die bisherigen gesetzlichen Flexibilisierungsinstrumente aus?
- Ist es hilfreich, wenn der 48-Stunden-Rahmen von der vorgegebenen täglichen Höchstarbeitszeit für bestimmte Bereiche befreit wird, so dass z. B. auch an einzelnen Tagen mehr als 10 Stunden gearbeitet werden darf bei entsprechend kürzerer Tätigkeit an anderen Tagen?
- Wäre eine Verkürzung der Ruhezeiten teilweise sinnvoll, um die tägliche Arbeitszeit auf mehrere Zeitintervalle an einem Arbeitstag verteilen zu können?
- Sollte es ein individuelles Recht auf Bestimmung der zeitlichen Lage der Arbeitszeit für die Beschäftigten vergleichbar mit § 8 Teilzeit- und Befristungsgesetz geben?
- Sollte dem Betriebsrat ein Mitbestimmungsrecht bei der Arbeitsorganisation/Arbeitsmenge gegeben werden, um Überforderungen zu vermeiden? Handelt es sich hierbei um eine Problematik von Industrie 4.0 oder um ein allgemeines Thema?

B: Juristische Einschätzung

Art. 6 b) RL 2003/88/EG gibt einen größeren Handlungsspielraum, der lediglich vorsieht, dass eine durchschnittliche Höchstarbeitszeit von 48 Stunden innerhalb eines 7-Tage-Zeitraums einzuhalten ist. Art. 16 b) RL 2003/88/EG gibt hierfür einen Bezugszeitraum von maximal 4 Monaten vor, innerhalb dessen diese Höchstarbeitszeit eingehalten werden muss. Ein generelles Sonn- und Feiertagsarbeitsverbot gibt es nicht. Arbeitnehmern, deren Arbeitszeit wegen der besonderen Merkmale der ausgeübten Tätigkeit nicht gemessen und/oder nicht im Voraus festgelegt wird oder von den Arbeitnehmern selbst festgelegt werden kann, kann eine größere Eigenverantwortung zugebilligt werden (Art. 17 Abs. 1 RL 2003/88/EU).

C: Handlungsoptionen und Handlungsempfehlungen

Eine weitergehende Ausnutzung der nach EU-Recht einzuhaltenden Rahmenbedingungen ist möglich. So könnte die Begrenzung der täglichen Arbeitszeit auf 8 bzw. 10 Stunden für bestimmte Arbeitsbereiche überdacht werden. Ebenso wäre für diese Bereiche eine Lockerung des Sonn- und Feiertagsarbeitsverbotes zu erwägen. Eine größere Flexibilität eröffnet aber auch größere Missbrauchsrisiken, denen durch geeignete Regelungen zu begegnen ist. Hierbei ist die Pflicht des Arbeitgebers, die Einhaltung der Arbeitszeiten zu gewährleisten, zu verstärken.

Ein individuelles Recht auf Bestimmung der zeitlichen Lage der Arbeitszeit für die Beschäftigten kann der größeren Eigenverantwortung Ausdruck geben.

Ob ein Überforderungsschutz durch Gewährung von betrieblichen Mitbestimmungsrechten bei der Festlegung der Arbeitsmenge oder der Arbeitsorganisation eingeräumt werden sollte, ist von der weiteren Entwicklung abhängig zu machen. Betriebs- und Tarifvertragsparteien haben im Übrigen schon aktuell die Möglichkeit, entsprechende Regelungen einverständlich zu treffen.

Arbeits- und Gesundheitsschutz

A: Steckbrief

Worum geht es:

Der Arbeitseinsatz in einer digitalisierten Arbeitswelt wird zunehmend zu einer Entgrenzung dahingehend führen, dass es neben dem klassischen Arbeitsplatz im Betrieb Tätigkeiten gibt, die gar nicht mehr an einen bestimmten Arbeitsort gebunden sind oder an der Wohnstätte des Arbeitnehmers ausgeführt werden. Gängige Mechanismen des Arbeitsschutzes werden nicht mehr ausreichend sein, um auch solche Arbeitsplätze zu erfassen. Arbeitnehmer werden auch zunehmend mit eigenen Arbeitsmitteln arbeiten („bring your own device“), bei denen der Arbeitgeber auf Standards keinen hinreichenden Einfluss mehr hat. Verbunden mit veränderten Arbeitsrhythmen können sich verstärkte Anforderungen an den Gesundheitsschutz ergeben. Eine veränderte Erreichbarkeit von Arbeitnehmern über E-Mails, soziale Netzwerke, Nachrichtendienste wie „WhatsApp“ etc. kann neue Gesundheitsrisiken erzeugen.

Sich ergebende Fragen und Handlungsfelder:

- Genügen die gesetzlichen Arbeitsschutzregelungen noch den veränderten Strukturen in einer Industrie 4.0 mit zeitlich und örtlich entgrenzten Arbeitsbedingungen oder sollten vorhandene Regelungen, wie die Bildschirmarbeits- oder die Arbeitsstättenverordnung, in ihren Geltungsbereichen ausgeweitet und neue Regelungen, wie z. B. für einen Überforderungsschutz, geschaffen werden?
- Folgt aus einer flexibleren Arbeitswelt möglicherweise ein inhaltlich anderer Schutzbedarf?
- Wie kann die Einhaltung eines ausreichenden Gesundheitsschutzes noch sichergestellt werden, wenn der Arbeitnehmer stärker eigenverantwortlich über seinen Arbeitseinsatz entscheidet, oder muss der Arbeitnehmer künftig stärker vor sich selbst geschützt werden?
- Sind die gesetzlich vorgesehenen Schutzmechanismen noch geeignet, steuernd auf die Arbeitswelt einzuwirken, oder laufen sie Gefahr, in der Praxis ignoriert zu werden?
- Sind technische Vorkehrungen zu treffen, um eine „Selbstausbeutung“ zu verhindern?
- Sollte für die Beschäftigten ein Recht auf Nichterreichbarkeit klargestellt werden?

B: Juristische Einschätzung

Der gesetzliche Gesundheitsschutz ist in verschiedenen Gesetzen geregelt, z. B. im Arbeitsschutzgesetz, Arbeitssicherheitsgesetz, div. Verordnungen etc. Zum Teil beruhen die Regelungen zum Arbeitsschutz auf europarechtlichen Vorgaben. Flankiert wird dies durch Rechte des Betriebsrats, wie z. B. in § 87 Abs. 1 Nr. 7 oder § 89 BetrVG. Zum Teil ist die Nichteinhaltung gesetzlicher Vorgaben bußgeldbewehrt, z. B. § 22 ArbZG, § 20 ASiG.

C: Handlungsoptionen und Handlungsempfehlungen

Teilweise ist der Handlungsbedarf, vorhandene Regelungen anzupassen, bereits heute erkennbar, wie z. B. in der BildschirmarbeitsVO. Für weitere Bereiche ist zu evaluieren, ob eine digitalisierte Arbeitswelt einen modifizierten Schutzbedarf auslöst oder davon ausgegangen werden kann, dass auch in einer durch Industrie 4.0 geprägten Arbeitswelt keine veränderten Anforderungen an den Arbeits- und Gesundheitsschutz zu stellen sind. Sollte ein veränderter Schutzbedarf erkennbar sein, müssen die bisherigen Regelungen daran angepasst werden. Es wird zu prüfen sein, wie ein Ausgleich zwischen Flexibilität und Gefährdungsschutz sichergestellt werden kann.

Es ist zu prüfen, welche technischen und sonstigen Möglichkeiten für einen besseren Schutz der Beschäftigten möglich sind. Hierbei wird es sich um einen kontinuierlichen Verbesserungsprozess handeln. Dabei kommt den Betriebsparteien eine besondere Rolle und Verantwortung zu.

Für die Beschäftigten besteht schon jetzt ein Recht auf Nichterreichbarkeit. Trotzdem ist im Hinblick auf häufiger bestehende falsche Vorstellungen dies klarzustellen.

Mitbestimmungsrechte des Betriebsrats aus § 87 Abs. 1 Nr. 6 BetrVG

A: Steckbrief

Worum geht es:

Dieser Themenkomplex befasst sich mit den Mitbestimmungsrechten des Betriebsrats bei der Einführung und Anwendung von technischen Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Das BAG lässt schon die objektive Möglichkeit der Überwachung ausreichen. Die modernen Arbeitsmittel sind in der Regel geeignet, das Arbeitnehmerverhalten zu überprüfen. Zeitaufwendige Verhandlungen mit dem Betriebsrat, so wird teilweise befürchtet, können zu Verzögerungen bei der Einführung der technischen Einrichtungen führen.

Sich ergebende Fragen und Handlungsfelder:

- Welche Möglichkeiten existieren, komplexe Verhandlungen mit dem Betriebsrat zu vereinfachen?
- Bedarf es neuer Schutzmechanismen oder müssen vorhandene Schutzmechanismen intensiviert werden?

B: Juristische Einschätzung

§ 87 Abs. 1 Nr. 6 BetrVG gibt dem Betriebsrat ein erzwingbares Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen, das dazu geeignet ist, die Leistung und das Verhalten der Arbeitnehmer zu kontrollieren. Das hier geltende positive Konsensprinzip verpflichtet die Betriebspartner zu einer Einigung. Gelingt eine innerbetriebliche Einigung nicht, so entscheidet eine Einigungsstelle, die mit neutralem Vorsitz ggf. durch Spruch entscheidet. Solange eine Einigung nicht erreicht ist, kann der Betriebsrat nach höchstrichterlicher Auffassung Unterlassung verlangen und dies ggf. im Wege einstweiligen Rechtsschutzes durchsetzen.

C: Handlungsoptionen und Handlungsempfehlungen

Arbeitgeber- und Arbeitnehmervertreter sind hierzu nicht einheitlicher Meinung: Aus Sicht der Unternehmen sollte bei technischen Veränderungen im Sinne von Industrie 4.0 überlegt werden, ob der Arbeitgeber unter noch näher zu definierenden Vorgaben zum Schutz der Persönlichkeitsrechte der betroffenen Arbeitnehmer ein begrenztes vorläufiges Einführungsrecht bekommt. Der Arbeitgeber könnte so die neue technische Einrichtung zumindest beschränkt in Betrieb nehmen und hätte damit nicht mehr das Risiko, infolge etwaig lang andauernder Verhandlungen mit dem Betriebsrat den technischen Anschluss zu verlieren oder Wettbewerbsnachteile zu erleiden.

Demgegenüber lehnen die Arbeitnehmervertreter ein vorläufiges Durchführungsrecht ab. Sie sehen darin einen Systembruch innerhalb der Mitbestimmungsrechte in sozialen Angelegenheiten aus § 87 BetrVG. Eine zeitgerechte Implementierung technischer Veränderungen im Hinblick auf Industrie 4.0 kann aus ihrer Sicht auch dadurch gewährleistet werden, dass betriebliche Rahmenvereinbarungen abgeschlossen werden, in denen technische Mindeststandards zum Schutz des Persönlichkeitsrechtes festgelegt sind. Auch ohne Systembruch könne damit eine zeitnahe Umsetzung technischer Neuerungen erreicht werden.

Beschäftigungssicherung und berufliche Fortbildung

A: Steckbrief

Worum geht es:

Die Prognosen für die Auswirkung von Industrie 4.0 auf die Beschäftigung sind höchst unterschiedlich. Während beispielsweise das Weltwirtschaftsforum in Davos 2016 davon ausgeht, dass in den nächsten 5 Jahren weltweit 7 Millionen Arbeitsplätze überflüssig werden und lediglich 2 Millionen neue entstehen, sind manche Prognosen auch gegenläufig. Für Deutschland scheint eine Prognose des IAB valide, die von einem Minus von 60.000 Arbeitsplätzen ausgeht. Das IAB unterstellt allerdings, dass sich bis 2025 ca. 920.000 Arbeitsplätze im Hinblick auf die erforderliche Qualifikation verändern und zwischen den Berufsfeldern umgeschichtet werden. Darüber hinaus entsteht in Unternehmen selbst im Rahmen von Industrie 4.0 kurzfristig zu erfüllender Qualifizierungsbedarf.

Industrie 4.0 fordert also neue Qualifikationen der Mitarbeiter. Auch einfache Hilfstätigkeiten werden womöglich ohne Wissen im Umgang mit vernetzten Systemen nicht mehr ausgeübt werden können. Der Mitarbeiter kann ohne ständige Weiterbildung die an ihn gestellten Anforderungen nicht erfüllen. Auf der anderen Seite verlieren Unternehmen, die diesen Fortbildungsbedarf ihrer Mitarbeiter nicht abdecken, möglicherweise den Anschluss zu Wettbewerbern.

Sich ergebende Fragen und Handlungsfelder:

- Wie können die Mitarbeiter den hohen Fortbildungsbedarf erfüllen?
- Welche staatlichen Fördermöglichkeiten für Weiterbildungs- und Qualifizierungsmaßnahmen existieren?
- Empfiehlt es sich, den Beschäftigten einen individuellen Anspruch auf Weiterqualifizierung zu geben, falls der Arbeitgeber Maßnahmen plant oder durchführt, die dazu führen, dass sich die Tätigkeit der betroffenen Arbeitnehmer ändert und ihre beruflichen Kenntnisse und Fähigkeiten zur Erfüllung ihrer Aufgaben nicht mehr ausreichen (§ 97 Abs. 2 BetrVG)?
- Empfiehlt es sich, Betriebsratsrechte bei der Beschäftigungssicherung und Qualifizierung, wie z. B. nach §§ 92a, 111f. und 97 BetrVG, zu erweitern?

B: Juristische Einschätzung

Das Arbeitsrecht sieht einen gesetzlichen Anspruch ebenso wenig wie eine gesetzliche Verpflichtung zur beruflichen Weiterbildung vor. Soweit vertragliche Verpflichtungen fehlen, kommt es darauf an, dass auf freiwilliger Basis ein Fortbildungsbedarf abgedeckt wird. Die betrieblichen Mitwirkungs- und Mitbestimmungsrechte des Betriebsrats haben hier nur ordnende Bedeutung.

C: Handlungsoptionen und Handlungsempfehlungen

Staatliche Förderungen beruflicher Weiterbildung können dazu beitragen, dass ein Qualifizierungsbedarf effektiv abgedeckt wird. Es wäre deshalb allgemein zu begrüßen, wenn der Staat diesbezügliche Förderungen intensiviert.

Hinsichtlich der Frage, ob eine Erweiterung von Mitbestimmungsrechten bei der Beschäftigungssicherung und zu Themen der beruflichen Qualifikation anzustreben ist, bestehen zwischen Arbeitnehmer- und Industrievertretern unterschiedliche Auffassungen: Eine Erweiterung der Mitbestimmungsrechte ist aus Sicht der Unternehmensvertreter nicht erforderlich und auch in Bezug auf eine Beschäftigungssicherung verfassungsrechtlich problematisch.

Demgegenüber ist nach Auffassung der Arbeitnehmerseite eine Ausweitung der Rechte des Betriebsrats insbesondere bei der Qualifizierung vorzunehmen, um die erforderliche Weiterbildung zu garantieren.

Den Beschäftigten sollte ein entsprechender Anspruch auf Weiterbildung eingeräumt werden. Umstritten ist hierbei allerdings, ob eine gesetzliche Verpflichtung für die Arbeitnehmer, sich einer beruflichen Fortbildung zu stellen, sinnvoll ist. Aus Sicht der Arbeitnehmerseite genügen tarifliche Vorgaben oder entsprechende arbeitsvertragliche Verpflichtungen.

Betriebsverfassungsrechtliche Grundlagen im Rahmen von Industrie 4.0

A: Steckbrief

Worum geht es:

Eine einheitliche gesetzliche Definition des Begriffs „Betrieb“ fehlt. Das BAG definiert den Betrieb als organisatorische Einheit, innerhalb derer der Unternehmer allein oder zusammen mit seinen Arbeitnehmern mithilfe sächlicher oder immaterieller Mittel bestimmte arbeitstechnische Zwecke fortgesetzt verfolgt, welche sich nicht auf die Befriedigung des Eigenbedarfs beschränken. Der „Betrieb“ ist beispielsweise für die Wahl von Betriebsräten sowie für die Ausübung etwaiger Mitbestimmungsrechte der zentrale Bezugspunkt. Er ist Anknüpfungspunkt zahlreicher weiterer gesetzlicher Regelungen wie beispielsweise den Kündigungsschutz der Arbeitnehmer. Industrie 4.0 ist geprägt durch flexible und dezentrale Organisationsstrukturen. Digitale Dienstleistungsfunktionen werden beispielsweise auf Plattformen ins Internet verlagert und durch „Crowdworker“ abgearbeitet. Ein einheitlicher Leitungsapparat fehlt oft. Zudem werden Anforderungen an Betriebsarbeit quantitativ und qualitativ mit weiter steigender Tendenz wachsen. Für Gewerkschaften wird es deutlich herausfordernder, mit den Beschäftigten zu kommunizieren, weil der Bezugspunkt Betrieb sich tendenziell entsprechend verändert.

Sich ergebende Fragen und Handlungsfelder:

- Ist der Betriebsbegriff noch ein taugliches Abgrenzungsmerkmal?
- Passt der Betriebsbegriff zu den dezentralen Organisationsstrukturen der Industrie 4.0?
- Empfiehlt es sich, § 3 BetrVG, also die Möglichkeit von Vereinbarungslösungen, im Hinblick auf neue Organisationsformen der Unternehmen auszuweiten?
- Sollten auch arbeitnehmerähnliche Personen durch Änderung des § 5 BetrVG in die Betriebsverfassung aufgenommen werden?
- Müssen im Hinblick auf die Digitalisierung auch die Arbeitsgrundlagen des Betriebsrates verbessert werden?
- Empfiehlt es sich, im Hinblick auf die durch die Digitalisierung veränderten Unternehmensstrukturen Gewerkschaftsrechte zu modifizieren?

B: Juristische Einschätzung

Im Zuge der fortschreitenden Digitalisierung der Arbeitsbedingungen wird der Betriebsbegriff, wie ihn das BAG in ständiger Rechtsprechung verwendet, ausgehöhlt. Ansätze davon sind bereits heute zu finden. Einen klassischen Betrieb findet man weitestgehend „nur“ noch dort, wo ein Unternehmer in mehr oder weniger klassischer Arbeitsteilung Wertschöpfung betreibt.

Für viele zukünftige Arbeitsbeziehungen bildet der Betriebsbegriff kein taugliches Abgrenzungsmerkmal (mehr). Dies hat allerdings wiederum zur Konsequenz, dass beispielsweise unternehmens- wie betriebsbezogene Mitbestimmungsrechte massiv an Bedeutung verlieren werden und damit im Endeffekt Arbeitsbedingungen unter Druck geraten können. Es besteht das Risiko, dass das System der Mitbestimmung ins Leere läuft.

C: Handlungsoptionen und Handlungsempfehlungen

Zur Erhaltung des Status quo der betrieblichen Mitbestimmung wird eine Anpassung/Erweiterung des § 3 BetrVG zur Errichtung von betriebsverfassungsrechtlichen Strukturen erforderlich werden.

Die Zahl der arbeitnehmerähnlichen Personen wird im Zuge von Industrie 4.0 weiter ansteigen. Arbeitnehmerähnliche Personen sind zwar vom Arbeitgeber wirtschaftlich abhängig, nicht jedoch persönlich abhängig. Vor diesem Hintergrund sind arbeitnehmerähnliche Personen bislang keine Arbeitnehmer i. S. d. BetrVG. Um diesen Personenkreis in den Schutzbereich des BetrVG einzubeziehen, kann sich eine Aufnahme der arbeitnehmerähnlichen Personen in § 5 BetrVG empfehlen.

Im Hinblick auf die zu erwartenden erheblichen Veränderungen durch die Digitalisierung geraten auch Gestaltungsmöglichkeiten der Arbeitnehmervertretung unter Druck. Das System der betrieblichen Mitbestimmung und der Unternehmensmitbestimmung setzt u. a. wirkungsvolle Instrumente der Arbeitnehmervertretungen voraus. Nur so können sie ihren Handlungsauftrag auch im Zeitalter von

Industrie 4.0 erfüllen. Hierzu können mitunter die erleichterte Hinzuziehung von Sachverständigen oder erweiterte Freistellungen gehören.

Es kann sich vor diesem Hintergrund auch empfehlen, Gewerkschaften den traditionellen Informations- und Kommunikationsplattformen (z. B. schwarze Bretter, Flyer, Betriebsversammlungen) vergleichbare Instrumente zur Werbung und Kommunikation mit den Beschäftigten zur Verfügung zu stellen.

Veränderte Weisungsstrukturen im Rahmen von Industrie 4.0

A: Steckbrief

Worum geht es:

Durch das Arbeitsverhältnis wird der Arbeitnehmer zur Leistung fremdbestimmter Arbeit in persönlicher Abhängigkeit verpflichtet. Zu den wesentlichen Merkmalen des Arbeitsverhältnisses gehört insbesondere die Weisungsgebundenheit. Der Arbeitnehmer hat grundsätzlich die Weisungen seines Arbeitgebers zu befolgen. Im Rahmen von Industrie 4.0 gewinnen Selbstorganisation und Autonomie an Bedeutung. Beispielsweise werden veränderte Situationen an der Produktionslinie direkt an Mitarbeiter des Logistikteilnehmers kommuniziert. Weisungen werden damit mitunter nicht nur vom Vertragsarbeitgeber, sondern wie im Beispiel von Kunden des Arbeitgebers erteilt. Auch Weisungen durch Systeme sind denkbar.

Sich ergebende Fragen und Handlungsfelder:

- Welche Folgen hat es für das Arbeitsverhältnis, wenn Weisungen nicht mehr nur vom (Vertrags-)Arbeitgeber, sondern auch von Dritten erteilt werden?
- Können autonome Systeme (eines Dritten) arbeitsvertragliche Weisungen erteilen?

C: Handlungsoptionen und Handlungsempfehlungen

Veränderte Weisungsstrukturen im Rahmen der Arbeitsbedingungen von Industrie 4.0 können durch die aktuellen rechtlichen Rahmenbedingungen abgebildet werden. Eine Anpassung rechtlicher Rahmenbedingungen erscheint zurzeit nicht erforderlich.

Durch das Weisungsrecht wird die Arbeitspflicht des Arbeitnehmers konkretisiert. Bei der Weisung handelt es sich rechtlich um eine einseitige, empfangsbedürftige Willenserklärung. Dass diese auch nicht von dem eigentlichen Vertragsarbeitgeber (selbst) abgegeben werden kann, ist bereits heute ein in der betrieblichen Praxis häufig vorkommender Fall (Stellvertretung/Arbeitnehmerüberlassung). Weisungen durch Maschinen sind regelmäßig dem „Absender“ zuzurechnen, soweit sie aus seiner Sphäre stammen.

Beschäftigtendatenschutz

A: Steckbrief

Worum geht es:

Im Zuge der Digitalisierung kommt der Datenverarbeitung eine neue Qualität zu („Big Data“). Durch Industrie 4.0 wird sich die Menge der personenbeziehbaren Beschäftigtendaten deutlich erhöhen. Diese Entwicklung, die mit der ab dem 25. Mai 2018 anwendbaren EU-Datenschutzgrundverordnung zusammenfällt, führt zu neuen Herausforderungen für einen wirksamen Beschäftigtendatenschutz (vgl. zum Datenschutz auch Seite 8 ff.).

Sich ergebende Fragen und Handlungsfelder:

- Bedarf es neuer Schutzmechanismen oder müssen vorhandene Schutzmechanismen intensiviert werden? Empfiehlt es sich z. B., den Datenschutz neben normativen Regelungen durch technische Vorkehrungen/Zertifizierungen, die Anreize für IT-Produzenten bieten, sicherzustellen?

- Empfiehlt es sich, dem besonderen Schutzbedürfnis von Arbeitnehmerinnen und Arbeitnehmern dadurch zu entsprechen, dass ein Beschäftigtendatenschutzgesetz geschaffen wird?

- Empfiehlt es sich, dem Betriebsrat ein Mitbestimmungsrecht beim Datenschutz einzuräumen?

B: Juristische Einschätzung

Das durch die Verfassung geschützte Recht auf informationelle Selbstbestimmung (vgl. zudem Artikel 8 der Charta der Grundrechte der Europäischen Union zum Schutz personenbezogener Daten) ist auch bzw. gerade im Zusammenhang mit Industrie 4.0-Szenarien zu gewährleisten.

Die Datenschutzgrundverordnung eröffnet den Mitgliedstaaten in Art. 88 einen eigenen Regelungsspielraum, durch Rechtsvorschriften oder durch Kollektivvereinbarungen die Datenverarbeitung im Beschäftigtenkontext zu regeln. Entsprechende Vorschriften umfassen gemäß Art. 88 Abs. 2 DSGVO angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

C: Handlungsoptionen und Handlungsempfehlungen

Neben normativen Regelungen erscheinen technische Vorkehrungen (Zugriffsrechte, Löschroutinen etc.) und Zertifizierungen als sinnvolles Mittel zur Herstellung eines effektiven Beschäftigtendatenschutzes.

Der Gesetzgeber sollte von der Öffnungsklausel des Art. 88 DSGVO Gebrauch machen, damit es nicht zu einer Verschlechterung des Beschäftigtendatenschutzes in Deutschland kommt. Dabei sollte insbesondere sichergestellt werden, dass der Handlungsspielraum der Betriebsparteien im bisherigen Umfang erhalten bleibt. Neben dem derzeit diskutierten Anpassungsgesetz zur DSGVO ist also ein eigenständiges und umfassendes Beschäftigtendatenschutzgesetz eine Maßnahme, die nicht nur dem besonderen Schutzbedürfnis der Arbeitnehmerinnen und Arbeitnehmer, sondern auch der Komplexität der Materie Rechnung tragen würde.

Ob es sich empfiehlt, dem Betriebsrat über die Möglichkeiten des § 87 Abs. 1 Nr. 6 BetrVG hinaus (siehe hierzu S. 26) ein Mitbestimmungsrecht beim Datenschutz einzuräumen, wird unterschiedlich beurteilt und bleibt daher offen.

Auswirkungen von Industrie 4.0 auf die Beschäftigtenbegriffe

A: Steckbrief

Worum geht es:

Insbesondere durch die Plattformökonomie, die für die Industrie 4.0 zunehmende Bedeutung erlangt, ist ein massives Anwachsen von angeblich Selbständigen teilweise festzustellen, teilweise zu erwarten. Die Schutzbedürftigkeit dieser Personen ist allerdings oft der von Arbeitnehmerinnen und Arbeitnehmern vergleichbar.

Sich ergebende Fragen und Handlungsfelder:

- Kann der traditionelle Arbeitnehmerbegriff beibehalten oder muss er erweitert werden?
- Sind Veränderungen beim Begriff der arbeitnehmerähnlichen Person bzw. auch beim Heimarbeitsgesetz erforderlich?
- Ist ein Gesetz für wirtschaftlich abhängige Soloselbständige erforderlich?
- Sind Soloselbständige verstärkt in die Sozialversicherungssysteme aufzunehmen?

B: Juristische Einschätzung

Die Frage, welchen Status Beschäftigte insbesondere in der Plattformökonomie haben, ist häufig umstritten. Teilweise kann es sich nach den bisherigen Kriterien um Arbeitsverhältnisse handeln, teilweise werden es Selbständige, teilweise können es auch arbeitnehmerähnliche Personen oder in Heimarbeit Beschäftigte sein. Die sozialen Schutzvorschriften sind damit völlig unterschiedlich, obwohl, wie erwähnt, die Schutzbedürftigkeit oft durchaus vergleichbar ist.

Die im „klassischen Arbeitsverhältnis“ und auch für die rechtliche Abgrenzung charakteristischen Merkmale wie „Eingliederung in den Betrieb“ und „Ausübung des Direktionsrechts durch den Arbeitgeber“ verlieren insgesamt in der Industrie 4.0 stark an Bedeutung. Daher stellt sich die Frage einer modifizierten Abgrenzung, die z. B., wie in der juristischen Debatte diskutiert, das unternehmerische Handeln und die tatsächlichen Möglichkeiten am Markt mehr betont.

Das Heimarbeitsgesetz ist anerkanntermaßen veraltet und kaum in der Lage, die neuen Beschäftigungsverhältnisse wirksam zu erfassen.

Der Schutz der Selbständigen, insbesondere derer ohne Beschäftigte, im System der Sozialversicherung ist nur rudimentär.

C: Handlungsoptionen und Handlungsempfehlungen

Das Heimarbeitsgesetz sollte so verändert werden, dass auch Crowdworker erfasst werden. Beim Begriff der arbeitnehmerähnlichen Person sollte überlegt werden, ob der für die wirtschaftliche Abhängigkeit erforderliche Entgeltanteil nicht zu senken ist.

Soloselbständige sollten verstärkt in die Sozialversicherungssysteme aufgenommen werden. Dies führt für sie zu einer besseren Absicherung und entlastet ggf. auch die Allgemeinheit, die ansonsten z. B. bei Altersarmut einzuspringen hätte.

Ansonsten sollte die weitere Entwicklung abgewartet und durch empirische Untersuchungen ein Handlungsbedarf geprüft werden.

Schlussbemerkung

Zum Abschluss sollen noch zwei weitere Themen kurz angesprochen werden.

Durch die Digitalisierung wird es auch auf europäischer Ebene Änderungsbedarf geben. So sind z. B. die Informations- und Beratungsrechte in den Richtlinien zu Europäischen Betriebsräten und zur Information und Konsultation im Hinblick auf die Veränderung durch Industrie 4.0 zu eng gefasst. So fehlen beispielsweise in der Richtlinie zur Information und Konsultation Arbeitszeitgestaltung, Datenschutz oder Arbeits- und Gesundheitsschutz. Auch die Definitionen von Betrieb, Arbeitgeber und Arbeitnehmer sollten überdacht werden. In der Richtlinie zu Europäischen Betriebsräten sind z. B. der Datenschutz und der Arbeits- und Gesundheitsschutz nicht genannt.

Ein weiterer Punkt betrifft die Individualrechte im Betrieb. Die Digitalisierung wird erwartungsgemäß sehr davon profitieren, wenn die Beschäftigten einbezogen und beteiligt werden. Mit Begriffen wie „das demokratische Unternehmen“ wird umschrieben, dass das Unternehmen der Zukunft auf selbständige, innovative Beschäftigte setzen, die Initiative ergreifen und sich aktiv einbringen muss. Hier wird die Frage zu untersuchen sein, ob die Individualrechte der Beschäftigten z. B. in der Betriebsverfassung, wie bei der Einberufung von Betriebsversammlungen nach § 43 Abs. 3 BetrVG, beim Beschwerderecht oder bei der Beteiligung an der Arbeit des Betriebsrats, verstärkt bzw. ergänzt werden sollten.

Ausblick

Mit Aufnahme der Tätigkeiten der Arbeitsgruppe „Rechtliche Rahmenbedingungen“ (AG 4) im Sommer 2015 konzentrierten sich ihre Arbeiten zunächst auf die Identifizierung möglicher Problemkreise sowie die Herausarbeitung lösungsorientierter juristischer Einschätzungen. Mit der vorliegenden Publikation werden mögliche Handlungsoptionen und Handlungsempfehlungen zu 17 Themenkomplexen für die politische Administration aus Sicht der Arbeitsgruppe vorgestellt. Diese werden in den nächsten Wochen mit verschiedenen Akteuren und Initiativen aus der Praxis (z. B. in Roundtable-Veranstaltungen) diskutiert und verifiziert. Ergänzend dazu werden noch einmal gezielt andere Länder und Rechtskulturen mit Blick auf Lösungen zu Industrie 4.0-Anwendungen analysiert. Im Anschluss daran werden die Ergebnisse für die Zielgruppen aus der Wirtschaft aufbereitet und im Rahmen von gesonderten Veranstaltungen kommuniziert.

AUTOREN:

RA Dr. Martin Ahlfeld, Weidmüller Holding AG & Co. KG (Leiter UAG 4 IP-Recht) | RA Till Barleben, ZVEI Zentralverband Elektrotechnik- und Elektroindustrie e.V. | RA Mathias Cellarius, SAP SE | RA Michael Dettmer, HDI Global SE | RA Verena zu Dohna-Jaeger, IG Metall | RA Dr. Alexander Duisberg, Bird & Bird LLP | Prof. Dr. Dr. Jürgen Ensthaler, Technische Universität Berlin (Leiter UAG 2 IT-Sicherheitsrecht und Datenschutzrecht) | Dr. Bernhard Fischer, SAP SE | RA Christian Greger, TRUMPF GmbH + Co. KG | RA Dr. Philipp Haas, Robert Bosch GmbH | RA Florian Hilbert, Siemens AG | RA Elisabeth Höller, thyssenkrupp AG | RA Nils Hullen, IBM Deutschland | RA Dr. Marc Kaiser, AUDI AG | RA Dr. Ulrich Keil, Schaeffler AG | RA Dr. Thomas Klebe, Hugo Sinzheimer Institut für Arbeitsrecht | RA Prof. Dr. Thomas Klindt, Kanzlei Noerr LLP (Leiter UAG 3 Produkthaftungsrecht und Produktsicherheitsrecht) | RA Dr. Jörg Kondring, Voith GmbH | RA Thomas Kriesel, BITKOM e.V. | RA Jenny Paschen, Vodafone GmbH | Thomas Schauf, Deutsche Telekom AG | RA Dr. Johannes Schipp, T S C Fachanwälte für Arbeitsrecht (Leiter UAG 5 Arbeitsrecht) | RA Dr. Hans-Jürgen Schlinkert, thyssenkrupp AG | RA Carmen Schmidt, Volkswagen AG | RA Tim Schwarting, Volkswagen AG | RA Martin Schweinoch, SKW Schwarz Rechtsanwälte (Leiter UAG 1 Zivilrecht und Zivilprozessrecht) | RA Dr. Siegfried Schwung, KUKA AG | RA Christian Steinberger, VDMA e.V. | RA Daniel van Geerenstein, VDMA e.V. | RA Marc Wirwas, HARTING KGaA | Wolfgang Zeiler, Siemens AG

Diese Publikation ist ein Ergebnis der AG Rechtliche Rahmenbedingungen (Plattform Industrie 4.0).

www.plattform-i40.de