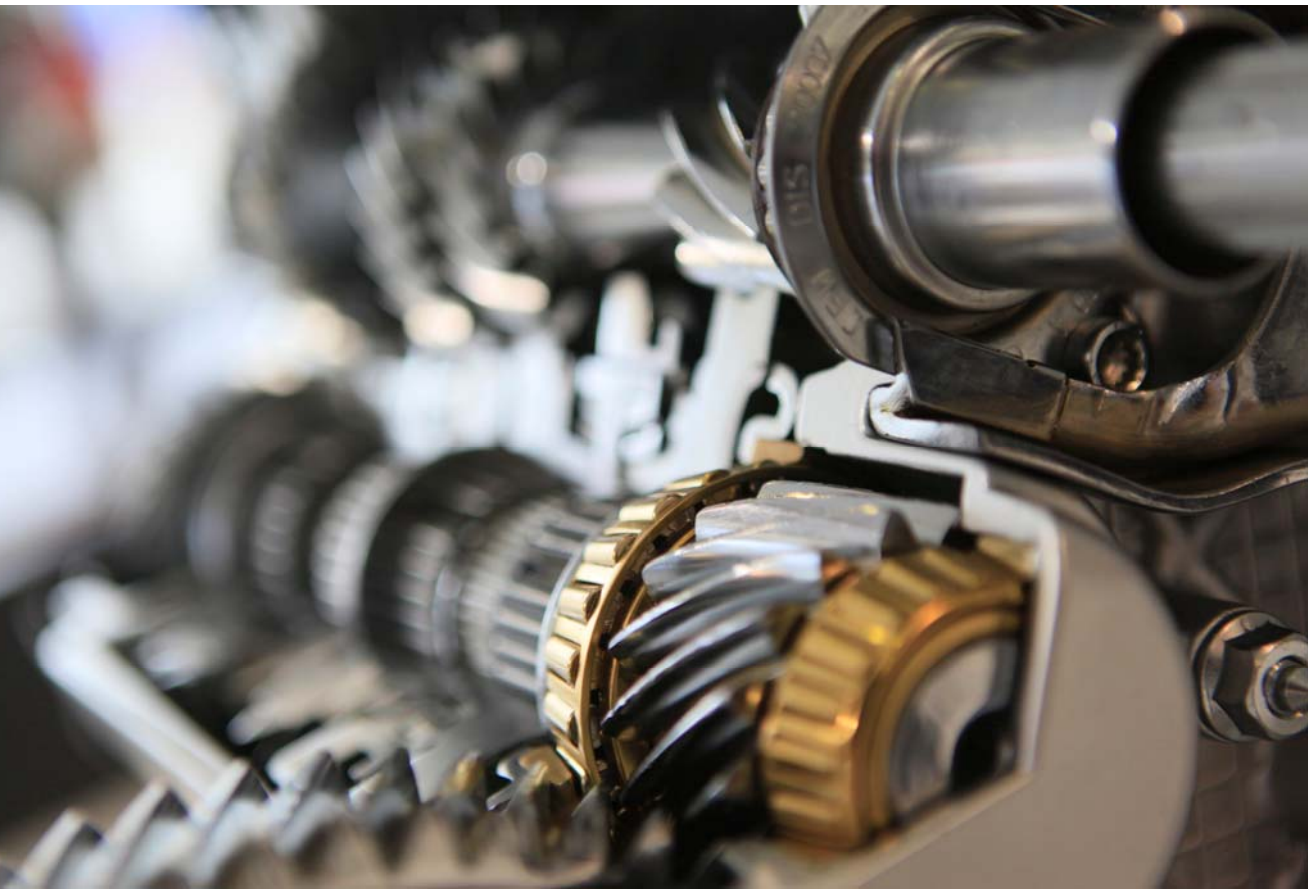
indy4
Industrie 4.0



Industrie 4.0 im Rechtsrahmen

Ulrich Herfurth (Hrsg)

CASTON LAW & BUSINESS INFORMATION

indy4

Ein Arbeitspapier
der interdisziplinären Expertengruppe

indy4

über

Herfurth & Partner

Rechtsanwaltsgesellschaft mbH
D-30159 Hannover
Luisenstrasse 5

fon +49-511-307 56-0
fax +49-511-307 56-10
mail info@herfurth. de
web www.herfurth.de

Verlag

Caston GmbH
Law & Business Information
D-30159 Hannover
Luisenstrasse 5
www.caston.info

Titelangaben

Industrie 4.0 im Rechtsrahmen
Herfurth, Ulrich (Hrsg)
September 2016
Caston Edition, Hannover
ISBN 978-3-936647-03-7

indy4

Industrie 4.0 im Rechtsrahmen

Ulrich Herfurth (Hrsg)
1. Auflage
Hannover, Stand 22.Spetember 2016

Inhalt

Seite

Vorwort 10
Ulrich Herfurth

Einführung

[1] **Rechtliche Aspekte zu Industrie 4.0**
Ulrich Herfurth

0. Industrie 4.0 – der Rahmen 13
1. Forschung und Entwicklung 19
2. Produktion 19
3. Logistik 25
4. Produkte 26
5. Informationstechnologie und Daten 27
6. Markt und Kunden 34
7. Wettbewerb 34
8. Personal und Arbeit 35
9. Steuern und Finanzen 36
10. Geschäftsführung und Aufsicht 37
11. Ausblick 38

Betrieb & Systeme

[2] **Verträge und Haftung in der Lieferkette**
Marc-André Delp

1. Vertragsabschluss 44
2. Vertragsgegenstand 47
3. Lieferung 47
4. Force Majeure 48
5. Gerichtsstand 49
6. International 50
7. Haftung 52
8. Produkthaftung 56

[3] **Provider, Plattformen und Netze**
Martin Heitmüller

1. Provider 58
2. Plattformen 59
3. Telekommunikation 63

Technologie und Daten

[4] **Industrie 4.0 und Datenschutz**
Dennis Jlussi

1. Einleitung 68
2. Datenschutz und Innovation 68
3. Arbeitnehmer-Datenschutz 69
4. Kunden-Datenschutz 71
5. Datensicherheit 71

[5] **Industrie 4.0 und Dateneigentum**
Dennis Jlussi

1. Einleitung 73
2. Daten 73
3. Eigentum an Daten 73
4. Geistiges Eigentum 75
5. Wettbewerbsrecht 76
6. Datenschutzrecht 77
7. Geheimschutzrechte 77
8. Vertragliche Regelungen 78
9. Fazit 78

[6] **Industrie 4.0 und Immaterialgüterrecht**
Joachim Gerstein, Sebastian Aisch

1. Das Territorialitätsprinzip 80
2. Das Patentrecht „in a nutshell“ 81
3. Software als patentgeschützter Gegenstand 83
4. Daten als Erzeugnisse 84
5. Patente für technische Standards 85

[7] **Strafrechtschutz für IT und Daten**
Antonia Herfurth

1. Einführung 89
2. Übersicht über die Rechtssituation 90
3. Die Straftatbestände 90
3. Fazit 98

Finanzen

[8] **Daten in Bilanz und Besteuerung**
Günter Stuff

1. Daten als Vermögenswert 103
2. Cloud-Computing im Steuerrecht 104
3. Umsatzsteuerliche Behandlung von Dienstleistungen 105
4. Verlagerung der Buchführung ins Ausland 106
5. Verrechnungspreise für internationalen Datenverkehr 106

Wettbewerb

[9] **Industrie 4.0 im Wettbewerbsrecht**
Prof. Dr. Christiane Trüe

1. Einführung und Grundlagen 111
2. Konkrete wettbewerbsrechtliche Fragen zu Industrie 4.0 113
3. Fazit 119

Personal

[10] **Personal und Arbeit unter Industrie 4.0**
Sabine Reimann

1. Individualarbeitsrecht 124
2. Kollektivarbeitsrecht 131

International

[11] **Industrie 4.0 in den USA**
Uzunma Bergmann

1. Allgemeine Wirtschaftslage 141
2. Industrie 4.0 in den USA 143
3. US-Umfeld für Investitionen 146
4. Informationen und Daten 150
5. Technikrecht 162

[12] **Industrie 4.0 in Brasilien**
Sabine Reimann

1. Allgemeine wirtschaftliche Lage in Brasilien 165
2. Industriestruktur 166
3. Umfeld für Investitionen 167
4. Informationen und Daten 170
5. Produktsicherheit, Produkthaftung 173
6. Normenwesen, Zertifizierung 173

[13] **Industrie 4.0 in China**
Xiaomei Zhang

1. Allgemeine wirtschaftliche Lage in China 176
2. Industrie 4.0 176
3. Umfeld für Investitionen 182
4. Informationen und Daten 185
5. Technikrecht 187

[3] **Industrie 4.0 in Russland**
Elena Duwensee

1. Allgemeine wirtschaftliche Lage in Russland 191
2. Industrie 4.0 191
3. Umfeld für Investitionen 195
4. Informationen und Daten 197
5. Technikrecht 202

[14] **Industrie 4.0 in Indien**
Dr. Jona Aravind Dormann

1. Allgemeine wirtschaftliche Lage in Indien 205
2. Industrie 4.0 in Indien 205
3. Umfeld für Investitionen 206
4. Informationen und Daten 209
5. Technikrecht 212

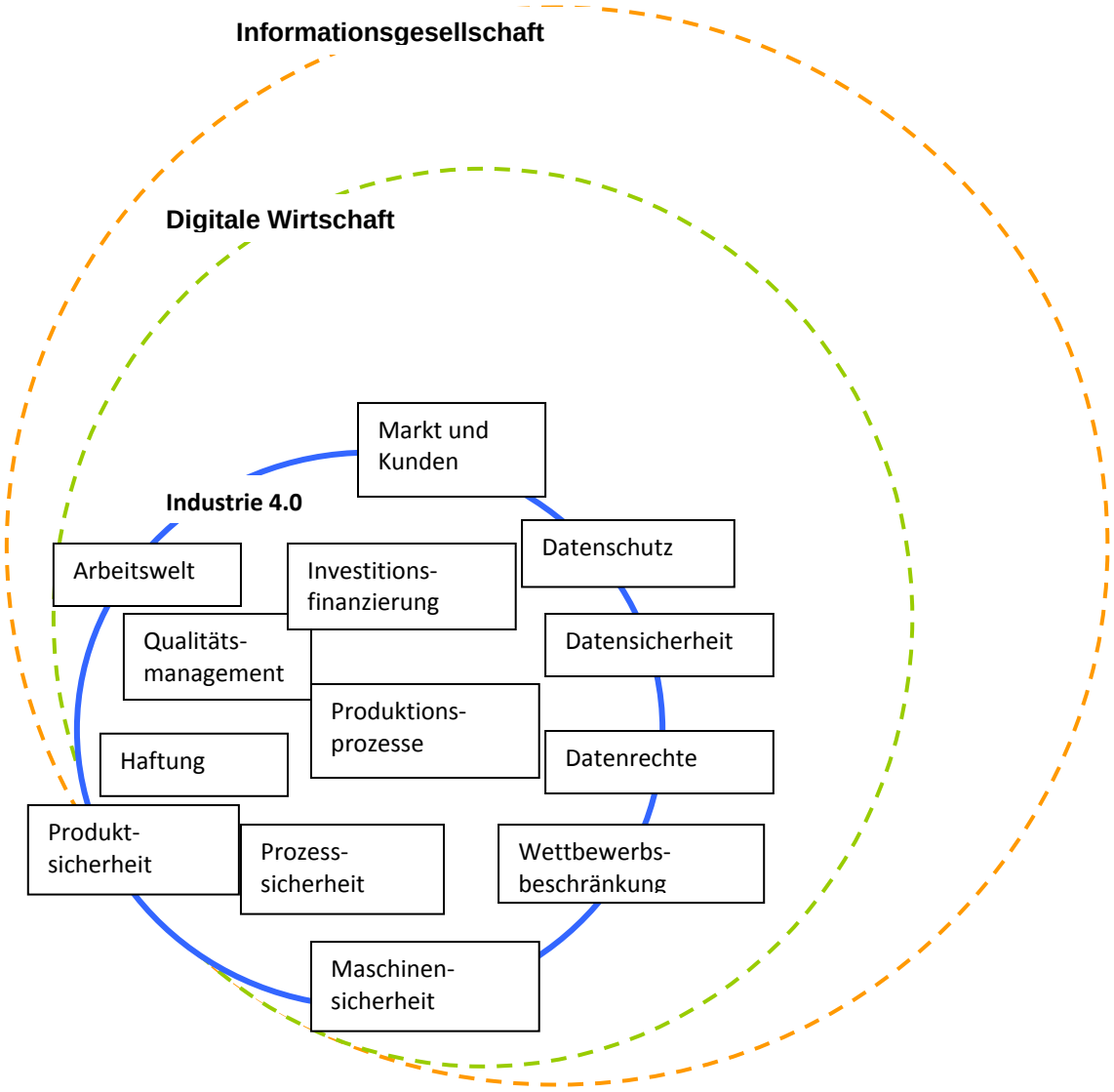
Indy4

Die Indy4 Gruppe 216

Indy4 Beteiligte 217

Autoren 218

Literatur 222


Informationsgesellschaft
Digitale Wirtschaft
Industrie 4.0
Markt und Kunden
Datenschutz
Datensicherheit
Datenrechte
Wettbewerbs-beschränkung
Maschinen-sicherheit
Produkt-sicherheit
Prozess-sicherheit
Haftung
Qualitäts-management
Arbeitswelt
Investitions-finanzierung
Produktions-prozesse

Vorwort

Die umfassende und vielschichtige technologische Entwicklung durch die Digitalisierung berührt die Unternehmen in allen Bereichen, im Betrieb und im Markt, operativ und strategisch. Auf allen Ebenen ergeben sich spiegelbildlich zur Praxis neue rechtliche Fragestellungen und Anforderungen, teilweise eben auch mit noch zahlreichen Unbekannten. Die als „Industrie 4.0“ bezeichnete Entwicklung umfasst all diese Ebenen und Fragestellungen.

Als Juristen sehen wir unsere Aufgabe darin, den Unternehmen als Rechtsanwendern neue Wege aufzuzeigen und die rechtlichen Rahmenbedingungen deutlich zu machen. Dazu gehört auch, dort Lösungen zu entwickeln, wo Gesetzgeber und Rechtsprechung noch keine Grundlagen geschaffen haben.

In einem ersten Schritt haben wir daher Dialoge mit Experten anderer Disziplinen aus Wissenschaft und Beratung geführt, um die Dimension und konkrete Anwendungsfälle zu untersuchen. Daraus hat sich sehr bald eine interdisziplinäre Expertengruppe entwickelt, die als „Indy4“ die Entwicklung unter den verschiedenen fachlichen Blickwinkeln betrachtet und im Dialog über die Fachgrenzen hinweg neue weiterreichende Erkenntnisse schafft. Als erstes Ergebnis konnte Indy4 im Juli 2015 das Eckpunktepapier Industrie 4.0 vorlegen, das bereits im Januar 2016 in zweiter und erweiterter Auflage erschienen ist (Report „Industrie 4.0 in Eckpunkten“, 2016). Bereits die Eckpunkte enthalten eine umfassende Übersicht über die rechtliche Seite von Industrie 4.0., eine umfassende Darstellung hätte den Rahmen hingegen gesprengt.

Der nun vorliegende Report „Industrie 4.0 im Rechtsrahmen“ bildet alle wesentlichen rechtlichen Felder von Industrie 4.0 ab. Er soll als Verständnisgrundlage für Unternehmen in der Praxis dienen, mag aber auch dem interessierten Juristen einen Überblick über die relevanten Fragen und Lösungsansätze geben.

Hannover, im September 2016

Ulrich Herfurth

Vorwort

Zur ersten Auflage des Eckpunktepapers zur interdisziplinären Betrachtung, Juli 2015, jetzt erschienen in der zweiten erweiterten Aufl. , Januar 2016

Industrie 4.0. ist ein Schlagwort, eine Entwicklung, ein Zustand – und eine Tatsache. Seit die Wirtschaftsverbände VDMA, ZVEI und Bitkom den Begriff geprägt haben und die Hannover Messe Industrie ihn als Leitthema gesetzt hat, zieht er die Aufmerksamkeit auf sich – von Politik, Wirtschaft und Gesellschaft. Sicherlich sind manche Begriffe und Vorstellungen zur Entwicklung noch unscharf. Das ändert aber nichts daran, dass sich mit dem Begriff Industrie 4.0 eine der größten industriellen Herausforderungen für Unternehmen und Gesellschaft verbindet. Es geht also nicht darum, ob sich ein Unternehmen an Industrie 4.0 als Projekt beteiligt, sondern wie es sich den Herausforderungen dieser globalen Entwicklung der „Integrated Industries“ stellt.

Aus der Beratung von international tätigen Produktionsunternehmen sind uns die Fragen zum technischen Zusammenspiel in der Wertschöpfungskette vertraut. Industrie 4.0 greift nun in viele Segmente und Disziplinen im Unternehmen ein. Wir haben daher einen Kreis von Experten eingeladen, die Entwicklungen vorausschauend in Eckpunkten zu betrachten. Zu den Beteiligten gehören Forschungsinstitute, Hochschulen und Berater, die die Thematik unter der Bezeichnung Indy4 untersuchen und die Felder aus den unterschiedlichen Blickrichtungen beleuchten.

Das erste Ergebnis legen wir nun Interessierten als Eckpunktepapier vor. Es kann und soll nicht als finales Ergebnis, sondern als ein Eintritt in weitere Betrachtungen, Untersuchungen, Analysen verstanden werden, aus dem sich konkrete Handlungsempfehlungen und Maßnahmen in den Unternehmen ableiten.

Hannover, im Juli 2015

Ulrich Herfurth

Einführung

Rechtliche Aspekte zu Industrie 4.0

Ulrich Herfurth, Rechtsanwalt in Hannover und Brüssel,
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

Die Entwicklung von Industrie 4.0 wird inzwischen in weiten Kreisen als grundlegende technologische und wirtschaftliche Veränderung über nahezu alle Branchen verstanden.

0. Industrie 4.0 - der Rahmen

01. Industrie 4.0 als konzertierte Aktion

Beachtlich ist dabei die konzertierte Aktion aller wichtigen Kräfte, die sich mit den großen Verbänden und inzwischen mit dem Bundeswirtschaftsministerium zur „Plattform Industrie 4.0 zusammengefunden haben".

Dazu schreibt das Ministerium[1]

> „Je mehr sich die Wirtschaft digitalisiert und vernetzt, desto mehr Schnittstellen ergeben sich - in Entwicklung, Produktion und Vertrieb, national und global. Das erfordert Kooperation und Beteiligung zahlreicher Akteure. Eine koordinierte Gestaltung des digitalen Strukturwandels ist Leitgedanke der Plattform Industrie 4.0.
>
> Die bisherige Verbände-Plattform wurde unter der Leitung von Bundeswirtschaftsminister Gabriel (BMWi) und Bundesforschungsministerin Wanka (BMBF) erweitert - in der breiten Allianz beteiligen sich neben der Politik Vertreter von Verbänden (BDEW, BDI, BITKOM, DIHK, VDA, VDMA, ZVEI) und Gewerkschaften (IG Metall) sowie der Wissenschaft (Fraunhofer Gesellschaft). Mit den inhaltlichen Schwerpunkten der Plattform beschäftigen sich fünf Arbeitsgruppen (Referenzarchitektur, Standardisierung und Normung / Forschung und Innovation / Sicherheit vernetzter Systeme / rechtliche Rahmenbedingungen / Arbeit, Aus- und Weiterbildung).
>
> Seit ihrer Gründung vor einem Jahr hat sich die Plattform Industrie 4.0 im Bereich Digitalisierung und Industrie zu einem der größten Netzwerke weltweit entwickelt. Die Plattform hat es in kürzester Zeit geschafft, Anwendungsbeispiele und Leitfäden für Unternehmen, insbesondere für den Mittelstand zu

[1] http://www.bmwi.de/DE/Themen/Industrie/industrie-4-0.html, August 2016

entwickeln. Zusammen mit dem Kompetenzzentrum 4.0 steht mittelständischen Unternehmen damit ein hervorragendes Informations- und Beratungsangebot zur Verfügung.

Unternehmen und Verbände der Plattform haben die Initiativen Labs Network Industrie 4.0 und Standardization Council Industrie 4.0 gegründet, um die Standardisierung und den Praxistransfer bei Industrie 4.0 zu beschleunigen. Das Labs Network Industrie 4.0 etwa soll Unternehmen den Einstieg in die Industrie 4.0 erleichtern, indem es KMU ermöglicht, neue Technologien zu testen. Weiterhin wurde, ebenfalls aus der Plattform heraus, das Referenzmodell RAMI 4.0 (Reference Architecture Model Industrie 4.0) entwickelt. Es fasst die wesentlichen technologischen Elemente der Industrie 4.0 in einem Modell zusammen und bietet Unternehmen aus verschiedenen Branchen eine einheitliche Orientierung."

Die Arbeit auf der Plattform Industrie 4.0 wird dabei in diversen Formen und Aktivitäten vorangetrieben:

Fachliche neuartige Fragen behandeln Arbeitsgruppen, so auch die „Arbeitsgruppe Rechtliche Rahmenbedingungen".

Die Umsetzung der Entwicklungen und den Zugang von kleinen und mittleren Unternehmen zur neuen Technologie fördern regional die Industrie- und Handelskammern mit ihren Netzwerkprogrammen und die vom Bundeswirtschaftsministerium eingerichteten elf Kompetenzzentren 4.0 in Deutschland mit Schulungs- und Entwicklungsprogrammen für KMU.

0.2. Technologie und Recht

Technologische Entwicklungen entstehen aus realen Bedürfnissen des Marktes und treiben die Entwicklungen in Wirtschaft und Gesellschaft an. Das Recht bildet in der Folge diese neuen Phänomene ab, um Antworten auf dabei entstehende Fragen zu finden und Lösungen für dabei auftretende Konflikte der Beteiligten zu entwickeln.

„Industrie 4.0" ist zwar ein Schlagwort, markiert aber damit eine technologische und gesellschaftliche Entwicklung von beachtlicher Bedeutung. Zwar erscheinen viele Bausteine im Zusammenwirken der vernetzten Maschinen, Betriebe und Unternehmen als bereits bekannt, tatsächlich wird die Dimension der Datenvernetzung in der Rechtspraxis letztlich dazu führen, dass heutige rechtliche Instrumente faktisch nicht mehr so einsetzbar sind, wie wir sie kennen.

Das Recht ist lebendig und passt sich neuen Gegebenheiten und Anforderungen an, durch privatautonome Vertragsgestaltung, durch Rechtsprechung und durch Gesetzesänderungen – und zwar in der Regel in dieser zeitlichen Reihenfolge. Für die Entwick-

lung zu Industrie 4.0 ist daher geboten, dass sich die Rechtssetzer und die Rechtsanwender frühzeitig und vorausschauend mit möglichen neuen Entwicklungen auseinandersetzen, um dazu Lösungen vorzubereiten. Systemimmanent ist dabei, dass dies eine Auseinandersetzung auf der Grundlage von zahlreichen Unbekannten bedeutet und die rechtliche Betrachtung mit Szenarien und Annahmen arbeiten muss.

Erst im Jahr 2015 hatte eine spürbare rechtliche Auseinandersetzung mit der Thematik begonnen, die nun weiterzuführen und zu vertiefen ist.[2] Inzwischen haben Wissenschaft und Rechtspraxis weitere Erkenntnisse und Ergebnisse herausgearbeitet und präsentiert. Zu nennen sind beispielhaft die „Göttinger Kartellrechtsgespräche“ und das „Göttinger Forum IT-Recht“ im Februar 2016 und die Bitkom Tagung „Rechtliche Aspekte zu Industrie 4.0“ im April 2016 mit der Arbeitsergebnissen aus der AG Recht. Plattform Industrie 4.0[3][4], Bitkom[5] und BDI[6] haben darüber hinaus inzwischen Publikationen vorgelegt, die sich mit den aktuellen rechtlichen Fragen auseinandersetzen

0.3. Technologische Entwicklungen im rechtlichen Kontext

Die technologische Entwicklung bildet sich rechtlich auf verschiedenen Ebenen ab: als staatliche Vorschrift, als kollektive technische Norm, als faktische Standards, als Stand der Wissenschaft und Technik und individuelle Vereinbarung. Bereits in dieser Zusammenstellung zeigt sich die Vielschichtigkeit und Dynamik der rechtlichen Zusammenhänge: aus dem Stand von Wissenschaft und Technik können sich technische Standards entwickeln, dazu können Normen geschaffen und Vorschriften gesetzt werden. Ob und wann die jeweiligen Elemente rechtlich zum Einsatz kommen, ist oft Frage des Einzelfalls – so reicht in der Regel die Berufung auf eine noch bestehende Norm nicht mehr aus, wenn die Technik inzwischen einen weiteren Entwicklungsstand erreicht hat.

[2] Bundesministerium für Wirtschaft und Technologie, Recht und funktionale Sicherheit in der Autonomik, Leitfaden für Hersteller und Anwender, Januar 2013;
Hans Markus Wulf, Clemens Burgenmeister, Industrie 4.0 in der Logistik – Rechtliche Hürden beim Einsatz neuer Vernetzungstechnologien, CR 2015, S. 404 ff;
Peter Bräutigam, Thomas Klindt, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, S. 1137 ff

[3] Daten im Kontext von Industrie 4.0, Plattform Industrie 4.0, Arbeitsgemeinschaft Rechtliche Rahmenbedingungen, März 2016

[4] Digitalisierte Industrie – Analoges Recht? Ein Überblick der Handlungsfelder, Plattform Industrie 4.0, AG Rechtliche Rahmenbedingungen, März 2016

[5] Rechtliche Aspekte von Industrie 4.0, Leitfaden, Bitkom, April 2016

[6] Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung, BDI, Nov 2015

Zu neuer Technologie einige Schlaglichter:

- Rechtswidrige Technologie lässt sich nicht vermarkten
- Der Rechtsrahmen wird zunehmend europäisch und international
- Neue Technologien sind oft nicht genau in vorhandenem Recht abgebildet
- Aber das Recht ist anpassungsfähig über Gesetzgebung und Rechtsprechung
- In Südkoreas Ethikcharta: „Menschen und Roboter müssen die Würde des Lebens, die Informations- und Technikethik respektieren".
- In Florida, Nevada und Kalifornien gibt es bereits Regelungen für den Einsatz autonomer Fahrzeuge

04. Anwendungen von Industrie 4.0

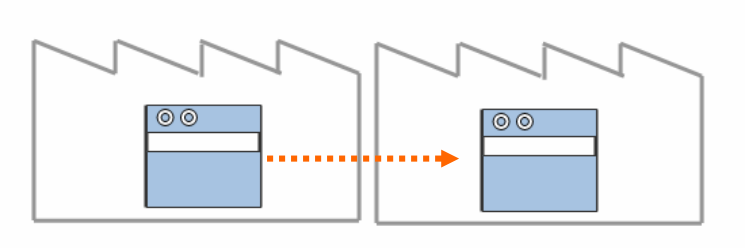
Als wichtige Werkzeuge von Industrie 4.0 nennt Bitkom

- Big Data Analysen,
- Cyber-Physical Systems
- 3D-Druck
- Cloud Computing

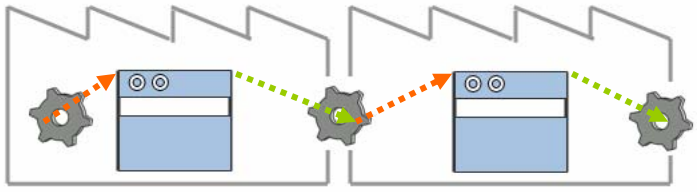
Die rechtliche Betrachtung der Mechanismen und Abläufe unter Industrie 4.0 zeigt dabei einen breiten Querschnitt von Aspekten. Dieser ist zunächst geprägt durch ein automatisiertes und eigenständig reaktives Zusammenwirken von Ressourcen, in Konstellationen, die zum Beispiel folgendermaßen kategorisiert werden können:

M2M	machine to machine
P2M	part to machine
M2X	machine to externals
M2S	machine to server
S2PRI	server to printer
S2L	server to logistics
P2L	part to logistics
H2M	human to machine

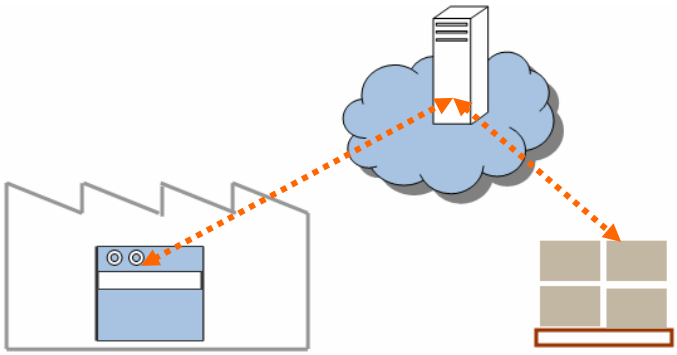
Aus all diesen Konstellationen leiten sich unterschiedliche rechtliche Fragen ab, die anhand der entsprechenden Prozesse dargestellt werden können. Im Folgenden sind einige der bereits in Diskussion befindlichen sowie weitere Fragen dargestellt.



Beispiel M2M



Beispiel P2M



Beispiel M2S | S2L | L2S

0.2. Rechtliche Themenfelder zu Technologie

Die klassische juristische Sichtweise orientiert sich nach Rechtsgebieten, anhand derer die im Unternehmen auftretenden Problemstellungen erfasst werden können. Dazu wird sich eine Betrachtung von Industrie 4.0 zunächst an die wichtigsten rechtlichen Felder anlehnen, die auch bereits heute im Verhalten von Unternehmen im Betrieb, im Markt und gegenüber Geschäftspartnern eine Rolle spielen:

- Gewährleistung
- Garantiehaftung
- Deliktische Verschuldenshaftung
- Gefährdungshaftung, Produktsicherheit, Produkthaftung
- Strafrechtliche Haftung
- Arbeitsschutz, Betriebssicherheit, Gesundheitsschutz
- Umweltschutz
- Wettbewerbsrecht
- Gewerblicher Rechtsschutz
- Datenschutz, Informationelle Selbstbestimmung
- Datensicherheit, Geistiges Eigentum
- Vermögensschutz, Eigentumsschutz

Allerdings stammt diese Strukturierung eher aus einer reaktiven Sichtweise, nämlich der nachträglichen Prüfung von Sachverhalten auf ihre rechtlichen Folgen hin.

0.3. Rechtliche Themenfelder nach Unternehmensbereichen

Für die vorausschauende rechtliche Unternehmensberatung ist hingegen eine an Unternehmensprozessen orientierte Betrachtung erforderlich. Diese Prozesse müssen in der juristischen Bewertung abgebildet werden. Da zu Industrie 4.0 die Prozesse, Zusammenhänge und Wirkungen naturgemäß noch nicht vollständig und abschließend erkennbar sind, hilft die Entwicklung von Szenarien, um mögliche Situationen technologisch, ökonomisch und juristisch zu profilieren und dazu Beurteilungen und Maßnahmen zu entwickeln. Die Prozesse lassen sich zunächst den wichtigen Unternehmensbereichen zuordnen:

- Forschung und Entwicklung
- Produktion
- Logistik
- Produkte
- Informationstechnologie und Daten
- Markt und Kunden
- Wettbewerb

- Personal und Arbeit
- Steuern und Finanzen
- Geschäftsführung und Aufsicht

1. Forschung und Entwicklung

Die Entwicklung neuer Prozesse und Produkte ist eine ständige Herausforderung für Unternehmen. Dabei nimmt ein systematisches Wissensmanagement eine wichtige Rolle ein. Wissen wird von Menschen generiert – im eigenen Betrieb oder bei Forschungs- und Entwicklungskooperationen bei Vertragspartnern. In beiden Konstellationen nehmen die Herausforderungen im Management des Wissens und in der Zuordnung der Ergebnisse deutlich zu. Die mächtigen Aufgaben im Industrie 4.0 – Wissen liegen in der rasch steigenden Komplexität mit vernetzten Partnern und der weitreichenden Spanne fachlicher Kenntnisse über Produktion, Maschinenbau und Informationstechnologie. Die aktuellen Kooperationen von Maschinenbau und Fahrzeugbau mit globalen Daten- und Internetkonzernen machen dies deutlich. Erste Fragen:

- Wer sollte an einer interdisziplinären Zusammenarbeit beteiligt sein?
- Wie lässt sich diese organisieren / arrangieren?
- Wie kann Überwachung nach innen und von außen erfolgen?
- Welche Zertifizierungssysteme sind verfügbar und geeignet?
- Wem stehen die Ergebnisse zu?
- Wer darf die Ergebnisse nutzen?
- Wie werden Mitarbeiter angemessen und rechtssicher an ihren Entwicklungen und Erfindungen beteiligt?

2. Produktion

Viele Betrachter sehen zurzeit die wesentlichen Änderungen hin zu einer Industrie 4.0-Struktur in der Produktion. Tatsächlich sind es die betrieblichen Abläufe und Prozesse, die durch digitale Vernetzung und automatisierte Vorgänge und Entscheidungen verändert werden; dabei stützen sich die Beteiligten auf ihre Erfahrungen aus CAM und CIM und denken diese in einer weiter intensivierten Verdichtung der Abläufe fort. Ob dies allein ausreicht, muss sich zeigen - die Entwicklung kann durchaus mit der Potenzierung von Datenmengen und Interaktionen sprunghaft eine neue Dimension erreichen, bei der die bisherigen Instrumentarien zur Steuerung nicht mehr ausreichen.

2.1. Unternehmensinterne Produktion

2.1.1. Internes Qualitätsmanagement

Die detaillierte Strukturierung der Produktionsabläufe folgt heute nicht nur technischen oder organisatorischen Normen, sondern Industriestandards und Unternehmens-Policies für Effizienz und Qualität. In Maschinenbau, Automotive und Aviation sind Qualitätsmanagementsysteme feste Grundlage der Produktion. Letztlich richten sich die Anweisungen und Handhabungen darin heute an die Menschen, die in der entsprechenden betrieblichen Aufgabe Verantwortung tragen. Sobald Maschinen und Systeme aber selbst verantwortliche Entscheidungen treffen, muss das Unternehmen neue Strukturen schaffen, die das verantwortliche Zusammenspiel von Mensch und Maschine neu definieren.

- Definition des QM durch das Management
- Automatische Fortschreibung aus Prozessdaten?
- Inhalte des QM-Manuals anpassen?
- Aufbau des QM-Manuals verändern?
- Art und Inhalt der Schulungen verändern?
- Überwachungs- und Kontrollinstrument im QM-Manual ändern?
- Definition von Schnittstellen der Maschinen im Betrieb zur Fehleridentifikation (wg Haftung des Maschinenherstellers)
- Datenmanagement / DM-Vereinbarungen / IT-Compliance (siehe unten "Daten")
- Outsourcing / Cloudmanagement / Vereinbarungen (siehe unten "Daten")

2.1.2. Internationale Arbeitsteilung im Konzern

In internationalen Konzernen, aber auch mittelständischen Unternehmen mit Betrieben im Ausland stellen sich spezifische Fragen zum Grenzübertritt von Leistungen und Produkten im automatisierten Prozess mit neuer Schärfe. Wenn also der Konzern Daten über Ländergrenzen austauscht, ins Ausland sendet oder Personen aus dem Ausland den Zugriff auf Daten im Inland (Europa) erlaubt, stellen sich erneut Fragen:

- Welche nationalen / supranationalen / internationalen Datenschutzvorschriften sind zu beachten (z.B. EU / Drittländer)?
- Haben die Daten einen Wert? Gilt die Überlassung als Lizenz? Sind dazu steuerliche Bestimmungen zu Verrechnungspreisen zu beachten?
- Werden Daten im Konzern ausgelagert? Zentralisiert?
- Entsteht dadurch eine steuerliche Betriebsstätte im Ausland?
- Wie wären dann die Erträge der Betriebsstätte zu ermitteln?

- Sind für die Überlassung von Daten im Konzern in das Ausland für Deutschland geltende Exportkontrollvorschriften zu beachten (Außenwirtschaftsgesetz, UN-Embargo, US-Embargo)?
- Sind für die Überlassung von Daten im Konzern in das Ausland dortige Importkontrollvorschriften oder Zollvorschriften zu beachten?
- Sind für die Überlassung von Daten im Konzern aus dem Ausland deutsche Importkontrollvorschriften oder Zollvorschriften zu beachten?

2.1.3. Arbeitsschutz, Betriebssicherheit, Gesundheitsschutz

Die automatisch gesteuerte und selbst entscheidende Maschine wird ein neuer „Arbeitspartner“ der Mitarbeiter. Kommt es sprichwörtlich zur „Arbeit Hand in Hand“, lassen sich die bisherigen Sicherheitskonzepte nicht mehr aufrechterhalten, etwa das Kapseln der Roboter in Käfigen. Berührungsfähige Systeme müssen neue Sicherheits- und Kontrollmechanismen umfassen, die wiederum den Mitarbeiter nicht seiner humanen Arbeitsweise berauben dürfen. Die Systeme müssen so angelegt sein, dass klar ist, wem das sicherere Verhalten zugetraut wird, dem Mitarbeiter oder dem intelligenten System.

- Darf sich das Konzept 4.0 hinsichtlich des Arbeitsschutzes (Lärm, Geruch, Verletzungsgefahr) zu Lasten des einzelnen Arbeiters auswirken?
- Muss / soll / kann mit Rücksicht auf die Gefahrenquelle differenziert werden?
- Sollen Menschen oder Maschinen Aufsicht / Kontrolle über Maschinen ausüben?
- Müssen/dürfen maschinelle Entscheidungen automatisch dokumentiert und aufbewahrt werden?
- Müssen / dürfen menschliche Entscheidungen automatisch dokumentiert und aufbewahrt werden?
- Ist "Outsourcing" möglich, wenn die Schnittstellen / Grenzen zwischen den Unternehmen immer weicher werden?

2.1.4. Umweltschutz

Es versteht sich, dass auch reaktive Systeme so angelegt sein müssen, dass Umweltvorschriften eingehalten und Umweltgefahren vermieden werden. Darüber hinaus bietet Industrie 4.0 die Chance, dass intelligente Systeme umweltfreundlicher agieren, weil sie in der Lage und darauf eingestellt sind, ihr Verhalten zu optimieren. Konzeptionen zum *smart home* und Energie-Managementsysteme in Betrieben weisen bereits heute die Richtung:

- Darf sich erhöhter Energiebedarf zu Lasten der Natur auswirken?
- Zulässigkeit nur unter Berücksichtigung / Einbeziehung erneuerbarer Energie (Kosteneffizienz)?
- Zulässigkeit nur unter Berücksichtigung / Einbeziehung der "fairen" Rohstoffgewinnung (Konfliktrohstoffe)?
- Wie lassen sich Prozesse energietechnisch optimieren?
- Welche öffentlichen Mittel stehen für Systemverbesserungen, auch durch Software, zur Verfügung?
- Wie gut müssen Maschinen recyclebar sein?

2.2. Lieferkette

Die bisherige Betrachtung konzentriert sich auf die Prozesse innerhalb eines Betriebes oder zwischen mehreren Betrieben in demselben Unternehmen. Eine neue Herausforderung entsteht, wenn die automatisierten Prozesse unternehmensübergreifend ablaufen. Besondere Bedeutung kommt dabei den zahlreichen Entscheidungsprozessen in den betrieblichen und dann auch geschäftlichen Abläufen zu, die durch intelligente Software auf Grundlage von Algorithmen getroffen werden und nicht mehr durch Willensbildung und Willenserklärungen von Menschen.

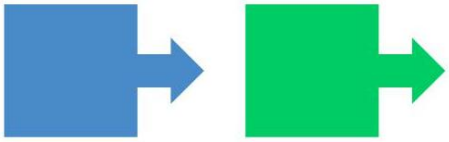
2.2.1. Allgemeines

Als Grundlage der geschäftlichen Zusammenarbeit bietet sich zunächst das aus dem Management von industriellen Lieferketten bekannte vertragliche Instrumentarium an, das entsprechend weiterentwickelt werden muss:

- Welche Vereinbarungen müssen in Rahmenlieferverträge neu aufgenommen werden (siehe vor allem unten "Daten")
  - Rahmenvertrag
  - NDA / Vertraulichkeitsvereinbarung
  - QSM Vereinbarung
  - Liefer-AGB
  - Werkzeugüberlassungsvereinbarung
  - Neu: Datennutzungsvereinbarung

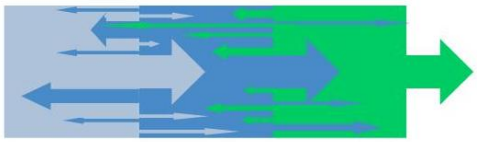
- Welches materielle Recht ist in einer internationalen Prozesskette zugrunde zu legen?
- Welche Gerichte sind örtlich zuständig?
- Welche Standorte sind für das anwendbare Recht und den Gerichtsstand maßgeblich (Lieferant, Leistungsempfänger, Prozessrechner, Datenspeicher, juristischer Sitz)
- Welche Auswirkungen hat es, wenn Server im Ausland betrieben werden?

Die Bedeutung der neuen Anforderungen lässt sich erkennen, wenn man sich die Entwicklung der technischen und geschäftlichen Beziehungen der Beteiligten von der Lieferkette bis hin zur integrierten Produktion vor Augen hält:



Lieferbeziehung

Shop in Shop



Industrie 4.0

Industrie 4.0 +

Abb.1:
Schema: Herfurth

Das Bild zeigt schematisch, wie die Abläufe sich ineinander durch Datenströme verflechten und verweben, so dass Leistungsschnittstellen zunehmend schwieriger oder faktisch gar nicht mehr zu identifizieren sind. Allein der organisatorische und wirtschaftliche Aufwand zur Sachverhaltsermittlung und Beweisführung könnte in der Rechtspraxis die Verfolgung oder Verteidigung von Rechten der beteiligten Unternehmen unmöglich machen. Die Dimension von auszuwertenden Daten kann durchaus ungleiche Kräfteverhältnisse weiter vertiefen.

Für den maschinellen Vertragsabschluß wirft sich zum Beispiel die Frage auf, ob von Maschinen autonom erzeugte Mitteilungen an andere Maschinen einen rechtlichen Erklärungscharakter haben. Immerhin lösen sie damit Aufträge aus und definieren Art und Umfang der Leistung des Empfängers der Information. Dazu hat das Recht derzeit die Sicht entwickelt, dass derartige Informationen als rechtsgeschäftliche Willenserklärungen des Betreibers des autonomen Systems anzusehen sind und diesen verpflichten. Die Maschine wird dabei als Agent betrachtet. Diese Wertung könnte sich aber ändern, wenn Maschinen mit künstlicher Intelligenz für ihren Betreiber nicht mehr vorhersehbare Entscheidungen treffen

2.2.2. Internationale Arbeitsteilung mit Lieferanten

Im Grundsatz stellen sich bei Auslandbezug mit Geschäftspartnern unter Industrie 4.0 zunächst die gleichen Fragen wie innerhalb eines Konzerns. Hinzu kommen aber die Aspekte, die sich mit Blick auf mögliche rechtliche Auseinandersetzungen ergeben.

Wenn Daten mit Lieferanten oder Kunden über Ländergrenzen ausgetauscht werden / Sendung ins Ausland / Zugriff aus dem Ausland:

- Welche nationalen / supranationalen / internationalen Datenschutzvorschriften sind zu beachten (z.B. EU / Drittländer)?
- Haben die Daten einen Wert? Gilt die Überlassung als Lizenz? Sind dazu steuerliche Bestimmungen zu Verrechnungspreisen zu beachten?
- Werden Daten im Konzern ausgelagert? Zentralisiert?
- Entsteht dadurch eine steuerliche Betriebsstätte im Ausland?
- Wie wären dann die Erträge der Betriebsstätte zu ermitteln?
- Sind für die Überlassung von Daten an Kunden Antiterrorismusvorschriften zu beachten?
- Liegen Tatbestände für Prüfungen nach dem Geldwäschegesetz vor?
- Sind für die Überlassung von Daten in das Ausland für Deutschland geltende Exportkontrollvorschriften zu beachten (Außenwirtschaftsgesetz, UN-Embargo, US-Embargo)?
- Sind für die Überlassung von Daten in das Ausland dortige Importkontrollvorschriften oder Zollvorschriften zu beachten?
- Sind für die Überlassung von Daten aus dem Ausland deutsche Importkontrollvorschriften oder Zollvorschriften zu beachten?
- Welche Dokumentationspflichten sind zu beachten und wie können diese bei Big Data erfüllt werden?

2.2.3. Gewährleistung der Lieferanten

Eine besondere Bedeutung im Zusammenspiel von Partnern in der Lieferkette erhält aber die Qualität der Produkte unter dem Gesichtspunkt der Haftung für fehlerhafte Leistungen und Mängel. Die informationsgestützte und automatisierte maschinelle Abwicklung von Geschäftsprozessen ersetzt dabei die individuelle Willenserklärung von Menschen. Maschinen haben keinen eigenen Willen; sie sind keine Personen, die Erklärungen abgeben können, sondern sie sind Sachen im Rechtssinne. Die von ihnen gesendeten Befehle und Informationen sind also letztlich den Menschen und damit Unternehmen als Willenserklärung zuzurechnen, die das weitreichend programmierte System so zum Einsatz bringen. Das Recht ordnet solche Systeme daher auch nicht als Vertreter oder Erklärungsboten ein, sondern als so genannte Erklärungsagenten.

- Wer definiert das Produkt bzw. den Vertragsgegenstand?
- Wer trägt Verantwortung für fehlerhafte Übermittlung?
- Welche rechtliche Bedeutung hat die Überlassung von Daten an Produktionspartner (vertraglich vereinbarte Beschaffenheit?)
- Sind automatisierte Prozessbefehle Willenserklärungen?
- Besteht die Pflicht zu einer Warenprüfung? Wenn ja, zu welchem Zeitpunkt (auch Teil- oder nur Endprodukte)?
- Wie weit kann der Datenempfänger mit allgemeinen Geschäftsbedingungen die kaufmännische Untersuchungs- und Rügeobliegenheit ausschließen?
- Welchen Service müssen Hersteller für Instandhaltung und Aktualisierung anbieten?
- Welche Entwicklungsstufen sind als Maßstab maßgeblich?

- Ob und inwieweit sind Haftungsbeschränkungen möglich?
- Wer haftet hier genau?
- Sind Verantwortungssphären (räumlich / zeitlich) überhaupt denkbar?
- Wem sind Fehler in automatisierten Abläufen von Maschinen- und Datenvorgängen zuzurechnen?
- Wer übernimmt Haftung für Menschen und Maschinen, selbst wenn Menschen alles richtig getan haben?
- Müssen/ sollen / können Unterschiede in der Haftung davon abhängig gemacht werden, ob Menschen gehandelt haben?
- Wann (ab welchem Beitrag) kann noch von einer menschlichen Handlung ausgegangen werden?

3. Logistik

In der Logistik bestimmt die Digitalisierung bereits weitgehend die innerbetrieblichen und externen Abläufe. Wege und Standorte von Material, Teilen, Paketen, Paletten und Containern lassen sich in Echtzeit exakt bestimmen und nachvollziehen. Die Effizienzgewinne, wie etwa bei der Chaotischen Lagerung, sind beachtlich. Die Logistikbranche sieht eine Reihe von Faktoren als Treiber der Entwicklung, so etwa

- intelligente Transportmittel
- M2M-Kommunikation
- Sensorik und Echtzeit-Monitoring
- Predictive Maintenance
- automatisierte Vertragsschlüsse
- elektronische Frachtdokumente
- Cloudplattformen zur elektronischen Steuerung und als Marktplätze
- Einsatz mobiler Endgeräte / BYODs
- private Lieferdrohnen.

4. Produkte

4.1. Gewährleistung gegenüber Kunden

Im Grundsatz stellen sich die Fragen zu Lieferanten spiegelbildlich in der Beziehung zu Kunden.

4.2. Garantiehaftung gegenüber Nutzern

Und sicherlich stellen sich Fragen zur Haftung gegenüber Dritten, also Nutzern, die nicht Vertragspartner des Unternehmens sind, mit neuer Intensität, wenn womöglich Teile der Produktionsprozesse außerhalb der Kontrolle des Herstellers liegen:

- Ist eine Garantiehaftung überhaupt noch individuell möglich?
- Inwieweit wird innerhalb der Lieferkette „mitgehaftet“?

4.3. Deliktische Verschuldenshaftung gegenüber Dritten

Da sich eine deliktische Haftung auf menschliches Fehlverhalten aufgrund einer menschlichen Willensbildung stützt, stellt sich bei automatisierten Systemen, die Frage nach der zivilrechtlichen und strafrechtlichen Verantwortlichkeit.

- Wer hat im Einzelfall die Herrschaft über die Gefahrenquelle?
- Dürfen / Müssen Algorithmen Leben gegen Leben (rational) abwägen?

- Besteht ein Recht auf irrationale Entscheidungen?
- Welche ethischen Konflikte können entstehen, wenn ein Roboter nicht mehr zwischen Mensch und Maschine unterscheiden kann?

4.4. Gefährdungshaftung, Produktsicherheit, Produkthaftung

Die gleiche Frage betrifft die Gefährdungshaftung, die ohne Verschulden einer Person allein aus dem Versagen eines Produkts oder einer Anlage entsteht.

- Ob und inwieweit sind Haftungsbeschränkungen möglich?
- Wer haftet hier genau?
- Sind Verantwortungssphären (räumlich / zeitlich) überhaupt denkbar?
- Wem sind Fehler in automatisierten Abläufen von Maschinen- und Datenvorgängen zuzurechnen?
- Wer übernimmt Haftung für Menschen und Maschinen, selbst wenn Menschen alles richtig getan haben?
- Müssen / sollen / können Unterschiede in der Haftung davon abhängig gemacht werden, ob Menschen gehandelt haben?
- Wann (ab welchem Beitrag) kann noch von einer menschlichen Handlung ausgegangen werden?
- Bedarf es einer menschlichen Kontrolle (und Interventionsmöglichkeit) automatisierter Vorgänge?
- Ist ein Unternehmen, das fremdbestimmt produziert, Hersteller i.S.d. ProdHaftG?
- Wer ist bei 3D-Digitaldruck Hersteller i.S.d. ProdHaftG?
- Kann ein unvorhersehbar agierendes System versichert werden?
- Besteht für jeden Lieferanten in der Kette eine Versicherungspflicht? Sind Einschränkungen möglich (wenn z.B. einzelne Teilprodukte zum Endprodukt unterschiedliche Beiträge leisten)?

5. Informationstechnologie und Daten

Die Fragen zur Informationstechnologie sind naturgemäß das Herzstück von Industrie 4.0. Denn die IT-Systeme schaffen und erhalten die Funktionalität der vernetzten Produktion, und die Daten sind der digitale Rohstoff, mit dem die Systeme versorgt werden müssen.

5.1. Datensicherheit

Zunächst gilt es, die Daten gegen technische Störungen, Beschädigungen und Ausfälle zu sichern.

Dies ist vorrangig eine technisch-organisatorische Aufgabe, aber auch eine rechtliche Verantwortlichkeit des Managements. Es gehört zu den essentiellen Sorgfaltspflichten der Geschäftsleitung und der Aufsichtsgremien im Unternehmen, die betriebliche Sicherheit so einzurichten, dass Beschädigungen von Vermögensgegenständen, also auch Datenbeständen, verhindert werden.

Bei Unternehmen mit kritischer IT-Infrastruktur ist die Geschäftsleitung aber nicht nur gegenüber dem eigenen Unternehmen verpflichtet, sondern neuerdings auch gegenüber der Allgemeinheit: das neue IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme vom 24.07.2015) erlegt betroffenen Unternehmen im Störfall bestimmte Meldepflichten auf. Dadurch soll vermieden werden, dass Angriffe und Störungen auf weitere Systeme übergreifen und dass darauf gerichtete Angriffe abgewehrt werden können. Zu kritischen Infrastrukturen zählen solche in den Branchen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen - allerdings nur, wenn sie „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Der Gesetzgeber konkretisiert diese Merkmale derzeit noch genauer. Produktionsunternehmen unterliegen dem Katalog daher als solche nicht. Auch kleine Unternehmen (KMU) dürften kaum betroffen sein. Sie müssen aber jeweils damit rechnen, als Zulieferer und Dienstleister für Unternehmen mit kritischer Infrastruktur in vertragliche Pflichten und Haftung genommen zu werden.

Allerdings verlangt das Gesetz von den Unternehmen mit kritischer Infrastruktur auch, dass sie geeignete Maßnahmen treffen, um Störungen zu vermeiden. Die Störungen können sich dabei auf Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten und Prozesse beziehen, die für die Funktionsfähigkeit maßgeblich sind. Die erforderlichen Maßnahmen umfassen Infrastruktur, Personal, Störfallmanagement und Abschottungen von Prozessen und Bereichen.

Diese Anforderungen sind zwar öffentlich-rechtlicher Natur, und Verletzungen sind als Ordnungswidrigkeit teilweise mit Bußgeld bedroht, aber daraus lassen sich auch zivilrechtliche Schadenersatzansprüche ableiten. Dabei ist leicht vorstellbar, dass dieser Anforderungskatalog mit der Zeit und in abgestufter Form einen Leitbildcharakter entwickelt, der auch auf an sich nicht vom IT-Sicherheitsgesetz erfasste Unternehmen abstrahlt. Die Pflichten von Vorstand und Geschäftsführung würden dadurch im Rahmen der Business-Judgement Rule stärker konkretisiert.

5.1.2. *Datendienstleister*

Sobald ein Unternehmen zur Unterstützung oder Sicherung des IT-Betriebs externe Berater, Systemhäuser, Softwareanbieter, Rechenzentren und ganze Outsourcing-Systeme als Dienstleister einsetzt, sind deren Rechte und Pflichten sehr sorgfältig zu vereinbaren: Leistungsumfang, Leistungserfolg, Services, Service-Level, Haftung, faktische Haftungswerte, Versicherungen und anderes. Fragen zur Sicherung sind:

- Wo sollen / dürfen eigene Daten gespeichert werden?
- Wer kontrolliert den Datenaustausch?
- Wie können Daten - insbesondere in einer "Cloud" - gegen Zugriffe Dritter geschützt werden?

Besonders gefährlich können aber Eingriffe von Menschen oder von Menschen gesteuerter Systeme sein. Daher muss das Unternehmen Schutzmassnahmen gegen gleichartige Angriffe treffen, deren Angriffsrichtung und Angriffsmethode unterschiedlich sind und denen daher mit differenzierten Abwehrmaßnahmen begegnet werden muss. Dazu zählen vorrangig:

5.1.3. *Schutz gegen externe Datenangriffe durch Dritte*

Cyber Crime / staatliche Industriespionage durch ausländische Dienste oder private Spionage durch Wettbewerber. Hier sind vor allem technische und organisatorische Maßnahmen zum Schutz der Daten im Betrieb, in der Auslagerung und beim Transfer zu treffen gegen

- Datenmissbrauch
- Datendiebstahl
- Datensabotage (Blockade, Veränderung)
- Erpressung

5.1.4. *Schutz gegen externe Datenangriffe durch Vertragspartner*

Dabei gilt zunächst der gleiche Grundsatz wie gegenüber Dritten. Allerdings kommt hier gefahrerhöhend hinzu, dass Geschäftspartner systembedingt gerade Zugriff auf die IT-Systeme und Daten über Schnittstellen und nach Transfers haben müssen. Zu den technischen Sicherungen kommen damit rechtliche Instrumente hinzu, insbesondere vertragliche Verwendungsbestimmungen. Auch hier gelten die Risiken

- Datenmissbrauch
- Datendiebstahl

- Datensabotage (Blockade, Veränderung)
- Erpressung

Wie also können Daten gegen zweckwidrige Verwendung (auch des Vertragspartners) geschützt werden?

5.1.5. Schutz gegen interne Datenangriffe

Eigene Mitarbeiter stellen mit ca. 75% der Fälle von Wirtschaftskriminalität die größte Tätergruppe im Unternehmen dar. Dabei sind es typischerweise vertrauenswürdige und qualifizierte Personen in Schlüsselfunktionen im Unternehmen, die aus diversen Motiven ihre Stellung missbrauchen zu

- Datenmissbrauch
- Datendiebstahl
- Datensabotage (Blockade, Veränderung)
- Erpressung

Sicherlich werden Unternehmen mit Mitarbeitern vertragliche Regelungen zum Schutz des Unternehmens treffen, aber auch technologische Kontrollsysteme installieren müssen, die gerade dann eingreifen, wenn sich ein Mitarbeiter bewusst vertrags- und rechtswidrig verhält.

- Wer hat für eine fehlerfreie Übermittlung zu sorgen?
- Wer gilt als Verursacher, wenn die Grenzen nicht erkennbar sind?

5.2. Computerstrafrecht

Der Bedeutung von Daten als Wirtschaftsgut hat der Gesetzgeber mit den Straftatbeständen der Datenveränderung in § 303a StGB und der Computersabotage in § 303b StGB Rechnung getragen. Diese Normen ahnden das Löschen, Unterdrücken, Unbrauchbarmachen und Verändern von fremden Daten durch Unbefugte sowie erhebliche Störungen von Datenverarbeitungsanlagen durch Zerstörung, Beschädigung, Unbrauchbarmachung, Beseitigung oder Veränderung von Anlagen oder Datenträgern. Die Taten können im besonders schweren Fall mit bis zu zehn Jahren Freiheitsstrafe belegt werden, insbesondere wenn dadurch ein Vermögensverlust großen Ausmaßes herbeigeführt wurde. Das dürfte bei einem Cyberangriff auf ein Unternehmen in der Produktionskette regelmäßig der Fall sein.

Der unbefugte Zugriff auf Daten ist ebenfalls eine Straftat: Ausspähen und Abfangen von Daten, also „Datendiebstahl“ und die Datenhehlerei (§§ 202a, 202b, 202c und 202d StGB).

Sofern die mit den Daten dargestellten Informationen die Qualität von Geschäftsgeheimnissen haben, sind sie ebenfalls strafrechtlich geschützt (§§ 17 und 19 UWG).

Zwar liegt eine strafrechtliche Verfolgung primär im Interesse des Staates und nicht unmittelbar im Interesse des geschädigten Unternehmens – aber oft kann erst die Beteiligung am Strafverfahren als Anzeigeerstatter oder Nebenkläger dem Geschädigten Erkenntnisse zur Tat verschaffen, die nur im Rahmen eines strafrechtlichen Ermittlungsverfahrens gewonnen werden können. Ein Verantwortlicher im Unternehmen wird kaum auf diese Quelle als Grundlage für einen etwaigen zivilrechtlichen Haftungsprozess verzichten können. Dies gilt auch und gerade für Ermittlungen bei mutmaßlichen Angriffen aus den Reihen der eigenen Belegschaft.

5.3. Versicherung von Cyberrisiken

Versicherer erwarten, dass Cyberrisiken wachsende Bedeutung erlangen und dass der Bedarf an Versicherungen gegen Cyberrisiken wächst. Die bisherigen Modelle der IT-(Hardware) Versicherung, Software-Versicherung, Betriebshaftpflichtversicherung und der Vertrauensschadenshaftpflichtversicherung decken Cyberrisiken nicht oder nur teilweise ab. Erste Policenmodelle zum Schutz gegen Cyberrisiken sind auf dem Markt und umfassen zusätzlich auch Assistenz im Schadenfall.

5.4. Datenschutz, Informationelle Selbstbestimmung

Aus Sicht der Mitarbeiter und der Kunden kommt dem Datenschutz unter Industrie 4.0 erhöhte Bedeutung zu. Die Zuordnung von Daten als technische oder aber personenbezogene Daten ist oft umstritten, weil letztere dem gesetzlichen Personendatenschutz unterfallen. Damit ist deren Umgang streng reglementiert und auch Gegenstand von arbeitsrechtlichen individuellen oder kollektiven Regelungen und Vereinbarungen. Einige Fragen dazu sind:

- Müssen Bereiche existieren, in denen eine Datenerhebung untersagt ist?
- Welche Prozessdaten sind personenbezogene Daten (Kameraüberwachung von Arbeitsprozessen aus Sicherheitsgründen / Kooperation Mensch / Roboter)?
- Wie ist die Sammlung sensibler Daten Dritter zu beurteilen?
- Dürfen/müssen (relevante) Daten an (Sicherheits-)Behörden weitergegeben werden?
- Inwieweit dürfen Datenschutzbestimmungen (angesichts der Rechte Dritter) für Parteien disponibel sein?
- Wie muss die IT-Compliance-Struktur im Unternehmen geändert werden?

- Welches Datenschutzrecht gilt bei Auslandsberührung, also Datentransfer, Datenzugriff, Datenbearbeitung?

5.5. Vermögensschutz, Eigentumsschutz

Letztlich befürchten viele Unternehmen, dass sie die Hoheit über ihre Daten verlieren, weil sie bei anderen zumindest in Kopie lagern, im Rahmen der Produktion verändert werden, mit anderen Daten vermischt, aggregiert und ausgewertet werden und damit letztlich neue Datenbestände geschaffen werden. Fraglich ist also, wem an welchen Beständen primäre und sekundäre Rechte zustehen und wie diese gesichert und durchgesetzt werden können.
Ob die bisherigen Instrumente wie Urheberrecht und Schutz von Datenbanken ausreichen, um das neue Spektrum abzudecken, ist noch Gegenstand der Diskussion. Interessant wäre es, Rechtsinstrumente aus dem Sachenrecht für physische Gegenstände auf Daten zu übertragen. Fragen sind dann:

- Übertragung von Rechtsfiguren des Sachenrechts auf IP (Dateneigentümer, Datenbesitzer, Datenverwahrung, Datennutzungsrechte, Datenmiete, aber auch Datenlizenz)
- Wem gehören die Daten? Wer ist Dateneigentümer?
- Wer ist Datenbesitzer?
- Muss (ggf.: wie kann) verhindert werden, dass Daten über den konkreten Anlass hinaus genutzt werden?
- Begründet die über den konkreten Anlass hinaus getätigte Nutzung Ansprüche für den Datenlieferanten?
- Wer hat das Recht an Sekundärdaten, die sich aus Primärdaten ergeben?
- Darf der Datenempfänger überlassene Daten (anonym) auswerten?
- Darf der Datenempfänger überlassene Daten (anonym) von mehreren Überlassern auswerten / aggregieren / analysieren?
- Muss der Datenempfänger Informationen / Analysen / Auswertungsergebnisse an die Lieferanten der Primärdaten zurückgewähren / Einblick einräumen?
- Wie müssen / können solche Datenrechte und -pflichten in einer hoch verdichteten Datenmischbasis in einer Lieferkette / Prozesskette zugeordnet werden?
- Wie ist der Wert des Eigentums an einer Sache zu beurteilen, wenn diese ohne geeignete Software und Datenzufluss ihre Funktion nicht erfüllen kann?

5.6. Provider und Plattformen

In der vernetzten Produktion wird es einen erheblichen Bedarf an Infrastruktur für das Vorhalten, den Austausch und die Verarbeitung von Daten geben. Dabei sind Struktu-

ren nach ihrem Zweck zu unterscheiden, ob sie lediglich unilateral durch ein Unternehmen genutzt werden oder multilateral durch mehrere bzw. viele Teilnehmer.

5.6.1. Provider

Unilaterale Strukturen dienen den Interessen eines Unternehmens, indem dieses seine Daten und Prozesse an ein konkretes Rechenzentrum (*Host*) oder an Anbieter von Serverkapazitäten (*Cloud*) auslagert, gegebenenfalls auch mit ausgelagerter Software (*Software as a service*) oder als ausgelagerte Gesamtabwicklung von betrieblichen Funktionen (*Outsourcing*). Dabei können diese Dienste durchaus auch Dritten zur Verfügung gestellt werden, etwa als Online-Bestellplattform, Internetpräsenz, Serviceportal oder anderes – es bleibt aber stets bei dem Angebot des einen Unternehmens.

Die wesentliche rechtliche Problematik besteht dabei in der Gewährleistung der Funktionalität der Providerdienste zur Verfügbarkeit und Sicherheit der Daten, definiert nach Leistungsebenen auf Grundlage vertraglicher Vereinbarungen und Leistungsbeschreibungen (*service level agreements*).

5.6.2. Plattformen

Plattformen dienen als multilaterale Strukturen der Verknüpfung vieler, voneinander unabhängiger Nutzer. Sie stellen eine Infrastruktur zur Verfügung, auf der die Nutzer sich bewegen und ohne Zutun des Plattformbetreibers miteinander in Verbindung treten und Transaktionen abwickeln können.

Die besonderen rechtlichen Fragen zu Plattformen hängen mit einer nicht immer klar definierten Haftung für die Angebote und Transaktionen ihrer Nutzer zusammen. Grundsätzlich wird ein Plattformbetreiber die Gewährleistung und Haftung für Leistungsmängel seiner Nutzer vertraglich ausschließen, er will nicht für die Qualität der auf der Plattform vertriebenen Produkte rechtlich einstehen müssen, auch nicht für die Seriosität und Bonität von Anbieter und Nachfrager.

5.7. Telekommunikation

Die Übermittlung von Daten und das Angebot von Diensten im Rahmen der M2M-Kommunikation können die Beteiligten bestimmten Pflichten aus dem Telekommunikationsrecht unterwerfen. Die Übermittlung von Daten stellt rechtlich in der Regel Telekommunikation dar und umfasst häufig Telekommunikationsdienste im Sinne des Telekommunikationsgesetzes (TKG). Es kommt dabei nicht darauf an, dass die Informationen in der Telekommunikation von Mensch zu Mensch übermittelt werden.

Unterfällt ein M2M-Dienst dem TKG, hat der Erbringer der Dienste eine Anzahl von Pflichten zu erfüllen, die sich auf Kundenschutz, Frequenznutzung, Nummerierung, Fernmeldegeheimnis und TK-Überwachung beziehen.

6. Markt und Kunden

Bei dem Begriff Industrie 4.0 steht zunächst die Vorstellung betrieblicher Abläufe im Vordergrund. Tatsächlich beginnt aber die Informationskette bereits ganz am Anfang, also beim Kunden, der produktionsrelevante Daten generiert und damit künftig unmittelbar Prozesse auslöst. Die Informationen dringen dabei durch mehrere Stationen der Liefer- und Wertschöpfungskette. Bekannt ist dieser Vorgang bereits bei der Konfiguration von Autos durch die Kunden, die künftig im Online-Modus unmittelbar Produktionsdaten an den Autohersteller (OEM) und durch ihn an dessen Zulieferer von Tier 1 bis Tier 4 übermitteln.
Dabei sind die Daten nicht nur für die konkrete technische Herstellung relevant, sondern auch und mit wachsender Bedeutung als Kundendaten zur Bewerbung und dem Ausbau weiterer Geschäftsbeziehungen. Wenn die Daten nicht nur technische Funktion haben, sondern die persönlichen Vorstellungen und Werte des Kunden widerspiegeln, handelt es sich um Personendaten, die dem Datenschutz unterliegen. Auch hier steht die Frage im Raum, welcher Empfänger die Daten nutzen darf und in welchem Umfang. Wichtige Fragen sind:

- Welche Daten werden von Kunden generiert und unmittelbar in den Produktionsprozess eingespielt?
- Wie darf das Unternehmen diese Kundendaten individuell oder kollektiv nutzen?
- Inwiefern und in welchem Umfang darf ein Unternehmen Daten seiner Kunden an seine Geschäftspartner weitergeben?
- Welche Pflichten muss das Unternehmen seinen Geschäftspartnern auferlegen und überwachen?

7. Wettbewerb

Die enge Vernetzung von Datenbeständen und Informationen führt zwangsläufig zu einer Verdichtung der Beziehungen der Beteiligten untereinander. Geschäftspartner wissen mehr voneinander als Dritte und können dieses Wissen in neuer Dimension einsetzen, um Angebote und Leistungen für bestimmte Kunden so zu optimieren, dass Wettbewerber faktisch keine konkurrenzfähige Leistung anbieten können und damit vom Markt abgeschottet werden. Besonders bindungsgeneigt ist die Ausstattung der Kunden mit Software, die sich in ihrer Systematik hin zu Biotopen entwickelt und keine Alternativen mehr zulässt, zumindest keine Datenmigration ohne die Gefahr von Datenverlust oder Datendesorganisation. In vielen Fällen wird auch ein Systemwechsel allein an dem zu erwartenden wirtschaftlichen Aufwand scheitern. Wettbewerbsrecht-

lich kritisch sind insbesondere Vorgehensweisen zu beurteilen, bei denen der Anbieter verschiedene Programme und Funktionen miteinander so in Paketen verbindet, dass der Nutzer entweder keine Alternativen nutzen kann oder er darauf aus Bequemlichkeit verzichtet. Die Beispiele, in denen Anbieter von Software, Hardware, Netzleistungen und Speicherleistungen derartige Kopplungen lancieren, sind bereits heute im Markt von Verbrauchern, aber auch Unternehmen zahlreich. Wichtige Fragen sind zum Beispiel:

- Dürfen durch enge Verknüpfungen Mitbewerber faktisch ausgeschlossen werden?
- Wo ist die Grenze zum unzulässigen Verdrängungswettbewerb?
- Dürfen (und wenn ja, inwieweit) Erkenntnisse aus gelieferten Datenbeständen ausgewertet und (für andere Zwecke) verwertet werden?
- Wie können sich Datenzulieferer davor schützen, sich durch die Verfügbarmachung ihrer Daten / Programme selbst überflüssig zu machen?
- Wie sind Updates unter wettbewerbsrechtlichen Gesichtspunkten zu beurteilen?

8. Personal und Arbeit

Wenn Maschinen, Anlagen und Systeme immer weiter fortschreitend intelligente Funktionen übernehmen, werden sich neue Fragen zur menschlichen Arbeit ergeben. Bereits heute sind Menschen in den betrieblichen Prozesse intensiv maschinenbezogen tätig. Die Abläufe haben sich durch Informationstechnologie massiv verändert: einerseits sind zahlreiche einfache und höhere Tätigkeiten ersatzlos entfallen, andererseits sind für die heutigen Mitarbeiter die Anforderungen in der Handhabung von Systemen gestiegen. Dies gilt nicht nur in der Produktion, sondern auf allen Ebenen des Betriebes. Im Wegfall einfacher Arbeiten sehen Gewerkschaften und Sozialverbände Herausforderung für die Beschäftigungspolitik, in der steigenden Verdichtung der Kooperation von Mensch und Maschine eine ethische Herausforderung zur Erhaltung humaner Arbeitsplätze. Auf betrieblicher Ebene wird sich daher die schon heute bestehende Entwicklung und Diskussion fortsetzen: zu Steuerungen, Taktungen, Protokollierung, Sicherheitssysteme, Kommunikationserfassung und vieles mehr.
Dazu wichtige Fragen:

8.1. Grundsatzfragen

- Welche Rolle nimmt der Mensch im Werkprozess ein?
- Was passiert mit Arbeitsplätzen?
- Welche Ausbildungen / Studiengänge werden weniger / mehr nachgefragt werden?

- Besteht noch ein Bedarf für Betriebsräte?

- Wie verändern sich die Einflussmöglichkeiten von Betriebsräten / Gewerkschaften, wenn Arbeitskampf kein Druckmittel mehr ist?
- Welche Bedeutung haben Schwerpunktstreiks in einer (international) vernetzten Produktion?

8.2. Arbeitswelt

- Wie sollen / können / dürfen Arbeitsplätze ausgestaltet sein?
- Wie sollen / können / dürfen externe Plätze ausgestaltet sein?
- Wie kann / darf Überwachung zur Qualitätskontrolle ausgestaltet sein?
- Wie kann / darf Überwachung zum Arbeitsschutz ausgestaltet sein (Kameraüberwachung Mensch / Maschine)?
- Welche Informationsrechte / Mitwirkungsrechte / Mitbestimmungsrechte hat der Betriebsrat?
- Welche Fragen können / sollen von den Tarifpartner behandelt / festgelegt werden?
- Sollen die Vereinbarungen Allgemeingültigkeit haben?
- Erhalten Betriebsräte neue Kontrollrechte / Mitwirkungsrechte bei personenbezogenem Datenmanagement?

9. Steuern und Finanzen

Wenn in der vernetzten Wirtschaft Daten den wesentlichen Bestandteil einer technischen Funktionalität ausmachen oder als Wissen die Grundlage des Unternehmenserfolgs sind, stellt sich die Frage in neuer Dimension, wie der Wert solcher Datenbestände handelsrechtlich und steuerrechtlich zu beurteilen ist.

9.1. Steuern

Bereits heute können am Markt erworbene immaterielle Wirtschaftsgüter bilanziell aktiviert werden, für selbst geschaffene Wirtschaftsgüter hat das Unternehmen ein Wahlrecht zur Aktivierung oder Behandlung als Aufwand. Der Zuwachs oder aber die Irrelevanz von Datenbeständen sind dementsprechend zu behandeln. Für die steuerliche Anerkennung der bilanziellen Behandlung werden sich zahlreiche Grenzfälle mit Diskussionspotential ergeben. Fragen dazu sind:

- Sind Datenbestände aktivierbare Vermögensgegenstände?
- Wann können / müssen sie abgeschrieben werden?
- Inwieweit beeinflussen Datenbestände / Datenströme aus internen / externen Quellen die Funktionalität und den Wert einer Maschine / Anlage / geistiger Rechte?

9.2. Finanzen

Welchen Wert Datenbestände für das Unternehmen und seine Geldgeber haben, muss im Einzelfall ermittelt werden. Datenbestände können eine entscheidende Grundlage für Kundennutzen, Markterfolg und Ertragskraft eines Unternehmens sein. Sie können aber auch für die reine Funktionalität von Maschinen, Anlagen und Systemen eine kritische Größe sein, wenn durch sie erst Maschinen produktiv eingesetzt werden können. Die Schwankungsbreiten zur Bewertung von Maschinen und Anlagen werden größer werden – das bedeutet eine herabgestufte Bewertung von Maschinen als Sicherheiten in der Kreditvergabe für Anlageninvestitionen. Daher dürfte die Finanzierung durch Bankkredite zurückgehen, während markt- und ertragsorientierte Finanzierungsmodelle weiter Platz greifen, insbesondere durch spezialisierte Leasinganbieter.

- Inwieweit beeinflussen Datenbestände / Datenströme aus internen / externen Quellen die Funktionalität und den Sicherungswert einer Maschine / Anlage / geistiger Rechte für Finanzierungszwecke?
- Inwieweit verändert dies das Anlagevermögen und das Eigenkapital?
- Müssen neue Finanzierungsinstrumente eingesetzt werden? Leasing, Factoring etc?
- Wie verändern sich Finanzierungsmodelle, wenn ein Betrieb virtuell organisiert ist: gemietete Räume, geleaste Maschinen, fremdgesteuerte Prozesse, ausgelagerte Daten und Prozesse (Cloud / Outsourcing), Einsatz von Subunternehmern und Zeitarbeitern?

10. Geschäftsführung und Aufsicht

10.1. Haftung der Geschäftsführung und Aufsichtsorgane

Grundsätzlich haben Vorstand und Geschäftsführer die Geschäfte der Gesellschaft und des Unternehmens mit der Sorgfalt eines ordentlichen Kaufmanns zu führen. Das bedeutet also, dass sie die Pflicht haben, den Geschäftszweck bestmöglich zu verfolgen und dazu die richtigen und geeigneten Maßnahmen zu treffen. Fehler sind dabei nicht ausgeschlossen, wohl aber bei entsprechender Sorgfalt vermeidbare Fehler. Die Business Judgement Rule gesteht dem Geschäftsleiter also auch Irrtümer zu, allerdings keine beliebigen. Zur Vermeidung von Fehlern darf der Leiter auch nicht in Passivität verfallen, auch das Unterlassen kann einen Fehler darstellen, wenn Handeln geboten ist. Im Kontext von Industrie 4.0 bedeutet dies für Vorstände und Geschäftsführer eine ständige Herausforderung: einerseits dürfen sie das Unternehmen nicht von dynamischen Marktentwicklungen abkoppeln, andererseits müssen sie Wege und Methoden finden, mit oft noch unbekannten Risiken umzugehen. Fragen dazu sind:

- Welche Sorgfaltspflichten müssen Geschäftsführung und Vorstand bei Entscheidungen zur Einführung neuer Technologien beachten?
- Wo liegen die Grenzen der Business Judgement Rule?
- Welche Abwägungen muss ein Organ treffen?
- Welche Sicherungssysteme muss ein Organ einrichten?
- Wie muss es diese Systeme überwachen?
- Können sich Organe (GF / Vorstand) für Fehler / Schäden / Verletzungen aus fremdbestimmten Abläufen in ihrem Unternehmen freizeichnen?
- Welche Haftung trifft die Aufsichtsorgane?
- Wie sehen wirksame Haftungsübernahmen von Geschäftspartnern aus?
- Deckt die D&O Versicherung Haftungsfälle mit Fremdeinwirkung?

10.2. Maßnahmen der Geschäftsführung / Legal Controlling

Im Ergebnis müssen Vorstand und Geschäftsführer Methoden anwenden und Systeme einrichten, die ihnen eine möglichst weitreichende Einwirkungsmöglichkeit verschafft. Die Grundsätze des Risk Managements in der Skalierung von Schutzmaßnahmen gelten auch hier: technische Risiken vermeiden, rechtliche Risikokontrollen einrichten und Risikozuordnungen organisieren, wirtschaftliche Risiken finanziell absichern:

- Einrichtung von Sicherungs- und Kontrollsystemen als Risk-Management, Legal Controlling und Compliance Management
- Überwachung der Systeme als Risk-Management und Revision
- Sicherungs- und Kontrollvereinbarungen in Verträgen mit Geschäftspartnern
- Qualitäts- und Haftungsvereinbarungen in Verträgen mit Geschäftspartnern
- Monitoring von Vereinbarungen (Vertragscontrolling), Prozessen und Produkten
- Monitoring der rechtlichen Entwicklungen

11. Ausblick

Im Ergebnis wird das Recht eine flexible und belastbare Grundlage für die technologischen und wirtschaftlichen Entwicklungen unter Industrie 4.0 schaffen können. Vielfach werden sich bereits entwickelte und in der Praxis eingesetzte Methoden und Instrumente verwenden lassen, es wird aber auch bislang - zumindest in ihrer Dimension - weitgehend unbekannte Erscheinungen geben, für die das Recht neue Instrumente schaffen muss. Dies wird in weitem Umfang durch vertragliche Rechtsgestaltung geschehen, teilweise wird der Gesetzgeber für Klarheit sorgen müssen. Vorstände und Geschäftsführer stehen in der Verantwortung, ihr Unternehmen wettbewerbsfähig und rechtssicher in die Zukunft zu führen.

Betrieb & Systeme

Verträge und Haftung in der Lieferkette

Marc-André Delp, MLE ,Rechtsanwalt
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

Neben verschiedenen Aspekten rund um Industrie 4.0, beispielsweise bezüglich Arbeitswelt und Digitalisierung im Betriebsablauf, müssen auch die rechtlichen Fragen betrachtet werden. Ähnlich wie bei den Entwicklungen zum Autonomen oder Automatisierten Fahren mögen hier Unterschiede in der Betrachtung zwischen technologischer Entwicklung und rechtlichen Möglichkeiten bestehen. Wie weit ist die rechtliche Entwicklung im Vergleich zum technologischen Fortschritt? Sind technologische Entwicklungen unter Berücksichtigung des rechtlichen Hintergrundes erfolgt? Oder sind rechtliche Aspekte bei der Entwicklung vernachlässigt worden? „Die Technik ist weiter als das Recht[7]“ ist eine Ansicht im Rahmen der zunehmenden Automatisierung des Fahrens. Gilt diese Einschätzung auch für die Entwicklungen zu Industrie 4.0?

Auch die Bundesregierung hat sich des Themas angenommen. „Es geht vor allem auch um die Frage, wie das heutige Recht, das ganz wesentlich auf die Idee menschengesteuerten Verhaltens ausgerichtet ist, unter dem Gesichtspunkt maschinengesteuerter Kommunikationsfähigkeit weiterentwickelt werden muss[8].“, so ein Punkt der Plattform Industrie 4.0.

1. Vertragsabschluss

In unserer Rechtsordnung werden Willenserklärungen Personen zugerechnet. Verträge kommen durch Angebote einer Person an eine andere und die Annahme durch ebendiese andere Person zustande. Dies geschieht sowohl im klassischen Sinne bei direktem Kontakt dieser Personen (z.B. per Telefon), aber auch bei dem Einsatz technischer Hilfsmittel wie Email oder Fax bis hin zum Einsatz der elektronischen Signatur.
Bei der Zurechnung von Willenserklärungen nach dem Grad der Automatisierung zu unterscheiden. Solange keine echte künstliche Intelligenz eigenständig Entscheidungen trifft und die Willenserklärungen abgibt, wird man die Willenserklärungen dem Erklärenden als natürliche oder juristische Person zurechnen können.[9]

[7] ADAC-Generalsyndikus Werner Kaessmann, ADAC Motorwelt 3/2015 zu „Automatisertes Fahren“
[8] Memorandum der Plattform Industrie 4.0, S. 11, http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/memorandung-industrie-4-0,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, Abruf am 23.11.2015
[9] vgl. Spindler, Rechtsprobleme Industrie 4.0 – Einführung und Überblick vom 15. April 2016, Folie 4

Nunmehr ist die technische Entwicklung aber soweit, dass im Rahmen von M2X, M2M oder IoT Menschen mit Maschinen kommunizieren bis hin zu dem Moment, wo Maschinen untereinander und gegebenenfalls auch autonom kommunizieren, selbständig Befehle ausführen oder Bestellungen vornehmen. Rechtliche Fragestellungen ergeben sich in Situationen, in denen eine Maschine eine Bestellung durchführt. Dabei ist unter anderem zu klären, ob es sich bei diesem Bestellvorgang um eine Willensäußerung handelt, welche rechtliche Wirkung dieser Vorgang entfaltet und wem am Ende die Aktion der Maschine zuzurechnen ist.

Im Online-Handel und in Online-Shops klickt sich der Nutzer durch die Angebote und wählt sein Produkt aus. Die Bestellung erfolgt, indem er die Bestelloption betätigt, die Zahlungsweise angibt und nach Bestätigung der AGB des Verwenders letztendlich einen Menüpunkt zur Bestätigung der Bestellung anklickt. Da die Warenpräsentation im Online-Shop selbst noch kein Angebot im Rechtssinn sein soll, gibt der Nutzer mit seiner Bestellung ein Angebot zum Abschluss eines Kaufvertrages ab, der Online-Anbieter nimmt dieses Angebot automatisiert an. Dieser Vertragsabschluss zwischen Mensch und Maschine wird als rechtsverbindlich angesehen.

Wenn hingegen der Bestellvorgang durch eine Maschine ohne weitere Beteiligung einer Person ausgelöst wird und der Vertragsabschluss zwischen den Maschinen stattfindet, stellt sich die Frage, wie dieser Vertragsabschluss juristisch zu bewerten ist. Kann hier noch an die Handlung einer Person angeknüpft werden und wie weit ist feststellbar, ob die Erklärungen durch das System selbst oder durch den Nutzer des Systems erzeugt werden? Müssen sich die Unternehmen die Handlungen der Maschinen zurechnen lassen? Hierzu wird auf die Ausführungen und rechtlichen Bewertungen rund um den Bereich der Softwareagenten verwiesen. Computer / Maschinen haben keine eigene Rechtspersönlichkeit, sie können somit nicht als Träger von Rechten und Pflichten angesehen werden und damit letztendlich auch keine Erklärungen abgeben. Bei der Verwendung eines elektronischen Agenten auf Empfängerseite gilt eine Willenserklärung dann als zugegangen, wenn diese die Schnittstelle zum Agenten erreicht hat, sodass dieser unter Zugrundelegung normaler Verhältnisse die Möglichkeit der Verarbeitung hat [10].

Dem Betreiber einer Maschine werden die Inhalte einer sogenannten Maschinenerklärung als Absender dieser Erklärung zugerechnet[11]. Verantwortlich für eine Erklärung bleibt derjenige, aus dessen Sphäre die Erklärung kommt. Das bedeutet, dass eine Maschinenerklärung demjenigen zugerechnet wird, der sich beim Vertragsabschluss des autonomen Systems bedient bzw. das autonome System in die Vertragsdurchführung

[10] vgl. Cornelius, Vertragsabschluss durch autonome elektronische Agenten, in: MMR 2002, 353, 356
[11] vgl. Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 35

einbringt.[12] Dieser bleibt aber auch für fehlerhafte Maschinenerklärungen verantwortlich.[13]

Der Bundesgerichtshof hat Erklärungen eines Computers, bei denen der Nutzer vor Vertragsschluss zumindest die Rahmenbedingungen festgelegt hat, dem Nutzer des Systems als sogenannter Herr der Erklärung zugerechnet[14]. Dieses Modell wird in der Literatur auf autonome Agentenerklärungen übertragen. Hierbei ist der Mensch grundsätzlich für den Einsatz von Computerprogrammen rund um die Abwicklung von Rechtsgeschäften verantwortlich[15]. Allerdings wird bereits angemerkt, dass aufgrund der Lernfähigkeit und der damit verbundenen Unberechenbarkeit des Systems dieses Konzept möglicherweise nicht mehr lange tragbar sein und eine neue rechtliche Bewertung erforderlich wird[16].
Als Lösungsvorschlag für den Empfang von Maschinenerklärungen bieten sich vertragliche Vereinbarungen an, wonach der Empfänger den Zugang einer Nachricht zu bestätigen hat. Auch könnte vertraglich festgelegt werden, inwieweit Maschinenreaktionen ein rechtlicher Gehalt beizumessen sein soll oder ob darauf verzichtet wird[17]. Damit gibt der Betreiber der Maschine eine Erklärung durch Programmierung der Maschine ab, diese kann ihm zugerechnet werden[18].

In diesem Zusammenhang müsste auch geklärt werden, ob bei automatisierten Prozessen die abgegebenen Erklärungen angefochten werden können, beispielsweise ob sich das Unternehmen bei Einsatz einer Maschine und einer letztendlichen Falschbestellung auf einen Irrtum im Sinne des BGB berufen und den Bestellvorgang damit anfechten kann. Erklärungen von Maschinen könnten nach den allgemeinen Regeln des BGB beseitigt werden, z.B. durch Anfechtung.[19] Bezüglich der Erklärungsakte wird darauf verwiesen, dass diese den Personen zuzurechnen sind, die sich des autonomen Systems bedienen[20]. Dies stehe im Einklang mit den bestehenden Regelungen des Zivilrechts. Erklärungsfehler und deren Konsequenzen wären dann kein Problem der Zuordnung, sondern durch neue Haftungskonzepte zu bewältigen. In diesem Zusammenhang könn-

[12] vgl. Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 35
[13] vgl. Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 35
[14] vgl. BGH, Urteil vom 16.10.2012, Az: X ZR 37/12 = BGHZ 195, 126
[15] vgl. Cornelius, Vertragsabschluss durch autonome elektronische Agenten, in: MMR 2002, 353, 355; Bräutigam / Klindt, NJW 2015, 1137, 1138
[16] vgl. Bräutigam / Klindt, NJW 2015, 1137, 1138
[17] vgl. Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 35
[18] vgl. Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 35
[19] vgl. Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 35
[20] Vgl. Bräutigam / Klindt in Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung, BDI und Noerr, November 2015, S. 14

te eine Weiterentwicklung des Haftpflichtgesetzes erfolgen, beispielsweise eine Gefährdungshaftung bei autonomen Systemen mit klaren Haftungshöchstgrenzen[21].

2. Vertragsgegenstand

Im Rahmen der Automatisierung tritt die Frage nach der vertragsrechtlichen Einordnung auf[22]. Bei der Fertigung kleiner Serien und von Unikaten, einer technischen Möglichkeit im Rahmen von Industrie 4.0 und Abkehr von den bislang gängigen Massenprodukten, könnte das Kaufrecht an Bedeutung verlieren. Verträge über die Lieferung von Einzelanfertigungen würden sich dann nicht mehr als Kaufvertrag einordnen lassen, sondern als Werklieferungsvertrag.

Im Übrigen treten vermehrt Dienste in den Vordergrund, die aus einem Gegenstand sogenannte Smart Things machen. Wenn sich ein Leistungsschwerpunkt ableiten lässt, dann ist dieser für die vertragliche Beurteilung entscheidend. Lässt sich hingegen gerade kein Leistungsschwerpunkt ermitteln, so sind die Einzelleistungen zu betrachten. Kann der Gegenstand nur in Kombination mit dem Internetdienst genutzt werden, so liegt ein Kaufvertrag vor, bei dem der Dienst vertraglicher Bestandteil ist. Wird dieser Dienst abgeschaltet, liegt ein Mangel vor und es gelten die Regelungen des Kaufvertrages zur mangelhaften Ware. Kann der Gegenstand auch ohne den Dienst genutzt werden, so ist der Erwerb des Gegenstandes rechtlich ein Kaufvertrag, die Dienste sind dann ein Dienstvertrag. Stellt der Anbieter des Internetdienstes diese Leistung ein, muss eine rechtliche Beurteilung nach dem allgemeinen Leistungsstörungsrecht erfolgen.

3. Lieferung

Nach § 377 Abs. 1 HGB bestehen beim Warenkauf zwischen Kaufleuten für den Käufer besondere Untersuchungspflichten.

> *„Ist der Kauf für beide Teile ein Handelsgeschäft, so hat der Käufer die Ware unverzüglich nach der Ablieferung durch den Verkäufer, soweit dies nach ordnungsmäßigem Geschäftsgange tunlich ist, zu untersuchen und, wenn sich ein Mangel zeigt, dem Verkäufer unverzüglich Anzeige zu machen.“*

[21] Vgl. Bräutigam / Klindt in Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung, BDI und Noerr, November 2015, S. 14
[22] vgl. Bräutigam / Klindt, NJW 2015, 1137, 1138

Darüber hinaus gilt gemäß Absatz 2

> *„Unterlässt der Käufer die Anzeige, so gilt die Ware als genehmigt, es sei denn, dass es sich um einen Mangel handelt, der bei der Untersuchung nicht erkennbar war.“*

Erfolgt ein Vertragsabschluss durch Maschinen, so stellt sich die Frage, ob auch in diesem Fall eine Pflicht zur Warenprüfung besteht, ob eine Wareneingangskontrolle durch Maschinen zu erfolgen hat und ob diese überhaupt möglich wäre. Des Weiteren ist fraglich, ob es sich bei einem Vertragsabschluss M2M noch um einen Individualvertrag handelt (und ob Maschinen einen Individualvertrag abschließen könnten), oder ob dieser auf Grundlage von AGB erfolgt.

Denn § 377 HGB ist zwar im Rahmen von Individualvereinbarungen abdingbar, durch Individualvereinbarung kann die Rügepflicht verschärft, gemildert oder ganz aufgehoben werden[23]. Eine Verschärfung der Rügepflichten in AGB ist hingegen unwirksam[24].

4. Force Majeure

Bei der Gestaltung eines Haftungsausschlusses in Verträgen werden regelmäßig Regelungen zur Höheren Gewalt (Force Majeure) aufgenommen. Die bislang gängigen Beispiele der Höheren Gewalt könnten im Rahmen der Automatisierung noch ergänzt werden.

Als Höhere Gewalt bezeichnet die Rechtsprechung ein von außen kommendes, nicht voraussehbares und auch durch äußerste vernünftigerweise zu erwartende Sorgfalt nicht abwendbares Ereignis[25]. In Verträgen wird regelmäßig die Haftung in Fällen Höherer Gewalt ausgeschlossen und werden dazu Sonderregelungen getroffen.

Kommunizieren nun M2x oder M2M, ist fraglich wie anfällig Maschinen für Stromausfälle sind. Ein Stromausfall fällt unter den Begriff der Höheren Gewalt, wenn er durch Naturgewalten wie Blitz oder Unwetter verursacht wird, nicht hingegen, wenn er andere Ursachen hat. Ist aber ein Stromausfall noch als Höhere Gewalt zu bewerten, wenn er zumutbar durch ein Notstromaggregat vermieden werden könnte?

Daher sollten Unternehmen mit zunehmender Automatisierung in ihrem Betriebsablauf Maßnahmen treffen, mit denen die Maschinen bei Stromausfall produktionsfähig

[23] vgl. Hopt in Baumbach/ Hopt, HGB, 36. A., § 377 Rn 57
[24] vgl. Hopt in Baumbach/ Hopt, HGB, 36. A., § 377 Rn 58
[25] vgl. BGHZ 100, 185, 188

und handlungsfähig bleiben. Anderenfalls drohen Produktionsstillstände, die trotz Stromausfall nicht zu einem Fall der Höheren Gewalt führen. Der Unternehmer bleibt damit für den Verzug verantwortlich und haftet dafür. Ein Notstromaggregat könnte dem Ausfall und damit einem Haftungsfall vorbeugen.

Zur Höheren Gewalt kann aber auch eine über einen längeren Zeitraum nicht funktionierende oder gestörte Internetverbindung gehören, innerhalb derer wichtige Daten von vernetzten Maschinen verloren gehen. Der Serviceanbieter könnte für etwaige Fehlfunktionen und Störungen verantwortlich gemacht werden, wenn er nicht im Rahmen der Definition von Höherer Gewalt in Verträgen diesen Fall der Höheren Gewalt zugeschrieben hat[26]. Dieses wird in der Praxis bereits umgesetzt. So findet sich beispielsweise eine Regelung, wonach „ein fehlerhaftes oder nicht funktionierendes Telekommunikationsnetz“ der Höheren Gewalt zuzurechnen ist[27].

5. Gerichtsstand

Mit dem Gerichtsstand wird das zuständige Gericht für ein gerichtliches Verfahren bezeichnet. Dabei ging es bislang um Rechtsstreitigkeiten zwischen Personen.

Der gesetzliche Gerichtsstand ist sowohl nach deutschem, als auch nach europäischem Zivilprozessrecht der Sitz des Beklagten. Davon abweichend gibt es einige bereits gesetzliche Ausnahmen (beispielsweise Gerichtsstand des Erfüllungsortes) und die Möglichkeit einer Gerichtsstandsvereinbarung. Eine Regelung zum Gerichtsstand bedarf grundsätzlich der Vereinbarung zwischen den Parteien, diese kann auch auf elektronischem Wege erfolgen.

Eine Gerichtsstandsvereinbarung kommt neben individueller Vereinbarung auch zustande, wenn bei einem auf elektronischem Wege geschlossenen Kaufvertrag die Einbeziehung allgemeiner Geschäftsbedingungen, die eine Gerichtsstandsvereinbarung enthalten, durch click wrapping erfolgt, die eine elektronische Übermittlung und eine dauerhafte Aufzeichnung der Vereinbarung ermöglicht. Dazu muss das Ausdrucken und Speichern des Textes der Geschäftsbedingungen vor Abschluss des Vertrages ermöglicht werden[28].

[26] Jörg Vocke, Chief Counsel Technology Siemens AG München in: Müller-Tauber, Industrie 4.0 und Recht – Rechtlich smart in die Zukunft in Wirtschaft – Das IHK-Magazin für München und Oberbayern 5/2015, www.muenchen.ihk.de/de/WirueberUns/Publikationen/magazin
[27] vgl. § 6.3 der AGB der Fidor Bank AG bezüglich des Angebots der Vermittlung von Bitcoins auf der Plattform www.bitcoin.de Februar 2015), www.bitcoin.de /de/AGB/Fidor, Abruf am 23.11.2015
[28] EuGH, Urteil vom 21.05.2015, Rs. C 322/14, El Madjoub vs. CarsOnTheWeb.Deutschland.GmbH, in CR 2015, S. 670)

Der Kaufvertrag wird in diesem Beispiel durch eine natürliche Person und die Website bzw. den Server des Verkäufers auf elektronischem Wege geschlossen.

Mit der zunehmenden Automatisierung ist aber fraglich, wo der gesetzliche Gerichtsstand im Falle eines Vertragsabschlusses zwischen Maschinen zu sehen ist. Möglicherweise können Lieferant/ Leistungsempfänger/ Prozessrechner/ Datenspeicher oder juristischer Sitz entscheidend einschlägig sein. Besondere Beachtung verdient der Fall, in dem sich der Server im Ausland befindet.

Stellt man sich auf den Standpunkt, dass die Anfrage des Kunden eine computergesteuerte Routine auslöst und der Anbieter hierzu keine aktive Handlung vornimmt, besteht rechtlich kein Unterschied zum Download. Beim Download wird der Server der Sphäre des Schuldners zugerechnet. Einen allgemeinen Gerichtsstand eines Servers sieht das deutsche Recht bislang nicht vor. Erfüllungsort beim Download von Daten auf ein Mobiltelefon bleibt daher der Sitz des Anbieters[29].

6. International

Die Ausfuhr von Waren und Technologie in das Ausland ist nicht unbeschränkt möglich, sondern unterliegt eventuellen Embargos und grundsätzlich den Ausfuhrvorschriften des Bundes. Das bedeutet, dass die Ausfuhr der Genehmigung bedarf und ansonsten verboten sein könnte. Dies gilt insbesondere, wenn die Waren, Technologie oder Software von Anhang I der EG Dual-Use VO oder Teil I Abschnitt A der Ausfuhrliste erfasst ist. (s. Art. 3 Absatz 1 EG Dual-Use VO und § 5 Außenwirtschaftsverordnung – AWV)[30]. Genehmigungen erteilt das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA).

Transfer von Waren und Daten

Bei der zunehmenden Vernetzung der Maschinen ist zu bedenken, dass es sich bei grenzüberschreitenden Sachverhalten, also wenn Daten oder Informationen aus Deutschland ins Ausland übertragen werden sollen, um einen Technologietransfer handeln kann. Dies wird bereits deutlich, wenn Produkte grenzüberschreitend im 3D-Druck hergestellt werden. In dem Fall wird die Ware zwar nicht physisch ins Ausland verbracht, sondern digital transportiert, um im Ausland zu entstehen – der Effekt ist der gleiche wie beim physischen Transport.

[29] vgl. Rayermann / Zimmer, Rechtliche Grundlagen des M-Commerce, in Gora / Röttger-Gerick, Handbuch Mobile Commerce, S. 112

[30] Technologietransfer und Non-Prolifration, Informationsblatt der BAFA, 2016, S. 10, http://www.bafa.de/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_technologietransfer_non_proliferation.pdf, Abruf am 10.08.2016;

Der häufigere Fall ist hingegen der Transfer von Daten aus Servern oder von maschinengenerierten Daten aus Prozessen. Sofern sich daraus technologische oder betriebliche Erkenntnisse ableiten lassen, kann dies Technologietransfer bedeuten. So ist vorstellbar, dass die Übertragung von Betriebsdaten von bei Kunden aufgestellten Robotern ins Ausland einen solchen Technologietransfer darstellt.

Ausfuhr von Technologie

Die bestehenden Genehmigungspflichten für den grenzüberschreitenden Güterverkehr gelten also grundsätzlich nicht nur für Waren, sondern auch für *Technologie* und Software.

Unter *Technologie* ist das spezifische technische Wissen zu verstehen, das für die Entwicklung, Herstellung oder Verwendung eines Produkts nötig ist.[31] Technologie kann in Form von Technischen Unterlagen oder Technischer Unterstützung erbracht werden.[32] Zu den Technischen Unterlagen zählen unter anderem Pläne, Diagramme, Modelle, Konstruktionszeichnungen.[33]

Neben den Beschränkungen für die Ausfuhr von Technologie bestehen auch Beschränkungen für die Erbringung bestimmter als *Technische Unterstützung* bezeichnete Dienstleistungen.[34] Technische Unterstützung wird in § 2 Abs. 16 AWG definiert:„Technische Unterstützung ist jede technische Hilfe in Verbindung mit der Reparatur, der Entwicklung, der Herstellung, der Montage, der Erprobung, der Wartung oder jeder anderen technischen Dienstleistung. Technische Unterstützung kann in Form von Unterweisung, Ausbildung, Weitergabe von praktischen Kenntnissen oder Fähigkeiten oder in Form von Beratungsleistungen erfolgen. Sie erfasst auch mündliche, fernmündliche und elektronische Formender Unterstützung.“[35] Neben den Waren im

[31] Technologietransfer und Non-Proliferation, Informationsblatt der BAFA, 2016, S. 11, http://www.bafa.de/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_technologietransfer_non_proliferation.pdf, Abruf am 10.08.2016;

[32] Vgl. Hohmann,Exportrechtliche Grenzen des Technologietransfers, http://www.exportmanager-online.de/2011/ausgabe-4-2011/exportrechtliche-grenzen-des-technologietransfers/, Abruf am 18.08.2016

[33] Vgl. Hohmann,Exportrechtliche Grenzen des Technologietransfers, http://www.exportmanager-online.de/2011/ausgabe-4-2011/exportrechtliche-grenzen-des-technologietransfers/, Abruf am 18.08.2016

[34] Technologietransfer und Non-Proliferation, Informationsblatt der BAFA, 2016, S. 23, http://www.bafa.de/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_technologietransfer_non_proliferation.pdf, Abruf am 10.08.2016;

[35] Technologietransfer und Non-Proliferation, Informationsblatt der BAFA, 2016, S. 23, http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_technologietransfer_non_proliferation.pdf, Abruf am 10.08.2016

engeren Sinne unterfällt auch die Technische Unterstützung als eigenständige und von einer Warenlieferung unabhängige Leistung der Genehmigungspflicht. Sofern Technische Unterstützung im Zusammenhang mit einer Warenlieferung erbracht wird und deren Ausfuhr genehmigungsbedürftig ist, unterliegt die Technische Unterstützung gemeinsam mit der Ware dem Kontrollverfahren.

In den Embargo-Vorschriften zum Außenwirtschaftsverkehr mit der Russischen Föderation wird anstelle der *Technischen Unterstützung* der Begriff der *Technischen Hilfe* verwendet, der aber den gleichen Inhalt definiert. Technische Hilfe ist gemäß Art. 1 Ziffer c der Verordnung (EU) Nr. 833/2014 „jede technische Unterstützung im Zusammenhang mit Reparaturen, Entwicklung, Herstellung, Montage, Erprobung, Wartung oder jeder anderen technischen Dienstleistung; technische Hilfe kann auch in Form von Anleitung, Beratung, Ausbildung, Weitergabe von praktischen Kenntnissen oder Fertigkeiten oder in Form von Beratungsdiensten erfolgen, einschließlich Hilfe in verbaler Form.[36]“

Technische Instruktionen für den Einsatz von Waren gelten hingegen nicht als Technische Unterstützung. Diese gehören als Gebrauchsanweisung zur Ware und werden von einer Genehmigung der Ware mit umfasst. Sie bedürfen daher keiner eigenen gesonderten Genehmigung.

Ausfuhr im Konzern

Die Ausfuhr von Waren und Technologie unterliegt der Ausfuhrkontrolle als staatliche Überwachung. Daher betreffen die Genehmigungspflichten auch Ausfuhren im Konzern. Diese Pflichten gelten unabhängig davon, ob Konzerngesellschaften an der Technologie Geistiges Eigentum besitzen und konzerninterne Compliance Regelungen zum Einsatz der Technologie im internationalen Rahmen unterhalten.

7. Haftung

Nach deutschem Recht sind nur natürliche Personen im rechtlichen Sinne verantwortlich. Mit der zunehmenden Automatisierung rückt auch die Frage der Haftung in den Vordergrund. Die Regelungen des BGB und damit im Zusammenhang die Beweisregeln werden derzeit als leistungsfähig genug angesehen, um die zunehmende Automatisie-

[36] Vgl. Verordnung (EU) Nr. 833/2014 des Rates vom 31. Juli 2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, Abruf am 22.08.2016

rung damit unter Haftungsaspekten regulieren zu können.[37] Im Automatisierungsprozess geht es um die Zurechnung von Verletzungshandlungen sowie die Verantwortlichkeit für ebendiese.

„Einen Schaden kann man nur einem Menschen als Verursacher, nicht aber einer Maschine zurechnen. Das heißt, im Moment laufen unter Umständen Geschädigte Gefahr, dass sie auf ihrem Schaden sitzen bleiben müssen, wenn sie sich zum Beispiel im Umgang mit einer autonomen Industriemaschine verletzen[38].“

Schuldhaftes Handeln und Automatisierung

Als Anknüpfungspunkt für eine Haftung kommt nur menschliches Handeln in Betracht. Somit muss als Zurechnungskriterium auf die Entscheidung zur Herstellung bzw. tatsächlichen Verwendung einer Technologie abgestellt werden[39]. Dabei ist das schuldhafte Inverkehrbringen oder die Entscheidung zur Nutzung für die Frage der Haftung entscheidend. Auf eine mögliche autonome Entscheidung einer Maschine zur Auslösung des Schadensverlaufes kommt es in diesem Fall nicht mehr an. Entscheidendes Kriterium der Haftung ist somit die Vorhersehbarkeit der schädigenden Kausalität aus Sicht des Herstellers bzw. späteren Verwenders[40].

Zur Frage der zivilrechtlichen Haftung lohnt sich ein Blick auf die Diskussionen zur Haftungsproblematik rund um das Automatisierte Fahren. Verursacht ein Fahrzeug einen Schaden durch Fahrfehler, haftet primär der Halter gegenüber dem Geschädigten (Gefährdungshaftung). Für technische Fehler / Produktfehler / technisches Versagen haftet der Hersteller, eine Versicherung wird den Hersteller im Rahmen der Produkt- und Produzentenhaftung in Anspruch nehmen. Auf die Automatisierung unter dem Begriff Industrie 4.0 bezogen besteht die Problematik der Haftung für ein Fehlverhalten der Systeme[41]. Beim Automatisierten Fahren stellt sich die Frage, wer den Unfall zu verantworten hat. Hier besteht eine Rechtsunsicherheit, da jeweils zu prüfen ist, ob ein Fehler der automatisierten Steuerung vorliegt und dieser einen Produktfehler darstellen kann (was zur Herstellerhaftung führt) oder ob eine Verantwortlichkeit des Fahrers vorliegt, der dann straf- und zivilrechtlich haften könnte.

[37] vgl. Spindler, Rechtsprobleme Industrie 4.0 – Einführung und Überblick vom 15. April 2016, Folie 9; Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 38
[38] Roboter haften nicht, Interview von Jutta Witte mit Professor Eric Hilgendorf, 15.11.2013, Ausgabe 46, www.vdi-nachrichten.com/Technik-Wirtschaft/Roboter-haften nicht, Abruf vom 20.11.2015
[39] Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 39
[40] Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 39
[41] vgl. Bräutigam / Klindt, NJW 2015, 1137, 1138

Diese spezielle Gefährdungshaftung aus dem Bereich des Automatisierten Fahrens ist im Rahmen von Industrie 4.0 nicht auf alle Anwendungen übertragbar. Eine verschuldensunabhängige Haftung für die Systeme scheidet mithin aus. Soweit erlerntes Verhalten der Software für den Verwender nicht vorhersehbar ist, wird man ihm regelmäßig kein Verschulden vorwerfen können. Eine Haftung kommt nur dann in Betracht, wenn der Verwender beim Einsatz des Systems mangelhafte Sorgfalt hat walten lassen[42].

Gefährdungshaftung für autonome Systeme

Eine Lösungsmöglichkeit ist die Einführung einer Gefährdungshaftung[43], vielleicht wie die für Tierhalter. Bei einer Gefährdungshaftung soll immer derjenige, der zu seinem Nutzen rechtmäßig einen gefährlichen Betrieb eröffnet und unterhält, den Schaden tragen, der in der Verwirklichung des Risikos bei einem anderen entsteht und von diesem nicht verhindert werden kann.[44] Allerdings wird hier allein der Gesetzgeber in der Lage gesehen, einen neuen Gefährdungshaftungstatbestand für den Einsatz künstlicher Intelligenz zu etablieren. Begründet wird dies damit, dass die verschuldensunabhängige Gefährdungshaftung Ausnahmecharakter hat.

Für die Begründung von Schadensersatz ist eine Kausalität zwischen Schädigungshandlung und dem entstandenen Schaden notwendig, diese Zuordnung ist derzeit jedoch noch problematisch.[45] Kausalitätsabläufe sind heutzutage nachvollziehbar, in einer vollständig oder weitgehend vernetzten Welt könnten solche Abläufe kaum noch erkennbar sein. [46]

Hinsichtlich digitaler Prozesse wird die Ansicht vertreten, dass sich Systemzugänge, Daten- und Prozessveränderungen meistens gut protokollieren und nachvollziehen lassen. Damit wäre auch überprüfbar, welche Partei und in welchem Umfang eine Schadensursache gesetzt hat und damit dafür verantwortlich ist.[47] Zu beachten ist aber, dass zur Nachweisbarkeit vertraglich sichergestellt werden sollte, dass die Vertragspartner Zugang zu den Daten haben.[48]

[42] vgl. Bräutigam / Klindt, NJW 2015, 1137, 1138
[43] vgl. Spindler, Rechtsprobleme Industrie 4.0 – Einführung und Überblick vom 15. April 2016, Folie 9
[44] vgl. Bräutigam / Klindt, NJW 2015, 1137, 1138
[45] vgl. Hötitzsch, Industrie 4.0 - Rechtliche Perspektiven der Smart-Factory, www.heise .de, Abruf vom 10.11.2015
[46] vgl. Hötitzsch, Industrie 4.0 - Rechtliche Perspektiven der Smart-Factory, www.heise .de, Abruf vom 10.11.2015
[47] Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 38
[48] Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 38

Kooperieren mehrere Partner in einem Projekt oder wirken mehrere autonome Systeme zusammen, könnte aber eine Identifizierung eines einzelnen Fehlers und die daraus resultierende Verantwortlichkeit schwierig sein. Gemäß § 830 Abs. 1 BGB tritt ihn einem derartigen Fall eine Gesamtschuldnerhaftung ein. Dies geschieht jedoch nur innerhalb einer deliktischen Haftung.[49] Daher wird empfohlen, bei unklaren Verursachungsbeiträgen für eine vertragliche Haftung vorab Regelungen zu treffen. Dazu gehört auch, die Haftungsbeiträge zu beziffern. Hier könnte der Anteil der einzelnen Partner an der Wertschöpfung, am Auftragswert usw. als Maßstab der Verteilung dienen.[50]

Die Systeme und Vernetzungen werden komplexe Gebilde schaffen, einzelne Fehler könnten sich dann unvorhersehbar auswirken. Der Zusammenhang von Ursache und Wirkung wird möglicherweise schwer feststellbar sein. Ein weiteres Problem würde auftreten, wenn der Fehler in einer nachträglichen Analyse nicht mehr reproduzierbar und rückverfolgbar sein wird.

Eigenhaftung von Systemen

Neben einer Gefährdungshaftung könnte auch eine Regelung dahingehend entwickelt werden, dass die vollständig autonom agierenden Systeme für sich selbst haften.[51] Die Haftung würde sich nach den allgemeinen Grundsätzen begründen lassen. Zur Absicherung der möglichen Schadensersatzforderungen könnte durch den Hersteller und den Betreiber des eingesetzten Systems eine Haftungsmasse angelegt werden. Hier wird die Ansicht vertreten, dass solange Handlungen auf Personen zurückgeführt und Produktfehler identifizierbaren Bereichen menschlichen Fehlverhaltens zugeordnet werden können, die Abgrenzung von Risikosphären der Rechtsprechung zum existierenden Recht überlassen werden kann. Die Grenze ist dort, wo die totale autonome Steuerung eintritt und dem Menschen keine Entscheidungshoheit und Eingriffsmöglichkeit mehr bleibt.[52]

Ähnlich wie bei den verschiedenen Automatisierungsstufen des Automatisierten Fahrens bestehen die Schwierigkeiten im Rahmen der Haftung darin, den Umfang der Verantwortlichkeit festzustellen. Inwieweit agierte eine Maschine autonom, wie weit waren noch menschliche Handlungen möglich, und konnte der Mensch zur Durchführung

[49] Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 38; Spindler, Rechtsprobleme Industrie 4.0 – Einführung und Überblick vom 15. April 2016, Folie 9
[50] Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 38
[51] vgl. Hötitzsch, Industrie 4.0 - Rechtliche Perspektiven der Smart-Factory, www.heise .de, Abruf vom 10.11.2015
[52] Vgl. Bräutigam / Klindt in Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung, BDI und Noerr, November 2015, S. 14

einer Handlung die Kontrolle von der Maschine zurückerlangen. Zu prüfen ist, wieweit der Mensch die Verantwortung übernehmen konnte oder inwieweit kann sie ihm zugerechnet werden.

Nach anderer Ansicht könnte bei Autonomen Systemen eine Verantwortungszuordnung nach den überkommenen Kausalitäts- und Zurechnungsprinzipien unmöglich sein[53]. Auch wird der Ansatz vertreten, dass man die Hersteller autonomer Maschinen verpflichten könnte, diese nur mit entsprechendem Versicherungsschutz auf den Markt zu bringen[54]. Nach anderer Ansicht ist in vernetzten Wertschöpfungsketten künftig zwischen der Haftung für fehlerhafte Datenquellen und Datenerzeugung einerseits und Fehlern in der Datenübermittlung andererseits zu unterscheiden[55]. Vielleicht reicht es jedoch auch aus, die bestehenden Haftungsregelungen beizubehalten und lediglich für die existierenden Graubereiche gesetzgeberisch Klarstellungen zu schaffen. Ein Ansatz könnte darin zu sehen sein, ein Gesetz über die Haftung für robotische Systeme mit kodifizierten Anforderungen für Betreiber und Hersteller zu entwickeln[56].

8. Produkthaftung

Auch hinsichtlich produkthaftungsrechtlicher Ansprüche ist fraglich, ob die Regelungen zur Produkthaftung im Falle zunehmender Automatisierung in gleichem Umfang angewendet werden können. Maßgebliche Grundlage ist das Produkthaftungsgesetz.

§ 1 ProdhaftG bestimmt den Schadensersatz des Herstellers. „Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen…“

Das Produkthaftungsgesetz begründet damit eine verschuldensunabhängige Haftung. Daher haftet der Hersteller auch dann, wenn ihm weder Vorsatz noch Fahrlässigkeit zur Last gelegt werden kann. Voraussetzung ist, dass ein Fehler nach dem Produkthaftungsgesetz vorliegt, also wenn die unter Berücksichtigung aller Umstände berechtigten Sicherheitserwartungen des Verbrauchers nicht erfüllt werden.

[53] Vgl. Bräutigam / Klindt in Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung, BDI und Noerr, November 2015, S. 14
[54] Roboter haften nicht, Interview von Jutta Witte mit Professor Eric Hilgendorf, 15.11.2013, Ausgabe 46, www.vdi-nachrichten.com/Technik-Wirtschaft/Roboter-haften nicht, Abruf vom 20.11.2015
[55] Alexander Duisberg, Rechtsanwalt bei Bird& Bird München, in: Müller-Tauber, Industrie 4.0 und Recht – Rechtlich smart in die Zukunft in Wirtschaft – Das IHK-Magazin für München und Oberbayern 5/2015, www.muenchen.ihk.de/de/WirueberUns/Publikationen/magazin
[56] vgl. Hötitzsch, Industrie 4.0 - Rechtliche Perspektiven der Smart-Factory, www.heise .de, Abruf vom 10.11.2015 mit Verweis auf Jochen Hanisch, Zivilrechtliche Haftungskonzepte für Roboter, in: Hilgendorf / Günther, Robotik und Gesetzgebung, Nomos-Verlag 2013, S. 109 ff.

Nach dem Produkthaftungsgesetz haftet der Hersteller. Dazu zählen

- der tatsächliche Hersteller des Endprodukts,
- der Hersteller eines Teilprodukts oder eines Grundstoffs, sofern dieses tatsächlich fehlerhaft war,
- der Importeur, der ein Produkt in die EU einführt, der Händler, soweit er auf dem Produkt seinen Namen, sein Warenzeichen oder ein anderes unterscheidungskräftiges Kennzeichen anbringt,
- sowie der Lieferant, wenn der Hersteller des Produkts nicht festgestellt werden kann. Dies gilt nicht, wenn der Lieferant innerhalb eines Monats den Namen seines Vorlieferanten oder Herstellers mitteilt.

Es haftet somit der Hersteller für die Schäden, die durch sein Produkt entstehen. Wenn eine autonom handelnde Maschine nun einen Mitarbeiter verletzt, wäre grundsätzlich der Hersteller der Maschine für den Schaden verantwortlich. Im Rahmen von Regressmöglichkeiten wird sich der Hersteller der Maschine an den Softwarehersteller wenden, wenn Ursache des Unfalls eine fehlerhafte Programmierung von Software war, die der Maschinenhersteller für seine Maschine hinzugekauft hat. Fraglich ist, inwieweit Maschinenhersteller jedoch für Fehler seiner autonom arbeitenden Maschine verantwortlich gemacht werden kann.

Bislang nur wenig wird die zerstörende Dritteinwirkung (Sabotage) in der Rechtswissenschaft diskutiert[57]. Die Verflechtung von Produktsicherheit und IT-Sicherheit wird als neue Herausforderung angesehen. Die Frage nach der Sabotagefestigkeit muss gestellt werden, es wird nach einer Ansicht zukünftig einen rechtlichen Tatbestand erwarteter Widerstandsfähigkeit gegen Eingriffe von außen geben. Dazu besteht allerdings weitergehender Klärungs- und Forschungsbedarf.[58]

Als Empfehlung wird angesichts der gesetzlich festgelegten und nicht beschränkbaren Produkthaftung angeregt, das Augenmerk auf die Qualitätssicherung zu legen und ihr einen hohen Stellenwert einzuräumen. Eigene Prozesse müssten der Qualitätssicherung unterliegen. Regelmäßige Funktionstests und Audits durch Dritte helfen dabei. Und die IT-Sicherheit sollte dabei mit umfasst sein.[59]

+++

[57] vgl. Bräutigam / Klindt, NJW 2015, 1137, 1142
[58] vgl. Bräutigam / Klindt, NJW 2015, 1137, 1142
[59] Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016, S. 39

Provider, Plattformen und Netze

Martin Heitmüller, Rechtsanwalt, Maître en Droit (F)
Herfurth & Partner Rechtsanwaltsgesellschaft mbH

In der vernetzten Produktion wird es einen erheblichen Bedarf an Infrastruktur für das Vorhalten, den Austausch und die Verarbeitung von Daten geben. Dabei sind Strukturen nach ihrem Zweck zu unterscheiden, ob sie lediglich unilateral durch ein Unternehmen genutzt werden oder multilateral durch mehrere bzw. viele Teilnehmer.

1. Provider

1.1. Funktionen

Unilaterale Strukturen dienen den Interessen eines Unternehmens, indem dieses seine Daten und Prozesse an ein konkretes Rechenzentrum (*Host*) oder an Anbieter von Serverkapazitäten (*Cloud*) auslagert, gegebenenfalls auch mit ausgelagerter Software (*Software as a service*) oder als ausgelagerte Gesamtabwicklung von betrieblichen Funktionen (*Outsourcing*). Dabei können diese Dienste durchaus auch Dritten zur Verfügung gestellt werden, etwa als Online-Bestellplattform, Internetpräsenz, Serviceportal oder anderes – es bleibt aber stets bei dem Angebot des einen Unternehmens.

1.2. Leistungen

Die wesentliche rechtliche Problematik besteht dabei in der Gewährleistung der Funktionalität der Providerdienste zur Verfügbarkeit und Sicherheit der Daten, definiert nach Leistungsebenen auf Grundlage vertraglicher Vereinbarungen und Leistungsbeschreibungen (*service level agreements*). Bereits heute dürfte die Leistungsfähigkeit und Sicherheit von Rechenzentren den IT-Strukturen in den meisten Unternehmen überlegen sein, bzw. nicht mit vertretbarem Aufwand von mittelständischen Unternehmen erreichbar sein. Unternehmen, die ihre Daten und Prozesse einem Provider anvertrauen, müssen allerdings nicht nur die Funktionalität vertraglich sicherstellen, sondern auch den Schutz ihrer Daten vor unbefugten Zugriffen.

1.3. Datenbestände

Provider haben regelmäßig kein eigenes begründetes Interesse an den fremden Daten ihrer Kunden, da sie lediglich im Wege der Auftragsverarbeitung damit befasst sind und die Daten nicht integraler Teil einer Produktions- oder Leistungskette sind. Daher dürfen Provider ihre Kundendaten nicht für eigene Zwecke nutzen oder Dritten verfügbar machen. Unternehmen als Kunden sollten sich vom Provider garantieren lassen, dass nur befugte Mitarbeiter Datenzugang erhalten und dass diese durch entsprechende Vertraulichkeitsvereinbarungen verpflichtet werden. Aus Sicht des Unternehmens müssen Unternehmensdaten gegen Einblicke Dritter geschützt werden und Personendaten nach den Vorgaben des Datenschutzrechts. Die Bedeutung von Zertifizierungen für Provider wird weiter zunehmen, insbesondere soweit sie die Einhaltung der Vertraulichkeitspflichten des Providers nachweisen.

1.4. Datenschutz

Auch im Verhältnis zum Provider unterliegt das Unternehmen den nationalen und europäischen Datenschutzbestimmungen, deren Wirksamkeit mit der demnächst zu erwartenden Verabschiedung der Europäischen Datenschutzgrundverordnung deutlich erhöht werden dürfte. Die Auslagerung von europäischem Datenschutz unterliegenden Personendaten auf Server in Drittstaaten ist bislang kaum rechtlich einwandfrei möglich, ebenso wenig der Zugriff von dort. Die von der Europäischen Kommission abgesegnete Praxis zur Datenübermittlung an Empfänger in den USA nach dem Konzept von *safe harbor* hat der EuGH in 2015 als unzulässig beurteilt[60]: die staatlichen Zugriffsrechte in den USA stellen den dortigen Datenschutz nicht dem in der EU gleich. Ob sich die Qualität effektiv durch die mit der EU-Kommission abgestimmten Musterklauseln zwischen Unternehmen im Sinne eines geschützten Datenumfelds herbeiführen lässt, ist zweifelhaft. Daraufhin hat die EU-Kommission mit der US-Regierung ein neues Konzept abgestimmt: *privacy shield*. Der Rechtscharakter, die inhaltliche Reichweite und die faktische Zuverlässigkeit dieses neuen Übereinkommens erscheinen vielen Datenschützern aber noch als unzureichend.

2. Plattformen

2.1. Funktionen

Plattformen dienen als multilaterale Strukturen der Verknüpfung vieler, voneinander unabhängiger Nutzer. Sie stellen eine Infrastruktur zur Verfügung, auf der die Nutzer sich bewegen und ohne Zutun des Plattformbetreibers miteinander in Verbindung treten und Transaktionen abwickeln können.

[60] Urteil des EuGH vom 06.10.2015 in der Rechtssache C-362/14.

Im Grundsatz sind Plattformen nach ihrer Funktion zu unterscheiden; sie sind Informationsplattform (*google*), Kontaktplattform (*facebook,* diverse Partnersuchportale), Kommunikationsplattform (*whats app*), Archivplattform (*Instagram),* Handelsplattform *(ebay,* Reiseportale*,* Autoportale, Immobilienportale, Finanzdienstleistungsportale*),* Verkaufsplattform *(Amazon),* Zahlungsverkehrsplattform *(paypal)* und anderes mehr. Dabei mischen sich Funktionalitäten im Rahmen von *Social Media* Angeboten, bis hin zu sich widersprechenden Angeboten wie unabhängige Preisvergleiche und Produktverkauf. Ob ein Portal rechtlich eine Plattform darstellt, bestimmt sich nach seiner konkreten Struktur.

Plattformen lassen sich nach ihrem Leistungsbild unterscheiden[61]:

- Content Provider — veröffentlicht eigene Inhalte
- Host Provider — stellt Speicherplatz bereit
- Access Provider — schafft Zugang zum Internet
- Usenet Provider — bietet Netzwerke für Diskussionsforen

Die besonderen rechtlichen Fragen zu Plattformen hängen mit einer nicht immer klar definierten Haftung für die Angebote und Transaktionen ihrer Nutzer zusammen. Grundsätzlich wird ein Plattformbetreiber die Gewährleistung und Haftung für Leistungsmängel seiner Nutzer vertraglich ausschließen, er will nicht für die Qualität der auf der Plattform vertriebenen Produkte rechtlich einstehen müssen, auch nicht für die Seriosität und Bonität von Anbieter und Nachfrager. Dass ein Plattformbetreiber ein geschäftliches Interesse an einem möglichst zuverlässigen Kundenportfolio hat, ist eine andere Frage, die er gerne mittels Kundenbewertungen beantwortet. Ob sich ein Plattformbetreiber auch dann von einer Haftung freizeichnen kann, wenn er die Verkaufsbedingungen für Transaktionen seiner Nutzer einheitlich vorgibt, ist zweifelhaft – er rückt damit möglicherweise aus Sicht des Nutzers nahe an das Bild als Anbieter der Leistung.

Kritisch ist auch die Haftung des Plattformbetreibers für rechtswidrige Inhalte, die von Nutzern eingestellt werden. Während in Kommunikationsplattformen die Verletzung von Persönlichkeitsrechten (eigenes Bild) und öffentlich-rechtlichen Schranken (Gewaltverherrlichung, Volksverhetzung u.a.) im Vordergrund steht, liegen die Risiken in Informations- und Handelsplattformen in Verletzungen des Urheberrechts, Designrechts, Markenrechts und anderer gewerblicher oder geistiger Schutzrechte. Die Haftung für derartige rechtswidrige Inhalte wird zurzeit von der Rechtsprechung nicht einheitlich behandelt: regelmäßig ist ein Plattformbetreiber verpflichtet, auf Verlangen des Verletzten rechtswidrige Angebote auf seiner Plattform zu entfernen, stets wenn eine gerichtliche Verfügung dies anordnet. Die Rechtsprechung hat aber inzwischen in Einzelfällen auch die Forderung aufgestellt, dass der Plattformbetreiber verpflichtet sein soll, die Rechtmäßigkeit der bei ihm eingestellten Angebote eigenständig zu überprüfen, jedenfalls wenn es sich um Wiederholungen einer bereits festgestellten Verlet-

[61] Rechtliche Aspekte von Industrie 4.0, Hochstrat u.a.

zung handelt. Gegen derartige Prüfungspflichten wenden sich die Plattformbetreiber mit dem Argument, dass eine Plattform einer Messe, einer Börse oder dem Anzeigenteil einer Publikation vergleichbar sei, nicht aber selbst Anbieter ist. Die Unterscheidung ist deshalb von Brisanz, weil die Entfernung von Inhalten nur eine Unterlassungspflicht darstellt, eine Verletzung einer Prüfungspflicht aber einen Schadensersatzanspruch mit weitreichenden Folgen begründen könnte.

Hinsichtlich der Haftung von Plattformen und deren Providern für Inhalte empfiehlt sich eine Differenzierung[62]:

- Content Provider — volle Haftung für Inhalte
- Host Provider — mit Sperrpflichten für Inhalte
- Access Provider — ohne eigene Sperrpflicht für Inhalte
- Usenet Provider — keine Haftung für Inhalte

Diese bislang überwiegend in Sozialen Medien und in Handelsplattformen auftretenden Verletzungen können in ähnlicher Form auch in industriellen Plattformen auftreten, etwa für den Einkauf, in der Logistik oder zum Personaleinsatz (*crowd working*). Dabei kann es sich um Verletzungen von technischen Schutzrechten (Patente, Muster, Design, auch Urheberrecht für Software) handeln, aber auch um die Bereitstellung von rechtswidrig erlangten Personendaten oder Unternehmensdaten. Greift ein Verletzter oder vermeintlich Verletzter die Veröffentlichung einer Information auf der Plattform an, kann die Entscheidung zur Entfernung des Angebots erhebliche wirtschaftliche Folgen für den Plattformbetreiber und den Anbieter mit sich bringen. Der Plattformbetreiber wird wegen des Schadenersatzrisikos dazu neigen, dem Verlangen nach dem Entfernen des Angebots nachzukommen, der Anbieter verliert damit zumindest vorübergehend sein Angebot auf der Plattform und damit möglicherweise Geschäft.

2.2. Einzelheiten zur Plattformhaftung[63]

Der Grundsatz - Notice and take down

Das aufgrund der europäischen E-Commerce-Richtlinie aus dem Jahr 2000 beruhende Telemediengesetz (TMG) hat in § 10 das sogenannte Notice and take down-Prinzip gesetzlich festgeschrieben. Danach sind Diensteanbieter für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben (§ 10 Nr. 1 TMG) oder wenn sie unverzüglich tätig werden, um die Information zu entfernen oder den Zugang zu ihr zu

[62] Rechtliche Aspekte von Industrie 4.0, Hochstrat u.a.
[63] vgl. hierzu Härting, Internetrecht, 5. Aufl., Rn. 2131ff.

sperren, sobald sie diese Kenntnis erlangt haben (§ 10 Nr. 2 TMG). Die Vorschrift § 10 TMG ist auf den klassischen Host-Provider zugeschnitten.

Das Urteil des BGH „Internet-Versteigerung I“

Durch das Urteil des BGH aus dem Jahr 2004, das sogenannte Internet-Versteigerung I-Urteil, kam der Notice and take down-Grundsatz jedoch ins Wanken. Rolex gab sich im Streit mit der Internetplattform ricardo.de nicht mit dem Herausnehmen der Ware aus dem Angebot nach Kenntniserlangung zufrieden, sondern verlangte zusätzlich, dass solche Verstöße auch für die Zukunft unterlassen werden.

Der BGH wendete die Haftungsprivilegierung des Notice and take-Down-Grundsatz aus dem seinerzeit noch geltenden § 11 Teledienstegesetz (TDG) nicht an mit der Begründung diese gelte nur für Schadenersatzansprüche, nicht jedoch für in die Zukunft wirkende Unterlassungsansprüche. Der BGH sah jedoch auch, dass eine zu stark ausgeweitete Unterlassungsverpflichtung, die dazu führt, jedes Angebot vor der Veröffentlichung im Internet auf Rechtsverletzung zu untersuchen, zu weit gehen würde und das ganze Geschäftsmodell in Frage stellen würde.

Es wurde daher entschieden, dass eine Unterlassungspflicht im Rahmen einer Störerhaftung nur im Falle einer Verletzung von Prüfpflichten anzunehmen ist. In dem entschiedenen Fall musste die beklagte Internetplattform die Vorfälle mit den Rolex-Uhren zum Anlass nehmen, Angebote solcher Uhren einer besonderen Prüfung zu unterziehen. Welche technischen Möglichkeiten hierbei zur Verfügung stehen, z.B. eine spezielle Software, war in dem Verfahren streitig.

Die weitere Entwicklung: das BGH-Urteil „Jugendgefährdende Medien bei eBay“

In seinem Urteil „Jugendgefährdende Schriften bei eBay“ aus dem Jahr 2007 konkretisierte der BGH die u.a. in der Entscheidung „Internet-Versteigerung I“ begründete Rechtsprechung weiter.

Auch bei diesem Urteil ging es um die Begründung von Unterlassungspflichten. Anlass waren hierbei nicht die Verletzung von Markenrechten, sondern die Verbreitung fremder jugendgefährdender Inhalte. Die Unterlassungspflichten wurden diesmal aus dem Wettbewerbsrecht hergeleitet.

Nach dem Bundesgerichtshof war die beklagte Internetplattform nicht nur verpflichtet, das konkrete jugendgefährdende Angebot, von dem sie Kenntnis erlangt hatte, unverzüglich zu sperren. Sie müsse ferner auch Vorsorge dafür treffen, dass es möglichst nicht zu weiteren gleichartigen Rechtsverletzungen kommt.

In dem Urteil wurde klargestellt, dass solche gleichartigen Rechtsverletzungen nicht nur Angebote sind, die mit den bekannt gewordenen Angeboten identisch sind, also das Angebot des gleichen Artikels durch denselben Versteigerer betreffen. Die beklagte Plattform hat nach dem Urteil auch zu verhindern, dass die ihr konkret benannten jugendgefährdenden Medien durch andere Bieter erneut über ihre Plattform angeboten werden.

Ferner kämen als gleichartig mit einem bestimmten Verstoß gegen das Jugendschutzrecht auch solche Angebote in Betracht, bei denen derselbe Versteigerer auf demselben Trägermedium Inhalte derselben jugendgefährdenden Kategorie anbietet.

Tendenzwende: Einschränkung der Prüfungspflicht der Plattformbetreiber, das BGH-Urteil „Kinderhochstühle im Internet“

In einem Urteil aus 2012 schränkte der BGH die Prüfungspflicht der Plattbetreiber jedoch wieder ein. Nicht mehr zumutbar seien Kontrollmaßnahmen, bei denen durch die Filtersoftware Verdachtsfälle von Markenverletzungen nicht aufgespürt werden können, sondern jedes Angebot, dass die klagegegenständlichen Marken enthält, zusätzlich noch einer manuellen Kontrolle unterzogen werden muss. Eine so weitgehende Kontrollpflicht lehnte der Bundesgerichtshof ab.

Fazit

Die ausschnittsweise dargestellte Rechtsprechung zeigt, dass die Rechtslage zur Plattformhaftung noch sehr unübersichtlich, von verästelter Rechtsprechung geprägt und schwer prognostizierbar ist. Diese Rechtsunsicherheit ist für den Markteintritt von neuen Industrie 4.0-Plattformen sicherlich nicht förderlich. Im Moment muss mit dieser Rechtsunsicherheit jedoch gezwungenermaßen kalkuliert werden. Die weiteren Entwicklungen sind eng zu verfolgen.

3. Telekommunikationsrecht

Die Betrachtung des Telekommunikationsrechtes ist für das Thema Industrie 4.0 von daher von Bedeutung, als dass in den meisten Fällen die M2M-Daten über ein Mobilfunknetz übertragen werden. Insbesondere die Übermittlung von Daten und das Angebot von Diensten im Rahmen der M2M-Kommunikation können die Beteiligten bestimmten Pflichten aus dem Telekommunikationsrecht unterwerfen.

Die Übermittlung von Daten stellt rechtlich in der Regel Telekommunikation dar und umfasst häufig Telekommunikationsdienste im Sinne des Telekommunikationsgesetzes

(TKG).[64] Es kommt dabei nicht darauf an, dass die Informationen in der Telekommunikation von Mensch zu Mensch übermittelt werden.

Die Kommunikationsinfrastruktur besteht zumeist in Form von Mobilfunknetzen, so dass die Netzbetreiber „Erbringer" der TK-Leistungen sind, Vertragspartner für bestimmte Dienste „Teilnehmer" und die Kunden der Dienste, z.B. Fahrer von *Connected Cars*, „Nutzer" im Sinne des TKG.

Ob es sich bei M2M-Kommunikationsplattformen um Telekommunikationsdienste handelt, hängt von der konkreten Funktion ab: die Übermittlung von Steuersignalen von und an beteiligte M2M-Geräte ist in der Regel ein Telekommunikationsdienst, bei der Bereitstellung von Inhalten auf der Plattform zum Abruf durch Nutzer ist die Übermittlung hingegen nicht das wesentliche Element. Zur Abgrenzung des Charakters gemischter Dienste wird gerne das ISO/OSI Schichtenmodell für Internetdienste herangezogen[65]. Die Schichten 1 bis 4 haben eher Übertragungscharakter, die Schichten 5 bis 7 eher Inhaltscharakter.

M2M-Dienste stellen in der Regel nicht die Übertragung von Informationen in den Vordergrund, sondern Inhalte und Funktionalitäten wie z.B. Fahrzeugdaten (Fahrweise, Ortung); sie sind damit typischerweise keine Telekommunikationsdienste, sondern Telemediendienste im Sinne des Telemediengesetzes (TMD).

Unterfällt ein M2M-Dienst dem TKG, hat der Erbringer der Dienste eine Anzahl von Pflichten zu erfüllen, die sich auf Kundenschutz, Frequenznutzung, Nummerierung, Fernmeldegeheimnis und TK-Überwachung beziehen. In Bezug auf die Haftungsverpflichtungen ist hervorzuheben, dass nach § 44a Satz 1 TKG die Anbieter von TK-Diensten für fahrlässig herbeigeführte Vermögensschäden ihrer Endnutzer nur in einem Umfang von 12.500,-- € pro Schadenfall und Endnutzer haften. Diese Summe kann im Rahmen der M2M-Kommunikation schnell überschritten werden und es sollte daher über eine vertragliche Erhöhung der Haftungssummen nachgedacht werden.[66]

+++

[64] Grünwald/Nüßing MMR 2015, 378, 379f.
[65] Schütz, in Beck, TKG, 4. Aufl. 2013, § 6 Rdnr. 35 ff
[66] Grünwald/Nüßing a.a.O.

Technologie & Daten

Industrie 4.0 und Datenschutz

Dennis Jlussi, Rechtsanwalt
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

1. Einleitung

Die fortschreitende Integration neuester Informations- und Kommunikationstechnologien in industrielle Fertigungsprozesse – Industrie 4.0 – wirft mehr und mehr rechtliche Fragen im Zusammenhang mit Daten auf. Die rechtlich zu bewertenden Sachverhalte sind dabei nicht durchgängig im strengen Sinn völlig neu, sie erreichen aber neue Dimensionen; dies rührt hauptsächlich aus der noch konsequenteren und weiterreichenden Umsetzung datengestützter Prozesse her (Big Data – sozusagen *even bigger*). Da das Datenschutzrecht zu einem praktisch überwiegenden Teil aus rechtlichen Abwägungen besteht, können Maßnahmen, die gleichartig, jedoch intensiver sind, durchaus zu anderen rechtlichen Bewertungen führen.

Dabei stellen sich hauptsächlich Fragen in den Bereichen Arbeitnehmerdatenschutz, Kundendatenschutz und technischer Datenschutz, letzteres sowohl hinsichtlich personenbezogener als auch betrieblicher Daten.

2. Datenschutz und Innovation im Spannungsverhältnis

Datenschutz(-recht) und Innovation stehen in einem beinahe natürlichen Spannungsverhältnis. Gegenüber technischen Neuentwicklungen, die schnell und international sind, ist das Recht träge und national oder bestenfalls europäisch.
Die Grundlagen des heutigen Datenschutzrechts basieren auf der europäischen Datenschutzrichtlinie 95/47/EG, die im Oktober 1995 beschlossen wurde. Selbst wenn man den vorherigen jahrelangen Beratungsprozess unberücksichtigt lässt: Die EDV-Landschaft 1995 bestand aus Windows 95, das noch standardmäßig ohne das Internetprotokoll TCP/IP und ohne Internetbrowser daherkam. Elektronische Informationen wurden zumeist auf Disketten verbreitet, CD-ROM-Laufwerke erfuhren erste Verbreitung. Von der ubiquitären Verfügbarkeit von Informationen, deren weltweiter Übermittlung praktisch in Echtzeit und den damit verbundenen Chancen und Risiken für Persönlichkeitsrechte und Unternehmensdaten haben der europäische und der nationale Gesetzgeber damals nichts geahnt.

Auch wenn das Datenschutzrecht durch kleinere Anpassungen am Gesetz, durch Sonder-Datenschutzrecht für Telemedien und elektronische Kommunikation sowie durch die Rechtsprechung bis hin zum Bundesverfassungsgericht zwischenzeitlich punktuell aufgefrischt wurde, so hat sich an der grundlegenden Erkenntnis wenig geändert: Es

bedarf einiger gedanklicher Anstrengungen, um das Datenschutzrecht als Maßstab an moderne datenbasierte Produkte und Prozesse anzulegen. Dabei verbleiben jedenfalls am *Cutting Edge* immer rechtliche Risiken, die sich durch geschickte juristisch begleitete Entwicklung minimieren, aber nicht völlig ausschließen lassen.

Übrigens: Die Datenschutz-Grundverordnung, die bei Verfassung dieser Zeilen noch nicht einmal formell beschlossen war und voraussichtlich erst im Laufe des Jahres 2018 effektiv in Kraft getreten sein wird, basiert auf dem im Jahr 2011 verfassten (und vermutlich teilweise noch davor konstruierten) Entwurf der Europäischen Kommission und hängt damit der technischen Entwicklung bereits bei Inkrafttreten eine dreiviertel Dekade hinterher.

3. Arbeitnehmer-Datenschutz

Manche Zukunftsszenarien der *Smart Factory* sehen menschenlose Fabriken vor. Die möglichen gesellschaftlichen Auswirkungen einer eventuellen dahingehenden Entwicklung sollen nicht das Thema dieser Abhandlung sein; der Autor geht davon aus, dass auf absehbare Zeit Menschen gebraucht werden, die Maschinen zumindest überwachen und eine Verantwortung für deren reibungsloses Funktionieren tragen.

Selbst wenn die *Smart Factory* mit weniger Menschen auskommt, so folgt daraus nicht das Ende des Arbeitnehmer-Datenschutzes. Im Gegenteil: Je smarter die Fabrik ist, desto mehr Anlass gibt es, über den Schutz der verbliebenen Arbeitnehmer nachzudenken. So werden etwa Roboter, die durch Kamera- und Ultraschallsysteme Menschen erkennen, die sich in ihren Aktionsradius begeben, um Kollisionen und mithin Verletzungen zu vermeiden, Daten verarbeiten, bei denen es sich um personenbezogene Daten handelt.

Dies nämlich sind alle „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ (§ 1 Abs. 1 Bundesdatenschutzgesetz). Damit können Daten einer bestimmten Maschine in einer Fabrik, für die ein bestimmter Mitarbeiter die Verantwortung trägt, als „sachliche Verhältnisse“ personenbezogen sein, jedenfalls wenn die Daten in Abhängigkeit von der Person stehen.
Das ist für sich genommen nicht neu; die Möglichkeit, anhand von Chargennummer und Dienstplan die konkret verantwortlichen Arbeiter ausfindig zu machen, dürfte bald so alt sein wie die Industrie selbst. Neu ist aber, dass es viel mehr Daten über die konkrete Maschine gibt, dass diese Daten übermittelt werden (an andere Maschinen, auf das Produkt, zur Fernüberwachung, an Lieferanten oder Abnehmer) und dass sie im Rahmen von Big-Data-Anwendungen automatisch ausgewertet werden. Bei konsequenter Datenanalyse ergibt sich daraus u.U. eine Komplettüberwachung des Arbeitnehmers hinsichtlich Leistung, Ausschuss, Retouren usw.

Vorzugswürdig ist die Verwendung anonymisierter Daten, also solcher, bei denen die Herstellung eines Bezugs zu bestimmten Arbeitnehmern gar nicht mehr möglich ist. Dies ist nicht immer ohne Verlust der Aussagequalität möglich, aber wo es möglich ist, handelt es sich um die rechtssicherste Methode: Wirksam und endgültig anonymisierte Daten unterliegen keinerlei datenschutzrechtlichen Anforderungen mehr.

Wo keine vollständige Anonymisierung möglich ist, bietet sich zur schonenden Datenverarbeitung eine teilweise Anonymisierung an, die i.d.R. darin besteht, eine anonymisierte Kopie eines Datensatzes zu erstellen, der dann für zumindest diejenigen Analysen verwendet wird, bei denen dadurch kein Verlust der Aussagequalität einhergeht. In Ausnahmefällen, in denen sensible Daten (z.B. solche, aus denen sich Gesundheitsdaten ablesen lassen) verarbeitet werden und eine Anonymisierung nicht möglich oder nicht erwünscht ist, können die Daten pseudonymisiert und die Zuordnungstabellen getrennt aufbewahrt oder sogar bei einer *Trusted Third Party* (TTP) hinterlegt werden, also bei einem Dritten, einer Art Daten-Treuhänder, wo der Zugriff durch klare, auch zugunsten der Arbeitnehmer wirkende Regelungen an bestimmte Bedingungen geknüpft und darauf beschränkt wird. Jedenfalls muss in aller Regel ausgeschlossen sein, dass der Endkunde oder Dritte in der Liefer- oder Vertriebskette erkennen können, welche Arbeitnehmer an der Herstellung beteiligt waren.

Nicht immer sind besondere Maßnahmen zur Anonymisierung oder Pseudonymisierung notwendig; die vom Datenschutzrecht vielfach vorgesehenen Interessenabwägungen können bei weniger sensiblen Daten auch zu deren Verwendbarkeit „nur“ unter den allgemeinen datenschutzrechtlichen Bedingungen führen. Hierbei sollte der Arbeitgeber jedoch stets die Betriebskultur im Auge haben und den Betriebsrat einbinden: Während manche Belegschaftsvertreter etwa alle Daten, die Rückschlüsse auf die individuelle Leitung von Arbeitnehmern zulassen, ablehnen, halten andere die Verwendung dieser Daten (unter Umständen und Auflagen) für sinnvoll, weil ungeeignete oder besonders motivationsarme Arbeitnehmer auch für die Kollegen eine Belastung darstellen können.

§ 87 Absatz 1 Nummer 6 des Betriebsverfassungsgesetzes kommt insofern eine Schlüsselrolle zu: Danach hat der Betriebsrat ein zwingendes Mitbestimmungsrecht bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Entgegen dem Wortlaut der Norm entspricht es gefestigter höchstrichterlicher Rechtsprechung, dass für die Bestimmung zur Überwachung schon die objektive Geeignetheit ausreichend ist. Die übrigen Details der Regelung sind Gegenstand umfangreicher und nicht immer einheitlicher juristischer Kasuistik, spezielle Fragen im Hinblick auf *Smart Factories* sind jedoch noch offen. Es dürfte in aller Regel kluger Unternehmenspolitik entsprechen, auch um des Betriebsfriedens Willen den Betriebsrat auch dann frühzeitig und kooperativ einzubeziehen und eine Betriebsvereinbarung herbeizuführen, wo die Anwendbarkeit der Vorschrift in Grenzbereichen fraglich ist.

4. Kunden-Datenschutz

Kundendaten stellen für die produzierenden Unternehmen einen wichtigen wirtschaftlichen Wert da. Manche Hersteller haben ihren Vertrieb deswegen auf das sogenannte Agenturmodell umgestellt (und viele mehr denken darüber nach), bei dem die Händler nur noch Handelsvertreter des Produzenten sind, um einfacher an mehr Kundendaten zu gelangen. Mehr, schnellerer und direkter Kundenkontakt ist für viele moderne Prozesse essentiell, etwa im *Lean Development*.

In zunehmendem Maße werden außerdem Produkte nach (End-)Kundenspezifikation hergestellt, die Individualisierung von Gütern verschafft den Herstellern einen Wettbewerbsvorsprung und eröffnet vielfach erst den Zugang zum Premiumsegment des jeweiligen Marktes. Automobile, Möbel, Bekleidung und vorgefertigte Bauteile für Einfamilienhäuser sind dafür nur die prominentesten Beispiele.

Datenschutzrechtlich relevant sind an sich nur die Daten natürlicher Personen. Das ist allerdings nicht auf Verbraucher beschränkt, auch am B2B-Geschäft sind mit Einzelkaufleuten und den Gesellschaftern von Personengesellschaften natürliche Personen beteiligt; die dabei auftretenden Fragen und Varianten sind vielfältig, aber die Formulierung abstrakter Vorgehensweisen wird sich an den restriktiv zu handhabenden Fällen zu orientieren haben, so dass letztlich in der Regel von der Geltung des gleichen Datenschutzniveaus wie für Endverbraucher ausgegangen werden sollte. Außerdem wird von einem Hersteller gegenüber seinen gewerblichen Kunden häufig ein ähnliches Schutzniveau schon um der geschäftlichen Diskretion Willen erwartet.

Wenn die Produkte in der *Smart Factory* selbst Daten zur Individualisierung tragen und mit den Maschinen kommunizieren, so sollten in aller Regel die direkten persönlichen Daten (Name, Adresse usw.) des Kunden nicht auch dort gespeichert sein, sondern z.B. eine pseudonyme Kennziffer verwendet werden. Diese Daten sollten nur an diejenigen Stellen weitergegeben werden, bei denen dies zur Vertragserfüllung notwendig ist, und diese Stellen sind zur Einhaltung des Datenschutzrechts zu verpflichten; dazu gehören effektive Kontrollrechte, die nicht nur auf geduldigem Papier bestehen dürfen. Auch hier ist ein höheres Schutzniveau erforderlich, wenn es sich um sensible Daten handelt, z.B. Gesundheitsdaten bei der Produktion von Medizinprodukten. Insoweit bietet sich eine erweiterte Pseudonymisierung an, erforderlichenfalls auch mit einer *Trusted Third Party*.

5. Datensicherheit

Der technische Datenschutz – also die Gewährleistung von Datensicherheit – erfüllt mehrere Zwecke. Einerseits sind seine Grundlagen in § 9 des Bundesdatenschutzgesetzes (nebst Anlage) festgehalten, denn der rechtliche Schutz von Persönlichkeits-

rechten würde leerlaufen, wenn die Daten nicht technisch gegen Missbrauch geschützt würden. Andererseits dient Datensicherheit aber auch unternehmenseigenen Zielen, nämlich der Bewahrung von Geschäftsgeheimnissen und Know-How und der Abwehr von Spionage und Sabotage.

Die geschäftlichen Risiken von Fehlern und Versäumnissen im Bereich der Datensicherheit sind vielfältig. Unternehmen wie Microsoft, Sony, Target, StudiVZ und viele andere können ein Lied davon singen. Wenn die Versäumnisse öffentlich werden, droht ein Reputationsverlust auf der Abnehmer-, aber möglicherweise auch auf der Zulieferseite. Goodwill wird gegenüber dem am öffentlichen Pranger stehenden Unternehmen eher ausbleiben. Es droht auch ein Wertverlust der Marke, was insbesondere bei Unternehmen, die diese in der Bilanz aktiviert haben, problematisch sein kann. Als rechtliche Risiken kommen Bußgelder und Schadensersatz hinzu; nach den allgemeinen Regelungen führen Versäumnisse u.U. auch zur persönlichen Haftung der zuständigen Führungskräfte.

Selbst wenn die Sache nicht öffentlich wird (für personenbezogene Daten wegen der Mitteilungspflicht an die zuständige Datenschutzbehörde schwer vorstellbar), droht der Verlust von exklusivem Wissen und damit eines Wettbewerbsvorsprungs, sowie (bei Sabotage) die Betriebsunterbrechung.

Deswegen sind entsprechende Kriterien auch vorbeugend bei der Risikobewertung zu berücksichtigen. Seit Basel II (unverändert in Basel III) sind IT-Risiken bei den operationellen Risiken des Kreditnehmers zu berücksichtigen („the risk of loss resulting von inadequate or failed internal processes, people and systems“). Die Banken haben sich lange schwergetan mit der Implementierung, zunehmend werden entsprechende Assessments aber vorgenommen oder Zertifizierungen verlangt (z.B. aus der ISO 27000-Reihe). Auch als Gegenstand der Abschlussprüfung (Audit) werden entsprechende Feststellungen rechtlich verlangt; insoweit sind ebenfalls verbindliche Standards erst langsam dabei, sich durchzusetzen, aber es wird daran kein Weg vorbei führen.

In Industrie-4.0-Prozessen und in der *Smart Factory* gibt es ersichtlich zusätzliche Angriffspunkte. Überall, wo Daten zusätzlich erfasst, übertragen oder gespeichert werden, besteht das potenzielle Risiko, dass ein Angreifer die Erfassung, Übermittlung oder Speicherung kompromittieren oder abgreifen könnte. Das heißt, dass innerhalb der Prozesse und Lieferketten, bei dem Austausch von Daten zwischen Maschinen, Produkten, Steuerung, Zulieferern, Vertrieb usw. an jeder Stelle die Daten gesichert werden müssen.

+++

Industrie 4.0 und Dateneigentum

Dennis Jlussi, Rechtsanwalt
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

1. Einleitung

In Zeiten des *Data Mining* werden nicht zufällig Begriffe aus dem Rohstoff- und Edelmetallabbau verwendet: Daten gelten als das Gold der Informationsgesellschaft. Das gilt auch und erst recht für die Industrie 4.0, wobei der etwas unscharfe Begriff hier nicht auf *Smart Factories* beschränkt bleiben muss. Jedenfalls dort allerdings gibt es eine Datenflut von allem, was aufgezeichnet, gemessen und eingegeben wird; aus diesen Daten lassen sich wertvolle Erkenntnisse gewinnen (*Big Data*). In den Bereichen Vertrieb und Kundenzufriedenheit fallen bei modernen Prozessen Daten an, und viele Produkte – gerade im Internet der Dinge – schicken möglicherweise zusätzliche Daten zum Produzenten.

Wem gehören all diese Daten? Und wer kann sie sich also wirtschaftlich nutzbar machen? Für die Beantwortung dieser Fragen gibt es zahlreiche – wie gleich zu zeigen sein wird, jedoch nur inselartig einschlägige – rechtliche Denkansätze. Letztlich bleibt es meistens eine Frage der Vertragsgestaltung.

2. Daten

Bevor die Eigentumsfrage geklärt werden kann, stellt sich zuerst die Frage: Was sind eigentlich Daten? Redet ein Informatiker von „Daten“ oder „Datenschutz“, meint er meistens Daten im technischen Sinn, also elektronisch lesbare Informationen, die entweder auf einem Datenträger gespeichert oder auf einem Signalträger übertragen werden. Mit anderen Worten: Einsen und Nullen. „Daten“ im rechtlichen Sinn sind aber eigentlich Informationen. Nur diese haben auch einen merkantilen Wert. In der digitalen Welt fallen beide Definitionen meistens zusammen, aber nicht immer. Außerdem sollen die folgenden Ausführungen auch noch Geltung beanspruchen, wenn die Daten analogisiert (also z.B. ausgedruckt) wurden.

3. Eigentum an Daten

Das Modell des Eigentums im deutschen Zivilrecht – das „Sachenrecht“ gehört sicherlich zu den ausgefeiltesten und dogmatisch ausgereiftesten juristischen Konstruktionen der Welt. Ihm ist ein ganzes „Buch“ (Oberkapitel) mit knapp 450 Paragraphen im Bürgerlichen Gesetzbuch (BGB) gewidmet; es ist zusätzlich Anknüpfungspunkt in zahlreichen weiteren wichtigen Normen des Zivilrechts.

Zentraler Ausgangspunkt des Sachenrechts ist, dass ein Eigentümer mit seinem Eigentum *„nach Belieben verfahren und andere von jeder Einwirkung ausschließen“* kann (§ 903 BGB). Das heißt: Erstens besteht das Eigentum aus zwei Elementen, einem Nutzungs- und einem Ausschließungsrecht; es gibt dem Eigentümer daher sowohl das Recht, die Sache selbst in beliebiger Weise zu nutzen (und sich nutzbar zu machen), aber eben auch das Recht, darüber zu entscheiden, andere davon abzuhalten.

Das Eigentum ist daher auch ein absolutes Recht, d.h., es wirkt gegenüber jedermann; während Rechte aus Verträgen grundsätzlich nur zwischen den Vertragsparteien gelten, die sich einander ausgesucht haben und den Vertrag miteinander eingegangen sind, gilt das Eigentum und die Rechte daraus automatisch gegenüber jedem Dritten.
Ein entscheidender Unterschied zwischen den Sachen, um die es im Sachenrecht geht, und Daten ist allerdings, dass jede Sache für sich genommen einzig ist. Man kann sie teilen, aber niemals gleichzeitig voll nutzen. Das ist bei Daten anders: Auch wenn der Wert sich häufig erst aus der Exklusivität der Daten ergibt, so kann man sie doch verlustfrei vervielfältigen und jede Vervielfältigung kann voll genutzt werden.

Wegen dieses Unterschieds haben Gedankenmodelle, die Daten wie Sacheigentum behandeln wollen, jedenfalls in jüngerer Zeit keine große Verbreitung gefunden. *Hoeren*[67] plädiert für eine Behandlung wie Eigentum und argumentiert u.a. damit, dass der strafrechtliche Schutz vor Datenveränderung und Computersabotage (§§ 303a, 303b StGB) im Bereich der Sachbeschädigungsdelikte eingeordnet wurde. Er übersieht dabei, dass diese Vorschriften seinerzeit durch das 41. Strafrechtsänderungsgesetz eingeführt wurden, mit dem die Budapester Konvention des Europarates gegen Cybercrime in deutsches Recht umgesetzt wurde; mit §§ 202a und 202b wurden weitere dadurch veranlasste neue Vorschriften gegen das Ausspähen und Abfangen von Daten in einen anderen Bereich, nämlich den der Privatschutzdelikte, eingeordnet. Die Einordnung erscheint danach – wenn man keine neuen Kategorien schaffen wollte – einigermaßen logisch, aber nicht zwingend, und damit eher zufällig – irgendwo musste der Gesetzgeber die neuen Paragraphen ja einordnen.

Zutreffend ist allerdings, dass das Eigentum an dem Datenträger, auf dem die Daten gespeichert sind, einen ersten wichtigen Anhaltspunkt gibt. Wie oben bereits ausgeführt, kann der Eigentümer mit seinem Datenträger verfahren, wie er möchte, also auch die gespeicherten Daten auslesen und verarbeiten – wenn nicht besondere Regeln, die im Folgenden zu besprechen sein werden, dies verhindern. Der Eigentümer (wobei diesem der berechtigte Besitzer z.B. aufgrund eines Pacht-, Miet- oder Leasingvertrags gleich steht) kann sein Nutzungs- und sein Ausschließungsrecht allerdings insoweit nur an dem konkreten Datenträger und den darauf gespeicherten Daten ausüben und aus dem Eigentumsrecht heraus nicht auch an den gleichen Daten auf einem anderen, fremden Datenträger. Hierfür bedarf es andere Rechte.

[67] *Hoeren*, MMR 2013, S. 486.

Der grundrechtliche (Art. 14 des Grundgesetzes) Eigentumsbegriff ist weiter und umfasst auch gesicherte relative Rechte. Diese werden aber jenseits eines Kernbereichs von der Rechtsordnung gestaltet und nicht von Art. 14 GG selbst – aus dem Artikel ein Eigentumsrecht an Daten herauszulesen wäre deshalb ein Zirkelschluss.

4. Geistiges Eigentum

Der Begriff des geistigen Eigentums hat sich – als Übersetzung des angloamerikanischen *Intellectual Property* – auch in der deutschen Sprache langsam durchgesetzt, was manche bedauern. Der veraltende Begriff der Immaterialgüterrechte traf es besser, weil er den Unterschied zu Sacheigentum besser hervorzuheben vermag. Zwar gelten auch Immaterialgüterrechte gegenüber jedermann, aber sie gewähren – mit Nuancen bei den einzelnen Schutzrechten – nur ein Ausschließungs- und kein (volles) Nutzungsrecht.

4.1. Patente und Gebrauchsmuster

Ob überhaupt und welche Daten Gegenstand von Immaterialgüterrechten sein können, ist bislang nur stellenweise geklärt. Im Patentrecht werden „Erzeugnisse“ geschützt, bei Verfahrenspatenten auch die direkten Erzeugnisse des geschützten Verfahrens. Können Daten ein „Erzeugnis“ sein? Für das Gebrauchsmusterrecht („kleines Patent“) hat der Bundesgerichtshof festgestellt, dass auch Daten als Signalfolge unter Umständen geschützt werden können.[68] Diesen Gedanken kann man möglicherweise auf das („große“) Patent übertragen.[69] Für besondere Daten (also nicht Messdaten usw.), die in patentfähigen Industrie-4.0-Prozessen erzeugt werden, kommt bei sorgfältiger Formulierung des Schutzanspruchs in der Patentschrift ein patentrechtlicher Schutz in Frage.

4.2. Urheberrecht

Geistige Werke

Urheberrechtlicher Schutz setzt eine persönliche geistige Schöpfung voraus. Maschinenerzeugte Daten kommen daher nicht in Frage. Auch in *Smart Factories* wird es weiterhin urheberrechtlich geschützte Daten geben, wie etwa die Designs und Konstruktionsskizzen, die in digitaler Form als CAM-Daten Verwendung finden. Ausgangspunkt dieser Daten bleibt dabei aber der Mensch, und für die Rechte an diesen Daten gelten keine anderen Regeln als jeher. Die Versagung urheberrechtlichen Schutzes für ma-

[68] BGH, GRUR 2004, 495 - Signalfolge.
[69] So inzident *Scharen* in Benkard, PatG, 11. Aufl. 2015, § 9 Rn. 31.

schinengenerierte Daten gilt auch für fotografische Daten; auch der einfache Lichtbildschutz (§ 72 UrhG) unterhalb des vollen Urheberrechts erfordert zumindest eine persönliche Herstellung der Fotografie.

Datenbanken

Ein anderes sogenanntes verwandtes Schutzrecht aus dem Urheberrechtsgesetz drängt sich eher auf: Das Datenbankschutzrecht.

Das *Sui-Generis*-Schutzrecht schützt nicht eine persönliche geistige Schöpfung, sondern ist eine Investitionsschutzvorschrift. Das Vorliegen einer Datenbank im informationstechnischen Sinn ist dafür nicht hinreichend (aber auch nicht notwendig); erforderlich ist eine erhebliche Investition in die Beschaffung, Überprüfung oder Darstellung von Daten. Die reine Aufzeichnung von Primärdaten, die in der industriellen Produktion ohnehin anfallen oder mit einfachen Mitteln gemessen werden können, erfüllt diese Voraussetzungen nicht. Gezielt aufwändig gemessene Daten sowie Sekundärdaten komplexer Big-Data-Analysen kommen als Schutzgegenstand hingegen in Frage.

5. Wettbewerbsrecht

Wo die eigentlichen Immaterialgüterrechte versagen, haben Gesetzgeber und Rechtsprechung noch einen ergänzenden Leistungsschutz aus dem Wettbewerbsrecht vorgesehen. Grundsätzlich gelten die Nachahmungsfreiheit und die Freiheit der Nutzung von Informationen. Lediglich dort, wo die Nutzung „unlauter“ ist und zur Ausnutzung wird, kann das Wettbewerbsrecht greifen.

Der Nachahmungsschutz (§ 4 UWG) schützt vor unlauteren Nachahmungen einer Ware oder Dienstleistung. Ob dies für Daten gelten kann, ist bislang ungeklärt; nach der hier vertretenen Ansicht können Daten auch dann Nachahmungen sein, wenn sie eigentlich (digital verlustfreie) Kopien sind. Denkbar ist noch, dass die Daten gar nicht selbst Produkt oder Dienstleistung sind, sondern „die für die Nachahmung erforderlichen Kenntnisse oder Unterlagen“ darstellen, die zur Unlauterbarkeit des Produkts führen, wenn sie unredlich erlangt wurden.

Abseits des Nachahmungsschutzes hat das Fallrecht noch weitere Aspekte der Unlauterbarkeit herausgebildet. Auf hoher Ebene zusammengefasst ist es danach erlaubt, auf Vorleistungen eines Wettbewerbers am Markt aufzubauen, nicht aber diese oder den Ruf des Unternehmens dabei auszubeuten. Die Übertragung dieser Prinzipien auf die Verwendung von Daten ist bislang ungeklärt; nach hier vertretener Ansicht wird die Grenze bei Daten dort überschritten sein, wo ein Unternehmen die Kosten und Risiken

des Produktionsverfahrens trägt und ein anderes die dabei entstehenden wertvollen Daten unredlich abgreift.

Insgesamt bietet das Wettbewerbsrecht (vorbehaltlich der unten diskutierten Geheimschutzrechte) allenfalls schwachen und auf bestimmte Konstellationen beschränkten rechtlichen Schutz von Daten, und dieser ist mit rechtlichen Unklarheiten behaftet.

6. Datenschutzrecht

Das Datenschutzrecht schützt personenbezogene Daten, also Angaben über eine bestimmte oder bestimmbare natürliche Person.[70] Der Schutz personenbezogener Daten basiert auf dem Recht auf informationelle Selbstbestimmung. Das Datenschutzrecht schafft keine Eigentumsordnung an Daten, und soweit es Verfügungsrechte zuweist, weist es sie dem Datensubjekt zu.

Dennoch müssen, wo sie wegen Personenbezugs der Daten einschlägig sind, die datenschutzrechtlichen Bestimmungen im konkreten Fall bei der Beurteilung der Verfügungsgewalt über Daten berücksichtigt werden. Denn weder ein Datenbankschutzrecht (s.o.) noch insbesondere ein vertraglicher Herausgabeanspruch (s.u.) sind für den Verpflichteten erfüllbar – und damit auch für den Anspruchsinhaber nicht durchsetzbar – wenn das Datenschutzrecht die Übermittlung der Daten hindert. Das Datenschutzrecht setzt einen äußeren Rahmen der rechtlichen Möglichkeiten – oder eben der rechtlichen Unmöglichkeit – der Datenübermittlung.

7. Geheimschutzrechte

Betriebs- und Geschäftsgeheimnisse genießen rechtlichen Schutz, insbesondere durch §§ 17 ff. UWG und §§ 203 f. StGB. Dieser rechtliche Schutz findet sein Fundament im Grundgesetz, nämlich in Artikeln 12 Abs. 1 und 14 Abs. 1.[71] Als Betriebs- und Geschäftsgeheimnisse sind dabei solche Tatsachen, Umstände oder Vorgänge anerkannt, die nicht offenkundig sind und nur einem begrenzten Kreis zugänglich; außerdem muss das Unternehmen ein berechtigtes Interesse an der Geheimhaltung haben. Diese Definition dürfte auf Daten, die im Rahmen von Industrie-4.0-Prozessen entstehen, häufig zutreffen.
Dies spricht – auch und gerade in Verbindung mit dem oben erörterten Ausgangspunkt des Eigentums am Datenträger – dafür, dass die Daten dem Unternehmen „gehören“, das die *Smart Factory* betreibt. Im Streitfall wird derjenige, der sich ohne ausdrückliche vertragliche Regelung ein anderes Ergebnis wünscht, den Begründungsaufwand auf seiner Seite haben. Es verbleiben gleichwohl beachtliche rechtliche Risiken bei diesem

[70] Näheres zum Thema *Datenschutz und Industrie 4.0* im entsprechenden Beitrag des Autors.
[71] *BVerfG*, Beschluss vom 14.03.2006, Az. 1 BvR 2087/03 (www.bundesverfassungsgericht.de).

Zwischenfazit: Für die Geltung dieser Prinzipien bei integrierten Produktionsprozessen und insbesondere, wenn die Daten auf gewisse Weise Derivate (auch) einer fremden Vorleistung sind, gibt es keine gesicherten Erkenntnisse.

8. Vertragliche Regelungen

Es empfehlen sich daher zur Vermeidung rechtlicher Risiken – und zur Vermeidung von Streit – stets klare vertragliche Regelungen über das „Eigentum“ oder (besser) die Herausgabe, Verfügungsgewalt und Nutzungsrechte an Daten. Dies gilt im Grunde für alle denkbaren Konstellationen, sowohl bei integrierten Industrie-4.0-Prozessen als auch bei *Big Data* und outgesourcter Datenverarbeitung oder –analyse.
Dabei sollte gegebenenfalls genau geregelt werden, wer welche Daten an wen zu übermitteln hat, wer sie aufzubewahren hat, wann sie zu löschen sind und ob dies nachzuweisen ist. Vertragliche Regelungen über die Gewinnung sekundärer Erkenntnisse und sonstige Verarbeitung der Daten, die Exklusivität sowie Fragen der technischen Datensicherheit (sowie die Haftung dafür) bieten sich ebenfalls an.
Dabei müssen datenschutzrechtliche Regelungen beachtet werden (s.o.). Da die Verwertung digitaler Güter im Insolvenzverfahren immer wieder Schwierigkeiten bereitet, wird es sich bisweilen anbieten, auch diesen Fall vertraglich zu regeln.
Außer im Datenschutzrecht sowie in der Verletzung von Schutzrechten Dritter finden vertragliche Regelungen ihre Schranken nur in den allgemeinen Bestimmungen, also etwa im AGB-Recht. Wo aber gesetzliche Zuweisungen von Risiken und Chancen fehlen, muss die zulässige vertragliche Regelungsbreite größer sein. Demnach dürfte sich insoweit die Verwerfung vertraglicher Regelungen durch das AGB-Recht auf Fälle deutlicher Übervorteilung beschränken.

9. Fazit

Zusammenfassend bleibt festzuhalten, dass die bestehenden rechtlichen Instrumente das „Eigentum“ an Daten schwer und nur auf einigen sachlichen Regelungsinseln gestalten. Daher ist es richtig und wichtig, die Verfügungsgewalt über Daten vertraglich zu regeln; intelligent gestaltete Verträge können die vom Gesetzgeber gelassene Lücke füllen und sind dann einer der Fälle, in denen gut gemachte rechtliche Gestaltung tatsächlich die Chance auf Wettbewerbsvorteile eröffnen kann.

+++

Industrie 4.0 und Immaterialgüterrecht

Dipl.-Ing. *Joachim Gerstein, Patentanwalt*
Dipl.-Inf. Sebastian Aisch, Patentanwalt
Gramm, Lins & Partner, Patentanwälte, Rechtsanwälte Hannover/Braunschweig

Die Vorteile eines zeitlich begrenzten, ausschließlichen Schutzes als Teil der staatlichen Gewalt zur Förderung von Innovationen und Sicherstellung von fairen Marktbedingungen wurden bereits im 19 Jahrhundert, also zur Zeit der Industrialisierung (Industrie 1.0) erkannt und durch entsprechende rechtliche Rahmenbedingungen in den Industrienationen etabliert. Die fundamentalen Rechtsprinzipien gelten bis heute fort und wurden zwischenzeitlich von fast allen Nationen übernommen.
Für Industrie 4.0 ist ein guter und verlässlicher Innovationsschutz essentiell, da mit den omnipräsenten Kommunikationswegen und –mitteln und einem globalisierten Welthandel die Gefahr der Nachahmung und Produktpiraterie weiter stark steigen wird. Mit der Zunahme der vertikalen Vernetzung von Industriebetrieben rückt neben dem Produktschutz selber auch der Schutz der Fertigungstechnologien in den Fokus. Der Patent, Marken- und Designschutz sowie das Urheberrecht spielen hierbei eine entscheidende Rolle.
Für Industrie 4.0 ist es entscheidend, ob die rechtlichen Rahmenbedingungen und Rechtsprinzipien für die modernen Technologien und wirtschaftlichen Paradigmen geeignet sind. Es lassen sich rechtliche Schwachstellen herauskristallisieren:

- Das Territorialitätsprinzip (Nationalismus der Schutzrechte)
- Softwarepatente
- Daten als Erzeugnisse
- Standardessentielle Patente

1. Das Territorialitätsprinzip

Ein fundamentales Rechtsprinzip aller nationalen Schutzrechte ist das sogenannte Territorialitätsprinzip. In der modernen Welt der Globalisierung und der räumlich nahezu unbegrenzten Datenströme scheint dieses Grundprinzip langsam aus der Zeit zu fallen und zu einem Anachronismus zu werden. Mehr noch, wird der Grundgedanke der Industrie 4.0 konsequent zu Ende gedacht, so dürfte das (veraltete) Territorialitätsprinzip den angestrebten Zielen von Schutzrechten, nämlich die Förderung von Innovationen und die Schaffung fairer Marktbedingungen, hindernd entgegenstehen.

Das Territorialitätsprinzip der Schutzrechte (Patent, Marke, Design) hat dabei zwei wesentliche Aspekte:

- ein Schutzrecht muss in dem Land angemeldet werden, in dem es später auch seine Schutzwirkung entfalten soll, und

- die Schutzwirkung ist auf das Land oder die Region beschränkt, in dem es gemäß den dortigen nationalen Bestimmungen erteilt worden ist.

Ist ein Schutz, bspw. ein Patentschutz, in nahezu allen Ländern dieser Welt gewünscht oder gar notwendig, so muss in jedem Land ein entsprechendes Schutzrecht angemeldet und zur Erteilung/Eintragung gebracht werden. Zwar wurde in der Vergangenheit dieses Territorialitätsprinzip an einigen Stellen aufgeweicht, indem durch Zusammenarbeit mehrerer Nationen in bestimmten Teilen dieser Welt ein gemeinsamer regionaler Rechtsraum aufgebaut wurde. Allerdings verbleibt das letzte Wort in der Regel bei den nationalen Patent- und Markenämtern, sodass die staatliche Souveränität hiervon unberührt bleibt.

Eine Ausnahme bildet die Europäische Marke sowie das in naher Zukunft verfügbare europäische Einheitspatent, mit dem die Möglichkeit eröffnet wird, mit einer einzigen Patent- oder Markenanmeldung einen Schutz für nahezu alle EU-Mitgliedsstaaten zu erhalten.

Die Industrie 4.0 lebt von einem länderübergreifenden Waren- und Datenaustausch. Nationale Kleinstaaterei passt nicht in dieses Konzept; will man nicht die Errungenschaften der Industrie 4.0 dem veralteten Nationalismus der Schutzrechte opfern. Hier kann nur die Weltgemeinschaft in Gänze eine Lösung finden, um in Zukunft Innovationen umfassend schützen zu können. Die hierfür notwendigen Anstrengungen sind jedoch immens und es bleibt fraglich, ob die einzelnen Nationen bereit sind, staatliche Souveränität abzugeben, um im Gegenzug dazu Innovationen und faire Marktbedingungen im globalen Kontext zu fördern. Es bedarf dabei nicht nur einer Einigung hinsichtlich des Mindeststandards, so wie er heute schon durch die Pariser Verbandsübereinkunft (PVÜ) besteht. Vielmehr bedarf es eines umfassenden Standards, der nicht nur alle wesentlichen Aspekte eines Patenterteilungsverfahrens abdeckt, sondern auch den Schutzbereich und das Patentverletzungsverfahren harmonisiert.

2. Das Patentrecht – „in a nutshell“

Ein Patent soll bei einer begrenzten Laufzeit (meist 20 Jahre) für technische Erfindungen seinem Inhaber einen ausschließlichen Schutz gewähren. Demnach ist es Dritten untersagt, die Erfindung in welcher Art auch immer kommerziell zu nutzen bzw. zu verwerten. Ein Patent verleiht seinem Inhaber somit ein alleiniges, ausschließliches Nutzungsrecht an der Erfindung.
Gemäß § 1 PatG (Deutsches Patentgesetz) und Art. 52 EPÜ (Europäisches Patentübereinkommen) müssen die folgenden Voraussetzungen kumulativ vorliegen, damit ein Patent erteilt wird und der Schutz entsteht:

- Vorliegen einer technischen Erfindung,
- die Erfindung ist neu,
- die Erfindung beruht auf einer erfinderischen Tätigkeit und
- die Erfindung ist gewerblich anwendbar.

In den meisten Patentgesetzen bedeutet die Neuheit, dass die Erfindung nicht aus dem Stand der Technik bekannt sein darf, wobei als Stand der Technik all jenes anzusehen ist, was zu einem bestimmten Stichtag (meist der Anmeldetag des Patentes) der Öffentlichkeit – egal wo auf der Welt – zugänglich gemacht worden ist. Zudem wird mit dem Kriterium der erfinderische Tätigkeit gefordert, dass die Erfindung sich nicht in naheliegender Weise aus dem Stand der Technik ergeben darf, wobei eine rein objektive Beurteilungsweise anhand rechtlicher Prüfkonzepte zugrunde zu legen ist.
Derzeit weist das Patentrecht in Deutschland und Europa allerdings eine noch unbefriedigende Anpassung an die Entwicklung im Bereich der Industrie 4.0 auf. Die folgenden Schwerpunkte müssen dabei besonders Berücksichtigung finden:

- Software als wesentlicher Teil patentfähiger Lösungen
- Digitale Daten als Erzeugnisse im patentrechtlichen Sinne

Dem Patentschutz sind dabei grundsätzlich nur rein technische Erfindungen zugänglich. Erfindungen außerhalb der Technik können hingegen einen Patentschutz nicht begründen. Da der Begriff „Technik“ einem zeitlichen Wandel unterliegt, findet sich in den meisten nationalen Gesetzgebungen keine Definition hierzu. Das bedeutet im Umkehrschluss, dass der Begriff in nahezu allen Ländern in mehr oder weniger starken Nuancen unterschiedlich ausgelegt wird.

Mit einem nationalen/regionalen Patentschutz lässt sich Schutz erreichen für die Herstellung, das Anbieten, in Verkehr bringen oder Gebrauchen von Erzeugnissen, das Ausführen von Verfahren oder das Anbieten zur Ausführung. Selbiges gilt für die unmittelbaren Verfahrenserzeugnisse.

Wenn nun das Herstellen eines Erzeugnisses, wovon auch digitale Daten mit umfasst werden können, länderübergreifend erfolgt, dann hängt es von der nationalen Rechtsordnung ab, ob eine Patentverletzung vorliegt oder nicht. Dies kann zu höchst unterschiedlichen Beurteilungen führen, was zu einer hohen Verunsicherung der Beteiligten führen kann.

3. Software als patentgeschützter Gegenstand

Als grundsätzlich dem Patentrecht zugänglich werden nur Innovationen angesehen, die auf einem technischen Gebiet liegen. Der Gesetzgeber spricht dabei Computerpro-

grammen als solchen explizit die Eignung als technische Erfindung ab (vgl. § 1 Abs. 3 Nr. 3 iVm Abs. 4 PatG; Art. 52 Abs. 2, iVm Abs. 3 EPÜ). Gleichwohl ist Software, genauer gesagt Computerprogramme, unter gewissen Umständen patentfähig, so dass diese vom Gesetzgeber gewählte Definition irreführend ist. Es wird angenommen, dass hierdurch viele computerimplementierten Innovationen ungeschützt geblieben sind, wodurch ein nicht unerheblicher immaterieller Schaden in der Deutschen Wirtschaft entstanden ist.

Die Rechtsprechung hat einen Prüfkatalog entwickelt, um festzustellen, wann eine Softwarelösung dem Patentrecht zugänglich ist oder nicht. Demnach muss vorliegen:

> *„Die Lösung einer technischen Aufgabe*
> *mittels konkreter technischer Mittel*
> *zur Erzielung eines technischen Effektes“*

Der Einsatz einer Datenverarbeitungsanlage ist dabei als ein technisches Mittel anzusehen, wobei dann ein weitergehender technischer Effekt durch das Computerprogramm, das auf der Datenverarbeitungsanlage abläuft, erzeugt werden muss. Dieser technische Effekt kann zum einen die Datenverarbeitungsanlage selber betreffen, d.h. sie wird von dem technischen Effekt vorteilhaft weitergebildet. Der technische Effekt kann aber auch außerhalb der Datenverarbeitungsanlage entstehen, bspw. auf einem anderen technischen Gebiet.

Bei der mit Industrie 4.0 einhergehenden stärkeren Verzahnung von Software und deren Ausführung durch unterschiedliche Beteiligte sowie verschiedensten Schnittstellen kommt die Möglichkeit von Patentschutz für solche softwaregestützten Prozesse zum Tragen, die auf eine neue und auf einer erfinderischen Tätigkeit beruhenden Weise einen technischen Effekt bewirken.

Folgende technische Anwendungen im Bereich der Computerprogramme werden dabei als unstrittig patentfähig angesehen, die auch für Industrie 4.0 eine zentrale Rolle spielen:

- Programme für das Messen, Steuern, Regeln
- Automatisierungssysteme in der Industrie
- Assistenzsysteme in Fahrzeugen
- Verschlüsselungs- und Codierverfahren (bspw. MPEG)
- Telekommunikationsanwendungen
- Signalübertragungsverfahren

Lösungen, die sich bspw. auf Optimierungsverfahren oder auf Simulationsverfahren stützen, werden indes sowohl in Deutschland als auch im Vergleich zu anderen Ländern höchst unterschiedlich beurteilt. Dies kann jedoch zu einem Wettbewerbsnachteil

führen, insbesondere wenn bei Erfindungen auf diesen Gebieten aufgrund der Rechtsunsicherheiten von einer Patentanmeldung abgesehen wird.

Ein Problem stellt sich dann, wenn die Zugänglichkeit von computerimplementierten Erfindungen territorial unterschiedlich gehandhabt wird. Dies gilt insbesondere für die USA, wo auf Computernetzwerken basierende, rein wirtschaftliche Geschäftsmodelle bislang zu Patenten führen konnten, während dies in Europa erfolglos blieb.

4. Daten als Erzeugnisse

Wegen des fundamentalen Territorialitätsprinzips entsteht eine Patentverletzung nur in dem Land, in dem entsprechender Patentschutz besteht. Wird die Erfindung hingegen im patentfreien Ausland genutzt, so liegt zunächst keine Patentverletzung vor. Werden nun Computerprogramme auf Servern außerhalb des patentfreien Inlandes ausgeführt, so besteht die Gefahr einer versehentlichen Patentverletzung im Ausland, wenn das im Ausland geschützte Verfahren oder wesentliche Verfahrensschritte tatsächlich auch unwissentlich in dem entsprechenden Land ausgeführt werden. Für einen Verwender, der die Ergebnisse im patentfreien Inland auswertet und weiterverarbeitet, ist dies nicht zwingend offensichtlich. Das Stichwort „Cloud Computing“ hat hierbei eine zentrale Bedeutung.

Grundsätzlich wird bei einem patentgeschützten Verfahren auch das unmittelbar aus dem Verfahren resultierende Erzeugnis mitgeschützt (vgl. § 9 PatG). Dies wird wohl in Zukunft auch auf die aus einem Computerprogramm resultierenden Daten und Datenströme zutreffen. So hat der BGH in seiner Entscheidung zum MPEG-Standard (BGH X ZR 33/10 – MPEG-2-Videosignalcodierung) angedeutet, dass wohl nicht nur Datenströme, die sich auf Videocodierverfahren stützen, mit geschützt sind, sondern dass dies wohl auf nahezu alle digitalen Verfahren zutreffen wird.

An sich territorial wirkende Patente für Erzeugnisse und Verfahren können somit internationale Datenströme erfassen, bspw. zwischen Zulieferer und Hersteller und Vertrieb, die in jeweils verschiedenen Staaten ihren Sitz haben. Ein großes Problem besteht für die Marktteilnehmer darin, die Existenz und Relevanz solcher Schutzrechte zu erkennen. Eine Rechtssicherheit durch eine Recherche von Patenten ist durch die Unmenge existierender Schutzrechte, Sprachvielfalt, fehlende Verfügbarkeit von effizienten Zugriffsmöglichkeiten auf die aktuellen Rechtsstände von Patenten und aufwendige Erfassbarkeit des Schutzbereiches kaum zu erzielen.
Damit kann der Import von Daten aus dem patentfreien Ausland ins patentgeschützte Inland problematisch werden, wenn die Erzeugung der Daten auf einem im Inland geschützten Verfahren beruht.

5. Patente für technische Standards

Industrie 4.0 als „Internet der Dinge“ setzt bei der digitalen Kommunikation vorwiegend auf dem Ethernet-Protokoll auf. Dieses ist ein Industriestandard nach IEE 802.xx. Über diesen globalen Datentransport hinaus ist aber auch eine Interoperabilität der

- Kommunikation auf Feldebene
- Identifikation der Feldteilnehmer (Sensoren, Aktoren, Maschinen, Bediengeräte etc.)
- Verschlüsselungstechnik
- Datenkompressionsverfahren
- Datenstrukturen (Befehlsstruktur, Informationsstruktur)

erforderlich. Hierzu müssen von den Beteiligten einheitliche Standards genutzt werden. Die zugehörige Technologie der Marktteilnehmer kann in durch Normungsgremien ausgehandelten Standards oder in proprietären Standards einzelner Marktteilnehmer oder Gruppen von Marktteilnehmern festgelegt sein. Die Frage, ob und unter welchen Bedingungen die zugehörigen Schutzrechte lizenziert werden, hängt nun entscheidend von den individuellen Vereinbarungen der Normungsgremien oder Marktteilnehmer ab.

Die Kommunikation auf der Feldebene wird bislang wesentlich geprägt durch

- proprietäre Standards von Marktführern (z.B. ProfiNET [Fa. Siemens und General Electric], EtherCAT [Fa. Beckhoff], EtherNet/IP [Fa. Rockwell], POWERLINK [Fa. B&R], Sercos, CC-Link IE [Fa. Mitsubishi], Modbus/TCP [Fa. Schneider Electric])

- nicht-proprietäre Industriestandards (z.B. USB, ZigBee, Bluetooth, WiMAX)

Die Identifikation von Feldteilnehmern ist für jedes Kommunikationsprotokoll in der Regel im zugehörigen Kommunikationsstandard definiert. Globale Identifikationsmodelle basieren auf herstellerspezifischen Methoden und werden durch herstellerübergreifende Aktivitäten standardisiert (z.B. FDT Group, HART Communication Foundation, OPC Foundation, PROFIBUS & PROFINET International and Fieldbus Foundation). Dabei wird in der Automatisierungstechnik oftmals die Electronic Device Description Language (EDDL) genutzt, die in der IEC 61804 genormt ist.
Die Verschlüsselungstechnik umfasst kryptografische Verfahren und Authentifzierungsverfahren. Dabei werden im großen Maße Industriestandards wie z.B. AES256, S/MIME, CIFS FileSystem und SHA512 ID eingesetzt.

Datenkompressionsverfahren sind für die Video- und Tonübertragung z.B. mit MPEG, MP3, HDMI standardisiert. Die zugehörigen Patente sind über Patentpools (MPEG LA,

SISVEL, Technocolor) verfügbar. Zudem wird eine Datenkompression im Zusammenhang mit der Verschlüsselungstechnik genutzt.

Datenstrukturen sind für Befehlssprachen z.B. zur Ansteuerung von 3D-Druckern oder den Informationsaufbau z.B. zur Gerätebeschreibung (Device Description (DD), Device Type Manager (DTM), Electronic Device Description Language (EDDL)) relevant. Sie folgen proprietären Standards, Industrienormen oder Open Source Definitionen.
Die zur Nutzung der proprietären Standards oder Industriestandards sowie der Open Source Technologien erforderlichen Patente sind nicht einfach zu recherchieren. Es fehlt auch eine zentrale Anlaufstelle, bei der sich die Marktteilnehmer auf effiziente Weise Lizenzen beschaffen können. Die Lizenzbedingungen sind intransparent.

Prinzipiell ist die Geltendmachung von Monopolrechten (Patenten) kein Verstoß gegen das Wettbewerbsrecht oder Kartellrecht. Sie stößt ausnahmsweise bei technischen Standards an ihre kartellrechtliche Grenze, wenn die patentierte Technologie zwingend im Standard vorgegeben ist. Dies gilt nicht nur für Industriestandards, sondern auch für proprietäre Standards und de-facto Standards. Die Patentinhaber sind dann verpflichtet, die Technologie zu FRAND-Bedingungen (Fair, Reasonable and Non-Discriminatory) zu lizensieren. Ein Unterlassungsanspruch kann ohne ein vorhergehendes Angebot eines akzeptablen Lizenzvertrages nicht geltend gemacht werden. Bei Schadensersatz- und Rechnungslegungsansprüchen hat zumindest der EuGH (EuGH Urteil vom 16.07.2015 – C-170/13, ECLI:EU:C:2015:477 – Huawei / ZTE) weniger Bedenken gegen eine unmittelbare Geltendmachung ohne vorheriges Lizenzangebot.

Mit der europäischen Normungsverordnung VO (EU) Nr. 1025/2012 vom 25.10.2012 hat es der Gesetzgeber versäumt, bindende gesetzliche Vorgaben zur Nutzung von standardessentiellen Patenten zu machen. Lediglich in Anhang II, Ziff. 4 c) der Verordnung findet sich die bereits zur Lösung des Konfliktes zwischen dem Patentrecht und Kartellrecht durch Rechtsprechung definierte Anforderung an technische Spezifikationen:

> „Lizenzen für jene Rechte des geistigen Eigentums, die für die Verwendung von Spezifikationen von wesentlicher Bedeutung sind, werden an Interessenten nach dem FRAND-Grundsatz (Lizenzvergabe zu fairen, vernünftigen und nicht diskriminierenden Bedingungen) vergeben; im Ermessen des Rechteinhabers schließt dies eine Lizenzvergabe ohne Gegenleistung für wesentliche Rechte des geistigen Eigentums ein.“

Die Realisierung von Industrie 4.0 erfordert somit von den Marktteilnehmern:

- Identifizierung relevanter standardessentieller Patente
- Beschaffung von Lizenzen, weltweit
- Einkalkulieren von Lizenzgebühren

Es besteht nun die Gefahr, dass die Summe der notwendigen Lizenzen eine wirtschaftliche Umsetzung eines Internet 4.0 Geschäftsmodells gefährdet.

Erfahrungen aus der Telekommunikationsbranche mit Patentstreitigkeiten zu GSM, LTE, ADSL, TETRA etc. haben gezeigt, dass ein großes Konfliktpotential besteht. Besonders gefährlich ist es, wenn Finanzinvestoren standardessentielle Patente z.B. von Forschungseinrichtungen erwerben und diese durch Patentverletzungsklagen versuchen, wirtschaftlich zu verwerten.

Im Zeitraum von 2013 bis 2015 hat China mit 2.541 Patentanmeldungen zu Industrie 4.0 die USA mit 1.065 Patentanmeldungen und Deutschland mit 441 Patentanmeldungen weit überholt (Quelle: Fraunhofer IAO, Stuttgart, Analyse der Entwicklung von Industrie 4.0 in China, White Paper 2015). Es ist zu erwarten, dass China in diesem Bereich auf Basis eigener Patente technische Standards definieren wird, die auch für ausländische Marktteilnehmer relevant werden.

Ein weiteres Problem ist, dass die notwendigen Lizenzen in der Regel nur an das letzte Glied der Wertschöpfungskette erteilt werden. Dies hat zur Folge, dass Hersteller von Bauteilen (z.B. Chiphersteller) oder von Geräten (z.B. Modemhersteller) den Endkunden dann keine Lizenzfreiheit garantieren können, auch wenn die notwendige Technologie in den gelieferten Bauteilen / Geräten vollständig implementiert ist. Die Patentinhaber haben zumeist durch eine geeignete Formulierung der Patentansprüche, die nicht auf die Bauteile / Geräte beschränkt sind, sondern erst vom Endkunden realisierte oder genutzte Systeme oder Verfahren unter Schutz stellen, dafür gesorgt, dass die Patentrechte nicht bereits durch das in Verkehr bringen der Bauteile oder Geräte erschöpft sind. Dies führt zu wesentlich höheren Lizenzgebühren auf der Grundlage des höchstwertigen Preises in der Wertschöpfungskette.

Marktführende Innovatoren versuchen frühzeitig mit eigenen Technologien und zugehörigen Patenten zur Standardisierung beizutragen, um sich dadurch einen großen Marktanteil bei durch Lizenzeinnahmen verringerten Kosten zu sichern.

Die Problematik standardessentieller Patente führt für Industrie 4.0 zu dem folgenden denkbaren Maßnahmenkatalog:

- alle zur Realisierung von Industrie 4.0 erforderlichen Patente weltweit sollten identifiziert werden, um sie nach Themengruppen geordnet in einer Datenbank einfach recherchieren zu können (Transparenz).

- die notwendigen Lizenzen sollten an einer zentralen Stelle für alle notwendigen Patente insgesamt mit einer einzigen fairen, angemessenen und nichtdiskriminierenden Lizenzgebühr verfügbar sein (FRAND-Lizenz).

- es sollte gesetzlich z.B. im TRIPS-Abkommen festgelegt werden, dass jegliche Patente, die in einem proprietären, nicht-proprietären, offenen oder de-facto Standard genutzt werden müssen, unabhängig von der Beteiligung des Patentinhabers an der Standardisierung zwingend bei einer zentralen Stelle zur dortigen Pool-Lizensierung einzubringen sind (Regelungen zu Zwangslizenzen sind in vielen Patentgesetzen enthalten).

- zumindest sollten die durch die Normungsgremien individuell geregelten FRAND-Lizenzverpflichtungen ihrer an der Standardisierung beteiligten Mitglieder durch eine weltweit gültige gesetzliche Regelung zur Sicherung eines Mindeststandards flankiert werden.

Die Marktteilnehmer, insbesondere der Mittelstand, sollte in jedem Fall versuchen, ein eigenes Patentportfolio aufzubauen, um im Konfliktfall für einen Gegenangriff gewappnet und in der Lage zu sein, Lizenzkosten durch Cross-Lizensierung oder Beteiligung an Patent-Pools zu reduzieren.

+++

Strafrechtschutz für IT und Daten

Antonia Herfurth, Juristin (LMU), Rechtsreferendarin
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

1. Einführung

„Die Wirtschaft steht an der Schwelle zu einer vierten industriellen Revolution. Dabei wachsen die reale und virtuelle Welt immer mehr zu einem Internet der Dinge zusammen.“[72] Durch die Entwicklung zu einer digitalen Wirtschaft, gewinnt insbesondere die Informationssicherheit an Bedeutung. Diese kann als Schutz von technischen Systemen vor Angriffen und Missbrauch verstanden werden. Kleine und mittelständische Unternehmen fürchten in diesem Zusammenhang um die Sicherheit ihrer Betriebsdaten und den Verlust von Geschäftsgeheimnissen.[73]

Tatsächlich ergeben sich durch die aktuellen technischen Entwicklungen mehr Tatgelegenheiten und neue Tatgelegenheitsstrukturen.[74] So wurden im Jahr 2014 in Deutschland etwa 50.000 Straftaten im Bereich Cybercrime begangen und dabei Schäden in Höhe von circa 39 Mio. Euro verursacht.[75] Hierbei ist von einem großen Dunkelfeld auszugehen. Eine Studie aus dem Jahr 2013 hat beispielsweise in Niedersachsen eine Dunkelziffer von 91 % errechnet.[76]

Eine Hürde der Strafverfolgung ist, dass viele der durch Computerkriminalität verletzten Rechtsnormen Antragsdelikte sind. Strafverfolgungsvoraussetzung ist somit grundsätzlich ein Antrag bei den Strafverfolgungsbehörden durch das betroffene Unternehmen. Erschwerend tritt hinzu, dass das Unternehmen in dem Moment, in dem es staatliche Hilfe in Anspruch nimmt, die Kontrolle über das Verfahren verliert. Denn Staatsanwaltschaft und Gericht sind im Strafprozess von Amts wegen verpflichtet das wirkliche Geschehen zu erforschen und aufzuklären.[77] Somit kann ein Unternehmen durch die Ermittlungen zur Wahrheitsfindung auch in ein negatives Licht rücken.

Die folgende Darstellung verschafft einen Überblick über potenziell einschlägige Strafrechtsnormen im Zusammenhang mit der Computerkriminalität.

[72] BMBF Industrie 4.0.
[73] BMBF Industrie 4.0.
[74] BKA Bundeslagebild 2014, S. 14.
[75] BKA Bundeslagebild 2014, S. 4.
[76] BKA Bundeslagebild 2014, S. 5.
[77] Engländer S. 10 Rn 20.

2. Übersicht über die Rechtssituation

Als „Motor der Fortentwicklung des Computerstrafrechts“[78] fungierten in der Vergangenheit insbesondere die Europäische Union und der Europarat. Durch die *Cybercrime-Konvention* des Europarates aus dem Jahr 2001 erfolgte eine Harmonisierung der nationalen Strafvorschriften im Bereich der Cyber-Kriminalität.[79] Die Union wirkt mittels Art. 83 Abs. 1 AEUV an der Bekämpfung der Computerkriminalität mit, indem sie „durch Richtlinien Mindestvorschriften zur Festlegung von Straftaten und Strafen in Bereichen besonders schwerer Kriminalität festlegen“ kann.

Relevante nationale Strafnormen im Zusammenhang mit dem Angriff auf und Missbrauch von Daten, die nicht personenbezogen sind, finden sich überwiegend im Strafgesetzbuch (StGB), vereinzelt im Gesetz gegen den unlauteren Wettbewerb (UWG). Handelt es sich um eine Verletzung personenbezogener Daten, ist auf Bundesebene insbesondere an das Bundesdatenschutzgesetz zu denken. Der Fokus liegt im Folgenden auf der Darstellung nationaler Normen, deren Ziel der nicht personenbezogene Datenschutz ist, insbesondere unter Betrachtung der Entwicklung Industrie 4.0.

Hierbei können die einschlägigen Normen klassifiziert werden:

- Angriffe gegen Informationssysteme durch das Ausspähen, § 202a StGB, und Abfangen von Daten, § 202b StGB, sowie die Vorbereitung dessen, § 202c StGB, die Datenhehlerei, § 202 d StGB, die Datenveränderung, § 303a StGB, und die Computersabotage, § 303b StGB,

- Urkundendelikte wie die Fälschung technischer Aufzeichnungen und beweiserheblicher Daten, §§ 268, 269 StGB, sowie die Urkunden- und Datenunterdrückung, § 274 StGB,

- das Vermögensdelikt des Computerbetrugs, § 263a StGB und

- Angriffe auf Daten- und Geheimnisschutz durch Verrat von Geschäfts- und Betriebsgeheimnissen, § 17 UWG, und Verleiten und Erbieten zum Verrat, § 19 UWG.

3. Die Straftatbestände

Im Folgenden werden die einzelnen Straftatbestände vorgestellt. Der juristische Aufbau eines vorsätzlich vollendeten Begehungsdelikts gliedert sich in Tatbestand, Rechtswidrigkeit und Schuld, wobei im Rahmen des Tatbestands zwischen objektivem und subjektivem Tatbestand differenziert wird. Der objektive Tatbestand erfasst die

[78] Eisele S. 3 Rn 4.
[79] Eisele S. 3 Rn 4.

tatbestandlichen Voraussetzungen einer Strafrechtsnorm (Täter, Tathandlung, Taterfolg und Ursächlichkeit), wohingegen der subjektive Tatbestand den Vorsatz des Täters thematisiert. Nachfolgend wird schwerpunktmäßig der objektive Tatbestand dargestellt, wohingegen auf die sonstigen Voraussetzungen nur eingegangen wird, sofern sich diesbezüglich Besonderheiten ergeben.

3.1. Angriffe gegen Informationssysteme

Computerspionage, „Datendiebstahl“,

§ 202a StGB stellt das Ausspähen von Daten unter Strafe. Dabei schützt die Norm die Verfügungsbefugnis des Berechtigten an dem gedanklichen Inhalt seiner Daten, sprich sein Geheimhaltungsinteresse.[80] Erfasst werden somit insbesondere Fälle der Datenspionage.

Das Tatobjekt „Daten“ ist in § 202a II StGB legal definiert als solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Voraussetzung ist, dass die Daten nicht für den Täter bestimmt und gegen unberechtigten Zugang besonders gesichert sind.[81] Unternehmen haben an dieser Stelle zu beachten, dass bloße Zugriffsverbote in Verträgen oder etwa das Abspeichern von Daten unter einem anderen Namen oder in einem anderen Verzeichnis keine geeignete Sicherung im Sinne der Norm darstellt.[82] Als geeignete Tathandlung muss der Täter sich oder einem anderen unter Überwindung der Zugangssicherung den Zugang zu Daten verschafft haben.[83]

> Beispiel:
> *Der Täter hackt den Server eines Unternehmens unter Einsatz von Backdoorprogrammen, Netzwerksniffern oder Trojanern.*

§ 202b StGB schützt, ebenso wie § 202a StGB, das Geheimhaltungsinteresse des Berechtigten. Indem es das Abfangen von Daten bestraft, stützt sich der Schutzbereich des § 202b StGB aber nicht auf den Geheimhaltungswillen, sondern auf das allgemeine Recht auf Nichtöffentlichkeit der Kommunikation.[84]

Tatbestandsvoraussetzung ist, dass sich der Täter unter Anwendung von technischen Mitteln Daten i.S.d. § 202a II StGB aus einer nichtöffentlichen elektronischen Datenübermittlung verschafft.[85] Der Tatbestand ist nur erfüllt, wenn sich die Daten zum Tatzeitpunkt im Übermittlungsvorgang befinden, sprich vom Täter „abgefangen“ wer-

[80] Eisele S. 33 Rn 1.
[81] § 202a I StGB.
[82] Eisele S. 38 Rn 16.
[83] § 202a I StGB; Jäger S. 374 Rn 541a.
[84] BT Drs. 16/3656, S. 11.
[85] § 202b StGB.

den.[86] Eines weiteren Aufzeichnens oder Speicherns der Daten bedarf es zur Erfüllung des § 202b StGB nicht.[87]

> Beispiel:
> *Ein Mitarbeiter sendet eine E-Mail an einen Kunden, die von einem Wettbewerber abgefangen und gelesen wird.*[88]

Begeht der Täter Vorbereitungshandlungen, die als solche bereits besonders gefährlich sind, unterliegt er der Strafbarkeit nach § 202c StGB.

Vorbereitungshandlungen

Strafbar macht sich danach, wer eine Tat nach §§ 202a, 202 b, 303 a oder 303 b StGB vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht.[89] Als Ausgleich zu der weiten Vorverlagerung der Strafbarkeit wird dem Täter die Möglichkeit der Strafaufhebung aufgrund tätiger Reue eröffnet.[90] Gibt er also die Ausführung der vorbereiteten Tat freiwillig auf, entfällt seine Strafbarkeit.[91]

> Beispiel:
> *Ein Software-Entwickler kreiert ein Hacking-Programm, das den Zweck hat Daten auf fremden Computern auszuspähen.*

In diesem Bereich entsteht eine praktische Frage, die Systemtester vor Schwierigkeiten stellt: allein der Besitz von Hacker-Software, die zu Testzwecken eingesetzt werden soll, wäre bereist strafbar.

Datenhehlerei

Im Dezember 2015 wurde mit § 202 d StGB ein neuer Straftatbestand eingeführt, die Datenhehlerei. Danach macht sich strafbar, wer Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Vortat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich

[86] Jäger S. 375 Rn 541b.
[87] Jäger S. 375 Rn 541b.
[88] Eisele S. 45 Rn 36.
[89] § 202c I StGB, § 303a III StGB, § 303b V StGB.
[90] §§ 202c II i.V.m. 149 II, III StGB.
[91] Eisele S. 47 Rn 44.

macht.[92] Subjektiv muss der Täter nicht nur vorsätzlich, sondern auch mit Bereicherungsabsicht oder Drittschädigungsabsicht handeln.[93]

> Beispiel:
> *Ein Mitarbeiter eines Unternehmens übernimmt von einem Hacker die bei einem Wettbewerber unbefugt kopierten Kundendaten, um diese Kunden selbst zu gewinnen.*
>
> Anders:
> *Ein Journalist übergibt Daten, die er auf vertraulichem Weg von einem Mitarbeiter als Whistleblower erhalten hat, vertraulich an einen Zeitungsredakteur zur Einschätzung. Dieser überspielt sich die Daten in Form einer Word- Datei auf einen USB-Stick.*

Computersabotage

Ein Angriff auf Informationssysteme kann ebenso durch die Begehung einer Datenveränderung nach § 303a StGB erfolgen. Geschütztes Rechtsgut ist das Interesse des Berechtigten an der unversehrten Verwendbarkeit von Daten.[94]

Auch hier sind alle Daten i.S.d. § 202a II StGB, über die der Täter nicht die alleinige Verfügungsbefugnis besitzt, geeignetes Tatobjekt.[95] Als Tathandlung muss der Täter Daten gelöscht, dem ein Unkenntlichmachen gleichgestellt ist, unterdrückt, unbrauchbar gemacht oder verändert haben.

Im Übrigen ist bereits der Versuch der Datenveränderung strafbar und § 303b StGB, die Computersabotage, stellt eine Qualifikation zu § 303a StGB dar, also eine Erweiterung des Grundtatbestandes um strafverschärfende Merkmale.[96]

> Beispiel:
> *Der Täter überschreibt Kundendaten im fremden Unternehmen, sodass diese unwiederbringlich unkenntlich gemacht sind.*

Geschütztes Rechtsgut der Computersabotage aus § 303b StGB ist „das Interesse der Betreiber und Nutzer von Datenverarbeitungen an deren ordnungsgemäßer Funktionsweise“[97].

Strafbar ist, wer eine Datenverarbeitung, die wesentliche Bedeutung für den Betroffen hat, erheblich stört.[98] Dies kann durch eine Datenveränderung geschehen, durch Ein-

[92] § 202d I StGB.
[93] § 202d I StGB.
[94] Jäger S. 370 Rn 536.
[95] Eisele S. 55 Rn 67.
[96] § 303a II StGB.
[97] BT-Drs. 16/3656, S. 13.

geben oder Übermitteln von Daten oder auch durch das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers.[99] Als Besonderheit muss der Täter bei der Tathandlung des Eingebens oder Übermittelns im subjektiven Tatbestand mit einer Nachteilszufügungsabsicht zu Lasten des Betreibers beziehungsweise Nutzers handeln.

Ferner ist bereits eine versuchte Computersabotage strafbar.[100]

Außerdem enthält § 303b II StGB eine Qualifikation zu § 303b I StGB. Danach wirkt sich strafschärfend aus, wenn die Datenverarbeitung für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung war.[101] Strafschärfung tritt auch bei einer Computersabotage in einem besonders schweren Fall ein, so zum Beispiel, wenn der Täter einen Vermögensverlust großen Ausmaßes herbeigeführt hat.[102]

> Beispiel:
> ein Mitarbeiter *löscht Daten auf dem Unternehmensserver die die Verträge mit wichtigen Kunden enthalten.*[103]

3.2 Urkundendelikte

Fälschung technischer Aufzeichnungen

§ 268 StGB bestraft die Fälschung technischer Aufzeichnungen. Somit wird die Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs geschützt und damit das Vertrauen in die technische Informationsgewinnung und die Echtheit technischer Aufzeichnungen.[104]

Tatbestandsvoraussetzung ist, dass der Täter eine unechte technische Aufzeichnung herstellt, eine technische Aufzeichnung verfälscht oder eine unechte oder verfälschte technische Aufzeichnung gebraucht.[105] Der Herstellung einer unechten technischen Aufzeichnung steht es gleich, wenn der Täter durch störende Einwirkung auf den Aufzeichnungsvorgang das Ergebnis der Aufzeichnung beeinflusst.[106] Die technische Aufzeichnung ist in § 268 II StGB legal definiert als eine Darstellung von Daten, Mess- oder Rechenwerten, Zuständen oder Geschehensabläufen, die durch ein technisches Gerät ganz oder zum Teil selbstständig bewirkt wird, den Gegenstand der Aufzeichnung all-

[98] § 303b I StGB.
[99] § 303b I StGB.
[100] §§ 303b III, V, 202 c StGB.
[101] § 303b II StGB.
[102] § 303b IV 2 Nr. 1 StGB.
[103] Eisele S. 63 Rn 86.
[104] Fischer § 268 Rn 2; Eisele S: 198 Rn 11.
[105] § 268 I StGB.
[106] § 268 III StGB.

gemein oder für Eingeweihte erkennen lässt und zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist, gleichviel ob ihr die Bestimmung schon bei der Herstellung oder erst später gegeben wird. Subjektive Voraussetzung des § 268 I StGB ist, das der Täter zur Täuschung im Rechtsverkehr oder aus Gründen der fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr handelt.[107]

Bereits der Versuch ist strafbar.[108]

Eine höhere Strafe droht, wenn der Täter eine Fälschung technischer Aufzeichnung in einem besonders schweren Fall begangen hat, beispielsweise einen Vermögensverlust besonders großen Ausmaßes herbeigeführt hat.[109]

> Beispiel:
> *Der Fahrer hat in seinem LKW ein digitales EU-Kontrollgerät. Er manipuliert das Gerät so, dass die Geschwindigkeit um 10 km/h zu niedrig aufgezeichnet wird.*[110]

Fälschung beweiserheblicher Daten

§ 269 StGB stellt die Fälschung beweiserheblicher Daten unter Strafe und schützt somit die Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs mit Daten.[111] Zweck der Vorschrift ist die Schließung computerspezifischer Strafbarkeitslücken im Bereich der Urkundendelikte.[112]

Der objektive Tatbestand ist erfüllt, wenn der Täter beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht.[113] Daten im Sinne der Norm sind „Informationen, die in einer primär für die maschinelle Verarbeitung bestimmten Form codiert“[114] und somit „nicht unmittelbar optisch wahrnehmbar“[115] sind. Aufgrund der Bedeutung des § 269 StGB als „computerspezifisches Urkundendelikt“ müssen die Daten geeignet sein im Rechtsverkehr Beweis für rechtlich erhebliche Tatsachen zu erbringen und aufgrund dessen alle Funktionen einer Urkunde erfüllen, sprich Beweis-, Garantie- und Perpetuierungsfunktion.[116] Daten i.S.d. § 269 StGB sind bereits unecht, wenn sie über die Identität des Ausstellers täuschen,

[107] §§ 268 I, 270 StGB.
[108] § 268 IV StGB.
[109] §§ 268 V i.V.m. 267 III 2 Nr. 2 StGB.
[110] NStZ 1994, 547.
[111] Fischer § 269 Rn 2; Eisele S. 202 Rn 24.
[112] BT Drs. 10/318, S. 31 f.; BT Drs. 10/5058, S. 33.
[113] § 269 I StGB.
[114] Erb in: MüKo Band 5 § 269 Rn 13.
[115] Koch in: Dölling / Duttge / Rössner § 269 Rn 3.
[116] Schuhr in: Spickhoff § 270 Rn 6; Weidemann in: BeckOK § 269 Rn 4 f.; Fischer § 269 Rn 4.

wohingegen bloße inhaltliche Datentäuschungen unerheblich sind.[117] Abschließend ist aufzuzeigen, dass durch die Tathandlung des Speicherns oder Veränderns eine in hypothetischer Hinsicht unechte oder verfälschte Urkunde vorliegen muss. Würde es sich also um ein wahrnehmbares Tatobjekt, eine Urkunde, handeln, müsste diese durch die Tathandlung unecht oder verfälscht worden sein.[118] Subjektiv muss der Täter zur Täuschung im Rechtsverkehr oder aus Gründen der fälschlichen Beeinflussung einer Datenverarbeitung im Rechtsverkehr gehandelt haben.[119]

Beispiel:
Ein Mitarbeiter setzt unbefugt eine fremde Zahlungskarte zur Zahlung von Waren mittels PIN im electronic-cash-Verfahren ein.[120]

Unterdrückung von Beweismitteln

Schließlich ist § 274 StGB als geeignetes Urkundendelikt im Zusammenhang mit Computerstraftaten anzuführen. Sinn und Zweck der Norm ist, den Bestand der genannten Beweismittel zu gewährleisten um somit mit ihnen Beweis erbringen zu können.[121]
Der Strafbarkeit unterliegt, wer eine echte technische Aufzeichnung i.S.d. § 269 StGB, welche ihm entweder überhaupt nicht oder nicht ausschließlich gehört, vernichtet, beschädigt oder unterdrückt.[122] Ebenso wird bestraft, wer beweiserhebliche Daten i.S.d. § 202a II StGB, über die er nicht oder nicht ausschließlich verfügen darf, löscht, unterdrückt, unbrauchbar macht oder verändert.[123] In subjektiver Hinsicht bedarf es neben dem Vorsatz stets einer Nachteilszufügungsabsicht des Täters.[124] Diese muss zum einen auf die Beeinträchtigung fremder Rechte gerichtet sein und zum anderen auf eine Beeinträchtigung des Beweisführungsrechts.[125]

Beispiel:
Ein Mitarbeiter löscht eine Datei mit einer Mängelrüge eines Kunden[126]

3.3 Vermögensdelikte

Computerbetrug

[117] Eisele S. 203 Rn 28.
[118] Koch in: Dölling / Duttge / Rössner § 269 Rn 5.
[119] §§ 269 I, 270 StGB.
[120] Eisele S. 204 Rn 30.
[121] Eisele S. 208 Rn 40; Weidemann in: BeckOK § 274 Rn 2.
[122] § 274 I Nr. 1 StGB; Eisele S. 208 f. Rn 42.
[123] § 274 I Nr. 2 StGB.
[124] § 274 I Nr. 1, 2 StGB.
[125] Eisele S. 210 Rn 46 f..
[126] NJW 1966, 557.

§ 263a StGB bestraft den Computerbetrug, indem der Täter durch Manipulation des Computers, dieses zu einem falschen Vorgang veranlasst. Geschütztes Rechtsgut ist das Vermögen. Geeignetes Tatobjekt des Computerbetrugs ist das Ergebnis eines elektronischen Datenverarbeitungsvorgangs, wobei der Begriff der Daten, als alle codierten und codierbaren Informationen, weit gefasst ist.[127] Als Tathandlung muss der Täter das Ergebnis durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst haben.[128] Zur Tatbestandsverwirklichung muss dem Betroffenen durch die Beeinflussung des Datenverarbeitungsvorgangs ein Vermögensschaden entstanden sein. Subjektive Tatbestandsvoraussetzung ist, dass der Täter neben Vorsatz mit Bereicherungsabsicht gehandelt hat.[129]

Bereits die versuchte Computersabotage ist unter Strafe gestellt,[130] ebenso wie bestimmte, für sich bereits gefährliche, Vorbereitungshandlungen.[131] Zuletzt kann sich ein besonders schwerer Fall strafschärfend zu Lasten des Täters auswirken, so zum Beispiel, wenn der Täter einen Vermögensverlust großen Ausmaßes herbeigeführt hat.[132]

> Beispiel:
> *Der Täter verschafft sich illegal Kenntnisse über diejenigen Programme, die Zahlungsvorgänge im Unternehmen steuern. Mithilfe dieser Kenntnisse setzt er zum richtigen Zeitpunkt eine automatische Überweisung auf sein eigenes Konto in Gang.*[133]

3.2. Daten- und Geheimnisschutz

Verrat von Geschäftsgeheimnissen

§ 17 UWG schützt den Inhaber eines Unternehmens vor Verrat von Geschäfts- und Betriebsgeheimnissen. Im Übrigen schützt es das Interesse der Allgemeinheit an einem unverfälschten Wettbewerb.[134]

Die Norm erfasst drei Fallkonstellationen: den Geheimnisverrat, die Betriebsspionage und die Geheimnisverwertung bzw. –hehlerei. Geheimnisverrat liegt vor, wenn eine

[127] § 263a I StGB; Jäger S. 377 Rn 543; Eisele S. 170 Rn 26.
[128] § 263a I StGB.
[129] § 263a I StGB.
[130] §§ 263a II, 263 II StGB.
[131] § 263a III StGB.
[132] §§ 263a II, 263 III StGB.
[133] BGHSt 40, 331.
[134] Janssen / Maluga in: MüKo Band 7 § 17 UWG Rn 9 f..

bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemanden mitteilt.[135] Um einen Fall der Betriebsspionage handelt es sich, wenn der Täter sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel, Herstellung einer verkörperten Wiedergabe des Geheimnisses oder Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert.[136] Für eine Geheimnisverwertung bzw. –hehlerei müsste der Täter ein Geheimnis durch Geheimnisverrat oder Betriebsspionage erlangt, sich sonst unbefugt verschafft, gesichert, unbefugt verwertet oder jemandem mitgeteilt haben.[137] Neben den objektiven Merkmalen muss der Täter subjektiv zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, gehandelt haben.[138] Zu beachten ist, dass sowohl bei der Betriebsspionage als auch der Geheimnishehlerei jeder Täter sein kann, es bedarf also, im Gegensatz zum Geheimnisverrat, keiner Beziehung des Täters zum Unternehmen.[139]

Bereits der Versuch[140] und das Verleiten und Erbieten zum Verrat[141] sind strafbar.

> Beispiel:
> Ein *Unternehmen stellt Getränke her. Bei der Herstellung wendet es eine bestimmte Rezeptur an. Die Rezeptur ist an sich bekannt, jedoch ist geheim, dass das Unternehmen von diesem Verfahren Gebrauch macht. Ein Mitarbeiter trägt dieses Geheimnis nach außen.*[142]

3. Fazit

Im Zusammenhang mit Computerkriminalität wird in Fachkreisen kritisiert, dass das moderne Strafrecht kein Strafrecht zum Schutz der Wirtschaft sei.[143] Es wird angeführt, dass die einschlägigen nationalen Normen hinter dem aktuellen technischen Entwicklungsstand zurückbleiben.[144] Die einschlägigen Straftatbestände erfuhren zwar durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität 2007 erhebliche Änderungen,[145] seither erfolgten auf nationaler Ebene jedoch keine bedeutsamen normativen Fortschritte.

---

[135] § 17 I UWG.
[136] § 17 II Nr. 1 UWG.
[137] § 17 II Nr. 2 UWG.
[138] § 17 I UWG.
[139] Janssen / Maluga in: MüKo Band 7 § 17 UWG Rn 77, 94.
[140] § 17 III UWG.
[141] § 19 I, II UWG.
[142] GRUR 1955, 424.
[143] Mansdörfer Industrie 4.0 und die Gefahren.
[144] Mansdörfer Industrie 4.0 und die Gefahren.
[145] Vgl. 41. StrÄndG v. 07.08.2007, BGBl. I, S. 1786.

Auch die internationale Kooperation ist ein guter Ansatz, befindet sich jedoch noch in den Anfängen.[146] So wurde mit der Cybercrime-Konvention ein wichtiger Schritt getan, dieser allerdings bereits vor 15 Jahren. Gemessen am technischen und industriellen Entwicklungsstand wird diese (Nicht-)Entwicklung den Anforderungen derzeit kaum gerecht. Zumal die Informationssicherheit auch in Zukunft nicht in seiner Komplexität nachgeben wird - proportional zum technischen Fortschritt entwickeln sich auch die Methoden der Täter.

Dies nutzte die Bundesregierung als Handlungsanstoß und verabschiedete im Jahr 2015 das sog. *IT-Sicherheitsgesetz*.[147] Zweck ist die Erhöhung der Sicherheit informationstechnischer Systeme. Das IT-Gesetz stellt dazu branchenspezifische Sicherheitsmindestanforderungen an Unternehmen.

Im Übrigen verfasste die Bundesregierung bereits im Jahr 2014 die *Digitale Agenda 2014-2017*, in der sie Grundsätze zur Digitalpolitik formuliert hat.[148] Dabei misst sie Politikfeldern wie der digitalen Wirtschaft oder Infrastruktur digitales Entwicklungspotenzial zu und versucht dieses durch vorgeschlagene Innovationsstrategien zu unterstützen und voranzutreiben.[149]

Allerdings werden sowohl das IT-Gesetz als auch die Digitale Agenda vielfach als ungenügend kritisiert. Es wird angeführt, dass das IT-Gesetz unzureichend und realitätsfern ausgestaltet sei[150] und die Digitale Agenda lediglich leere Phrasen enthalte, „die (zudem) zehn Jahre zu spät […] vorgelegt“[151] wurden.

Somit bleibt abzuwarten, wie sich der Gesetzgeber des Weiteren verhält und ob er in der Unzufriedenheit in Fachkreisen über den unzulänglichen Rechtsschutz im Bereich der Computerkriminalität nicht möglicherweise einen Impuls für weitere Maßnahmen sieht.

In der Gesamtbetrachtung - und insbesondere unter den Gesichtspunkten der Entwicklung zu Industrie 4.0 – lässt sich feststellen, dass das nationale Computerstrafrecht nur bedingt geeignet ist, einen effektiven Vermögensschutz von Unternehmen zu gewährleisten. Die Bekämpfung von Wirtschaftskriminalität leidet nicht an einem Regelungsdefizit, sondern an einem Vollzugsdefizit. Die Angriffe erfolgen eben in der Regel nicht durch den benachbarten Wettbewerber, sondern durch internationale Täterstrukturen. Diese können von privaten Tätern, von Wettbewerbsunternehmen oder von staatlichen Stellen ausgehen. Internationale Cyberkriminalität lässt sich aber nur sehr schwer ermitteln und im erfolgreichen Ermittlungsfall ebenso schwer im Ausland verfolgen.

[146] Mansdörfer Industrie 4.0 und die Gefahren.
[147] Vgl. BGBl. I 2015, 1324.
[148] Vgl. Bundesregierung Digitale Agenda.
[149] Vgl. Bundesregierung Digitale Agenda.
[150] Mansdörfer Industrie 4.0 und die Gefahren.
[151] Matzat Kommentar zur Digitalen Agenda; vgl. auch Steiner Kommentar zur Digitalen Agenda.

Unternehmen sind daher gut beraten, wenn sie sich technische und organisatorische Schutzmaßnahmen konzentrieren und sich nicht auf eine Abschreckung oder Ahndung durch das Strafrecht verlassen.

+++

Finanzen

Daten in Bilanz und Besteuerung

Günther Stuff, Steuerberater
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

Die wirtschaftliche Bedeutung von Daten schlägt sich bekanntlich in vielerlei Bewertungen nieder, am deutlichsten aber in manchmal astronomischen Kaufpreisen für Internetunternehmen, die viele Nutzer haben, aber noch keinerlei Gewinne.

Daher stellt sich die Frage, wie Daten neutral, also ohne Verkehrsgeschäft, zu bewerten sind und wie sich dieses auf die Finanzstruktur des Unternehmens, aber auch auf die steuerliche Behandlung auswirken kann.

1. Daten als Vermögenswert

Daten im Allgemeinen sind nicht aktivierbar. Wie wird es in einer immer stärker vernetzten Welt in Zukunft aussehen; also in einer Welt, in der Maschinen, Computer, Smartphones, Gebäude, Straßenverkehr und zuletzt der Mensch selbst untereinander vernetzt sind und permanent Daten erzeugen und austauschen? Werden dann nicht Daten, wie von IAS/IFRS-Standards für die Aktivierung von Immateriellen Wirtschaftsgütern gefordert, einzeln bewert- und veräußerbar?

Maschinen werden in Zukunft selbstständig Maschinen entwickeln und verbessern. Diese von Maschinen erzeugten Daten sind digitale Baupläne und erfüllen in diesem Fall wohl nach IAS/IFRS die Kriterien für selbstgeschaffene immaterielle Wirtschaftsgüter, die nach IAS-Standard zu aktivieren wären. Reine Datensammlungen, wie Telefonlisten, Datenlisten und anderes, die für betriebsinterne Zwecke verwendet werden, dürften dagegen auch in Zukunft nicht aktivierungsfähig sein. Werden diese Daten aber auf Datenträger übertragen und verkauft, handelt es sich wie schon heute um aktivierungsfähige Wirtschaftsgüter.

Die Abgrenzung zwischen Aktivierung und sofortiger gewinnmindernder Aufwendung wird sich in einer total vernetzten Welt schwieriger gestalten und erfordert neue Bewertungsstandards und Regeln. Deutschland ist mit den Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) oder den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) und anderen Regelwerken gerade am Anfang der Entwicklung modernerer Buchführungsstandards. Internationale Standards, wie IAS/IFRS, sind schon als ein Stück näher an der bereits jetzt existierenden digitalen Realität zu betrachten.

Bild: Bilanzielle Behandlung von Daten

Aktivierung	*Pflicht*	*Wahl*	*Verbot*
Von immateriellen Wirtschaftsgütern			
Handelsrecht / HGB			
▪ Entgeltlich erworben	**X**		
▪ Unentgeltlich erworben		**X**	
▪ Selbst geschaffen		**X**	
▪ Aber: Marken, Drucktitel, Verlagsrechte, Kundenlisten, oder vergleichbar			**X**
▪ Daten (Betriebsgeheimnisse, Know How ?)		**?**	**?**
Handelsrecht / IFRS			
▪ Entgeltlich erworben	**X**		
▪ Unentgeltlich erworben, (sofern einzeln bewertbar und veräußerbar)	**X**		
▪ Selbst geschaffen (sofern einzeln bewertbar und veräußerbar)	**X**		
▪ Aber: Marken, Drucktitel, Verlagsrechte, Kundenlisten, vergleichbar			**X**
▪ Daten (Betriebsgeheimnisse, Know How ?)			**?**
Steuerrecht (DE)			
▪ Entgeltlich erworben	**X**		
▪ Eingelegte Wirtschaftsgüter	**X**		
▪ Unentgeltlich erworben			**X**
▪ Selbst geschaffen			**X**
▪ Aber: Marken, Drucktitel, Verlagsrechte, Kundenlisten, oder vergleichbar			**?**
▪ Daten (Betriebsgeheimnisse, Know How ?)			**?**

2. Cloud-Computing im Steuerrecht

Die Auslagerung von Datenbeständen und Datenverarbeitungsprozessen, und damit auch der Steuerung von Produktionsprozessen, an andere Standorte als die der physischen Nutzung werfen neue steuerliche Fragen auf. Die wichtigsten Fragen für die steuerliche Behandlung von Daten in der „Cloud“ sind:

- Gründet man mit Cloud-Computing eine Betriebsstätte?
- Wie ist die umsatzsteuerliche Behandlung der Leistungen zwischen Anbieter und Leistungsempfänger?
- Was bedeutet es, seine Buchführungsdaten ins Ausland zu verlagern?

Oft sind Server, die Daten eines Unternehmens verarbeiten oder speichern, im Ausland angesiedelt. Das Vorliegen einer (steuerlichen) Betriebsstätte im Ausland führt zur beschränkten Steuerpflicht im Land der Betriebsstätte. Ob eine Betriebsstätte vorliegt, ist anhand der jeweiligen Doppelbesteuerungsabkommen (DBA) zu prüfen.

Innerstaatlich gilt § 12 Abgabenordnung (AO), wonach eine Betriebstätte jede feste Geschäftseinrichtung oder Anlage ist, die der Tätigkeit eines Unternehmens dient. In der Regel hat derjenige eine Betriebsstätte am Serverstandort, der die **Verfügungsmacht** über den oder die Server ausübt; das ist meistens der Cloudservice-Provider, denn in der Regel wird der Leistungsempfänger nicht einen **bestimmten Server** sondern nur die Rechnerkapazität mieten. Oft werden Daten auch über mehrere Server mit verschiedenen Standorten überall auf der Welt verteilt. Das könnte im Extremfall zu einer Vielzahl von Betriebsstätten in diversen Ländern führen. Die größten Anbieter von Cloud-Dienstleistungen haben ihre Rechnerkapazitäten überwiegend in den USA angesiedelt. Da auch deutsche Provider, zumindest in der Vergangenheit, ebenfalls Rechnerkapazitäten in den USA angemietet hatten, kommt es zu einer erheblichen Datenkonzentration auf dem Boden der USA. Unterhält oder kontrolliert ein deutsches Unternehmen eigene Server im Ausland, kann es also durchaus dazu kommen, dass die Finanzverwaltung am ausländischen Standort eine Betriebsstätte annimmt und die dort zuzuordnenden Gewinne der örtlichen Besteuerung unterwirft. Sofern diese Behandlung von der deutschen Finanzverwaltung akzeptiert wird, kommt es (zunächst) zu einer Doppelbesteuerung der entsprechenden Erträge. Dies bedeutet mindestens eine administrative, gegebenenfalls auch eine finanzielle Mehrbelastung für Unternehmen.

3. Umsatzsteuerliche Behandlung von Dienstleistungen

Daneben stellt sich die Frage, wie umsatzsteuerlich zu bewerten ist, wenn der Serverprovider seinen Sitz im Ausland hat oder dort eine Betriebsstätte unterhält. Die Dienstleistung „Cloud-Computing“ stellt eine sonstige Leistung im Sinne des § 3 Abs. 9 UStG dar. Ort der Leistung zwischen Unternehmern ist der Sitz des Leistungsempfängers. Wird sie am Ort der Betriebsstätte des Leistungsempfängers erbracht, gilt der Ort der Betriebsstätte als Ort der Leistung. Ist der Ort der Leistung Deutschland, ist die Leistung in Deutschland umsatzsteuerpflichtig. Gleichwohl können Nicht-EU-Staaten in ihren Gesetzen vorsehen, dass die Leistung auch im Anbieterland der Umsatzsteuer unterworfen ist.

4. Verlagerung der Buchführung ins Ausland

Die mit BMF-Schreiben vom 14.11.2014 veröffentlichten GoBD stellen erhöhte Anforderungen an die Sicherheit und Reproduzierbarkeit der gespeicherten Daten. Datensicherheit bedeutet, Sicherung gegen Verlust, also z.B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl und gegen unberechtigte Eingaben und Veränderungen. Verlagert ein Unternehmen seine Buchführung ins Ausland, muss die Finanzverwaltung dem vorher zustimmen (§ 146 Abs.2a AO). Die GoBD schreiben auch vor, dass die Betriebsprüfung auf die Buchführungsdaten in vollem Umfang zugreifen kann. Eine Zustimmung zur Verlagerung der Buchführung ins Ausland wird also versagt werden, wenn ein solcher Zugriff dann nicht mehr uneingeschränkt möglich wäre. Die Finanzverwaltung wird auch darauf achten, ob zum Beispiel Steuerstrafverfahren oder Ordnungswidrigkeiten vorlagen, Abgabeverpflichtungen nicht eingehalten werden oder häufige Zahlungsverzögerungen vorgekommen sind. In solchen Fällen wird es wahrscheinlich auch nicht zur Zustimmung einer Verlagerung der Buchführungsdaten ins Ausland kommen - vermutet das Finanzamt eine Beeinträchtigung der Besteuerung oder des Zugriffs auf die Daten, wird es die Zustimmung versagen. In solchen Fällen sieht die Finanzverwaltung die Buchführung als nicht ordnungsgemäß an, was zu Schätzungen der Besteuerungsgrundlagen führt.
Dem Finanzamt muss also nachgewiesen werden, dass es bei der Verlagerung der Buchführung ins Ausland nicht zu Beeinträchtigungen bei Sicherheit, Reproduzierbarkeit und Datenzugriff kommen kann.

5. Verrechnungspreise für internationalen Datenverkehr.

Produktionsprozesse unter Industrie 4.0 bewegen systembedingt große Mengen an Daten: im Rahmen von Bestellungen, zur Maschinensteuerung, an Werkstücken zur Weiterbearbeitung, in der Logistik und im Rahmen von Wartung beim Kunden. Wenn ein Unternehmen einem anderen Daten überlässt, dient dies in erster Linie der Erledigung seiner Aufträge – Daten können aber darüber hinaus weiteren Nutzen haben und damit auch für den Empfänger einen eigenen zusätzlichen Wert.

Fließen wertvolle Daten in grenzüberschreitenden Prozessen an Empfänger im Ausland, auch innerhalb eines Konzerns, stellt sich die Frage nach der Bewertung und Vergütung. Die Problematik von Verrechnungspreisen für internationalen Datenverkehr ist vornehmlich im Lichte des OECD-Reports zur Gewinnverkürzung und Gewinnverlagerung zu betrachten.

Gewinne, die mit immateriellen Wirtschaftsgütern erwirtschaftet werden, tragen durch Fehlzurechnungen unter Umständen erheblich zur Gewinnverlagerung oder Gewinnverkürzung bei. OECD und G20 haben dieses Problem erkannt und versuchen im Rahmen von BEPS (*Base Erosion and Profit Shifting*) durch Überarbeitung der Ver-

rechnungspreisrichtlinien eine bessere Zuordnung zu erreichen. Am 05.Okt. 2015 wurde hierzu nun das Ergebnis veröffentlicht.

Obwohl im Grundsatz rechtliches Eigentum und vertragliche Vereinbarungen die Grundlage für die Findung der Verrechnungspreise darstellen, hat die OECD hierin nicht allein die Kriterien für eine Zuordnung von Erträgen durch Nutzung immaterieller Wirtschaftsgüter gesehen. Soweit auch andere Unternehmen im Konzernverbund bei der Entwicklung maßgeblichen Einfluss auf die Funktion der Immateriellen Wirtschaftsgüter nehmen oder nennenswerte Risiken übernehmen, sind ihnen entsprechende Vergütungen zuzuwenden. Damit kann der rechtliche Eigentümer nicht alleine die aus der Nutzung seiner Immateriellen Wirtschaftsgüter resultierenden Erträge vereinnahmen. Auch unter diesem Aspekt sind künftige Transfer-Pricing-Modelle zu beleuchten. Der bisher auch von der Finanzverwaltung präferierte Fremdvergleichsgrundsatz dürfte daher lediglich noch bei Vergütungen für das Halten der Rechte (z.B. Patente) und das eingesetzte Kapital eine größere Rolle spielen.

Als wichtige Funktionen für die Bewertung immaterieller WG sieht die OECD folgende Punkte an (siehe: Punkt 6.56 „Aligning Transfer Pricing Outcomes with Value Creation, Actions 8-10-2015 Final Reports):

- Design und Kontrolle von Forschungs- und Marketingprogrammen
- Leitung von und Festlegung der Prioritäten für Kreativunternehmen, einschließlich der Bestimmung des Ablaufs der sog. „bluesky-Forschung“
- Kontrolle über strategische Entscheidungen in Bezug auf Entwicklungsprogramme von Immateriellen Wirtschaftsgütern
- Management und Budgetkontrolle
- Verteidigung und Schutz von Immateriellen Wirtschaftsgütern
- Laufende Qualitätskontrolle von Funktionen, die von unabhängigen und verbundenen Unternehmen ausgeübt werden.

Die OECD sieht in erster Linie die Preisvergleichs- und die Gewinnaufteilungsmethode als die am besten geeigneten Verrechnungspreismethoden zur Bewertung von Immateriellen Wirtschaftsgütern an. Auch sind bei der Verrechnungspreisfindung Faktoren wie Genauigkeit der Finanzprognosen, Wachstumsraten, Abzinsungssätze, Nutzungsdauern der Immateriellen Wirtschaftsgüter, Steuern und Zahlungsart, in angemessener Weise zu berücksichtigen.

Das OECD-Papier wirft, besonders für schwierig zu bewertende Immaterielle Wirtschaftsgüter, noch eine Vielzahl von Fragen auf, die noch geklärt werden müssen, bevor eine Umsetzung in den entsprechenden DBA bzw. nationalen Gesetzen erfolgen kann. Es zeigt aber auch, dass das heutige Verständnis zu Leistungsverrechnungen im Konzern und den damit zusammenhängenden möglichen Gewinnverschiebungen über Ländergrenzen hinweg den neueren Entwicklungen auf dem Weg zu Industrie 4.0 angepasst werden muss.

Wettbewerb

Industrie 4.0 im Wettbewerbsrecht

Prof. Dr. Christiane Trüe, LL.M. (East Anglia), Hochschule Bremen
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

Die wirtschaftliche Bedeutung von Daten schlägt sich bekanntlich in vielerlei Bewertungen nieder, am deutlichsten aber in manchmal astronomischen Kaufpreisen für Internetunternehmen, die viele Nutzer haben, aber noch keinerlei Gewinne.

1. Einführung und Grundlagen

Industrie 4.0 wirft auch im Bereich des Kartellrechts neue Fragen auf, die es erforderlich machen zu prüfen, ob die bestehenden Grundsätze und Regelungen in der Lage sind, diese zu beantworten bzw. zu angemessenen Lösungen zu führen. Das Bundeskartellamt hat daher bereits Anfang 2015 einen „Think Tank" der 6. Beschlussabteilung gegründet, um als Kartellbehörde angemessen auf die Herausforderungen der Internetökonomie für die Kartellrechtsanwendung reagieren zu können. Der Think Tank hat am 9. Juni 2016 ein Arbeitspapier zum Thema „Marktmacht von Plattformen und Netzwerken" vorgelegt[152], auf das im Folgenden mit eingegangen wird.

Daten sind heutzutage ein Wirtschaftsgut und spielen daher eine wichtige, wenn auch je nach Markt, Branche oder beteiligten Unternehmen sehr unterschiedliche Rolle im Wettbewerb. Sie sind vielfach ein wichtiger Inputfaktor für die Entwicklung von Gütern und Dienstleistungen. Ohne Zugang zu ihnen oder zu einem Netzwerk oder einer Plattform, z.B. für Werbung, Vertragsanbahnung oder Datenaustausch, kann es sein, dass Unternehmen von weiterer wirtschaftlicher Tätigkeit in manchen Geschäftsbereichen ausgeschlossen oder erheblich benachteiligt sind. Das Besitzen von Daten, der Anschluss an ein Netzwerk oder die Mitnutzung einer Plattform kann auf der anderen Seite einen Wettbewerbsvorteil bedeuten oder sogar existenznotwendig sein, um im Wettbewerb zu bestehen. Insoweit verlangt die datenbasierte Industrie 4.0 die Anwendung der Wettbewerbsregeln, um zu vermeiden, dass Unternehmen sich aufgrund von Abstimmungen über Datensammlung, -verbreitung oder -nutzung wettbewerbswidrige Vorteile verschaffen, andere Unternehmen durch Verweigerung des Zugangs zu Daten, Netzen oder Plattformen willkürlich aus dem Markt ausgeschlossen werden und Monopole entstehen. Hier stellt sich die Frage nach Besonderheiten der „Datenmärkte", der „Netzwerkmärkte" oder der „Plattformmärkte" gegenüber anderen Märkten und damit nach etwaigen besonderen Wettbewerbsregeln oder Besonderheiten bei der Anwendung der Wettbewerbsregeln auf eine Kooperation von Unterneh-

[152] abrufbar unter http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Meldungen%20News%20Karussell/2016/09_06_2016_ThinkTank.html.

men bei Daten und bei der Beurteilung des Verhaltens marktmächtiger oder marktbeherrschender Unternehmen.

Von anderen Wirtschaftsgütern unterscheiden sich Daten insbesondere dadurch, dass sie i.d.R. nicht verbraucht werden und somit prinzipiell beliebig oft genutzt werden können. Allerdings kann die Exklusivität des Zugangs zu einer Datensammlung, einem Netzwerk oder einer Plattform diese wertvoller machen, wenn die Alleinkenntnis der Daten einen Wettbewerbsvorteil bedeutet. Gleichzeitig vergeht der Wert von Daten sehr schnell; wertvoll sind in aller Regel nur aktuelle Daten. Hinzu kommt, dass das Wirtschaftsgut „Datum" nicht universell einsetzbar ist, sondern Daten spezifisch für ihre bestimmten Verwendungszwecke sind. Manche Daten sind für eine Branche oder ein bestimmtes Unternehmen interessant und für andere völlig uninteressant, so dass diese dafür nicht bereit wären zu zahlen oder sonst eine Gegenleistung zu erbringen, für andere sind sie dagegen sehr wertvoll, weil ihre Wettbewerbsfähigkeit davon abhängt, dass sie (auch) über die Daten verfügen. Was Netzwerke oder Plattformen angeht, so kann davon ausgegangen werden, dass diese eine hohe Nutzerzahl voraussetzen, um für weitere Nutzer interessant zu sein, und dass bei jedenfalls bei werbebasierten Diensten eine Obergrenze existiert, bei deren Überschreiten die Nutzerzahl wegen zu viel Werbung abnimmt[153].

Aufgabe des Kartellrechts ist es, prinzipielle Chancengleichheit im Wettbewerb herzustellen. Positionen auf dem Markt sollen auf Leistungen beruhen und nicht auf Absprachen oder Abstimmungen mit anderen Unternehmen, mit denen ein Unternehmen im Wettbewerb steht. Dem liegt die Annahme zugrunde, dass der Wettbewerb im Allgemeinen unter den Unternehmen Innovation und Leistungen befördert, zur Bildung angemessener Preise führt und damit für die Verbraucher und die Allgemeinheit die besten Ergebnisse hervorbringt. Die prinzipiell freie privatautonome Vertragsgestaltung findet daher ihre Grenze u.a. im Kartellrecht. Dabei müssen zum einen Verträge der Unternehmen individuell auf ihre Vereinbarkeit mit dem Kartellrecht geprüft werden. Zum anderen kann es hilfreich sein, Muster-Vertragsklauseln für bestimmte Rechtsfragen zu entwickeln, die eine kartellrechtskonforme Vertragsgestaltung von Verträgen über Daten erlauben.

Kartellrecht regelt den Wettbewerb auf nationaler Ebene wie auf EU-Ebene im EU-Binnenmarkt. Wo die Digitalisierung und ihre Folgewirkungen grenzüberschreitend und sogar eher global als begrenzt auf den EU-Binnenmarkt auftreten, ist das nationale Recht (z.B. das deutsche Gesetz gegen Wettbewerbsbeschränkungen) zur Lösung kartellrechtlicher Probleme vielfach nicht mehr geeignet. Dies muss dann – in Ermangelung eines Welt-Kartellrechts –auf EU-Ebene mit EU-Wettbewerbsrecht, insbesondere auf der Grundlage der Art. 101 und 102 des Vertrags über die Arbeitsweise der EU (AEUV) und dem zu deren Konkretisierung und Durchführung erlassenen EU-Sekundärrecht versucht werden. Der Umgang mit Daten und Internetdiensten ist dabei kartellrechtlich oft noch unklar. Man kann Daten dem Eigentumsschutz unterstellen und Datensammlungen einen zumindest eigentumsähnlichen dinglichen absoluten

[153] Vgl. Arbeitspapier BKartA (Fn. 1), Zusammenfassung S. 10 ff., 25 ff., 31, ff.

Schutz gewähren.[154] Die dadurch geschaffene Rechtsposition wäre wettbewerbsrechtlich besonders zu bewerten und kann u.U. eine marktmächtige Stellung schaffen. Dabei stellt sich allerdings die Frage, ob ein eigentumsähnlicher Schutz wie beim geistigen Eigentum durch eine entsprechende schöpferische Tätigkeit gerechtfertigt werden kann. Dies wird bei unterschiedlichen Daten auch unterschiedlich zu beurteilen sein. Das Schutzinteresse derjenigen, deren Daten gesammelt werden, derjenigen, die gesammelte Daten nutzen möchten und derjenigen, die von der Nutzung ggf. ausgeschlossen sind, dürfte zudem je nach Art der Daten und dem Verhältnis zum Datensammler und zum Datennutzer sehr unterschiedlich sein und verlangt möglicherweise z.T. andere als die bisher für Waren- und Dienstleistungsmärkte gefundenen rechtlichen Lösungen.

2. Konkrete wettbewerbsrechtliche Fragen bei Industrie 4.0

Im Folgenden sollen einige wettbewerbsrechtliche Fragen von Industrie 4.0 herausgegriffen werden, ohne dass dabei ein Anspruch auf umfassende Erörterung erhoben werden kann.

2.1. Feststellung des relevanten Marktes im Bereich Industrie 4.0

Eine Wettbewerbsbeschränkung kann nur festgestellt werden, wenn der Umfang des Marktes, auf dem relevanter Wettbewerb stattfindet, bestimmt worden ist, weil nur dann geprüft werden kann, welcher Wettbewerb beschränkt sein könnte.
Für den Bereich der Daten als Wirtschaftsgut stellt sich als relevanter Markt derjenige dar, auf dem die Daten gehandelt werden oder auf dem sie Grundlage einer wirtschaftlichen Tätigkeit sind. Zu beachten ist dabei, dass das Wirtschaftsgut „Datum“ nicht universell einsetzbar ist, sondern Daten spezifisch für ihre bestimmten Verwendungszwecke sind. Manche Daten sind für eine Branche oder ein bestimmtes Unternehmen interessant und für andere völlig uninteressant, so dass diese dafür nicht bereit wären zu zahlen oder sonst eine Gegenleistung zu erbringen. So zeigen Suchanfragen im Internet bei Suchmaschinen, woran ein Internetnutzer gerade oder – bei der Überwachung der Suchanfragen über längere Zeit – generell interessiert ist. Für die angefragten Branchen ist das hochinteressant, für Unternehmen anderer Branchen in aller Regel nicht. Die Suchmaschinen können dem potentiellen Kunden aufgrund der Suchdaten spezifischere und an seinen Bedürfnissen ausgerichtete Ergebnisse aus den angefragten Branchen zeigen und Werbung gezielt auf seine Interessen gerichtet einspielen. Einkäufe im Internet zeigen, bei welchen Waren oder Dienstleistungen sich das Interesse im Kauf manifestiert hat. Ortsinformationen zeigen, wo sich der Nutzer gerade aufhält und möglicherweise ortsspezifische Informationen brauchen bzw. empfänglich für ortsspezifische Werbung sein kann. Auch hier kann Werbung effizienter einge-

[154] Auch auf EU-Ebene gibt es Überlegungen dazu, wie Daten geschützt werden können; eine Harmonisierung des Schutzes für Datenbanken sieht insbesondere Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 (ABl. L 77/20) über den rechtlichen Schutz von Datenbanken vor.

setzt und können potentielle Kunden gezielter angesprochen werden. Ggf. kann auch die Ware oder Dienstleistung spezifisch auf Kundenbedürfnisse abgestimmt und individuell gestaltet werden. Generell kann auf der Grundlage von Daten über die Kundenbedürfnisse bei der Entwicklung neuer Produkte und Dienstleistungen spezifischer auf die Kunden eingegangen und effizienter produziert werden; das Risiko, an den Kundenbedürfnissen vorbei zu produzieren, wird minimiert.[155] Für die Bestimmung des relevanten Marktes bestimmter Daten, Netzwerke oder Plattformen heißt dies, dass die Bestimmung des relevanten Markts viele unterschiedliche Parameter berücksichtigen muss.

Im Falle ihrer Sammlung über einen Zeitraum hinweg können Ortsdaten darüber hinaus das Erstellen von Bewegungsprofilen erlauben und damit weitere Rückschlüsse auf die Person. Dies ist auch der Fall bei der Sammlung medizinischer Daten z.B. durch Messung der Bewegungsaktivität, des Kalorienverbrauchs, des Blutdrucks etc. Hieraus kann nicht nur abgeleitet werden, wofür sich der Nutzer interessieren und welche Werbung ihn ansprechen könnte, sondern es kann sich z.B. auch errechnen lassen, ob eine Person ein gutes oder eher ein schlechtes Versicherungsrisiko ist oder welche Ausfallzeiten der- oder diejenige als Arbeitnehmer oder sonstiger Vertragspartner erwarten lässt. Rückschlüsse auf die Person oder sogar die eigentliche Persönlichkeit lassen sich auch aus dem Austausch persönlicher Daten und Informationen in sozialen Netzwerken gewinnen.

Daten z.B. über Produktionsprozesse oder der Zusammensetzung von Produkten o.ä. wie auch Daten über die Preiskalkulation und Preisfestsetzung sind dagegen von Interesse für die Hersteller und Händler ähnlicher Produkte, können aber als Ergebnisse von Forschung und Entwicklung Betriebsgeheimnisse und Gegenstand von Rechten geistigen Eigentums sein.

Diese Skizze zeigt bereits, wie unterschiedlich der relevante Markt sein kann. Es muss jeweils im Einzelfall geprüft werden, welcher Markt relevant ist.

2.2. Kooperation von Wettbewerbern

Datenpools

Unternehmenskooperationen werfen vielfach kartellrechtliche Probleme auf, wenn sie sich wettbewerbsbeschränkend auswirken können. Dies gilt auch für Unternehmenskooperationen bei der Sammlung, Verteilung und Nutzung von Daten und Wissen. Weiter können Netzwerke von Unternehmen zur Sammlung, Verbreitung und Auswertung von Daten sinnvoll sein, weil es auch bei Daten Größenvorteile gibt: Viele Einzel-

[155] Vielfach wird es sich hierbei indes um personenbezogene Daten handeln, die besonders geschützt sind und deshalb aus Datenschutzgründen nicht ohne weiteres frei zur Verfügung gestellt werden können, dazu die neue Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1.

datensammlungen von einzelnen Unternehmen sind teuer und erreichen im Zweifel mangels Masse eine geringere Qualität als eine große Sammlung für mehrere oder eine Vielzahl von Unternehmen. Ob die Kooperation von Wettbewerbern aber bei einer gemeinsamen Datenbank endet oder Grundlage für weitere Zusammenarbeit bis hin zu wettbewerbsrechtlich bedenklichem abgestimmten Verhalten ist, ist dann eine zweite Frage. Eine Abstimmung kann schon darin liegen, dass aufgrund der gemeinsamen Auswertung mehrere Unternehmen ihr Verhalten im Wettbewerb an denselben Grundlagen ausrichten. Kartellrechtlich ist es daher problematisch, wenn sich Wettbewerber zu solchen Netzen zusammenschließen und damit zumindest in Teilbereichen ihrer Aktivitäten ihren Wettbewerb beschränken oder einstellen und durch Kooperation ersetzen. Bezogen auf die Marktposition von Wettbewerbern kann es zudem einen erheblichen Unterschied machen, ob einer von ihnen Zugang zu solchen Daten oder zu dem Datennetzwerk hat oder nicht. Besonders problematisch ist dies, wenn sich mehrere marktmächtige Unternehmen mit einer solchen Kooperation ihre Position sichern, diese ausbauen und untereinander den Markt aufteilen und durch Zugangsverweigerung für andere diese aus dem Markt drängen oder für Newcomer den Marktzugang unmöglich machen.

Hier können Probleme ähnlich denen von Einkaufskooperationen z.B. in Form von Einkaufsgenossenschaften entstehen. Im Rahmen der Einkaufsplanung und Lagerhaltung von Einzelhandelsunternehmen spielen die Verkaufsdaten, ermittelt namentlich über die Scanner von Supermarktkassen, eine wichtige Rolle. Diese können dann z.B. bei wettbewerbsrechtlich relevanten Einkaufskooperationen von Einzelhandelsunternehmen ebenfalls von Belang sein, wenn der gemeinsame Einkauf geplant und Marktmacht gegenüber der Marktgegenseite ausgeübt werden soll – ein Beispielsfall für Größenvorteile bei einer Datensammlung. Die Vernetzung erlaubt gerade kleinen und mittleren Unternehmen, auf mehr Daten zuzugreifen und dies für ihre eigene Position im Markt zu nutzen. Gleichzeitig kann die Kooperation aber über das zum Ausgleich des Größennachteils gegenüber der Marktgegenseite Notwendige hinausgehen und damit wettbewerbsrechtlich bedenklich sein.

Wissens- und Forschungspools

Ähnliche Probleme wie bei Datenpools können auch bei Forschungs- und Wissenspools bestehen. Auch hier kann es sein, dass Wettbewerber für Forschungs- und Wissenstransferzwecke miteinander kooperieren oder Lizenzvereinbarungen miteinander eingehen. Hier kann im Falle einer Wettbewerbsbeschränkung aufgrund einer solchen Kooperation dennoch eine Freistellung bereits nach der Technologietransfer-Gruppenfreistellungsverordnung bestehen.
Insgesamt bleibt jedoch zu beachten, dass durch solche Kooperationen die Unternehmen nicht mehr so sehr als getrennte Einheiten im Wettbewerb agieren, sondern die Grenzen zwischen ihnen verschwimmen und nicht mehr klar erkennbar sind. Stets wird ein Unternehmen bei seinen wettbewerbsrelevanten Entscheidungen auch die Frage zu berücksichtigen haben, wie sich diese Entscheidungen auf die Kooperationspartner auswirken und Schäden für die Kooperation vermieden werden können. Dabei kann

nicht ausgeschlossen werden, dass Entscheidungen mit Rücksicht auf die Wettbewerber-Kooperationspartner anders ausfallen als dies bei einzig auf den Vorteil des eigenen Unternehmens im Markt bezogenen Entscheidungen der Fall wäre.

Geoblocking

Geoblocking ist im Internet-Handel ein wesentliches Problem. Wenn Unternehmen durch Geoblocking Kunden ausschließen, so kann dies auf Gebietsvereinbarungen zwischen Unternehmen zurückzuführen sein, die ihre Kunden gebietsweise aufteilen und dazu per Software deren Zugriff auf einen Online-Vertragsschluss blockieren. Klauseln, aufgrund derer Unternehmen nicht ins Ausland liefern und zu diesem Zweck Geoblocking verwenden, finden sich z.B. in Verträgen zwischen Unternehmen. Nach einer Untersuchung der EU-Kommission ist Geoblocking weit verbreitet.[156] Im EU-Binnenmarkt sind Gebietsaufteilungen besonders problematisch, weil sie die zwischen den Mitgliedstaaten abgeschafften Grenzen und staatlichen Beschränkungen zwischen den Mitgliedstaaten aufgrund der EU-Grundfreiheiten für Waren, Personen und Dienstleistungen auf privatem Wege wieder einführen und damit das Funktionieren des Binnenmarktes stören können.

2.3. Beschränkungen des Wettbewerbs gegenüber der Marktgegenseite

Beschränkung des Datenwettbewerb als Preiswettbewerbsbeschränkung

Im Verhältnis zum Verbraucher ist an Daten besonders, dass sie häufig als „Währung“ genutzt werden, d.h. dass die Nutzer von Internetdiensten statt mit Geld mit der Preisgabe ihrer Daten bezahlen. Beschränkt man diese Möglichkeit für die Verbraucher, z.B. mit dem Ziel des Verbraucherschutzes, können diese nicht mehr mit der Preisgabe ihrer Daten um die Leistungen der Datensammler konkurrieren. Fraglich ist daher, ob und inwieweit der Preis in Daten kartellrechtlich einem Preis in Geld gleichgesetzt werden muss. Unter Unternehmen abgestimmte Preisfestsetzungen gehören zu den verbotenen Kernbeschränkungen. Eine Vereinbarung unter Unternehmen oder ein Beschluss einer Unternehmensvereinigung darüber, dass bestimmte Leistungen nur gegen Preisgabe bestimmter Daten erbracht werden, könnte dem gleichzuordnen sein. Auch hierin liegt ein Eingriff in den Wettbewerb, der kartellrechtlich relevant sein kann. Rechtfertig- und freistellbar mögen solche Abstimmungen z.B. im Rahmen von Selbstbeschränkungen zum Verbraucherschutz sein.

Soweit ein Eingriff in den Wettbewerb staatlicherseits oder durch die EU im Interesse des Verbraucherschutzes durch Rechtsetzung erfolgt, muss stets berücksichtigt werden, ob die Beschränkung hinreichend gerechtfertigt werden kann. Verbote etwa von Unternehmen in Verträgen mit ihren Kunden, ihre Daten auch Wettbewerbern zur

[156] Vgl. http://ec.europa.eu/germany/news/kartellrecht-geoblocking-laut-sektoruntersuchung-der-eu-weit-verbreitet_de.

Verfügung zu stellen, sind dagegen i.d.R. Wettbewerbsbeschränkungen, die nicht ohne Weiteres gerechtfertigt werden können.

Bindungen im Vertikalverhältnis

Problematisch kann auch eine zu enge Bindung von Teilnehmern der vor- oder nachgelagerten Märkte, also im vertikalen Verhältnis, sein, wenn nicht Wettbewerber direkt miteinander den Wettbewerb beschränken, sondern Anbieter und Nachfrager eine besonders enge Bindung eingehen, die jeweils Wettbewerber als alternative Vertragspartner ausschließt. Dazu können Daten über Geschäftsbeziehungen und insbesondere z.B. Kundenwünsche und –interessen genutzt werden, um Angebote und Leistungen jeweils so individuell zuzuschneiden, dass Wettbewerber des Anbieters dem Kunden nur unter unwirtschaftlichem Aufwand Alternativen anbieten können. Dies gilt besonders im Bereich der Software. Nach der Nutzung einer Software über einen längeren Zeitraum ist es oft kaum möglich, zu einer anderen Softwarelösung zu wechseln, ohne die erste zumindest für die alten Bestandsdaten weiter zu nutzen (und zu bezahlen), um weiter auf diese zugreifen zu können.
In diesem Bereich ist auch der wettbewerbsbeschränkende Bereich von Koppelungsverträgen problematisch, aufgrund derer die Marktgegenseite gezwungen wird, weitere Produkte von dem Vertragspartner zu beziehen und nicht auf dessen Konkurrenten auszuweichen. Auch Anbieter von Software, Hardware, Netzleistungen und Speicherleistungen versuchen derartige Kopplungen am Markt durchzusetzen. Koppelungsverträge sind als Regelbeispiel wettbewerbsbeschränkenden Verhaltens in EU-Wettbewerbsrecht (Art. 101 Abs. 1 lit. e) AEUV) ausdrücklich verboten, so dass ein Unternehmen es nicht zur Bedingung für einen Vertragsabschluss machen darf, dass die Vertragspartner zusätzliche Leistungen annehmen, die weder sachlich noch nach Handelsbrauch in Beziehung zum Vertragsgegenstand stehen. Die Verpflichtung zum Bezug von Updates dürfte daher noch nicht unter das Koppelungsverbot fallen, die zum Bezug anderer, nicht nachgefragter und nicht zur Nutzung der Vertragsgegenstands-Software notwendiger anderer Software dagegen schon. Die Regelbeispiele illustrieren, was jedenfalls verbotene Wettbewerbsbeschränkungen sind, und sind nicht abschließend. Weichere Formen von Koppelungsverträgen, mit denen Kunden zwar nicht vertraglich, aber in anderer Weise zur Entgegennahme von gekoppelten Waren oder Leistungen veranlasst und damit am Erwerb von Wettbewerberprodukten gehindert werden, können daher sehr wohl auch verboten sein.

2.4. Missbrauch marktbeherrschender Stellung

Allgemein

Vor allem größere und marktmächtige Unternehmen müssen die Frage im Auge behalten, ob sie im Rahmen der Entwicklung und Nutzung digitaler Technologien oder bei der Herrschaft über Datensammlungen, Netzwerke oder Plattformen eine marktbe-

herrschende Stellung haben, die sie dazu verpflichtet, ihre Marktmacht besonders verantwortlich zu gebrauchen. Dies gilt für führende Softwareunternehmen wie Microsoft ebenso wie für Netzwerkdienste und Plattformen wie Google, Facebook, Amazon Marketplace oder Ebay. Jedoch gehören Marktmacht und Unternehmensgröße nicht zwingend zusammen. Auch kleinere Unternehmen können aufgrund ihrer Leistungen oder Produkte eine marktbeherrschende Stellung einnehmen. Von einer marktbeherrschenden Stellung wird allgemein bereits ausgegangen, wenn ein Unternehmen einen 50-%igen Marktanteil hat. Auch ein darunter liegender Anteil kann genügen, wenn es nur ein größeres Unternehmen gibt und die anderen auf dem relevanten Markt tätigen Unternehmen nur über ganz geringe Anteile verfügen. Besondere Märkte mögen daher auch eine besondere Bewertung der Marktbeherrschungsschwelle erfordern. Welche Schwelle eine Marktbeherrschung beim Markt der Daten, Netzwerke und Plattformen angemessen ist, wird sich noch in der Praxis herausbilden müssen. Das Bundeskartellamt geht insbesondere für die Prüfung der Marktmacht von Plattformen und Netzwerken davon aus, dass weiterhin eine Gesamtbetrachtung aller relevanten Umstände erforderlich ist. Dieses gelte insbesondere für die direkten und indirekten Netzwerkeffekte, deren Vorliegen – ebenso wie die Marktanteile – für sich genommen keine Aussagekraft habe, sondern nur das Prüfprogramm entscheidend beeinflusse[157]. Die oben unter 3.a) dargestellte Betrachtung von Daten als Währung kann auch bei der Feststellung von Marktmacht eine Rolle spielen: Wie die Marktmacht von Unternehmen im Rahmen der Spürbarkeit von Wettbewerbsbeschränkungen bzw. bei der Feststellung einer Marktbeherrschung u.a. danach beurteilt wird, ob ein Unternehmen in der Lage ist, Preise oberhalb des Wettbewerbsniveaus aufrechtzuerhalten, so kann sich Marktmacht auch daraus ergeben, dass ein Unternehmen in der Lage ist, die Preisgabe von Daten für seine Leistungen in einem Ausmaß durchzusetzen, das seinen Wettbewerbern nicht möglich ist. Eine rein monetäre Betrachtung greift hier zu kurz und kann nach bisherigem Stand u.U. nicht die notwendige Wettbewerbskontrolle auslösen, wenn zwar eine große Daten- aber eine (noch) geringe monetäre Preismacht besteht.

Aktuelles Beispiel des Missbrauchs einer marktbeherrschenden Stellung im Datenbereich ist Facebook, gegen das das Bundeskartellamt ein Verfahren eröffnet hat, weil der Verdacht des Konditionenmissbrauchs besteht. Darunter versteht man eine unangemessene Nutzung der Marktmacht mit dem Ziel, den Vertragspartnern – hier also den Facebook-Nutzern – Vertragsbedingungen aufzuzwingen, die diese nur wegen des Mangels an anderen Alternativen akzeptieren und sie – insbesondere unter Hintanstellung berechtigter Datenschutzinteressen oder sogar unter Verstoß gegen geltendes Datenschutzrecht – unangemessen benachteiligen.

Essential Facilities

[157] S. 11 der Zusammenfassung des Arbeitspapiers zum Thema „Marktmacht von Plattformen und Netzwerken“ (abrufbar unter http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Meldungen%20News%20Karussell/2016/09_06_2016_ThinkTank.html.

Ein Missbrauch marktbeherrschender Stellung kommt auch nach der Essential-Facilities-Doktrin in Betracht. „Essential facilities“ oder wesentliche Einrichtungen sind solche, ohne deren Mitbenutzung einem Marktteilnehmer der Zugang zu verbundenen Märkten nicht möglich ist. Daher müssen die Inhaber z.B. von Infrastruktureinrichtungen oder Rechten, die über diese Einrichtungen oder Rechte den Zugang zu vor- oder nachgelagerten Märkten beherrschen, anderen Unternehmen die Mitbenutzung ihrer Einrichtungen oder Rechte gestatten, selbst wenn sie selbst auf den vor- oder nachgelagerten Märkten tätig sind und sie damit gezwungen werden, einen Wettbewerber zu unterstützen. Präzedenzfälle und entsprechende gesetzliche Regelungen gibt es z.B. bei netzgebundenen Diensten in Verkehr, Energieversorgung und Wasserver- und -entsorgung, Telekommunikation etc. sowie bei Patenten und Urheberrechten. Nach der EuGH-Rechtsprechung kann die Verweigerung einer Lizenz an einem Schutzrecht missbräuchlich sein, wenn die Zugangsverweigerung willkürlich und geeignet ist, jeglichen Wettbewerb auf einem nachgelagerten Markt auszuschließen. Im Softwarebereich ist insoweit die Weigerung des marktbeherrschenden Unternehmens Microsoft, Interoperabilitätsinformationen zu liefern und ihre Nutzung zu gestatten, als Missbrauch einer marktbeherrschenden Stellung angesehen worden.[158]

Auch Daten (-banken oder -sammlungen) oder Einrichtungen zur Datensammlung wie Suchmaschinen wie auch Netzwerke und Plattformen können solche essential facilities sein. Unternehmen stellen ihre Daten Konkurrenten normalerweise nicht zur Verfügung, weil das Haben der Daten oder der Zugang zu ihnen die Marktposition verbessert und auf der anderen Seite der Wettbewerber ohne Zugang zu den Daten im Wettbewerb schlechter dasteht. Daten und ebenso Plattformen und Netzwerke werden daher anderen vorenthalten und bekommen dadurch eine Exklusivität, wodurch Wettbewerber von manchen Geschäftsbereichen ausgeschlossen werden können. Beschränkungen des Wettbewerbs über Beschränkungen des Zugangs sind daher jedenfalls dann bedenklich, wenn andere Unternehmen auf den Zugang angewiesen sind und es keine oder jedenfalls keine wirtschaftlich sinnvollen Alternativen des Zugangs gibt. Wo z.B. ein Werbedienstleister für den Marktzutritt auf Daten wie Suchmaschinenergebnisse über Kundenpräferenzen für das Angebot zielgerichteter Werbung angewiesen ist, kann der Nichtzugang zu den Daten eine Marktzutrittsschranke sein, wenn es kein alternatives Datenangebot gibt und es dem Newcomer auch nicht möglich ist, sich durch eine eigene Datensammlung Zugang zu verschaffen.

3. Fazit

Die aufgegriffenen wettbewerbsrechtlichen Fragen von Industrie 4.0 zeigen beispielhaft einige der neu auftretenden Fragen im Wettbewerbsrecht. Es ist mit Sicherheit zu erwarten, dass die Entwicklung von Industrie 4.0 auch im Wettbewerbsrecht weitere neue Fragen aufwerfen wird.

+++

[158] EuG T-201/04

Personal

Personal und Arbeit unter Industrie 4.0

Sabine Reimann, Rechtsanwältin
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

Industrie 4.0 wirft viele neue Fragen zur menschlichen Arbeit auf. Das Bundesministerium für Arbeit hat sich mit dem Grünbuch „Arbeiten 4.0“, im April 2015 vorgestellt, bereits intensiv mit der Entwicklung der Arbeit unter Industrie 4.0 auseinandergesetzt. Bis Ende 2016 wird der Dialogprozess Arbeiten 4.0 als Rahmen für einen teils öffentlichen, teils fachlichen Dialog über die Zukunft der Arbeitsgesellschaft dienen. Das Grünbuch enthält eine Reihe konkreter Leitfragen, die unter Einbindung von Fachleuten aus Wissenschaft und Wirtschaft, Sozialpartnern und Verbänden behandelt werden sollen.

Wie wird die Arbeit der Zukunft unter Industrie 4.0 aussehen?

Es wird weniger Maschinenbediener als vielmehr Erfahrungsträger und Entscheider geben und damit hebt sich die klare Abgrenzung zwischen Produktions- und Wissensarbeit auf. Denken und Handeln über den eigenen Fachbereich hinaus werden immer wichtiger. So ist die IT-Kompetenz in Zukunft Voraussetzung für die Arbeit in Industrie 4.0. Die erhöhten Anforderungen im Hinblick auf Komplexität, Flexibilität und auch Problemlösung führen zu einem gesteigerten Bedarf an Verständnis für das Zusammenspiel aller Akteure im Wertschöpfungsprozess.

Zwar wird es einfache Tätigkeiten, die von Beschäftigten mit einem geringeren Qualifikationsniveau, wie zum Beispiel Verwaltungs- oder Hilfsarbeiten, ausgeführt werden, auch in Zukunft geben. Sobald aber Maschinen kostengünstiger diese Arbeiten ausführen können, wird sich der Druck, dass diese Tätigkeiten durch technische Lösungen ersetzt werden, erhöhen.

Arbeit wird zunehmend zeit- und ortsunabhängiger. Dadurch entstehen zum einen Chancen für eine weiterentwickelte Organisation der Arbeit, wie zum Beispiel eine größere Flexibilisierung und neue Arbeitszeitmodelle (Home-Office, Gleitzeit, Vertrauensarbeitszeit, Arbeitszeitkonten oder Jobsharing), aber zum anderen eben Gefahren für den Arbeitnehmer im Bereich Gesundheit am Arbeitsplatz. Die Anforderungen an Flexibilität, Erreichbarkeit, Mobilität und Selbstorganisation haben insbesondere durch die Nutzung mobiler Arbeitsmittel (Smartphones, Laptops, Tablet-PCs) ein Niveau erreicht, dass nicht ohne Auswirkung auf die Gesundheit der Beschäftigten bleibt. Unbestritten ist, dass die aktuellen Befunde zur Zunahme psychischer Belastungen, Stress

und Burn-Out mit neuen Anforderungen bei den Arbeitsbedingungen in Zusammenhang stehen. 159

Möglicherweise wird die Digitalisierung in einigen Bereichen dazu führen, dass klassische Unternehmensstrukturen nicht mehr zeitgemäß sind und sich auflösen. Auf Grund moderner Kommunikationsmittel werden vielleicht die hierarchisch geleiteten Abteilungen und Unterabteilungen weniger benötigt, da in wechselnden Zusammensetzungen die Arbeit geleistet werden wird.

Faktoren wie lebenslanges Lernen auf der einen Seite und die Aus- und Weiterbildung der Mitarbeiter auf der anderen Seite sind Kernpunkte der Arbeit in Industrie 4.0. Möglicherweise sind neue Arbeitszeit- oder Entgeltmodelle nötig, um die Mitarbeiter mitnehmen zu können.

1. Individualarbeitsrecht

Im Individualarbeitsrecht geht es darum, die Vorstellungen der Arbeitsgeber und der Arbeitnehmer über die Bedingungen des Arbeitsverhältnisses aneinander anzugleichen. Sind die derzeitigen Arbeitsverhältnisse, im Hinblick auf die Zusammenarbeit von Mensch und Maschine, noch zeitgemäß? Können die starken Absatzschwankungen160, die aufgrund der Individualisierung der Produkte erwartet werden, durch die bestehenden Arbeitsverhältnisse abgedeckt werden? Wie kann Beschäftigung in Zukunft aussehen? Gibt es die Notwendigkeit, die bestehenden Arbeitsverträge zu ändern, zum Beispiel unter dem Aspekt Pflicht zur Weiterbildung?

1.1. Beschäftigungsarten

Um die auch derzeit schon vorhandenen Kapazitätsschwankungen beim Personal aufzufangen, wird auch heute bereits – neben der Stammbelegschaft - auf Zeitarbeit und Werkverträge zurückgegriffen.

Zeitarbeit

Die Zeitarbeit ist seit 1972 geregelt im Gesetz zur Regelung der Arbeitnehmerüberlassung. Der Verleiher benötigt eine Erlaubnis, die von der zuständigen Agentur für Arbeit erteilt wird. Der Vertrag zwischen Verleiher und Entleiher muss schriftlich abgeschlossen werden und die besonderen Merkmale der für den Leiharbeitnehmer vorgesehe-

[159] „Folgen für die Arbeitsorganisation“, Sören Tuleweit, IG BCE, vom 23.10.2015, https://www.igbce.de/aib-arbeitsrecht-im-betrieb-digitalisierung/116344?highlightTerms=industrie,4.0&back=#

[160] So Professor Spath in der Studie „Produktionsarbeit der Zukunft – Industrie 4.0“, Frauenhofer-Institut für Arbeitswirtschaft und Organisation IAO, S. 43, S.71

nen Tätigkeiten, die dafür erforderlichen beruflichen Qualifikationen sowie die Arbeitsbedingungen von vergleichbaren Arbeitnehmern der Stammbelegschaft enthalten.

Aus Sicht des Arbeitgebers als Entleiher ergeben sich durch die Leiharbeitsverträge einige Vorteile. Der Entleiher ist flexibler in der Anzahl der Beschäftigten; jederzeit kann ein Mitarbeiter entliehen werden. Er zahlt keine Sozialabgaben; die werden vom Verleiher bezahlt. Außerdem hat er keine Kündigungsschutzregelungen zu beachten. Andererseits kann es auch eintreten, dass ein Arbeitgeber relativ kurzfristig nicht über Leiharbeiter verfügen kann.

Aus Sicht des Leiharbeitnehmers ist zu berücksichtigen, dass er nur bis zu maximal einem Jahr pro Entleihung an einen Entleiher entliehen werden kann und dass es zu unterdurchschnittlichen Arbeitsentgelten kommen kann. Zwar sieht das AÜG eine Gleichbehandlung i.S.d. equal pay vor, das Gesetz hat aber hiervon die Möglichkeit der Abweichung durch Tarifverträge eröffnet. Von dieser Möglichkeit wurde flächendeckend Gebrauch gemacht.

Nicht zuletzt kann aus Sicht des Verleihers der administrative Aufwand erhöht sein. Das AÜG findet bei einer Arbeitnehmerüberlassung zwischen Konzernunternehmen im Sinne des § 18 Aktiengesetzes (AktG) keine Anwendung, wenn der Arbeitnehmer nicht zum Zweck der Überlassung eingestellt und beschäftigt wird. Sind ein herrschendes und ein oder mehrere abhängige Unternehmen unter der einheitlichen Leitung des herrschenden Unternehmens zusammengefasst, so bilden sie einen Konzern; die einzelnen Unternehmen sind Konzernunternehmen. Unternehmen, zwischen denen ein Beherrschungsvertrag (§ 291 AktG) besteht oder von denen das eine in das andere eingegliedert ist (§ 319 AktG), sind als unter einheitlicher Leitung zusammengefasst anzusehen. Von einem abhängigen Unternehmen wird vermutet, dass es mit dem herrschenden Unternehmen einen Konzern bildet. Die Regelung in Absatz 3 Nr. 2 stellt klar, dass die Privilegierung des Konzernverleihs nicht für die Arbeitnehmerüberlassung durch Personalführungsgesellschaften gilt, deren Zweck die Einstellung und Überlassung von Personal ist.

Im Vergleich zum Werkvertrag sind weiterhin die Beteiligungsrechte des Betriebsrates zu berücksichtigen, sowie die Tatsache, dass die Leiharbeitnehmer im Betrieb des Entleihers dieses Gremium mitwählen dürfen.

Werkverträge

Man könnte auch an flexiblere Werk- und Dienstverträge denken, auch um Knowhow von außen in das Unternehmen zu holen. Der Unternehmer überträgt bestimmte Aufgaben im Rahmen eines Werkvertrags auf einen Werk- oder Subunternehmer. Der Werkunternehmer verpflichtet sich, eine bestimmte Leistung (das Werk) zu erbringen bzw. herzustellen, d.h. der Erfolg ist geschuldet. Dieser erledigt die Arbeit mit eigenem Personal. Da Werkunternehmer häufig nicht tarifgebunden sind, können sie Arbeiten

zu günstigeren Konditionen anbieten als Leiharbeitsfirmen oder der Unternehmer selbst.

Bei der Vergabe von Aufträgen an Werkunternehmer oder externe Dienstleister ist der Betriebsrat nicht zu beteiligen. Das ist auch ein Grund, weshalb Werkverträge oder Verträge mit externen Dienstleistern so beliebt sind. Die Vorteile für Unternehmen liegen auf der Hand:

- die Rechtsrisiken für den Arbeitgeber sinken,
- die Personalkosten sinken,
- Mitbestimmungsrechte des Betriebsrats bestehen – wenn überhaupt – nur eingeschränkt und
- der Kündigungsschutz für Werksarbeitnehmer gilt gegenüber dem Werksvertragsunternehmer und nicht gegenüber dem Auftragnehmer.

Als Nachteil könnte sich u.a. der Verwaltungsaufwand, den Werksvertrag so auszugestalten, dass die tatsächliche Ausführung möglich ist, herausstellen. Denn hier können sich Probleme hinsichtlich der rechtlichen Einordnung des Vertrages ergeben. Es kommt entscheidend auf die tatsächliche Ausführung und Überwachung der Arbeiten an. Dagegen ist nicht entscheidend, wie ein Vertrag bezeichnet ist und wie die zu erbringenden Leistungen dort beschrieben sind. Je näher jedoch der Werkvertrag an die Arbeitnehmerüberlassung rückt, desto größer ist das Risiko, dass es sich tatsächlich nicht um einen Werkvertrag handelt. Dies gilt insbesondere in den Fällen, in denen die Tätigkeiten in den Räumlichkeiten des Auftraggebers mit dessen Betriebsmitteln erledigt werden und er Weisungen hinsichtlich der eigentlichen Ausführung der Arbeiten gibt oder die einzelnen Arbeitsschritte so detailliert im „Werkvertrag“ beschrieben sind, dass dem „Werkunternehmer“ kaum eigener Entscheidungsspielraum mehr bleibt.

Crowdsourcing

Eine Beschäftigungsart der Zukunft könnte das so genannte crowdsourcing, das Arbeiten im Internet als Digital Worker, sein. Hierbei lagert das Unternehmen bestimmte Tätigkeiten aus und vergibt die Aufgaben an Menschen außerhalb des Unternehmens. Vorteil für das Unternehmen ist es, dass es weltweit auf ein großes Reservoir an Arbeitskräften zugreifen kann. Zu den Tätigkeiten können relativ einfache Tätigkeiten, wie Schreiben von Produktbeschreibungen oder Recherchieren von Adressen, aber auch komplexe Tätigkeiten wie das Schreiben von Computerprogrammen gehören. Auf keinen Fall ist außer Acht zu lassen, dass es auch für diese Beschäftigungsart vertragliche Regelungen zu Datenschutz, Patentrechten oder Betriebsspionage geben muss. Die Crowdworker als Freelancer hingegen haben zwar die Vorteile, die Arbeit leichter zu erlangen und unter freier Arbeitseinteilung arbeiten zu können, haben aber keinen Anspruch auf übliche Arbeitnehmerrechte wie Kündigungsschutz, Entgeltfortzahlung oder Urlaub.

Flexi-Verträge

Im Zuge der schon begonnenen Flexibilisierung der Arbeitszeit haben Überstundenarbeit und Arbeitszeitkonten wesentlich an Bedeutung gewonnen, um kurz- und mittelfristige Schwankungen in der Nachfrage aufzufangen. Während aber bezahlte und unbezahlte Überstunden nur bei steigender, positiver Nachfrage zur Auftragsbewältigung eingesetzt werden können, werden auf den Arbeitszeitkonten bei steigender Nachfrage Zeitguthaben gebildet und bei sinkender Nachfrage wieder abgebaut. Arbeitszeitkonten ermöglichen damit im Vergleich zu Überstunden sowohl eine Flexibilität nach oben als auch nach unten, bei variablen Ausgleichszeiträumen.161

Unterschieden wird zwischen Kurzzeit- und Langzeitkonten. Langzeitkonten sind ein Instrument zur individuellen Lebensarbeitszeitgestaltung. Das steuer- und sozialversicherungsfreie Ansparen von Entgelt steht dem Verzicht des Arbeitnehmers auf Entgelt für geleistete Arbeit entgegen. Das Langzeitkonto dient der Abwicklung von zukünftigen Freistellungszeiten unter Fortzahlung von Arbeitsentgelt.
Kurzzeitkonten (oder auch Flexi-, Ausgleichs- oder Jahresarbeitszeitkonten) hingegen werden über Zeiträumen von meist bis zu einem Jahr geführt. Auf der einen Seite kann durch eine kapazitätsorientierte Verteilung von Arbeitszeiten auf betrieblicher Ebene flexibel auf Marktentwicklungen reagiert werden, andererseits werden Beschäftigte dann an das Unternehmen gebunden, weil anfallende Überstunden für private Belange oder Qualifizierungen genutzt werden können. Die hierdurch entstehende höhere Arbeitszeitensouveränität für die Beschäftigten wirkt sich positiv auf die Mitarbeiterzufriedenheit aus.
Als Beispiel für ein Kurzzeitkonto sei hier das „Korridormodell“ genannt. Es sieht vor, dass die vertraglich geregelte Arbeitszeit über einen bestimmten Zeitraum, der anhand der benötigten Kapazitäten und der Abläufe im Betrieb festgelegt wird und dadurch nicht unbedingt einem Kalenderjahr umfassen muss, erreicht werden muss. Der Arbeitgeber legt unter Vorankündigung Höchst- und Niedrigzeiten fest. Der Arbeitnehmer arbeitet im Rahmen eines so genannten Korridors von z.B. einer Monatsarbeitszeit im Plusbereich und einer Wochenarbeitszeit im Minusbereich. Der Monatslohn ist verstetigt und nicht abhängig von der tatsächlich erbrachten Arbeitsleistung. Verlässt der Arbeitnehmer den Korridor über den Plusbereich hinaus, wird ihm die Arbeit als Mehrarbeit entgolten. Gerät der Arbeitnehmer auf Grund von Kurzarbeit über den Minusbereich des Korridors hinaus, tritt die Agentur für Arbeit mit der Entgeltleistung anstelle des Arbeitgebers ein.

Arbeit auf Abruf

Laut §12 Teilzeit- und Befristungsgesetz können Arbeitnehmer und Arbeitgeber vereinbaren, dass der Arbeitnehmer seine Arbeitsleistung entsprechend dem Arbeitsaufwand zu erbringen hat. Die Vereinbarung muss eine bestimmte Dauer der wöchentli-

[161] Ines Zapf in IAB Forschungsbericht 03/2012, Flexibilität am Arbeitsmarkt durch Überstunden und Arbeitszeitkonten

chen und täglichen Arbeitszeit festlegen. Dabei geht das BAG162 davon aus, dass die „bestimmte Dauer“ in §12 I S.2 keine feste Arbeitszeit verlangt, da die mit der Abrufarbeit bezweckte Flexibilisierung nur erreicht werden kann, wenn hinsichtlich der Dauer der wöchentlichen und täglichen Arbeitszeit keine starren gesetzlichen Vorgaben bestehen. Wenn absehbar ist, dass nicht immer die volle Arbeitsleistung gebraucht wird, können 25% der Mindestarbeitszeit (oder, anders gerechnet, 20% der Gesamtarbeitszeit) flexibilisiert werden. Der Arbeitgeber kann über diese Zeit frei verfügen.

Ist eine tägliche bzw. wöchentliche Arbeitszeit nicht festgelegt, gelten drei aufeinander folgende Stunden täglich bzw. zehn Stunden wöchentlich als vereinbart. Der Arbeitgeber muss dem Arbeitnehmer die Lage seiner Arbeitszeit jeweils mindestens vier Tage im Voraus mitteilen. Hieraus könnte sich die Problematik ergeben, dass der Arbeitgeber kurzfristig auch ohne Arbeitnehmer auskommen müsste.

Einerseits hat der Mitarbeiter die Sicherheit, dass die vereinbarte Mindestarbeitszeit auf jeden Fall vergütet wird - und die Chance, bei erhöhtem Arbeitsanfall mehr zu verdienen. Andererseits kann der Unternehmer wesentlich flexibler disponieren, als es bisher möglich war. Die einzige Einschränkung besteht für ihn darin, dass er die flexible Arbeitszeit nach § 12 Abs. 2 TzBfG vier Tage im Voraus abrufen muss.
Von dieser Regelung kann durch Tarifvertrag auch zuungunsten des Arbeitnehmers abgewichen werden.

1.2. Arbeitsschutz

Zum Arbeitsschutz werden die Maßnahmen, Mittel oder Methoden zum Schutz der Beschäftigten vor arbeitsbedingten Sicherheits- und Gesundheitsgefährdungen gezählt. Beschäftigte sind u.a. laut §2 II Nr. 1 ArbSchG Arbeitsnehmerinnen und Arbeitnehmer.
Der Arbeitsschutz wird unterschieden in den allgemeinen und den sozialen Arbeitsschutz.

Der allgemeine Arbeitsschutz soll das Leben und die Gesundheit der Arbeitnehmer schützen. Außerdem soll die Arbeitskraft erhalten werden und das Arbeitsumfeld und die Arbeit menschengerecht ausgestalten werden.
Unter den sozialen Arbeitsschutz fallen Regelungen zu beispielsweise Arbeitszeiten und Kündigungsschutz.
Bei der Industrie 4.0 müssen die Arbeitsschutzgesetze im Hinblick darauf, ob sie der qualifizierten flexibleren Arbeit von Morgen genüge sind, näher betrachtet werden.

1.3. Betrieblicher Gesundheitsschutz

Aus zweierlei Sicht kommen auf den betrieblichen Gesundheitsschutz neue Aufgaben zu.

162 BAG, Urteil vom 7. Dezember 2005 - 5 AZR 535/04 § 12 TzBfG

Zum einen kann die Zusammenarbeit mit intelligenter Technologie zu Gefährdungen der körperlichen Gesundheit führen. Denn neben den Arbeitskräften kann auch die Technologie an sich Prozesse steuern. Ein Beispiel sind Roboter, die nicht mehr innerhalb von Schutzkäfigen eingesetzt werden, sondern als "kollaborierende Roboter" Hand in Hand mit den Beschäftigten arbeiten. Diese Leichtbauroboter können Zusammenstöße und Quetschungen verursachen. Solche Unfälle zu verhindern, ist derzeit eine große Aufgabe für die Arbeitsgestaltung. Der Arbeitsschutz fordert, dass Menschen nicht durch die Technologie gefährdet werden.163

Erste Schritte in diese Richtung sind kollaborierende, sensitive Leichtbauroboter mit so genannten sensorischen Schutzmänteln, die bereits heute z.B. in der Automobilindustrie im Einsatz sind. Sie reagieren auf Berührungen oder halten an, wenn der Mensch ihnen in die Quere kommt. Außerdem werden bereits Kamerasysteme zur Überwachung der Roboteraktivitäten in Kollaboration mit Menschen eingesetzt und immer weiter verbessert.

Auch psychische Belastungen können durch die Zusammenarbeit mit intelligenter Technologie entstehen. Menschen werden in hybriden Systemen eine hohe Verantwortung tragen, während sie zugleich der Technologie unterlegen sind. Sie können weit weniger Daten verarbeiten und weniger Komplexität berücksichtigen als Maschinen - zugleich aber wird von ihnen erwartet, Fehler der technologischen Systeme schnell zu korrigieren. Dies können sie aber immer weniger, weil ihnen durch die Automatisierung eigene Erfahrungen mit der Prozesssteuerung und damit Kompetenzen verloren gehen.

Die ständige Erreichbarkeit über Smartphone, Tablet & Co. hat in den letzten Jahren ihren Tribut gefordert – in Form von Stress und psychischen Erkrankungen bei vielen Beschäftigten.164

Zeitliche und räumliche Entgrenzung der Arbeit

Ist die flexible Arbeit, die Industrie 4.0 voraussetzt, auch unter Anwendung der bestehenden Gesetze im Hinblick auf Arbeitszeit und Arbeitsort möglich?
Der Zweck des Arbeitszeitgesetzes ist es, die Sicherheit und den Gesundheitsschutz der Arbeitnehmer bei der Arbeitszeitgestaltung zu gewährleisten und die Rahmenbedingungen für flexible Arbeitszeiten zu verbessern.

Das Gesetz legt in §3 eine maximale Arbeitszeit von 8 Stunden täglich bzw. 10 Stunden täglich fest, wenn innerhalb von sechs Kalendermonaten oder 24 Kalenderwochen im Durchschnitt acht Stunden werktäglich nicht überschritten werden. Die gesetzlichen Ruhezeiten (§5 ArbZG) von 11 Stunden sowie das Sonntagsarbeitsverbot (§9 ArbZG)

[163] IG Metall, „Mensch mit Maschine“, vom 06.01.2015, https://www.igmetall.de/neue-herausforderungen-fuer-den-betrieblichen-gesundheitsschutz-15064.htm
[164] „Zukunft der Arbeit“, Angela Krüger, DGUV, http://www.arbeit-und-gesundheit.de/3/2164

grenzen die Arbeitszeiten weiter ein. Allerdings ist nach der herrschenden Rechtsmeinung eine geringfügige Unterbrechung oder eine, die den Arbeitnehmer kaum belastet, nicht als Unterbrechung der Ruhezeit zu werten, da sie den Erholungszweck nicht gefährden. Auch hier ist also Auslegungsspielraum.

Laut § 7 ArbZG können Abweichungen zur maximalen Arbeitszeit und zu den Ruhezeiten durch Tarifverträge oder durch Betriebsvereinbarungen getroffen werden. Im Rahmen der Arbeitszeitflexibilisierung entstanden somit neben der Regelarbeitszeit Modelle wie Jahresarbeitszeit, Arbeitszeitkonten, Gleitzeit, Halbtagsarbeit, Teilzeit, Arbeitsplatzteilung oder Jobsharing, Lebensarbeitskonten, Vertrauensarbeitszeit, Modulare Arbeitszeit, Telearbeit, Zeitautonome Arbeitsgruppen, Arbeit auf Abruf und Individuelle Arbeitszeit. In § 13 ArbZG werden die Bundesländer ermächtigt, weitere Ausnahmen für die Sonntagsarbeit zu bestimmen.

Es gibt also Regelungsspielraum sowohl für die Arbeitszeiten, die Ruhezeiten als auch für das Sonntagsarbeitsverbot. Dieser müsste genutzt werden, um die noch höher flexibilisierte Arbeit in Industrie 4.0 gesetzeskonform gestalten zu können.

Auch unter dem Stichpunkt „mobile Arbeitszeit“, die wir zum Teil ja schon als Home-Office oder Bereitschaftsdienst kennen, muss prinzipiell die Arbeitszeit definiert werden. Auch bei zeitlich „entgrenzter“ Arbeit muss gesondert betrachtet werden, in wie weit die Koppelung Leistung - Entgelt nachzuvollziehen bleibt: es muss genau definiert werden, für welche Art der Leistung/ der Tätigkeit welches Entgelt zu leisten wäre (wie es das zum Beispiel schon bei der Funkbereitschaft bei der Feuerwehr gibt: Ruhezeiten werden geringer entlohnt als aktive Zeiten.)

Moderne Kommunikationsmittel ermöglichen Arbeitsleistung zeitlich flexibel, an verschiedenen Orten und in wechselnden Teams.

Durch die Arbeitsschutzvorschriften, wie z.B. die Arbeitsstättenverordnung, werden hohe bürokratische Hürden für den Mitarbeitereinsatz an anderen Orten aufgebaut. Der Arbeitgeber ist nach derzeitiger Rechtslage verpflichtet, eine Gefährdungsbeurteilung für jeden Arbeitsplatz vorzunehmen und Dokumente über das Ergebnis dieser Beurteilung bereit zu halten. Die Einschätzung fällt jedoch schwer, soweit Arbeitnehmer an wechselnden Orten außerhalb des Betriebsgeländes tätig sind. Die Pflicht zur Gefährdungsbeurteilung muss ausdrücklich auf den Bereich beschränkt werden, der dem Einflussbereich des Arbeitgebers unterliegt. Das wird auch dem Zweck des ArbSchG und der zugrundeliegenden europäischen Richtlinie 89/391/EWG gerecht: Der Arbeitnehmer soll vor Gefahren bei der Arbeitsleistung geschützt werden, aber nicht vor Gefahren, denen er sich selbst aussetzt.

In der Novelle zur Arbeitsstättenverordnung 2015 ist vorgesehen, Telearbeitsplätze im Home Office denen im Büro gleichzustellen. Dies hätte die Konsequenz, dass der Arbeitgeber auch im Privatbüro des Arbeitnehmers dafür zu sorgen hätte, dass der Arbeitsschutz, auch im Hinblick auf Ergonomie usw., eingehalten würde.

Vertragspflicht Weiterbildung

Welche Konsequenzen hat es, wenn ein Arbeitnehmer sich nicht fort-/weiterbilden will oder kann? Gibt es eine Pflicht zur Weiterbildung?
Der Unternehmer kann grundsätzlich das Anforderungsprofil einer Stelle ändern und damit dem Wandel hin zu Industrie 4.0 Rechnung tragen. Auch ohne eine Vertragsänderung oder eine Änderungskündigung kann der Arbeitgeber vom Arbeitnehmer verlangen, dass er sich z.B. die digitalen Fähigkeiten, die für diese Stelle erforderlich sind, aneignet.

Verpflichtet der Arbeitgeber in diesem Rahmen den Arbeitnehmer zu einer Fortbildung, muss er die Kosten prinzipiell tragen. Ist diese Fortbildung im Rahmen der Arbeitszeit und überfordert den Betrieb wirtschaftlich oder steht zu erwarten, dass der Mitarbeiter die notwendigen Kenntnisse nicht erlangen kann, ist der Arbeitgeber, unter dem Gesichtspunkt der Zumutbarkeit, nicht dazu verpflichtet, für eine Fortbildung zu sorgen.

Eine betriebsbedingte (Änderungs-) Kündigung kann dann gerechtfertigt sein, wenn sich das Anforderungsprofil deutlich von der Tätigkeitsbeschreibung im Arbeitsvertrag unterscheidet.

Eine Kündigung aus verhaltensbedingten Gründen käme dann in Betracht, wenn der Arbeitnehmer die notwenige und zumutbare Fortbildung, nach entsprechenden erfolglosen Abmahnungen, verweigert.

2. Kollektivarbeitsrecht

Der Kerngedanke des kollektiven Arbeitsrechts, entwickelt und weiterentwickelt durch den Gesetzgeber und die Tarifpartner, ist es, mögliche Interessengegensätze zwischen Arbeitgebern und Arbeitnehmern auszugleichen.

2.1. Betriebsverfassungsrecht

Liegt unter Industrie 4.0 auch dann noch ein Betrieb vor, wenn die Arbeit flexibel und mobil erledigt wird? Ist der Anwendungsbereich des Betriebsverfassungsgesetzes dann überhaupt noch eröffnet?

Das Betriebsverfassungsgesetz definiert den Begriff des Betriebes nicht. Die Rechtsprechung und Literatur haben eine Begriffsbestimmung vorgenommen, die sich an Sinn und Zweck des Betriebsverfassungsgesetzes orientiert. Danach ist ein Betrieb „eine organisatorische Einheit, innerhalb derer ein Arbeitgeber allein oder mit seinen Arbeit-

nehmern mit Hilfe von technischen und immateriellen Mitteln bestimmte arbeitstechnische Zwecke fortgesetzt verfolgt, die sich nicht in der Befriedigung von Eigenbedarf erschöpfen“. Das Fehlen einer räumlichen Einheit hingegen spricht nicht gegen einen einheitlichen Betrieb. Denn §4 BetrVG geht davon aus, dass auch Betriebsteile außerhalb des Betriebes zu diesem gehören. So ist auch betriebliche Tätigkeit außerhalb der Betriebsstätte, wie bei Monteuren oder Außendienstlern, möglich.

Mehrere rechtlich selbstständige Unternehmen können auch gem. §1 I 2 BetrVG einen gemeinsamen Betrieb im betriebsverfassungsrechtlichen Sinn haben. So liegt dann ein gemeinsamer Betrieb vor, wenn zusätzlich zu o.g. Voraussetzungen der Einsatz der menschlichen Arbeitskraft von einem einheitlichen Leitungsapparat gesteuert wird. Die einheitliche Leitung muss ich auf die Entscheidungen des Arbeitgebers im Bereich der personellen und sozialen Angelegenheiten des gemeinsamen Betriebes beziehen.
Somit ist auch im Hinblick auf die flexible Arbeit unter Industrie 4.0 sehr wohl das Betriebsverfassungsgesetz anwendbar, da es sich trotz räumlicher Entgrenzung um einen Betrieb in dessen Sinne handeln kann.

Zusammenarbeit mit dem Betriebsrat

er Betriebsrat als Interessenvertretung der Arbeitnehmer nimmt die ihm vom Gesetzgeber gegebenen Rechte und Pflichten so wahr, dass die Arbeit unter menschenwürdigen, gedeihlichen und möglichst wenig gesundheitsschädlichen Bedingungen erledigt werden kann. Er sorgt für eine gute Zusammenarbeit zwischen Arbeitgeber und Arbeitnehmer.

Gerade im Hinblick darauf, dass die Industrie 4.0 die Qualität der Arbeit, die Arbeitszeiten und auch den Schutzumfang des Arbeitnehmers verändern wird, ist ein Betriebsrat dazu da, diese Veränderung im Wege von Betriebsvereinbarungen für den Betrieb und die Mitarbeiter sinnvoll umzusetzen.

Mitbestimmungsrechte des Betriebsrates

Gemäß §87 I Nr.6 BetrVG ist die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, mitbestimmungspflichtig. Das Bundesarbeitsgericht stellt hier darauf ab, dass diese technische Einrichtung auch nur objektiv geeignet sein muss; eine tatsächliche Nutzung zur Überwachung wird nicht vorausgesetzt.
Voraussetzung für die ordnungsgemäße Einführung und Anwendung ist die Zustimmung des Betriebsrates, die in einer Betriebsvereinbarung, z.B. im Wege eines datenschutzrechtlichen Verbotes der Auswertung oder durch ein Einverständnis, niedergelegt wird. Dadurch werden Unternehmen nicht von der Einführung wichtiger elektronischer Hilfsmittel abgehalten, sondern lediglich bei der Absicht der Leistungs- oder Verhaltenskontrolle eingeschränkt.

Im Wege der Mitbestimmung über die täglichen Arbeitszeiten und die Pausen können gemäß §87 I Nr.2, Nr.3 BetrVG i.V.m. dem ArbZG Betriebsvereinbarungen geschlossen werden, die zum Beispiel Lebens- oder Jahresarbeitszeit regeln. Die Flexiblere Arbeit könnte durch solche Betriebsvereinbarungen auch unter den bestehenden Arbeitsschutzgesetzen kontrolliert werden. Hierin könnte auch eine Regelung zum Thema „ständige Erreichbarkeit“ entstehen.

Im Hinblick auf das Crowdsourcing hat der Betriebsrat sowohl Informationsrechte als auch Mitbestimmungsrechte.

Die Informationsrechte können sich aus den §§ 80,90, 92, 92 a, 106 und 111 BetrVG ergeben. So ist zum Beispiel bei § 80 Absatz 2 BetrVG im Gesetz klargestellt, dass sich die Unterrichtung „auch auf die Beschäftigung von Personen, die nicht in einem Arbeitsverhältnis zum Arbeitgeber stehen“, erstreckt. Bei § 92 a BetrVG werden in Absatz 1 als Thema für die Beratung ausdrücklich „neue Formen der Arbeitsorganisation, Änderungen der Arbeitsverfahren und Arbeitsabläufe, ... Alternativen zur Ausgliederung von Arbeit oder ihrer Vergabe an andere Unternehmen ...“ genannt.

Mitbestimmungsrechte können sich aus den §§ 95, 111 BetrVG ergeben. Gem. §90 BetrVG kann der Fremdfirmenanteil festgelegt werden. Darüber hinaus kann bei externem Crowdsourcing eine Betriebsänderung wegen einer grundlegenden Änderung der Betriebsorganisation und/oder der Einführung grundlegend neuer Arbeitsmethoden (§ 111 Nr. 4 und 5 BetrVG) vorliegen und der Betriebsrat einen Interessenausgleich und Sozialplan verhandeln.

Auf freiwilliger Basis zwischen Betriebsrat und Unternehmen können Vereinbarungen geschlossen werden, die zum Beispiel Mindestarbeitsbedingungen für Crowdworker, die für das Unternehmen arbeiten, festlegen.

2.2. Tarifrecht

Das Grundgesetz garantiert in Art.9 Abs.3 die Tarifautonomie: Arbeitnehmer und Arbeitgeber haben das Recht, sich zu Gewerkschaften und Arbeitgeberverbänden zusammenzuschließen und ihre Arbeits- und Wirtschaftsbedingungen frei von staatlichen Vorgaben eigenverantwortlich zu regeln. Dies geschieht vor allem durch Tarifverträge. Sie können sowohl für einzelne Unternehmen als auch für ganze Branchen abgeschlossen werden. Ihr Geltungsbereich kann regional begrenzt sein oder das Bundesgebiet insgesamt umfassen.

Was kann von Tarifpartnern behandelt und festgelegt werden?

Sind Tarifverträge auch in Zukunft unter Industrie 4.0 geeignete Mittel? Was sind die Regelungsinhalte von Tarifverträgen?
Tarifverträge regeln Rechte und Pflichten der Arbeitnehmer und Arbeitgeber, beispielsweise über Lohnhöhe, Arbeitszeit, Urlaub oder andere Arbeitsbedingungen. Die-

se Regelung ist allein Aufgabe der Tarifpartner. Die Gewerkschaften bzw. deren Spitzenorganisationen und der Arbeitgeber bzw. die Arbeitgeberverbände oder deren Spitzenorganisationen müssen sich einig werden.
Tarifverträge regeln die Arbeitsbedingungen kollektiv und für einen festgelegten Zeitraum und werden in Abständen an die wirtschaftliche Entwicklung angepasst. Tarifverträge erfüllen verschiedene wichtige Funktionen:

- Schutzfunktion: Der Schutz abhängig Beschäftigter durch die Schaffung zwingender tariflicher Mindestarbeitsbedingungen ist eine wichtige Aufgabe des Tarifvertrages. Eine Unterlegenheit des Arbeitnehmers aufgrund von wirtschaftlicher Abhängigkeit soll durch kollektives Handeln ausgeglichen werden.

- Ordnungsfunktion: Der Tarifvertrag setzt einen Standard, der ein Maßstab für die entsprechende Branche ist, indem er die Rechtsbeziehungen zwischen den Parteien regelt. Er setzt innerhalb seines Geltungsbereiches ein verbindliches Lohn- und Gehaltsgefüge fest.

- Verteilungsfunktion: Die Beteiligung der Arbeitnehmer am Ertrag des Unternehmens wird sichergestellt und die Einkommensverteilung unter den Arbeitnehmern wird durch Festlegung von Lohn- und Gehaltsgruppen geregelt.

- Friedensfunktion: Tarifverträge halten das Arbeitsleben über längere Zeiträume von Kräfte zehrenden Konflikten frei.

Aufgrund dieser Funktionen von Tarifverträgen sieht man, dass es auch in Zukunft elementar wichtig sein wird, die Arbeitsbedingungen im Hinblick auf große Flexibilität zu regeln. Auch die Bundesarbeitsministerin hat neue Tarifverträge, die den gestiegenen Anforderungen an Flexibilität Rechnung tragen, gefordert.165
Sollen Vereinbarungen Allgemeinverbindlichkeit haben?

Tarifverträge verpflichten einerseits alle Arbeitgeber des Geltungsbereichs, die dem jeweiligen Arbeitgeberverband angehören, sowie andererseits alle Arbeitnehmer, die Mitglied der beteiligten Gewerkschaft sind. (Es ist allerdings gängige Praxis, auch unorganisierte Arbeitnehmer an dem tarifvertraglich Vereinbarten teilhaben zu lassen.)

Ein Tarifvertrag kann dann auch für Arbeitnehmer und Arbeitgeber rechtsverbindlich werden, selbst wenn sie nicht tarifgebunden sind, wenn der Tarifvertrag für allgemeinverbindlich erklärt wird. Rechtsgrundlage hierfür ist § 5 Tarifvertragsgesetz. Der Antrag zugunsten einer Erklärung der Allgemeinverbindlichkeit eines Tarifvertrages kann von einer Tarifvertragspartei beim Bundesminister für Arbeit und Sozialordnung gestellt werden. Dieser kann im Einvernehmen mit einem Tarifausschuss, der aus je drei Vertretern der Spitzenorganisation der Arbeitnehmer und Arbeitgeber besteht, einen Tarifvertrag für allgemeinverbindlich erklären. Voraussetzung gem. §5 TVG ist, dass der Tarifvertrag in seinem Geltungsbereich für die Gestaltung der Arbeitsbedingungen überwiegende Bedeutung erlangt hat oder die Absicherung der Wirksamkeit der tarif-

[165] In Wirtschaftswoche vom 04.12.2015

vertraglichen Normsetzung gegen die Folgen wirtschaftlicher Fehlentwicklungen eine AVE verlangt und die Allgemeinverbindlichkeit von öffentlichem Interesse ist.

Die Allgemeinverbindlichkeit eines Tarifvertrages bewirkt, dass die Rechtsnormen dieses Tarifvertrages auch für alle sonst nicht tarifgebundenen Arbeitgebern und Arbeitnehmern innerhalb des sachlichen und räumlichen Geltungsbereiches des Tarifvertrages verbindlich werden. Sie wirkt somit wie ein staatliches Gesetz über Mindestarbeitsbedingungen.

Unter dem Aspekt, dass die Allgemeinverbindlichkeit eines Tarifvertrags den sozialen Schutz der Arbeitnehmer und gleichzeitig den Schutz der Arbeitgeber vor Konkurrenten, die Wettbewerbsvorteile durch Tarifunterschreitungen erreichen wollen, bezweckt, muss man sicherlich auch unter Industrie 4.0 darüber nachdenken, inwieweit eine Allgemeinverbindlichkeit für den sozialen Frieden sorgen kann.
Derzeit sind weniger als 1% aller Tarifverträge allgemeinverbindlich und die Tendenz der letzten Jahre ist rückläufig.166

2.3. Beschäftigten-Datenschutz

Wie sind unter Industrie 4.0 und dem damit verbundenen Datenstrom die Interessen von Arbeitnehmern und Arbeitgebern an ihren Daten angemessen zu schützen?

Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Eine Person ist dann bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Beispiele für sensible Mitarbeiterdaten sind z.B. Aufenthaltsdaten, Bewegungsprofile, Nutzungsprofile und Gewohnheiten der Mitarbeiter, die durch die Struktur der Arbeit in Cyber-Physischen-Systemen entstehen. Auch Mobilgeräte oder andere Kommunikationsgeräte, die für die Kommunikation mit den Maschinen zur Hilfe genommen werden, kreieren permanent neue Daten, an Hand derer man diese Profile erstellen und dem Mitarbeiter zuordnen könnte. Je größer das Zusammenspiel zwischen Mensch und Maschine, desto mehr Daten werden entstehen.

[166] Bundesministerium für Arbeit und Soziales
Verzeichnis der für allgemeinverbindlich erklärten Tarifverträge Stand: 1. Juli 2016

Technische Daten können zu personenbezogenen Daten werden, sobald es Verknüpfungsmöglichkeiten gibt und die Daten mit einem nicht unverhältnismäßig großen Aufwand einer bestimmten oder bestimmbaren Person zugeordnet werden können.167

Weitere sensible Daten sind Daten zum Gesundheitszustand des jeweiligen Mitarbeiters, wie zum Beispiel Sehschwächen oder Bewegungseinschränkungen, die sich aufgrund des Arbeitsplatzes ergeben.

Auch die Möglichkeit der Videoüberwachung der Mitarbeiter über die, in den Mobilgeräten integrierten, Kameras ist gegeben und somit als potenzieller Konfliktpunkt zu betrachten. Die Kontrollstrategien inklusive verstärkter Überwachung des einzelnen könnten zunehmen.

Ist das Endgerät im Eigentum des Unternehmens so könnte durch eine Anonymisierung, indem z.B. die Endgeräte, die für die Verwendung der Daten genutzt werden, von mehreren Personen genutzt würden und damit eine Verknüpfung mit personenbezogenen Daten vermieden würde, der Datenschutz eingehalten werden.

Grundsätzlich haben Arbeitnehmer das Recht auf Schutz ihrer personenbezogenen Daten. Dies ergibt sich aus dem informationellen Recht auf Selbstbestimmung (allgemeines Persönlichkeitsrecht) gem. Art. 2 Abs.1 GG, Art. 1 Abs. 1 GG, § 1 BDSG, § 4 Abs. 11 BDSG.

Der Erlaubnistatbestand in § 32 BDSG gibt die Möglichkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, wenn dies für die Entscheidung über die Begründung eines Beschäftigtenverhältnisses oder nach der Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist und die schutzwürdigen Interessen des Betroffenen gewahrt sind oder der Betroffene in die Verarbeitung seiner Daten eingewilligt hat.

Eine Interessenabwägung nach dem Grundsatz der Verhältnismäßigkeit im Hinblick auf die Erforderlichkeit ist immer notwendig.

Eine Einwilligung des Betroffenen ist jedoch umstritten, da von einer Freiwilligkeit innerhalb eines Arbeitsverhältnisses nicht so weiter ausgegangen werden kann. Liegt hingegen eine gesetzliche Erlaubnis vor, kommt es auf eine Einwilligung des Betroffenen gar nicht mehr an.

Eine solche gesetzliche Erlaubnis kann in Tarifverträgen gesehen werden, in denen festgelegt wird, inwiefern die Daten erhoben, verarbeitet oder genutzt werden dürfen. Ebenso sind sogenannte Bindung Corporate Rules, die den Datenaustausch innerhalb Konzernen regeln, denkbar. Diese müssen von den europäischen Datenschutzbehörden des Landes, aus dem Daten übertragen werden sollen, verifiziert werden.

[167] „Industrie 4.0 und Arbeitnehmerdatenschutz“, Andreas Lober u.a., Sonderheft 10/2015, S. 19, www.personalwirtschaft.de

In § 75 II BetrVG wird ausdrücklich das allgemeine Persönlichkeitsrecht des Arbeitnehmers als vom Arbeitgeber und Betriebsrat zu schützen und zu fördern aufgeführt. Diese Vorschrift verpflichtet die Betriebspartner, selbst alles zu unterlassen, was die Persönlichkeitsrechte der Arbeitnehmer verletzt.

Gleichwohl kann durch eine Betriebsvereinbarung auch der Eingriff in das allgemeine Persönlichkeitsrecht gerechtfertigt sein; wenn nicht durch eine ausdrückliche gesetzliche Regelung gestattet, so durch schutzwürdige Belange z. B. des Arbeitgebers. Bei einer Kollision des allgemeinen Persönlichkeitsrechts mit den schutzwürdigen Interessen des Arbeitgebers ist eine Güterabwägung unter Berücksichtigung der Umstände des Einzelfalls erforderlich.

Als Korrektiv für das zulässige Maß einer Beschränkung des allgemeinen Persönlichkeitsrechts dient der Grundsatz der Verhältnismäßigkeit: die getroffene Regelung muss geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen sein, um den erstrebten Zweck zu erreichen.

Individualvertraglich gibt es zum Schutz der personenbezogenen Arbeitnehmerdaten die Möglichkeit der Einholung der Einwilligung des Arbeitnehmers durch vertragliche Gestaltung. Aber auch hier muss es auf die Freiwilligkeit der Erteilung ankommen.

Datensicherheit

Wer sorgt für die Sicherheit der Daten? Auch die weiter zunehmende Praxis der Arbeit per Smartphone wirft Probleme auf. Wie sieht die Rechtslage hinsichtlich der Daten aus, wenn das Endgerät dem Mitarbeiter gehört? BYOD (bring your own device) birgt zumindest für den Arbeitgeber zu regelnde Problematiken, denn er muss u.a. gewährleisten, dass personenbezogene Daten, die der Mitarbeiter auf dem privaten Endgerät (oder auch im Home-Office) verarbeitet, gegen Verlust oder Missbrauch geschützt sind. Wer hat Zugang- und Zugriff auf die Daten auf dem privaten Endgerät? Kann ein Arbeitgeber die Daten von sich aus löschen oder sperren?

Oder anders herum gedacht: wie sichert der Arbeitgeber die unternehmenseigene Software gegen Angriffe von außen, die wissentlich oder willentlich vom Endgerät des Arbeitnehmers ausgehen?

Auch hier wird sich den Arbeitgebern mangels gesetzlichen Regelungen lediglich die Lösung durch vertragliche Gestaltung bzw. per Betriebsvereinbarung oder gar Tarifvertrag anbieten.

+ + +

International

Industrie 4.0 in den USA

Uzunma Bergmann, Attorney at Law (New York), Hannover
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

1. Allgemeine Wirtschaftslage

Auf der Seite des Auswärtigen Amts heißt es: die USA haben nach wie vor den Status als weltweit stärkste Wirtschaftsmacht inne. Insbesondere das durch „ unternehmerische Initiative und freien Handel gekennzeichnete Wirtschafts- und Finanzsystem“ hebt die USA im Wettbewerb um die stärkste Wirtschaftsmacht hervor.

Nach Angaben des U.S Departement of Commerce hat sich das Bruttoinlandsprodukt (engl. „Gross Domestic Product“ =GDP) nach ersten Schätzungen im zweiten Quartal 2016 gerade einmal um 1,2 % jährlich gesteigert und liegt dabei deutlich hinter den Erwartungen zurück. Ein weiterer Schätzwert, welcher auf vollständigeren Daten basiert, wird am 26. August 2016 veröffentlicht. Das Wachstum des US- BIP ist größtenteils auf die persönlichen Konsumausgaben zurückzuführen. Die Erwirtschaftung des BIP/ GDP setzt sich in der Regel wie folgt zusammen: der US-Dienstleistungssektor erwirtschaftet ca. 67%), der Industriesektor ca. 20 %, (davon 1% Landwirtschaft) und die Staatsquote liegt bei ca. 13 % (Bundes- und Staatenebene).

Die US- Wirtschaft hatte lange mit den Folgen der Wirtschafts- und Finanzkrise im Jahre 2008 zu kämpfen. Zunächst eroberte die Immobilienbranche den Markt und führte in den Jahren 2011 bis 2013 die US- Wirtschaft mit hohen Zuwachsraten deutlich an. Mittlerweile liegt der Preis der Immobilien in den Ballungsgebieten jedoch wieder auf dem Preisniveau von 2008. Deswegen kann man nun durchaus die momentane Konsumstärke der US- Amerikaner als „Motor“ des Aufschwungs bezeichnen.

Der derzeitige Stand der Industrieproduktion bereitet den produzierenden Unternehmen weiterhin große Sorgen. Diese entwickelte sich im Jahr 2015 noch deutlich schlechter als in den vorangegangenen Jahren. Die Auftragseingänge der Industrie gehen zurück und auch die Investitionen in neue Projekte verzeichnen einen deutlichen Rückgang. Die meisten Unternehmer thesaurieren ihre Gewinne nur noch und nutzen diese größtenteils für Aktienrückkäufe. Eine Entspannung der Lage in Industrie und Produktion ist derzeit nicht in Sicht.

Im Rahmen der Geldpolitik haben sich dagegen Neuerungen ergeben. Die Rate des Leitzinses (auf Basis der FED- Federal Reserve) ist erstmals seit neun Jahren wieder an-

gehoben worden. Im Dezember hat die FED den Leitzins um insgesamt 0,25 % angehoben, nachdem er zuvor auf einem Niveau nahe null gelegen hat.
Momentan herrscht noch allgemeine Unsicherheit über die Richtung, in die sich die US-Wirtschaft entwickelt und ob die FED im Zuge dessen neue Zinsschritte vornimmt. Dabei wird auch die Entwicklung der globalen Konjunktur und Finanzwelt einen großen Einfluss auf zukünftige Zinsentscheidungen haben. Momentan bewegt sich der Schlüsselsatz in der Spanne zwischen 0,25 und 0,5 % (Target Range, seit 16.12.2015) und befindet sich damit immer noch unter dem normalen Niveau.

Nach wie vor sind die USA eine Exportnation und stark im Außenhandel vertreten. Zusammen mit Deutschland, Japan und China gehören sie zu den weltgrößten Exporteuren. Die Hauptabnehmer von US- Exporten sind Länder wie China, Kanada, Mexiko, Japan und Deutschland. Um den Außenhandel zu stärken hat die USA bilaterale Freihandelsabkommen mit 20 Staaten abgeschlossen (Australien, Bahrain, Chile, Costa Rica, Dominikanische Republik, El Salvador, Guatemala, Honduras, Israel, Jordanien, Kanada, Kolumbien, Mexiko, Marokko, Nicaragua, Oman, Peru, Panama, Südkorea und Singapur).

Am 05. Oktober 2015 kam es zum Abschluss der Verhandlungen über ein regionales Handelsabkommen im asiatisch- pazifischen Raum, auch unter dem Namen Trans- Pazifische Partnerschaft (TPP) bekannt. Mit der Ratifikation des Abkommens kann TPP schließlich in Kraft treten. Damit ist jedoch nach momentanen Einschätzungen frühestens Ende 2016 zu rechnen.

Die EU und die USA verhandeln ebenfalls seit 2013 über eine Transatlantische Handels- und Investitionspartnerschaft (TTIP= Transatlantic Trade and Investment Partnership). Das Ziel ist hierbei eine die größte und bedeutendste Freihandelszone der Welt zu schaffen. Ob und wann TTIP umgesetzt wird, steht auch nach drei Jahren Verhandlungen noch zur Debatte.

Nach Einschätzung des IWF wächst die US-Wirtschaft in den kommenden Jahren trotz bisher eher strauchelnder Zahlen. Zwar wird für das Jahr 2016 nur noch ein Wirtschaftswachstum von 2,2 % statt 2,4% erwartet, jedoch wird das Wachstum laut Prognosen im Jahr 2017 auf 2,5 % ansteigen. Folgt man der Beurteilung des IWF befindet sich die USA wirtschaftlich derzeit „in einem guten Zustand“. Langfristig wird das Wirtschaftswachstum in den nächsten Jahren aber auf etwa durchschnittlich 2 % absinken. Ansonsten bleiben die Prognosen für das künftige Wirtschaftswachstum solide.

Gegenwärtig treiben die Unternehmen die US-Wirtschaft auf allen Ebenen an und fördern dadurch mitunter das Wirtschafswachstum.
Marketingaktionen wie der „Cyber Monday“ und „Black Friday“ sind mittlerweile den meisten Kunden ein Begriff und lassen die Ausgaben für Konsumgüter regelrecht in die Höhe schießen. Mit verschiedenen Rabatten werden die Kunden in dem Zeitraum nach Thanksgiving zum Kaufen anregt. Der Handelsriese Amazon hat jüngst den sogenann-

ten „Prime Day“ eingeführt, der dieses Jahr am 12.07.2016 stattfand. Die Verkäufe überstiegen sogar die vom vorangegangenen „Prime Day“, „Cyber Monday“ und „Black Friday“ .Daran lässt sich erkennen, dass besonders dem Ecommerce eine immer bedeutendere Rolle zukommt. Mit cleveren Aktionen, wie der von Amazon, können die Kunden an das Unternehmen gebunden und beachtliche Gewinne erwirtschaftetet werden. Um beispielsweise die Rabatte des „Prime Day“ nutzen zu können, muss man zunächst Prime-Kunde von Amazon werden oder bereits sein. Anhand dieser Entwicklungen lässt sich schließen, dass die Kunden in den USA sich immer mehr vom klassischen Einkauf in Ladengeschäften entfernen und stattdessen den bequemeren Weg über den Onlinehandel wählen.

Um Innovationen und das Wachstum in der Produktion zu steigern, hat die US-Regierung zudem verschiedene Initiativen wie „Educate to Innovate“ gestartet (die darauf abzielt, eine Million Studienabsolventen in Wissenschaft, Technologie, Ingenieurwesen und Mathematik in den nächsten zehn Jahren hervorzubringen) sowie das „National Network for Manufacturing Innovation“ (NNMI).

Das NNMI ist eine von der Regierung getragene Organisation, die Raum für technologische Forschung und Entwicklungen von neuen Herstellungsprozessen bietet. Sie bringt öffentliche und rechtliche Ressourcen zusammen mit technologischer Innovation und Forschung, um Innovationstätigkeit zu unterstützen und die Vermarktung von technologischen Errungenschaften zu fördern. Das NNMI hat zum Ziel, „Unternehmen zu unterstützen, die andernfalls nicht in die Forschung und Entwicklung von Zukunftsfähigen Herstellungsprozessen investieren würden, indem sie die besten Kräfte und Fähigkeiten aus dem öffentlichen und privaten Sektor in ein gemeinsames Umfeld für Hochtechnologie einbringt“.

2. Industrie 4.0 in den USA

Während Deutschland sich fest auf die Entwicklung seines Plans zu Industrie 4.0 konzentriert, liegen andere Länder in der Herausforderung, eine „smarter world“ zu erreichen, nicht weit dahinter. Die Verknüpfung von Menschen, Geräten und Internet ist weithin bekannt oder wird weithin bezeichnet als das „Internet of Things“.

Das Internet der Dinge (IoT) umfasst die Mehrheit der neuen technologischen Entwicklungen von Smartphones zu Smart Cities und Smart Factorys und es ist als das „buzz word“ für jeden Technologie- und Produktentwickler.

2.1. Industrial Internet

Das Gegenstück zu Industrie 4.0 ist in den USA das „*Industrial Internet*“. Das Industrial Internet beschreibt die Entwicklung eines Konzeptes, dass sich in der nahtlosen Integ-

ration von Menschen, physischen Objekten, Datenanalysen und virtuellen Welt verkörpert.

Der Begriff Industrial Internet wurde durch das Industrial Internet Consortium (IIC) geprägt, einer Non-Profit-Organisation, die 2014 von GE, AT&T, Cisco und IBM gegründet wurde. Das IIC hat zum erklärten Ziel die „ weit verstreuten Initiativen in diesem Ökosystem zu verbinden und Objekte mit Menschen, Prozessen und Daten durch gemeinsame Strukturen, Interoperabilität und offene Standards zu verbinden“. Das Konsortium hat inzwischen 212 Mitglieder aus den Bereichen Gesundheit, Energie, Produktion, Öffentliche Verwaltung und Verkehr. Das Industrial Internet und Industrie 4.0 sind vergleichbare Konzepte, unterscheiden sich aber in einigen wesentlichen Punkten. Während Industrie 4.0 einen nationalen Fokus hat und von Seiten der Bundesregierung in Deutschland betrieben wird, ist das IIC eine Mitglieder offene Organisation mit großen Konzernen als wesentliche Stake Holding. Außerdem ist das deutsche Konzept Industrie 4.0 auf Produktionsprozesse konzentriert, während das Industrial Internet alle Arten von Geschäftsprozesse umspannt.
Die folgende Übersicht, erstellt von der Manufacturers Alliance for Production and Innovation, illustriert anschaulich die Unterschiede der beiden Konzepte. Noch im Sommer 2015 sah die US-Wirtschaft den Vergleich von Industrie 4.0 und IIC so:

Comparison aspects	**Germany / Industrie 4.0**	**USA / Industrial Internet Consortium**
Key authors	German Government	Large multinationals
Key stakeholders	Government, academia, business	Business, academia, government
Taxonomy of revolutions	Four revolutions	Three revolutions
Support platforms	Government industrial policy	Open membership nonprofit consortium
Sectoral focus	Industry	Manufacturing, energy, transportation, healthcare, utilities, cities, agriculture
Technological focus	Supply chain coordination, embedded systems, automation, robots	Device communication, data-flows, device controls and integration, predictive analytics, industrial automation
Holistic focus	Hardware	Software, hardware, integration
Geographical focus	Germany and its companies	Global marketplace
Corporate focus	SMEs	Companies of all sizes
Optimization focus	Production optimization	Asset optimization
Standardization focus	On agenda	Recommendations to standards organizations
Economic approach	Normative economics	Positive economics
Overall business approach	Reactive	Proactive

Inzwischen haben sich die Konzepte inhaltlich und strategisch aufeinander zu bewegt.

Um die Machbarkeit möglicher Projekte sicherzustellen, führt die IIC Testverfahren durch: kontrollierte Prüfstände (*Testbeds*) , die mit der entsprechenden IIC Referenzarchitektur im Einklang stehen müssen und mit denen werden Lösungen entwickelt und getestet in einer Umgebung, die realen Bedingungen entspricht. Die IIC betreibt mehrere Prüfstände für kleine, mittlere und größere Anforderungen:

- Kleine Testbeds kurzfristige Projekte mit einem schnellen Ergebnis, überwiegend durch die Mitgliederunternehmen finanziert.

- Mittlere Testbeds konzentrieren sich üblicherweise auf ausgewählte, angestrebte Projekte, die teilweise durch die öffentliche Hand oder die Wissenschaft finanziert werden.

- Große Testbeds sind mehrjährige Projekte, die kontinuierlich neue Produkte und Services hervorbringen sollen. Oft sind dies branchenübergreifende Projekte mit mehreren Millionen Dollar Budget und Privat Public Partnerschaften.

2.2. Herausforderungen für das Internet der Dinge

Wie jedes andere neue Konzept sieht sich die Einführung des Internets der Dinge zahlreichen Herausforderungen ausgesetzt. Viele sind gerätebezogen wie Lebensdauer und Skalierbarkeit von Batterien, aber die meistdiskutierten Herausforderungen betreffen Regulierung, Interoperabilität, Sicherheit, Wartung und Aktualisierung (Updates).

Viele IoT-Entwickler sind sich darüber einig, dass ein Industriestandard erforderlich ist, um die Konformität von Geräten zu gewährleisten und Produktionsstandards sicherzustellen. Außerdem ist wichtig, dass neue Geräte mit bestehenden und neu entwickelten Netzwerken und Infrastrukturen kompatibel sind und schon anpassungsfähig genug, um mit verschiedenen Anwendungsplattformen und Kommunikationssystemen arbeiten zu können.

Weil IoT-Geräte dafür bestimmt sind, sich selbst zu regulieren und zu optimieren , muss großer Wert auf das menschliche Element und die Rückkopplung mit dem Gerät gelegt werden, insbesondere in den Fällen, in denen nur eine Sekunde Verzögerung den gesamten medizinischen Prozess oder Produktionsprozess aus dem Gleis bringen kann. Zusätzlich ist zu beachten, dass die erforderlichen Wartungen und Updates für eine viel größere Anzahl von Geräten im Internet als heute eine Überflutung darstellen kann, wenn dafür keine angemessene Vorsorge getroffen ist.

3. US-Umfeld für Investitionen

3.1. Arbeitsmarkt

Die USA sind von jeher ein Wunschziel für ausländische Arbeitnehmer und Investitionen, nicht zuletzt wegen ihrer relativ freundlichen Einwanderungsbestimmungen, die sich in der großen Zahl von H-1B Arbeitserlaubnissen jedes Jahr widerspiegeln. Andererseits zeigen sich bestimmte Bereiche des öffentlichen Amerika im Licht der jüngsten terroristischen Angriffe und der wachsenden Anti-Islam-Haltung weniger offen für eine Erhaltung von unbeschränkter Einwanderung, gleich ob legal oder auf andere Weise.

Staaten wir Alabama, Arizona, Indiana, South Carolina und Utah haben Gesetze verabschiedet, die die Polizei ermächtigen, Menschen über ihren Migrationsstatus zu vernehmen. Einige andere Bundesstaaten erleben Bürgerunruhen vor dem Hintergrund der Tötung von Angehörigen einer Minderheit durch die Polizei und diskriminierendem „Stop and frisk"- Vorgehensweise, also Anhalten und Durchsuchen.

Auch die bevorstehenden Präsidentenwahlen werden mit Diskussionen über die Einwanderungspolitik überflutet, wobei viele Hoffnungsträger der Republikaner sich für eine ernsthafte Beschränkung der Einwanderung aussprechen. Der Kandidat Donald Trump, hat dazu aufgerufen, an der Grenze zwischen den USA und Mexiko eine massive Mauer zu errichten, während er gleichzeitig erklärt, dass er im Fall seiner Wahl alle syrischen Flüchtlinge, die sich bereits legal in den USA aufhalten, wieder deportieren will.

Obwohl sich die Demokraten weiterhin über das Erfordernis für eine Einwanderungsreform einig sind, die einen Weg zur Einbürgerung für illegale Migranten eröffnet und/ oder der Abschiebung für bereits im Land Befindliche einen Riegel vorschiebt, bleibt Einwanderung ein heiß diskutiertes Thema und eine Besorgnis für alle Arbeitgeber, insbesondere in Staaten mit einem hohen Anteil an Immigranten.

Der US-Arbeitsmarkt sendet momentan weitestgehend gemischte Signale aus. Die Arbeitslosenquote ist im Juni 2016 auf 4,9 % gesunken und hat sich demnach positiv entwickelt. Allein im Juli 2016 konnte die Anzahl von Beschäftigten einen Anstieg von 255.000 Stellen verbuchen. Das übertrifft die bisherigen Schätzungen bei Weitem. Hingegen sinkt die Erwerbsquote stetig ab und liegt momentan bei 62,6 %. Das ist der bisher niedrigste Stand seit der Wirtschafts- und Finanzkrise. Hinsichtlich der Anzahl von Langzeitarbeitslosen ist die Quote deutlich gesunken. Im Mai 2016 lag sie lediglich noch bei 1,9 Millionen. Die Zahl von Beschäftigten, welche unfreiwillig in Teilzeit angestellt sind, stieg hingegen auf 6,43 Millionen im Mai 2016 an.

Im Großen und Ganzen bewerten jedoch Organisationen wie die IWF die Entwicklungen auf dem US- Arbeitsmarkt als durchaus positiv. Im Jahr 2016 stehen die USA nach Angaben des IWF arbeitstechnisch so gut da wie noch nie nach der Finanzkrise. Es

konnten insgesamt schon 2,4 Millionen neue Jobs geschaffen werden. Der Beschäftigungsaufbau schreitet also weiterhin voran. Der Stundenlohn stieg im Jahresvergleich um etwa 2,4 % Die insgesamt verbesserte Lage auf dem Arbeitsmarkt kurbelt vor allem die Wirtschaft durch vermehrte Ausgaben für Konsumgüter an.

Viele befürchten aufgrund der jüngsten Entwicklungen auf dem Arbeitsmarkt die Anhebung des Leitzinses. Experten wiegeln diese Ängste jedoch ab, da die FED höchstwahrscheinlich erst mögliche Folgen des Brexit-Votums und die Präsidentschaftswahl in den USA abwarten wird. Zudem war das US- Wirtschaftswachstum im letzten Quartal von 2016 zu schwach und dahingehend ist eine Zinserhöhung nach Einschätzung der Ökonomen eher unwahrscheinlich.

3.2. Arbeitsrecht

3.2.1 Freiberufliche Tätigkeiten und flexible Arbeitsbedingungen:

Der Trend der freiberuflichen Beschäftigung hat sich in den Vereinigten Staaten dramatisch verstärkt und gefährdet mittlerweile das klassische Bild der US-Arbeitsmarktstruktur. Nach einem 2015 erschienenen Bericht der Freelancers Union ist bereits etwa jeder dritte Beschäftigte freiberuflich tätig – die Zahl entspricht 34% der Erwerbsbevölkerung bzw. 35 Millionen Amerikanern.

Diese Zahlen stellen eine Steigerung dar gegenüber dem Bericht, der 2006 vom US-Rechnungshof veröffentlicht wurde, und demzufolge 31% der amerikanischen Beschäftigten freiberuflich, befristet oder in Teilzeit beschäftigt waren.

Dieser Anstieg von flexiblen Arbeitsverhältnissen kann mit mehreren Faktoren erklärt werden: Die weite Verbreitung mobiler Technik, die es ermöglich, von beliebigen Orten aus zu arbeiten; Entlassungswellen nach 2005, die mehr Menschen die Gründung kleiner, von zuhause aus betriebener Unternehmen abverlangt haben; in letzter Zeit ist der steigende Wunsch der Beschäftigten nach einer besseren work-life-balance hinzugetreten.

Freiberuflichkeit und andere flexible Arbeitsmodelle nutzen sowohl dem Arbeitgeber als auch dem Arbeitnehmer. Der Arbeitgeber kann sich die Dienste der besten Beschäftigten ortsunabhängig sichern. Produktivität, Effizienz und Zufriedenheit sollen dabei steigen, während Arbeitnehmerfluktuation und die damit verbundenen Einarbeitungskosten reduziert werden können. Der Arbeitnehmer erlebt eine bessere work-life-balance und reduziert Stress, was wiederum zu einer höheren Produktivität beiträgt.

Während dieses moderne Arbeitsmodell viele Vorteile haben mag, so stellt es die freiberuflichen Beschäftigten doch auch vor große wirtschaftliche Herausforderungen, weil wichtige arbeitsrechtliche Schutzbestimmungen nicht anwendbar sind. Zu dem wirtschaftlichen Stress aufgrund volatilen Einkommens und der Möglichkeit von Lohn-

wucher kommt hinzu, dass die meisten Freiberufler aufgrund ihres Beschäftigungsstatus keinen Kranken- oder Arbeitslosenversicherungsschutz genießen. Viele Unternehmen schließen Freiberufler auch von ihren Betriebsrenten-Programmen aus, wodurch Versorgungslücken bei längerer Arbeitslosigkeit und im Alter entstehen.

Der Bedarf an freiberuflicher und flexibler Arbeit zeigt keine Anzeichen der Stagnation, daher sollte das Arbeitsrecht modernisiert werden, um den Problemen dieses Beschäftigungsmodells Rechnung zu tragen. Das US-Arbeitsministerium hat eine Anhörung zu der Verwendung von elektronischen Geräten durch stundenweise Beschäftigte außerhalb des Betriebsgeländes gestartet. Es ist zu hoffen, dass diese Anhörung das Ministerium in die Lage versetzt, Richtlinien zu flexiblen Arbeitsmodellen und/oder Verordnungen zur Verbesserung der Arbeitsbedingungen von Freiberuflern zu erarbeiten.

3.2.2. Arbeitszeit und Überstunden

Die Novellierung der Verordnung zur Überstundenvergütung ist ein weiterer Punkt, der die Beschäftigten in den USA derzeit betrifft. Das geltende Arbeitsrecht sieht vor, dass Arbeitnehmer mit einem Jahresgehalt bis 23.660 US$ automatisch Überstundenvergütung erhalten, wenn sie länger als 40 Stunden pro Woche arbeiten. Dieser Automatismus greift jedoch nicht bei Arbeitnehmern, die als leitende Angestellte, Verwaltungsangestellte oder besonders qualifizierte Angestellte gelten; dadurch entsteht eine wirtschaftliche Härte für Menschen mit niedrigem Einkommen, die Leitungsaufgaben übernehmen.

Um die dadurch entstehenden Fälle der unbezahlten Überstunden zu bekämpfen, plant das US-Arbeitsministerium eine Novelle der Bestimmungen, die weitere 13,5 Millionen Beschäftigte unter den Anwendungsbereich des Fair Labor Standards Act stellt. Die Mehrzahl dieser Beschäftigten ist derzeit ausgenommen, weil sie als leitende Angestellte, Verwaltungsangestellte oder besonders qualifizierte Angestellte gelten.

Die US-Handelskammer und andere Gegner dieser Novelle argumentieren, dass die vorgeschlagenen neuen Regelungen besonders Beschäftigte in kleinen Betrieben treffen würden. Mehrere Arbeitgeberverbände gehen davon aus, dass Arbeitgeber zur Umgehung der neuen Überstundenregelungen ihre Beschäftigten zu Lohnarbeitern auf Stundenbasis umdeklarieren würden, womit den Beschäftigten alle Vorteile eines Angestelltenverhältnisses mit Festgehalt entgingen. Der US-Einzelhandelsverband prognostiziert, dass die Arbeitgeber eher die Gehälter und Boni kürzen oder die Arbeitszeit verkürzen, um Überstundenvergütungen zu vermeiden.

Es ist außerdem noch unklar, wie die neuen Überstundenregelungen Beschäftigte in flexiblen Arbeitsverhältnissen und in Heimarbeit betreffen, insbesondere in Abwesenheit klarer Richtlinien zur Regulierung dieser Beschäftigungsmodelle.

3.3. Geistiges Eigentum

Die Bedeutung des Schutzes von geistigem Eigentum *(Corporate, Patente, Datenbanken, Know-how, Betriebsgeheimnisse)* kann nicht überschätzt werden. Das Vermögen in geistigem Eigentum in einem Unternehmen hat herausragende Bedeutung – und IP-basierte Unternehmen haben einen wesentlichen Anteil am Wachstum der US- Wirtschaft.

Die USA haben das fortschrittlichste IP-Rechte-System in der Welt und sind der größte Markt für rechtsgeschützte Güter, mit jährlich über 80.000 nationalen Patenteintragungen und über 300.000 neuen Markenregistrierungen.

Nach Angaben des US Patent and Trademark Office (USPTO) sind die USA die bei weitem größte Quelle für internationale Patente unter dem Patent Cooperation Treaty; seine Erfinder machen etwa ein Drittel der weltweit angemeldeten Patente aus.

Ein Rechtsinhaber in den USA findet eine klare Struktur für den Rechtsschutz und die Registrierung für IP-Rechte vor, nämlich durch entsprechende Behörden, die dem Rechtsinhaber Unsicherheit, Zeit und Kosten erspart. Rechtsinhaber in den USA haben auch Zugang zu einer breiten Palette von Instrumenten zur Rechtsdurchsetzung, angefangen bei Zivilprozessen und Strafverfolgung, bis hin zu Grenzkontrollen und behördlichen Maßnahmen.

Der in den USA verfügbare breite inländische IP-Schutz wird durch Behörden durchgesetzt, insbesondere durch das USPTO, das US Copyright Office, die Food and Drug Administration (FDA), das Plant Variety Protection Office (Datenschutz), das Indian Arts and Crafts Board und die ITC, eine unabhängige Verwaltungsbehörde, die IP-Streitigkeiten über Importe von potenziellen rechtsverletzenden Waren behandelt.

Als Unterzeichnerstaat verschiedener internationaler Abkommen und bilateraler Vereinbarungen sind die USA in der Lage, nicht nur den von den Mitunterzeichnern verlangten Mindeststandard zu gewährleisten, sondern auch Vorteile aus den Schutzvorschriften der Abkommen zu gewähren, die unter nationalem Recht nicht bestehen. Die USA streben weiterhin danach, den IP-Rechtsschutz, insbesondere auch wegen der Herausforderungen konstanter Produktpiraterie und anderen Verletzungen aus bedeutenden Märkten wie China und Indien, zu verbessern.

Das jüngste, von dem Director der USPTO, Michelle Lee, mit dem Europäischen Patentamt (EPO), den Intellectual Property Office of the Philippines (IPOPHIL), unterzeichnete Memorandum of Understanding, ist ein solcher Schritt zur Schaffung einer internationalen Harmonisierung von Verfahren zum Schutz von geistigem Eigentum.

4. Informationen und Daten

Die zu erwartenden Vorteile aus Industrie 4.0 und seinem Gegenstück aus den USA sind zahlreich und wurden bereits umfangreich in Artikeln, technischen Papieren und Vorträgen in den letzten Jahren beschrieben. Dennoch wird den potentiellen Risiken, die als ein Ergebnis aus der Übernahme dieses Konzeptes entstehen können, wenig Aufmerksamkeit gewidmet.

Technologie-Experten sind der Meinung, dass potentielle Risiken wohl in drei Kategorien eingeteilt werden können: Privacy, Security and Safety, also Privatheit und Personendatenschutz, Sicherheit von Daten und Sicherheit von Gegenständen und Prozessen.

4.1. Privatheit

Das Internet of Things ist dazu gedacht, das tägliche Leben leichter zu machen und die Bedienungen unserer Geräte intuitiver. Man stelle sich vor, dass das Smartphone alle Verabredungen managt, Erinnerungen sendet und mit dem Auto kommuniziert, um den günstigsten GPS- gesteuerten Weg zu finden, das Trainingsgerät sagt, wann und wie lange man laufen soll, Kalorienverbrauch gegenüber Kalorienaufnahme abgleicht, den Blutdruck misst, an den jährlichen Arzttermin erinnert und die Kaffeemaschine exakt 10 Minuten nach Rückkehr vom täglichen Joggen startet, natürlich überwacht durch das Gerät am Handgelenk.

Nun muss man sich vorstellen, dass all diese Informationen über persönliche Vorlieben, Gesundheit, Ausgaben und sogar persönliche Stimmungen durch mehrere integrierte Systeme verarbeitet und gespeichert werden, um den Nutzer mit noch zuverlässigeren, besseren Services zu versorgen. All diese so zusammengetragenen Informationen liefern ein nahezu vollständiges Bild der Person des Trägers und seines Verhaltens und lässt wenig Spielraum für den Menschen für Informationen, die gegenüber dem „System“ privat bleiben. Es sind Informationen über den Träger. Die Informationen werden vermutlich frei an das IT-Gerät gegeben, wem aber gehören die Informationen und wer entscheidet, wie sie verwendet werden dürfen? Hinzu kommt die Problematik der „collateral information“, also der Daten, die das Gerät nebenher einsammelt, während der Träger die gewählte Funktion des Gerätes nutzt. Die Sammlung, Nutzung und Speicherung all dieser Informationen muss daher gut reguliert werden.

4.2. Recht auf Schutz der Privatsphäre und auf Datenschutz

Das US-amerikanische Bundesdatenschutzgesetz (*Federal Privacy Act*) wurde 1974 zur Regulierung der Sammlung, Pflege, Nutzung und Weitergabe der personenbezogenen Daten von Privatpersonen durch Bundesbehörden erlassen. Dieses Gesetz verkörpert

die Prinzipien des fairen Umgangs mit Informationen und schützt die Privatsphäre des Einzelnen dadurch, dass es vorsieht, dass die Regierung offen legt, welche Aufzeichnungen über Privatpersonen geführt werden und dem Austausch von solchen Daten Einschränkungen auferlegt. Schließlich verleiht es Einzelpersonen das Recht, die Regierung wegen Verletzungen der Bestimmungen des Gesetzes zu verklagen.

Viele der Prinzipien des fairen Umgangs mit Informationen, die in dem Datenschutzgesetz festgelegt sind, finden sich in den Datenschutzgesetzen anderer Länder, einschließlich in Teilen der EU-Datenschutzrichtlinie von 1995.

4.2.1. *Bundesrecht / Federal Law*

In den USA existiert kein einheitliches nationales Gesetz zur Regelung der Sammlung, der Nutzung und dem Schutz von Privatsphäre und persönlichen Daten von Privatpersonen. Es existieren jedoch umfangreiche Bundesgesetze, Staatsgesetze sowie sonstige Regelungen, die zum Schutz beitragen und den Großteil der Rahmenbedingungen für den Datenschutz in den USA darstellen. Obgleich es keine ausdrücklich benannte zentrale Datenaufsichtsbehörde gibt, wird die Bundeshandelskommission, die Federal Trade Commission (FTC) allgemein als die "de-facto" Regulierungsbehörde für den Schutz der Privatsphäre in den USA angesehen.

Zu diesen wichtigen Bundesgesetzen gehören unter anderem:

- *Electronic Communications Privacy Act* und *Communications Act*
  betrifft kundenspezifische geschützte Netzwerkinformationen, sog. Consumer Proprietary Network Information,

- *Children's Online Privacy Protection Act*
  das Gesetz zum Schutz der Privatsphäre von Kindern im Internet von 1998,

- *Financial Services Modernization Act*
  Gesetz zur Modernisierung von Finanzdienstleistungen von 1999 (der GLBA),

- *Fair Credit Reporting Act*
  Gesetz zur Regelung des Datenschutzes bei Konsumentenkrediten,

- *Telephone Consumer Protection Act*
  sowie das Telefon-Verbraucherschutzgesetz von 1991

- *Health Insurance Portability and Accountability Act*
  das Gesetz zur Übertragbarkeit von Krankenversicherungen und zur Rechenschaftspflicht der Krankenversicherer von 1996 (HIPPA).

Im Jahr 2015 wurden mehrere Entwürfe für Bundesgesetze zum Schutz der Privatsphäre und personenbezogener Daten eingebracht. Diese umfassen u.a.:

- *Data Broker Accountability and Transparency Ac*t
  das Gesetz zur Rechenschaftspflicht und Transparenz von Informationsvermittlern würde es Verbrauchern ermöglichen, auf ihre Daten zuzugreifen und diese zu korrigieren. Verbraucher hätten danach das Recht, Datenvermittler daran zu hindern, ihre persönlichen Daten für Marketingzwecke zu verwenden, weiterzugeben oder zu verkaufen. Der Gesetzentwurf befugt ferner die Federal Trade Commission (FTC) zur Durchsetzung des Gesetzes und zur Einrichtung einer zentralen Website, auf der Verbraucher eine Liste der erfassten Datenvermittler sowie von Information über Verbraucherrechte einsehen können.

- *Consumer Privacy Protection Act*
  das Gesetz zum Schutz von Verbraucherdaten würde einen rechtlichen Rahmen für Benachrichtigungspflichten bei Sicherheitsverletzungen schaffen. Dieses Gesetz würde ein breites Spektrum an Schutz für personenbezogene Daten wie Kontodaten, Sozialversicherungsnummern, biometrische Daten bis hin zu persönliche Gesundheitsinformation sowie Zugang zu privaten digitalen Fotos und Videos bieten.

- *Student Digital Privacy and Parental Rights Act*,
  würde den Verkauf oder die Veröffentlichung von personenbezogenen Daten von Studenten durch Betreiber von Webseiten oder anderen Online-Diensten verbieten. Nach diesem Gesetzesentwurf könnten Eltern von einer Bildungseinrichtung Zugang zu allen Informationen über ihre Kinder verlangen und diese herunterladen, oder diese löschen oder korrigieren lassen.

4.2.2. *Consumer Privacy Bill of Rights*

In einem Schritt hin zum Aufbau eines nationalen Datenschutzrechts für den Schutz der Verbraucherdaten in den USA hat Präsident Obama am 27. Februar 2015 die Consumer Privacy Bill, eine Charta der Datenschutzrechte von Verbrauchern drei Jahre erneut eingebracht, nach dem ersten Versuch im Februar 2012.

Dieser Entwurf flankiert den *Data Security and Breach Notification Act* von 2015, der Unternehmen vorschreibt, jeden Verstoß gegen ihre Daten zeitnah offenzulegen, um das Risiko eines Identitätsdiebstahls zu reduzieren.

Falls der Entwurf umgesetzt wird, wird er die Sammlung, Verbreitung und Speicherung von Kundendaten durch Datenvermittler und andere Unternehmen regeln. Das Weiße Haus erklärte, der Entwurf würde „Verbrauchern mehr Kontrolle über ihre Daten ermöglichen, Unternehmen klarere Möglichkeiten bieten, ihr verantwortungsvolle Haushalterschaft über Daten zu signalisieren und verschafft jedem die Flexibilität, im digitalen Zeitalter auch weiterhin Neues zu entwickeln“.

Das Gesetz wäre auf jede Person anwendbar, die „im innerstaatlichen Handel personenbezogene Daten sammelt, erzeugt, verarbeitet, behält, verwendet oder preisgibt bzw. solche Daten, sammelt, erzeugt, verarbeitet, behält, verwendet oder preisgibt, die den innerstaatlichen Handel betreffen." Im Gegensatz zu der derzeitigen Situation, würden nach diesem Gesetz auch gemeinnützige Organisationen der Kontrolle der FTC unterfallen.

Der Begriff „personenbezogene Daten" im Sinne des Gesetzes bezieht sich auf alle nicht-öffentlich verfügbaren Daten, die unter der Kontrolle der erfassten Organisation stehen, die mit einer Einzelperson oder einem Gerät, das im direkten Zusammenhang mit einer Einzelperson steht, in Verbindung gebracht werden können. Personenbezogene Daten würden auch „eindeutig beschreibende Informationen über persönliche Computer oder Kommunikationsgeräte" und andere „einzigartige dauerhafte Identifikatoren" mit einschließen.

Bestimmte Organisationen sind von dem Gesetz ausgenommen, einschließlich solcher

- mit 25 oder weniger Mitarbeitern, die nur Daten von Mitarbeitern und Bewerber verarbeiten;
- die keine „sensiblen Daten" verarbeiten und entweder (1) in einem Zeitraum von 12 Monaten personenbezogene Daten von weniger als 10.000 Einzelpersonen und Geräten sammeln oder (2) mit 5 oder weniger Beschäftigten;

Das Gesetz würde im Wesentlichen von der Bundeshandelskommission (FTC) sowie von den Justizministern der Bundesstaaten mittels Rechtsschutz durch Unterlassungsverfahren durchgesetzt werden. Bei einer Verletzung des Gesetzes berechnet sich die Strafe mit nach der Zahl der Verletzungstage, multipliziert mit einem von der FTC festgelegten Betrag (von nicht mehr als $ 35.000) nach der Zahl der direkt betroffenen Verbraucher, multipliziert mit einem Betrag von bis zu $ 5.000.

Die *Consumer Privacy Bill of Rights* bestimmt einen Katalog von Grundsätzen zu Datenschutz und Privatheit:

- *Transparenz*

  Betroffene Organisationen müssten Einzelpersonen präzise, deutliche und leicht verständliche Hinweise mit zutreffenden, klaren und zeitnahen Informationen über die Datenschutz- und Sicherheitsrichtlinien der Organisation geben.

- *Individuelle Kontrolle*

  Einzelpersonen würden mit Instrumentarien zur Kontrolle ihrer persönlichen Daten ausgestattet, die im angemessenen Verhältnis zu den Risiken für die Privatsphäre stehen. Das Gesetz sieht ferner vor, dass Einzelpersonen ihre Zu-

stimmung zur Verarbeitung ihrer Daten unter bestimmten Voraussetzungen widerrufen können.

- *Gezielte Sammlung und verantwortungsvolle Nutzung*

  Personenbezogene Daten müssen auf eine Weise gesammelt, aufbewahrt und verwendet werden, die im Hinblick auf den Kontext und zur Minimierung von Risiken für die Privatsphäre der Einzelperson angemessen sind. Das Gesetz definiert den Begriff „Kontext" an Hand mehrerer Faktoren einschließlich des Umfangs und der Häufigkeit der Interaktionen zwischen den Einzelpersonen und der Organisation, des Verständnisses eines Nutzers, wie die Organisation gesammelte Daten verarbeitet sowie der Art der verarbeiteten personenbezogenen Daten. Von den erfassten Organisationen wird verlangt, dass sie personenbezogene Daten innerhalb einer angemessenen Frist nach Erfüllung der Zwecke, für die die Daten erhoben wurden, löschen und zerstören.

- *Beachtung des Kontexts*

  Betroffene Organisationen müssten personenbezogene Daten auf eine Weise verarbeiten, die in Hinblick auf ihren „Kontext", d. h. in Hinblick auf das Verhältnis zwischen der Einzelperson und der Organisation angemessen ist. Von nicht regelkonform handelnden Organisationen wird verlangt, dass diese eine Risikoanalyse durchführen und Einzelpersonen eine „gesteigerte Transparenz- und Individualkontrolle" bieten.

- *Sicherheit*

  Betroffene Organisationen müssten eine Bewertung des Sicherheitsrisikos vornehmen und auf deren Grundlage angemessene Schutzmaßnahmen zur treffen.

- *Zugriff und Richtigkeit*

  Betroffene Organisationen müssten generell Einzelpersonen Zugriff zu ihren Daten ermöglichen. Zusätzlich haben die Organisationen angemessene Schritte zu unternehmen, die Richtigkeit der sich unter ihrer Kontrolle befindenden personenbezogenen Daten sicherzustellen und den Einzelpersonen zu ermöglichen, ihre personenbezogenen Daten zu bestreiten, zu vervollständigen oder zu berichtigen.

- *Rechenschaftspflicht*

  Von den erfassten Organisationen würde verlangt werden, Schulungen für Angestellte anzubieten, interne Datenschutzbewertungen durchzuführen und von Dritten, welche die Daten erhalten, zu verlangen, dass sie diese in Über-

einstimmung mit den vereinbarten Verpflichtungen der erfassten Organisation verwenden.

Der Entwurf der *Consumer Privacy Bill of Rights* hat starke Kritik sowohl von Verbraucherdatenschützern als auch Branchenbeteiligten erhalten. Der Gesetzesentwurf ist durch Stellungnahmen, die seine Mängel hervorheben, ins Stocken gebracht worden, u. a. durch Behauptungen, er enthalte nur schwache Regelungen zur Durchsetzbarkeit, unzureichende Definitionen der wesentlichen Begriffe, gewähre Privatpersonen keine Klagerechte, und schaffe für zu viele Organisationen Ausnahmen. Außerdem beschränke er die Durchsetzungsbefugnisse der Justizminister der Bundesstaaten und würde die FTC für ihre zusätzlichen Aufgaben nicht angemessen ausstatten.

Eine beträchtliche Anzahl an Streitpunkten ist noch zu bereinigen, bevor das Gesetz verabschiedet wird. Es stellt jedoch einen wichtigen Schritt zur Verbesserung des Datenschutzes und zur Schaffung einer dringend erforderlichen nationalen Regelung dar, insbesondere angesichts der wiederkehrenden Datenschutzverletzungen und der potenziellen Streitigkeiten mit dem Aufkommen des Internet der Dinge.

4.2.3. *Einzelstaatliches Recht / State Law*

Das Recht der US-Bundesstaaten hat sich ebenfalls rasch entwickelt, um die Verwendung und Erhebung von personenbezogenen Daten zu regulieren. Gegenwärtig existiert eine Vielzahl staatlicher Gesetze, die den Schutz der Privatsphäre von Kindern im Internet regeln sowie die Benachrichtigung über das Sammeln von Daten, die Datenschutzerklärungen für Webseiten, Cyber-Stalking, Benachrichtigungen im Fall von Sicherheitsverstößen, den Zugriff von Arbeitgebern auf die Social-Media-Accounts ihrer Angestellten und das Recht einer Einzelperson auf Datenvernichtung.

Beispiel Kalifornien

Der Staat Kalifornien gilt weithin als der Staat mit den umfangreichsten Datenschutzgesetzen in den Vereinigten Staaten. Die Einrichtung des Amtes für den Schutz der Privatsphäre und die Verabschiedung eines Gesetzes über Benachrichtigungen bei Sicherheitsverletzungen sind nur zwei Beispiele aus einer langen Liste von Maßnahmen, die von dem Staat unternommen worden sind, um den Schutz der Privatsphäre im Staat zu verbessern.

Die folgenden Angaben verdeutlichen Kaliforniens Zukunftsorientiertheit mit Bezug auf den Schutz der Privatsphäre:

Im Oktober 2015 hat Kalifornien mit dem *Electronics Communications Privacy Act*, dem Datenschutzgesetz für elektronische Kommunikation, das umfassendste Gesetz zum

Schutz der digitalen Privatsphäre im ganzen Land verabschiedet. Das Gesetz verbietet staatlichen Vollstreckungsbehörden bzw. anderen Untersuchungsstellen, ein Unternehmen zu zwingen, ihnen ohne eine gerichtliche Anordnung Metadaten oder digitalen Schriftwechsel (einschließlich E-Mails, Texte oder auf einer Cloud gespeicherte Dokumente) auszuhändigen. Das Erfordernis einer gerichtlichen Anordnung stellt eine wesentliche Änderung gegenüber dem Federal Electronic Communications Privacy Act dar, nach dem lediglich eine Vorladung (*Subpoena*) erforderlich ist, um Informationen zu erhalten, die älter als 180 Tage sind, falls diese für Zwecke des Gesetzesvollzugs benötigt werden.

Das Recht über die Offenlegung von Informationsweitergabe, das *Information Sharing Disclosure (Shine the Light) Law*, erfordert, dass Unternehmen die Daten Dritter, mit denen sie persönliche Kundendaten ausgetauscht haben, offen legen. Kunden müssen über die Offenlegung informiert werden und eine Nichtbeachtung kann ein Bußgeld in Höhe von $ 3.000 pro Verstoß zur Folge haben.

Im Bereich der Technik regelt Kalifornien zum Schutz der Privatsphäre die Spracherkennungsfunktionen von Fernsehgeräten mit Einschränkungen der Wiedererkennungsfunktionen der Geräte. Benutzer müssen über die Existenz solcher Spracherkennungsfunktionen sowie auf den Umfang der Nutzung der dadurch gesammelten Daten durch den Hersteller informiert werden.

Der *Student Online Personal Information Protection Act (SOPIPA)* beschränkt die Verwendung und Offenlegung von Informationen in Bezug auf Schüler, von Kindergartenkindern bis hin zu Schülern des 12. Jahrgangs. Er verbietet es Betreibern von Webseiten oder Online-Diensten, Informationen, die diese auf ihren Webseiten oder Diensten gesammelt haben, dafür zu verwenden, mit ihrer Werbung direkt auf die Schüler, ihre Eltern oder Erziehungsberechtigten zu zielen oder Daten über die Schüler zu sammeln. Den Betreibern ist es ebenfalls untersagt, spezifische Informationen in Bezug auf die Schüler zu verkaufen oder offen zu legen.

Einige staatliche und bundesstaatliche Gesetze ermöglichen es Einzelpersonen und Gruppen von Einzelpersonen, gerichtlich gegen Datenschutzverletzungen vorzugehen. Solche Gerichtsverfahren können im Ergebnis zur Verhängung von beträchtlichen Bußgeldern bzw. der Zuerkennung eines erheblichen Schadensersatzes führen.

> *Die Sony Corporation hat infolge von Klagen über Datenschutzverletzungen schätzungsweise 2 Milliarden US-Dollar verloren. Nachdem Cyber-Angriffe auf das Sony PlayStation Netzwerk im Jahr 2011 den Diebstahl persönlicher Daten von ca. 77 Millionen Konten zur Folge hatte, wurde Sony in über 55 Sammelklageschriften verklagt. In den Klageschriften wurde geltend gemacht, Sony habe Kunden über die Attacke zu spät informiert. Infolge des unbefugten Zugriffs auf ihre von dem Sony Network gespeicherten persönlichen Identifikations- und Finanzinformationen hätten Kunden Schäden erlitten.*
>
> *Im Oktober 2015 hat sich Sony auch zur Zahlung einer Abfindung von rund 8*

Millionen US-Dollar an seine ehemaligen und aktuellen Mitarbeiter bereit erklärt. Zu diesem Vergleich kam es nach Forderungen der Angestellten in Bezug auf den Diebstahl ihrer persönlichen Informationen im Rahmen eines Hacker-Angriffs auf das Unternehmen im Jahr 2014.

4.2.4. *Selbstregulierung*

Zusätzlich zu den Bundesgesetzen und den Gesetzen der Bundesstaaten, die bereits in Kraft sind, haben einige Branchen Richtlinien zur Selbstkontrolle eingeführt, die die „Best Practices" für die jeweilige Branche darstellen. Obgleich diese Richtlinien mangels Rechtsverbindlichkeit nicht als Gesetze betrachtet werden, sind sie bindend für die Mitglieder dieser Branche und erzeugen somit einen Standard für Rechenschaftspflichten, der von Aufsichtsbehörden angewendet werden kann, um die Einhaltung und Durchsetzung sicherzustellen.

Selbstregulierung ist auch in Situationen wirkungsvoll, in denen der Staat aufgrund der Bestimmungen des 1st Amendment (freie Rede) der US-Verfassung nicht eingreifen darf. Denn ungeachtet des 1st Amendment können die Selbstregulierungsrichtlinien der Industrie ihre Mitgliedsunternehmen aus Gründen des öffentlichen Wohles ohne staatliche Beteiligung zur Einhaltung zwingen.

In den USA bestehen wirkungsvolle Selbstregulierungstandards in der Werbe-, Unterhaltungs- und Alkoholindustrie. In der Werbeindustrie haben sich alle Mitglieder der Network Advertising Initiative (NAI) sich damit einverstanden erklärt, den NAI-Kodex einzuhalten, der aus gründlichen jährlichen Überprüfungen, laufenden technischen Überwachungen und der Festlegung eines klaren Verfahrens für die Untersuchung und Bewertung von Beschwerden über Nichteinhaltungen besteht.

Das Better Business Bureau spielt ebenfalls eine wichtige Rolle bei der Selbstregulierung der Werbeindustrie, da es den Advertising Self Regulatory Council (ASRC) verwaltet, der in Verbindung mit der National Advertising Division (NAD) zu 200 Durchsetzungsentscheidungen geführt hat, die die Werbestandards des ASRC verteidigen.

In der Medien- und Unterhaltungsbranche gehören zu den Interessengruppen der Branche die Recording Industry Association of America (RIAA), die über 85% der in den USA aufgezeichneten Musik vertreibt; die Motion Picture Association of America (MPAA) sowie die Entertainment Software Association (ESA). Diese Organisationen haben jeweils Richtlinien zur Selbstkontrolle eingeführt und unterhalten diese, um für ihre Musik, Filme und Videospiele geeignete Altersangaben und Inhaltsangaben festzulegen.

Die Alkoholindustrie hat durch ihre wichtigsten Industrieverbände - den Distilled Spirits Council of the United States (DISCUS), das Beer Institute (BI) und das Wine Institute

(WI) Richtlinien zur Regelung des Verkaufs und der Vermarktung von alkoholischen Getränken an Minderjährige eingeführt.

4.2.5. *Die Rolle der FTC im Datenschutz*

Als wichtigste Datenschutzregulierungsbehörde in den USA ist die Federal Trade Commission (FTC) verantwortlich für die Einhaltung und Durchsetzung der Gesetze, Richtlinien und Best Practices, die für die Wirtschaftsbranchen verbindlich sind. Die „Best Practices" sind selbstauferlegt und in der Regel ein Ergebnis der Zusammenarbeit zwischen der Industrie und staatlichen Stellen und privaten und akademischen Organisationen. Diese arbeiten gemeinsam daran, den Datenschutz voranzutreiben und gleichzeitig Innovationen bei den beteiligten Industriepartnern zu fördern. Nachdem die Richtlinien festgelegt und von Mitgliedern der Industrie angenommen worden sind, können sie durch die FTC und andere Behörden durchgesetzt werden.

Die FTC ist zwar nicht die einzige Agentur für die Umsetzung der US-Datenschutzgesetze, führt aber die meisten Durchsetzungsverfahren. In ihrer Rolle als Regulierungsbehörde leitet die FTC Verfahren gegen Unternehmen ein, wenn deren Praktiken als „grundlegend unfair oder irreführend" erachtet werden, weil sie die Sicherheitsbestimmungen, die Datenschutzbestimmungen und den Schutz von Verbraucherinformationen nicht einhalten.

Die FTC ist befugt, Ermittlungen zu möglichen Verletzungen einzuleiten, Zivilklagen anzustrengen, Unterlassungsanordnungen zu erlassen und Beschwerden bei Gericht einzureichen. Die FTC erstellt auch Berichte zum Datenschutz und anderen Fragen, die mit dem Verbraucherschutz zusammenhängen. Ein solcher Bericht ist der Bericht über das Internet der Dinge (IoT) aus dem Jahr 2015, der vorschlägt, dass Entwickler von IoT-Produkte die Best-Practice-Standards der Netzsicherheitsbranche übernehmen.

Eine Nichteinhaltung von gesetzlich vorgeschriebenen Datenschutzbestimmungen seitens eines Unternehmens wie etwa von Unternehmen die im Bereich medizinischer Informationen, mobile Apps, und finanzielle Daten tätig sind, wird als eine Verletzung angesehen, die die FTC ahndet. Des Weiteren wird eine Nichteinhaltung von selbstauferlegten Richtlinien oder von Unternehmen veröffentlichten Datenschutzrichtlinien ebenfalls als eine „irreführende Verhaltensweise" i. S. d. Paragraphen 5 des FTC Act eingestuft, da die Öffentlichkeit sich auf eine solche Aussage verlässt.

> *Im März 2016 erklärten sich Lord & Taylor, eine nationale Kette damit einverstanden, FTC Vorwürfe von Verbrauchertäuschungen im Zusammenhang mit ihrer Online Marketing Kampagne für ihre Design Lab Kollektion gütlich beizulegen. Im Zuge des Vergleichs in Bezug auf die Vorwürfe ist es Lord & Taylor untersagt, fälschlich zu darzustellen, ihre bezahlten Anzeigen kämen von einer unabhängigen Quelle und es wird von ihr gefordert, dass ihre Einflussnehmer klar offen legen, wann sie im Gegenzug für ihre Empfehlung entschädigt worden sind.*

Nach einem jahrelangem Rechtsstreit erklärte sich die Wyndham Hotels Gruppe im Dezember 2015 dazu bereit , die von der FTC vorgebrachten Vorwürfe, die Sicherheitsverfahren des Unternehmens setzen die Finanzdaten von Hunderttausenden von Kunden unfair Angriffen durch Hacker aus, gütlich beizulegen. Das Bundesberufungsgericht bestätigte die Befugnis der FTC, Datensicherheitsstandards durchzusetzen und verteidigte damit die Rolle der FTC im Rahmen des „Schutzes der Privatsphäre der Verbraucher und der Förderung stärker Sicherheitsstandards".

Im Jahr 2013 strengte die FTC auch Durchsetzungsverfahren im wachsenden Sektor des Internets der Dinge an. TRENDnet, ein Unternehmen, das Videokameras herstellt, legte Vorwürfe der FTC in Bezug auf die von dem Unternehmen hergestellten ferngesteuerten Heimvideokameras gütlich bei. Trotz zahlreicher öffentlichen Äußerungen, dass die Kameras „sicher" seien, führten Mängel in der Software zu einer Preisgabe privater Kamera-Feeds von Hunderten von Kunden über das Internet. Der Vergleich mit der FTC legte Trendnet umfangreichen Pflichten auf, einschließlich eines Verbots zukünftiger Falschdarstellungen ub Bezug auf seine Kamera-Sicherheit; der Schaffung eines umfassenden Informationssicherheitsprogramms; des Einverständnisses dazu, sein Sicherheitsprogramm für die nächsten 20 Jahre alle zwei Jahre von Dritten überprüfen zu lassen und Kunden aktualisierte Sicherheitsmitteilungen sowie kostenlose technische Unterstützung zukommen zu lassen.

Die FTC koordiniert ihre Maßnahmen häufig mit den Bundesbehörden.

Im Jahr 2010 unterzeichnete die FTC eine einvernehmliche Einigung (consent order) mit der Rite Aid Corporation und ihren 40 Tochtergesellschaften zur Beilegung von möglichen Verstößen gegen den FCT Act. Diese FTC Vereinbarung resultierte aus dem $ 1 Million Vergleich der Corporation in Bezug auf mögliche Verletzungen der Datenschutzregelung des Health Insurance Portability und Accountability Act von 1996 (HIPAA) im Zusammenhang mit einem Versäumnis, sensible Kundeninformation bei der Entsorgung von Verschreibungen und Medikamentenflaschen in Müllcontainern zu schützen.

4.3. *Dateneigentum im Internet der Dinge*

Die Frage nach der Eigentümerstellung an Daten, die von einem IoT-System (IoT = Internet of Things, Internet der Dinge) übertragen werden, wird viel diskutiert, ist aber noch unbeantwortet. Es gibt freilich durch die integrierte Natur von IoT-Geräten und den zahlreichen ineinandergreifenden Hard- und Softwarekomponenten zahlreiche Akteure, die jeder für sich ein Interesse an der Eigentümerstellung an diesen Daten haben könne.

Die gegenwärtige Situation ist, dass niemandem diese Daten gehören. Nach US-amerikanischem Recht gibt es kein Recht an einem einzelnen Datensatz oder sogar einer Mehrzahl an isolierten Datensätzen. Gleichwohl, eine Datenbank im Sinne einer Sammlung oder Zusammenstellung von Daten kann unter Umständen urheberrechtlichen Schutz genießen.

Der *Copyright Act* (17. U.S.C. § 101) definiert eine Zusammenstellung als eine Sammlung besehender Elemente, die

> *dergestalt ausgewählt sind, dass das sich daraus ergebende Gesamtwerk im Ganzen eine originäre geistige Schöpfung darstellt.*

Bei den bestehenden Elemente, auf die das Gesetz Bezug nimmt, kann es sich ihrerseits um rechtlich geschützte, proprietäre Informationen handeln, oder um einfache Tatsachen, die nicht geschützt sind. Wenn die in der Datenbank enthaltenen Elemente ihrerseits nicht rechtlich geschützt sind, dann genießen die Daten allenfalls als Zusammenstellung rechtlichen Schutz.

Nicht alle Datenbanken werden durch den Copyright Act als Zusammenstellung rechtlich geschützt. Der U.S. Supreme Court hat in dem Fall Feist Publications vs. Rural Telephone Service Company entschieden, dass eine Datenbank hinsichtlich der Auswahl der Elemente, ihrer Zusammensetzung und Anordnung Originalität aufweisen muss, um geschützt zu sein. Das Gericht befand, dass „die schiere alphabetische Anordnung von Daten ist nicht originell genug für urheberrechtlichen Schutz, es sei denn, die Auswahl oder die Zusammensetzung weisen Originalität auf“. Wenn z.B. ein Endnutzer ein Pedometer oder ein ähnliches Activity-Tracking-Gerät verwendet, dann wird es beim Nutzer sicherlich an der geistigen Schöpfung und mithin an der Originalität der Daten im Sinne der rechtlichen Anforderungen fehlen. Zusätzlich werden in IoT-Systemen in Echtzeit verarbeitet und weiterverbreitet, wodurch es Entwicklern und Anbietern schwer fallen dürfte, den gesetzlichen Anforderungen an die Originalität der Zusammensetzung zu erfüllen. In Abwesenheit gesetzlichen Schutzes sind die Rechtspositionen der Beteiligten unklar und müssen von Fall zu Fall untersucht werden.

Jedenfalls schützt das Urheberrecht nicht die Extraktion einzelner Tatsachen (die nicht geschützt werden können) aus der Datenbank, solange nicht die ganze Sammlung kopiert wird. Der begrenzte Urheberrechtsschutz für Datenbanken gebietet es den Entwicklern und Eigentümern von Datenbanken, auf vertraglicher Grundlage die unerwünschte Nutzung ihrer Datenbanken zu verhindern und so ihre Chancen auf Unterlassungs- und Schadensersatzansprüche im Fall der Zuwiderhandlung zu erhöhen.

Die Frage nach dem Eigentum an einer Datenbank ist nicht nur wegen des potenziellen Werts der Datenbank selbst (für datenbasierte unternehmerische Entscheidungen, zielgerichtete Werbung und Produktverbesserungen) von großer Wichtigkeit, sondern verschafft auch Klarheit darüber, wer die Daten eigentlich für sich nutzen und Dritten zur Nutzung überlassen darf. Während das Eigentum an der Datenbank durch vertragliche Regelungen zwischen den Beteiligten sicher geklärt werden können, bedarf es

klarer Abgrenzungen hinsichtlich der Befugnisse aller Beteiligten auf dem Weg der IoT-Daten vom Gerät zum integrierten System.

Wenn das Eigentum an der Datenbank im Internet der Dinge standardmäßig den Unternehmen und Geräteherstellern zufallen soll, würde dies Fragen über die Reaktionen von Verbrauchern aufwerfen, die sich über die Kontrolle über die Sammlung, Nutzung und Eigentümerstellung hinsichtlich ihrer persönlichen Daten machen.

Nach Alex Pentland, Professor für Medienwissenschaften am MIT, wird das Versagen beim Definieren und Kontrollieren des Flusses und des Eigentums an Daten zu öffentlichen Protesten und Überregulierung und somit letztlich zu einer Verzögerung des IoT führen. Pentland hat ein Regulierungsmodell ersonnen, das er „New Deal on Data“ nennt und dem zufolge Verbraucher stets genau erfassen könnten, welche Daten durch ihre IoT-Geräte gesammelt werden. Verbraucher könnten danach auch entscheiden, ob sie die Sammlung und Verbreitung ihrer Daten überhaupt zulassen möchten. Pentland ist der Auffassung, dass einige Unternehmen unter dem Erfordernis einer ausdrücklichen Einwilligung leiden würden, jedoch die geschaffene Transparenz letztlich dem Verhältnis zwischen Verbrauchern und Unternehmen dient, indem Vertrauen geschaffen wird.

Das „New Deal on Data“-Regulierungsmodell ist bereits im praktischen Einsatz im Ort Trento (Italien), im Zusammenarbeit mit Telecom Italia und Telefónica. Hunderte Familien haben sich registriert, um Benachrichtigungen über die generierten Daten zu erhalten und Kontrolle über deren Nutzung und Weitergabe auszuüben. Das Modell soll die These belegen, dass Menschen mehr Daten freigeben, wenn sie sich im Klaren darüber sind, was zu welchem Zweck und unter welchen Sicherheitsbedingungen gespeichert wird.

4.4. Datenherrschaft und Datennutzung

Selbst wenn man das persönliche Empfinden, beobachtet zu werden, beiseite lässt, ist es wichtig, in Erinnerung zu behalten, dass all die persönlichen Informationen aus den verschiedenen Geräten in Netzwerken verarbeitet und/oder gespeichert werden – offen für Angriffe von Cyber-Tätern oder für anderen Missbrauch.

Die Sicherheit der gespeicherten Daten ist daher von schwerwiegender Bedeutung für die Befürworter des IoT. Bereits jetzt gibt es Berichte über Fälle, in denen Personen Kinder über gehackte Babyüberwachungsmonitore beobachten, und über Einbrüche und Zerstörungen, die durch kompromittierende Überwachungs- und Sicherheitsanlagen möglich wurden. Die gesteigerte Abhängigkeit von der Integration von Informationssystemen ist tatsächlich eine potenzielle Brutstätte für Kriminalität gegenüber Wohnungen und Unternehmen (von Verzerrungen in der Angabe von Energieverbrauch bis hin zur Verfälschung von sensiblen Informationen und der Störung wesentlicher Informationen für Dienste wie Banken, Polizei und Krankenhäuser).

Die US Federal Trade Commission empfiehlt, dass Unternehmen bei der Entwicklung von Produkten für das Internet of Things sich an den best practices orientieren, die auch für Cyber- Sicherheit gefordert sind. Als Antwort auf die Bedenken zu privacy und potenziellem Datenmissbrauch hat die FTC einen Report ausgegeben, der unter anderem Empfehlungen zur Überwachung und Wartung von Geräten beinhaltet. Sie will die Hersteller auch dazu anhalten, den Umfang der von Geräten gesammelten Daten soweit wie möglich zu beschränken. Allerdings bleibt abzuwarten, wie und ob diese Empfehlungen von den Herstellern und Entwicklern angenommen werden und wie sie durchgesetzt werden können.

5. Technikrecht

Für die Entwicklung neuer Technologien und Produkte sind die technischen Rahmenbedingungen mit entscheidend.

5.1. Produktsicherheit und Produkthaftung

Die Technologiewelt ist voll ausgefüllt mit der Planung für und der Produktion von IoT verträglichen Geräten. Praktisch jedes Technologieunternehmen hat Pläne, IoT-Produkte in nächster Zeit auf den Markt zu bringen, jedes mit unterschiedlicher Codierung, Sicherheits- und Herstellungsstandards. In Anbetracht der gegenwärtig fehlenden Regulierung zu Herstellung, Tests, Codierung, Sicherheit, Wartung und Fortentwicklung dieser Geräte erscheint es nahe liegend, dass der Gebrauch dieser Produkte durch Fehlfunktionen ein extrem hohes Risiko für Schäden an Leben und Vermögen beinhaltet. Das FDC schätzt, dass über 25 Milliarden Geräte im Jahr 2020 miteinander verbunden sein werden. Google Chairman und Ex-CEO Eric Schmidt sagte auf dem World Economic Forum in Davos: „Es wird so viele IP-Adressen, so viele Geräte, Sensoren geben, Dinge die man trägt, Dinge, die miteinander interagieren, dass man es nicht einmal empfindet. Es wird Teil des täglichen Lebens sein. Man stelle sich vor, man geht in einen Raum und der Raum ist dynamisch. Mit der Erlaubnis des Trägers interagiert er mit den Dingen, die im Raum vor sich gehen."

Man kann sich die Auswirkungen an dem Tag vorstellen, wenn einfache Geräte nicht so funktionieren wie geplant; wenn der Wecker nicht klingelt; das Telefon nicht lädt und schließlich sich das Auto weigert zu starten und man gezwungen wird, zum Zug zu rennen, was zu spät sein kann. Wenn man diese Auswirkungen nur mit 10 % steigert, kann man sich die Bedeutung der potenziellen, finanziellen und persönlichen Verluste, die bei einer Fehlfunktion eines IoT-Produkts entstehen können, vorstellen.

IoT-Produkte werden praktisch in jeder Branche entwickelt, angefangen bei medizinischen Geräten, Energiemanagement, Automobilen und ihren Teilen, Robotern und

künstlicher Intelligenz bis hin zu öffentlichen Bereichen wie Kommunikation und Banking. Wenn diese Produkte auf dem Markt verfügbar sind, werden sich die Produktmängel zeigen, gefolgt von den unausweichlichen Produkthaftungsprozessen. Man kann sich vorstellen, dass die bisherige Basis für Haftung, insbesondere Fahrlässigkeit, verschuldensunabhängige Haftung, Garantieverletzung, falsche Angaben, Betrug etc. in all diesen Fällen zur Anwendung kommen. Die praktische Anwendung wird sich in Breite zeigen, sobald die Präzedenzfälle vorliegen.

5.2. Standardisierung, Zertifizierung

Die Befürworter von Industrie 4.0 betrachten die Schaffung von Standards als einen wesentlichen Teil ihres Programms und arbeiten daran, Standards zu schaffen, die über das gesamte Programm Anwendung finden sollen. Demgegenüber hat das IIC eine andere Haltung hinsichtlich Standards eingenommen und empfiehlt, Leitlinien für Standardorganisationen herauszugeben, die diese eigenverantwortlich für die Entwicklung von Standards anwenden sollen.

Das IIC strebt einen Konsens mit der Industrie zu Plattformen und Interoperabilität an, weniger Normen und Anforderungen. Standardisierung steht auf der Agenda für Industrie 4.0, nicht aber auf dem Programm der IIC.

+++

Industrie 4.0 in Brasilien

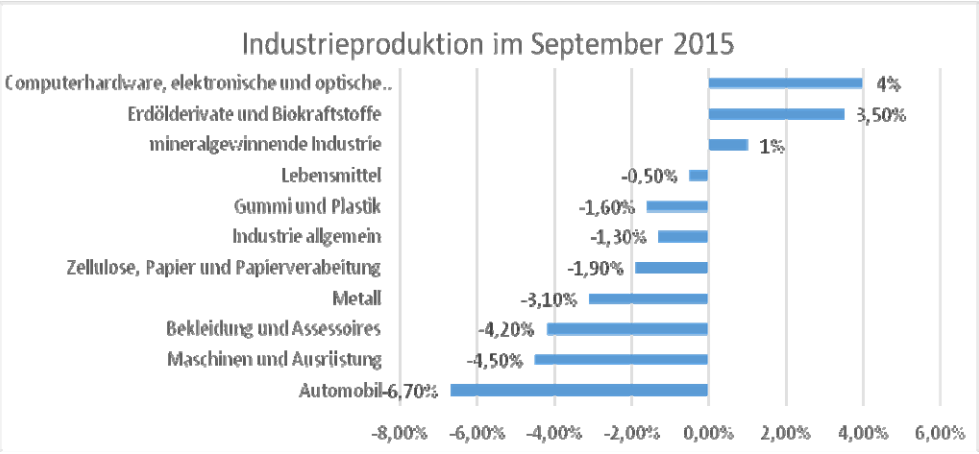
Sabine Reimann, Rechtsanwältin
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

1. Allgemeine wirtschaftliche Lage in Brasilien

Zusammenhängend mit politischer Stabilität, einer stabilen Währung und aufgelegten Programmen der Regierung zur wirtschaftlichen Förderung wie zum Beispiel PAC war Brasilien im Jahre 2015 mit einem BIP von 2.353 Milliarden US-Dollar die siebtgrößte Wirtschaftsmacht weltweit.

Die derzeitige allgemeine Wirtschaftslage in Brasilien ist schwierig. Inflation, Rezession und Korruption lähmen das Land. Mit einem Bruttosozialproduktrückgang um -3,0% für 2015 und einem prognostizierten Rückgang um 3,8% für 2016 wird die prekäre Lage des Landes deutlich.[168]

Die Entwicklungen in den Branchen KFZ, Maschinenbau, Chemie und Bau im Allgemeinen sind rückläufig bzw. deutlich rückläufig. Die Industrieproduktion ist im September 2015 auf ein Rekordtief von 9,5% im Vergleich zum Vorjahr gesunken, immerhin noch -1,3% im Vergleich zum Vormonat August.



Eigene Graphik, Daten: IBGE

Die Inflationsrate ist von 6,75% im September 2014 auf 9,49% im September 2015 angestiegen. Im Juli 2016 wird eine Inflation von 8,73% erwartet. Der Basiszinssatz wurde bereits auf stattliche 14,25% angehoben, um Anleger für den Kauf von Staatsanleihen

[168] Stand der Daten: IMF, April 2016

anzulocken und den Real zu stärken. Seit Dezember 2014 stieg die Arbeitslosenquote kontinuierlich von 4,3% auf 7,6% im September 2015. Für 2016 wird eine Quote von 9,2, % und für 2017 sogar 10,2% prognostiziert.

Ein Aufwärtstrend ist nicht absehbar.

2. Industriestruktur

Brasilien hat im 20. Jahrhundert erfolgreich den Schritt zur Industrienation gemeistert. Die Industriestruktur ist breit aufgestellt und profitiert von den Schutzmaßnahmen der Regierung. Es herrscht große Diversität. Neben der Rohstoffgewinnung gibt es die verarbeitende Industrie zur Herstellung von Gütern wie zum Beispiel Nahrungsmittel, Eisen, Stahl, Textilien, Fahrzeuge, Chemikalien, Papier, Schiffe und elektronische Ausrüstungen.

Das industrielle Zentrum des Landes ist die Metropolregion São Paulo, die ein Drittel zur Gesamtproduktion Brasiliens beiträgt. Weitere Zentren befinden sich in Rio de Janeiro, Belo Horizonte, Porto Alegre und Fortaleza.

2.1. Wahrnehmung von Industrie 4.0 in Brasilien und Perspektive für Brasilien

Industrie 4.0 wird in Brasilien derzeit nur zurückhaltend wahrgenommen. Aus Sicht Brasiliens sind die Vorreiter für die Automatisierung der Prozesse Deutschland, Frankreich und die U.S.A. In einzelnen Veröffentlichungen in der Presse wird Industrie 4.0 vorgestellt. So wird z.B. darauf hingewiesen, dass der Arbeiter 4.0 in Zukunft vier Kompetenzen mitbringen müsse: ein interdisziplinärer Abschluss anstatt eines Abschlusses in einer Disziplin, Anpassungsfähigkeit und Flexibilität im Hinblick auf den Umgang mit Maschinen, Entscheidungsfähigkeit über dringliche Tätigkeiten bzw. Abläufe, gute Zusammenarbeit mit den Menschen.

Es wird erwartet und gehofft, dass Brasilien sich der digitalen Industrie zuwendet, da die Notwendigkeit erkannt wird, auf mittlere Sicht wettbewerbsfähig bleiben zu können. Denn schließlich fordere der brasilianische Konsument, der die größte Antriebskraft der brasilianischen Wirtschaft ist, immer mehr Individualität in Bezug auf das Produkt.

Probleme bei der Umsetzung/ Hemmnisse

Eines der Probleme bei der Umsetzung dürfte der Fachkräftemangel sein. Der Grund hierfür wird im elitären und auf eine akademische Karrierelaufbahn ausgerichteten

Schulsystem gesehen. Ein duales System nach deutschem Vorbild konnte sich, im Hinblick auf Dauer und Kosten, nicht durchsetzen. Dass es ein Mindestmaß an qualifizierten Fachkräften gibt, ist dem SENAI-/SENAC-System, der brasilianischen Varianten des IHK-/HWK-Systems in Deutschland, zu verdanken. Der SENAI bildet für die Industrie, der SENAC für Handel und Dienstleistungen aus. Die hohe Nachfrage können diese jedoch nicht bedienen.

Als problematisch könnten sich auch die hohen Investitionskosten in der Umstellung auf Industrie 4.0 in der derzeitigen wirtschaftlichen Lage erweisen.

Beispiele von Unternehmensprojekten

Anwendungsfelder für die automatisierte Fertigung findet man in Brasilien derzeit in erster Linie in der Kfz-Industrie, zum Beispiel in der Fabriklogistik und der Flexibilisierung der Lieferketten. So besitzt T-Systems in São Bernardo do Campo ein Labor und einen Showroom für M2M-Systeme und testet in einigen Kfz-Werken die vor Ort entwickelte M2M-Plattform iVES (Visibility Enterprise Service). Der Flugzeughersteller Embraer führte ein Jahr vor Produktionsstart des Geschäftsjets Legacy 500 über 12.000 Stunden 3D-Flugsimulationen durch.

Siemens hingegen setzt sich auf andere Art und Weise mit Industrie 4.0 auseinander. Bereits im Oktober 2014 hat Siemens auf ihrer Anwenderkonferenz PLM Industrie 4.0 in São Paulo vorgestellt. Zum 01.06.2015 hat Siemens zur Teilnahme an einer Ausschreibung mit Preisverleihung zum Thema „Wie ändert Digitalisierung Brasiliens Zukunft?“ aufgerufen. Im September 2015 wurden die Preise an die zehn besten Ergebnisse vergeben (siehe: *Prêmio de Inovação Siemens 2015***)**. Die vier Themenpfeiler waren: die Zukunft der Industrie, die intelligente Infrastruktur, erneuerbare Energie und Gesundheitssorge.

3. Umfeld für Investitionen

3.1. Politisches und rechtliches Klima

Brasilien ist eine präsidiale Demokratie. Der Nationalkongress als brasilianisches Parlament besteht aus zwei Kammern, dem Senat (Senado Federal) und der Abgeordnetenkammer (Câmara dos Deputados). Der Senat besteht aus 81 Abgeordneten, 3 pro Bundesstaat inklusive Bundesdistrikt, die alle 8 Jahren gewählt werden. Die Abgeordnetenkammer besteht aus 513 Sitzen, die nach dem Verhältniswahlrecht alle 4 Jahre besetzt werden. Der Präsident ist zugleich auch Staatsoberhaupt.

Die politische Lage ist bestimmt durch Parteienvielfalt, in der keine Partei mehr als 20% der Stimmen hat. Die Präsidentin Dilma Rouseff (seit 2011) gehört der PT (Partido dos Trabalhadores), der gemäßigt linksgerichteten Arbeiterpartei an. Der Senat hingegen wird geleitet von Eduardo Cunha, der der PMDB (Partido do Movimento Democrático Brasileiro), einer Zentrumspartei - oder aus linker Sicht einer Rechtspartei -, angehört. Um regieren zu können, muss die Präsidentin immer wieder neue Mehrheiten im Abgeordnetenhaus und im Senat finden.

Die Mehrheitsverhältnisse im Senat sind gegensätzlich zu denen in der Abgeordnetenkammer, so dass es bei Gesetzesvorlagen bzw. –Änderungen immer zu großen Machtkämpfen kommt und sich die Parteien gegenseitig blockieren.

Seit Anfang Mai 2016 ist Präsidentin Dilma Rouseff ihres Amtes enthoben. Ihr werden vorgeworfen, Geld ohne Zustimmung des Kongresses ausgegeben und Haushaltszahlen geschönt zu haben. Am 09.08.2016 wurde im Amtsenthebungsverfahren ein weiterer Schritt gegangen: der Senat stimmte für die Überweisung des Verfahrens an ein Tribunal zur Klärung der Vorkommnisse. Die Amtsgeschäfte hat kommissarisch ihr Vertreter Michel Temer (PMDB) übernommen.

Große Probleme entstehen durch die scheinbar dem System immanente Korruption und deren Akzeptanz. Mit dem Aufdecken des Skandals um Petrobras (lava-jato genannt) beginnt ein Umdenken. Hilfreich hierbei ist das neue Antikorruptionsgesetz Lei No. 12.846 aus 2013, das als schärfstes Gesetz weltweit gilt, weil die verschuldensunabhängige Haftung für Unternehmen eingeführt wurde. Unternehmen können erstmals im vollen Umfang bestraft werden, wenn Mitarbeiter einen Beamten oder Konkurrenten bestechen. Das Unternehmen haftet für jeden korrupten Vorgang nicht nur selbst, sondern auch mit Konsortien, Tochtergesellschaften und im Ausland.

Protektionismus, Abschottung, Öffnung des Landes

Seit 2011 zeigt Brasilien wieder verstärkt protektionistische Maßnahmen, wie zum Beispiel die hohe Importsteuer, die auf ausländische Produkte erhoben wird, um den unlauteren Wettbewerb gegenüber brasilianischen Produkten in Schranken zu halten. Somit werden inländische Erzeuger zum Nachteil europäischer Unternehmen begünstigt.

Der *Local Content* (Inlandsanteil) wird durch indirekte Maßnahmen wie z.B. subventionierte Finanzierung durch die Brasilianische Entwicklungsbank oder Steuervergünstigungen für Unternehmen, die einen bestimmten Nationalisierungsgrad erreichen, gesichert.

Als Beispiel hierfür sei Inovar-Auto genannt, das Förderprogramm für die Automobilindustrie. Sind die spezifischen Voraussetzungen erfüllt (z.B. Investitionen in die inländi-

sche Forschung und Entwicklung) bietet das Programm eine Ermäßigung der Industrieproduktesteuer (IPI) um bis zu 30%.

Arbeitsrecht

Die brasilianische Verfassung *Constituição da República Brasileira* von 1988 gibt einen Katalog von Arbeitnehmerrechten vor, die besonders reformresistent sind, da Änderungen der Verfassung entsprechend hohe parlamentarische Mehrheiten erfordern. Hierzu gehören u.a. der branchenübergreifende und bundesweite Mindestlohn, die maximale tägliche Arbeitszeit von acht Stunden, mindestens ein bezahlter Ruhetag pro Woche, die Überstundenzulage von 50% über den regulären Stundensatz und der Mindestjahresurlaub von 30 Tagen.

Das Arbeitsgesetzbuch *Consolidação das Leis do Trabalho* ist von 1943 und regelt sowohl das private als auch öffentliche Individualarbeitsrecht als auch das Kollektivarbeitsrecht. Vorherrschend im brasilianischen Arbeitsrecht ist das Prinzip des Arbeitnehmerschutzes (*proteção do empregado*), das in den vier folgenden Grundsätzen konkret zum Ausdruck kommt:

- Unwiderruflichkeit von Arbeitnehmerrechten bedeutet, dass z.B. die Änderung eines Arbeitsvertrages nur im gegenseitigen Einverständnis und nur zugunsten des Arbeitnehmers möglich ist (mit wenigen Ausnahmen).

- Die von den Vertragsparteien praktizierten tatsächlichen Verhältnisse gehen den dem Arbeitnehmer nachteiligen Vertragsklauseln vor (primazia da realidade).

- Grundsätzlich ist der Arbeitsvertrag auf unbestimmte Zeit geschlossen (continuidade de relação de emprego).

- Im Zweifel oder bei Interessenskollision findet die den Arbeitnehmer begünstigende Auslegungsalternative einer Norm oder Vereinbarung Anwendung (in dubio pro operador).

Schutz geistigen Eigentums

Der Schutz geistigen Eigentums ist in der Verfassung, verschiedenen Bundesgesetzen und internationalen Verträgen geregelt.
Marken sind ab dem Moment ihrer Eintragung beim brasilianischen Marken- und Patentamt (INPI) geschützt. Alle Rechte in Bezug auf eine Marke hängen davon ab, ob diese in Brasilien registriert ist. Es können nur Marken, die auch genutzt werden, geschützt werden.

Erfindungen, die die Voraussetzungen von absoluter Neuheit, gewerblicher Anwendbarkeit und erfinderische Tätigkeit erfüllen, können als Patent (gemäß dem Gesetz über gewerbliches Eigentum Lei N°9.279/1996) eingetragen werden. Das Patent wird für 20 Jahre erteilt. Patente können auch erlöschen, so z.B. wenn sie in zwei oder mehr aufeinander folgenden Jahren nicht genutzt werden.
Im Gesetz Lei N°9.610/1998 ist das Urheberrecht geregelt. Alle geistigen Schöpfungen, unabhängig in welcher Form sie vorliegen, sind als geistiges Eigentum geschützt. Die Anmeldung von geistigen Werken ist in Brasilien nicht zwingend, sollte zur Sicherung der Rechte und als Nachweis der Rechtsinhaberschaft aber vorgenommen werden.
Der Rechtsschutz für Software (geregelt im Software-Gesetz Lei N°9.609/1998) gilt unabhängig von einer Eintragung. Es kann eine Eintragung beim INPI vorgenommen werden.

4. Informationen und Daten

4.1. Grundlagen

Die Regelungen über Informationen und Daten finden sich in unterschiedlichen Gesetzen und Regelungen. So ist bereits in den Artikeln 5, 10 und 12 der brasilianischen Verfassung der Schutz der Privatsphäre als konstitutionelles Recht festgeschrieben.
Ein Spezialgesetz zum Datenschutz personenbezogener Daten gibt es noch nicht. Vielmehr befinden sich aber verschiedene Entwürfe von Abgeordnetenkammer, Justizministerium und Senat in Diskussion.[169]

Bemerkenswert hingegen ist das neue Internet-Gesetz *Marco Civil da Internet* (Lei 12.965/2014), das im Juni 2014 in Kraft getreten ist. Es wird als „erste Internet-Verfassung der Welt“ bezeichnet und ist für private und öffentliche Einrichtungen und Privatpersonen anwendbar.

Ziele dieser Gesetzgebung sind:

- Förderung des Rechts auf den Zugang zum Internet für alle Bürger;
- Förderung des Zugangs zu Informationen und Wissen sowie die Teilnahme am kulturellen Leben und öffentlichen Angelegenheiten;
- Förderung von Innovation und der Verbreitung von neuen Technologien und Modellen für Nutzung und Zugang sowie
- Förderung der Einhaltung der offenen technischen Standards, die Kommunikation, Erreichbarkeit und Interoperabilität zwischen Anwendungen und Datenbanken.

Es beinhaltet:

[169] Jens Velten in DBVJ-Mitteilungen 2/ 2015, „Übersicht über den Persönlichkeitsschutz im digitalen Umfeld in Brasilien und in Deutschland“

- die Sicherung der Redefreiheit, der Kommunikationsfreiheit und der Freiheit des Denkens, in den Bestimmungen der Verfassung;
- den Schutz der Privatsphäre;
- den Schutz der persönlichen Daten, gemäß dem Gesetz;
- die Erhaltung und Sicherung der Netzneutralität, in Übereinstimmung mit weiterer Gesetzgebung;
- die Erhaltung von Stabilität, Sicherheit und Funktionalität des Internets, durch technische Praktiken kompatibel mit internationalen Standards;
- die Haftung von Akteuren entsprechend ihrer Aktivitäten, in Übereinstimmung mit dem Gesetz und
- den Erhalt des partizipativen Charakters des Internets.

4.2. Datenschutz (personenbezogene Daten)

Viele der Bestimmungen des Gesetzes *Marco Civil* Lei 12.965/2014 hinsichtlich des Schutzes personenbezogener Daten kennen wir aus der EU-Datenschutzgrundverordnung. So dürfen Daten nicht einfach weitergegeben werden, Provider müssen Nutzer informieren, welche Daten sie für welche Zwecke sammeln und nach Vertragsende müssen Daten gelöscht werden. Die Nutzer müssen ausdrücklich der Datenverwendung zustimmen.

Bei jeder Sammlung, Speicherung, Aufbewahrung oder Verarbeitung von Daten, in denen mindestens eine dieser Handlungen in Brasilien erfolgt, muss das brasilianische Datenschutzrecht gewahrt werden, unabhängig davon, wo sich die Rechenzentren und die Daten selbst befinden.

Bei Datenschutzverletzungen gibt das Gesetz vier Sanktionen vor: Abmahnung mit Fristsetzung zur Anwendung von Abhilfemaßnahmen, Geldstrafe bis zu 10% des Umsatzes des letzten Geschäftsjahres abzüglich Steuern, zeitweise Einstellung der Tätigkeiten, die zum Verstoß geführt haben, und Verbot der Tätigkeiten, die zu Verstoß führen.

Das Internet-Gesetz Marco Civil sieht die Vorratsdatenspeicherung ausdrücklich vor. Die Verbindungsdaten müssen vom Provider für die Dauer von einem Jahr, die Zugangsdaten für die Dauer von 6 Monaten gespeichert werden.

Im Gesetz *Lei do Cadastro Positivo* 12.414/2011 wird die Erhebung und die Ansicht von Daten (Registrierung) von natürlichen oder juristischen Personen in Datenbanken über Finanzdaten und Kreditverläufe geregelt. Die Maßstäbe für die Sammlung dieser Daten zur Darstellung der wirtschaftlichen Situation sind festgelegt. Die Daten müssen objektiv, klar verständlich, wahrhaftig und leicht zu verstehen sein. Zum Beispiel hat der Registrierte das Recht

- auf Löschung seiner Daten, wenn er es möchte;
- auf Mitteilung der Änderung seiner Daten;
- auf Information vor der Speicherung seiner Daten und
- auf freien Zugang zu diesen gespeicherten Daten.

Im Gesetz *Lei de Acesso à Informação* 12.527/2011 gibt es ebenfalls einen Abschnitt über den Schutz der persönlichen Informationen. Die Privatsphäre, das private Leben die Ehre und die Bilder von Personen sind geschützt. Dieser Schutz gilt gegenüber Dritten und auch gegenüber öffentlichen Bediensteten. Ohne Zustimmung des Betroffenen können diese persönlichen Informationen nur in folgenden Fällen verwandt werden:

- Notwendigkeit der Prävention oder der medizinischen Diagnostik
- Statistiken und Erhebungen im öffentlichen Interesse
- Nachkommen einer gerichtlichen Anordnung
- Zum Schutz der Menschenrechte
- Zum Schutz des öffentlichen Interesses

Datensicherheit (gegen unbefugten Zugriff)

Es existiert kein Spezialgesetz zur Datensicherheit. Regelungen findet man in einzelnen Klauseln in unterschiedlichen Gesetzen.
Es gibt aber viele Regelungen zur Datensicherheit in der öffentlichen Verwaltung. Regelungen zur Datensicherheit sind verfassungsrechtlich in Art. 37, §7 der Brasilianischen Verfassung gefordert. Hier sollen einige Beispiele aufgezählt sein:

- So findet man im Arbeitsgesetzbuch *CLT* ausdrücklich das Recht zur Kündigung des Arbeitsvertrages bei Verletzung des Betriebsgeheimnisses (Art. 482, Unterstrich g).

- Im Strafgesetzbuch *Código Penal* ist im Abschnitt über die Unverletzlichkeit von Geheimnissen eine Haftstrafe von 3 Monaten bis 1 Jahr bzw. Geldstrafe vorgesehen bei Offenlegung von Geheimnissen betrieblicher Art (Art. 154-A). Unter diesen Artikel fallen auch Verstöße bzw. unbefugte Zugriffe auf Ausrüstungen und Systeme, mit der Intention, diese zu schädigen oder Daten oder Informationen zu zerstören.

- Im Gesetz über die nationale Politik zur Informatik Lei 7.232/1984 findet man unter Art.2 XIII als Ziel die Errichtung von Mechanismen und juristischen Instrumenten zum Schutz der gespeicherten, verarbeiteten und übermittelten Daten sowie den Schutz der Privatsphäre.

- Im Gesetz über gewerbliches Eigentum Lei 9.279/1996 ist im Abschnitt über unlauteren Wettbewerb geregelt, dass eine Straftat begeht, wer Kenntnisse, Informati-

onen oder vertrauliche Daten ohne Zustimmung veröffentlicht, nutzt oder gebraucht, die in der Industrie, im Handel oder Dienstleistungen genutzt werden, und zu denen er aufgrund des vertraglichen oder arbeitsrechtlichen Verhältnisses Zugang hatte (Art. 195 XI), auch nach Vertragsbeendigung.

5. Produktsicherheit, Produkthaftung

Die Produkthaftung ist in Art. 931 des Zivilgesetzbuches *Código Civil* und - soweit es Anwendung findet - in Art. 12 des Verbraucherschutzgesetzes *Código de Defesa do Consumidor(CDC)* geregelt. Anwendung findet das CDC, wenn es sich um ein Verbraucherverhältnis handelt (auf der einen Seite ein Endverbraucher und auf der anderen ein Lieferant).

Der brasilianische oder ausländische Hersteller, Bauunternehmer oder Produzent sowie der Importeur haftet für Schäden, die dem Verbraucher aufgrund eines defekten Produktes verursacht werden. Die Haftung ist verschuldensunabhängig.

Die Haftung des Händlers ist hingegen nur subsidiär, wenn der Hersteller, Bauunternehmer, Produzent oder Importeur nicht identifiziert werden kann, das Produkt ohne klare Informationen über Hersteller, Produzent (Anbauer), Bauunternehmer oder Importeur vertrieben wurde oder wenn der Händler das Produkt nicht sachgemäß aufbewahrt hat. Hersteller und Produzenten haften vom Anfang an als Gesamtschuldner (Art. 25, § 2 CDC) und verschuldensunabhängig. Sobald aber die Aufbewahrung unsachgemäß war, dann zählt nach Art. 13 I CDC auch der Händler zu den in Art.12 CDC genannten Lieferanten, weil der Defekt auch durch die Aufbewahrung entstanden sein könnte.
Die Frist, eine Klage auf Produkthaftung einzureichen, ist bei der Haftung nach den allgemeinen Vorschriften drei Jahre, bei Anwendung des Verbraucherschutzgesetzes fünf Jahre.

6. Normenwesen, Zertifizierung

Produkte, für die in Brasilien obligatorisch eine Zertifizierung verlangt wird, müssen bei einer von der staatlichen Prüfungsbehörde INMETRO akkreditierten Institution geprüft und zertifiziert werden. INMETRO ist das gesetzlich geforderte Konformitätszeichen für unterschiedlichste Produkte. Überprüft werden u.a elektrische und elektronische Produkte und Komponenten. Die Einteilung in Zonen entspricht der europäischen ATEX-Richtlinie. INMETRO akzeptiert bereits vorhandene Zertifikate (Qualitätsmanagement, Typenprüfung), wenn diese von einer durch INMETRO anerkannten Stelle ausgestellt sind. Anerkannt ist auch die IECEx Zulassung, das Zulassungsverfahren erfordert aber

noch die Einhaltung einiger nationaler Besonderheiten. Konformitätserklärungen, ausgestellt in Eigenverantwortung des Herstellers, werden nicht anerkannt.

Im Rahmen der INMETRO-Zertifizierung müssen Testreports vorgelegt werden. Die Produktprüfungen müssen in der Regel in Brasilien selbst durchgeführt werden. Eine so genannte Factory Inspection beim Hersteller ist Voraussetzung und muss jährlich wiederholt werden.

Für ausländische Hersteller, die eine INMETRO-Zertifizierung zur Zulassung ihrer Produkte in Brasilien benötigen, bedeutet dies, dass ihre brasilianischen Lizenzinhaber (Brazilian Registration Holder - BRH) die INMETRO-Zertifikate für sie verwalten müssen.

Nach der INMETRO-Zertifizierung erfolgt für Medizinprodukte die Registrierung bei der ANVISA (Behörde für Gesundheitsüberwachung). Erst mit der Registrierung ist den Unternehmen die Herstellung, der Import und der Export von medizinischen, pharmazeutischen und kosmetischen Produkten gestattet.

Für die Zulassung von Produkten aus dem Bereich IT, Telekom und Radio ist die ANATEL (nationale Telekommunikationsagentur) zuständig.

Bei der ICP-Brasil (*Infraestrutura de Chaves Públicas e Privadas*) handelt es sich um eine digitale Zertifizierung, eine öffentlich-rechtlich geregelte Form der Verschlüsselung, geregelt in der Medida Provisória 2200/2001. Mit der Zertifizierung gilt der Nachweis der Identität der natürlichen Person oder von Unternehmen im Internet und die Sicherheit von bestimmten Transaktionen, wie z.B. die Einkommenssteuererklärung, die elektronische Unterschrift oder das Ausstellen von elektronischen Vollmachten bei der Steuerbehörde, wird garantiert.

+ + +

Industrie 4.0. in China

Xiaomei ZHANG, Juristin (China), Mag. iur. (D)
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

1. Allgemeine wirtschaftliche Lage in China

Seit der Reform- und Öffnungspolitik in den 70er Jahren erlebte China in den folgenden 30 Jahren ein gewaltiges Wachstum, mit einer Steigerung des Bruttoinlandsproduktes von durchschnittlich 9,8% pro Jahr von 1978 bis 2012. Im Jahr 2010 hat China Japan als zweitgrößte Volkswirtschaft der Welt abgelöst. In den letzen Jahren hat sich die Wirtschaftsentwicklung aber verlangsamt. Chinas Wachstumsmodell mit Export und Investitionen als Treiber hat in der globalen Rezession in 2009 Nachteile gezeigt. 2014 lag die Wachstumsrate nur bei 7,4%. Es ist das geringste Wachstum seit 1990. Die Jahre des zweistelligen Wachstums sind vorbei. Die Regierung hat eine „neue Normalität" ausgerufen. Mit dem grundlegendsten Strukturwandel seit der Reform- und Öffnungspolitik muss China zurechtkommen.

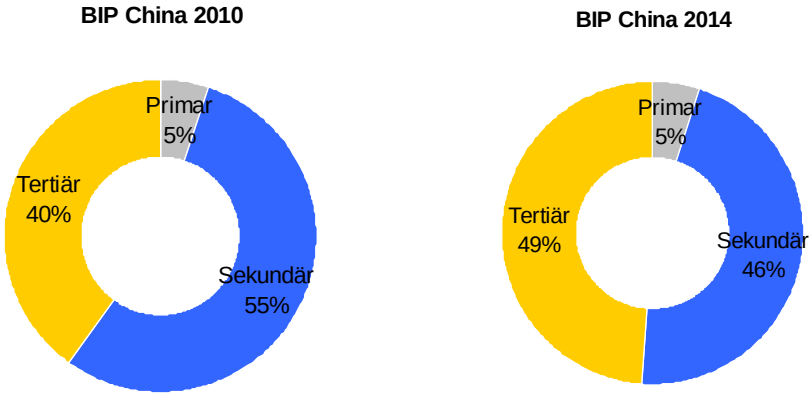
2. Industrie 4.0

2.1. Wirtschaftliche Entwicklung

Gemessen an der Wertschöpfung wird Chinas Wirtschaft noch von dem sekundären Sektor getrieben. Im Vergleich zu anderen Schwellenländern hat China als „ Werkbank der Welt" eine starke Industrie entwickelt[170]. Dienstleistungen haben allerdings stetig an Bedeutung aufgeholt und deren Beitrag zur Wirtschaftsleistung hat denjenigen des sekundären Sektors in 2014 zum ersten Mal knapp überholt.

[170] Phillipp Ehmer, Strukturwandel in China, Deutsche Bank Research , 28.01.2011

Anteile der Sektoren in China, % des BIP



Quelle: Finance. Sina

Über lange Zeit hinweg wurde/wird China als Werkbank der Welt mit Low-Technologie angesehen. Die Marke „Made in China“ stand/steht für billige Massenware. Die hohen Marktanteile der chinesischen Produkte und ihr geringer Anteil an der Wertschöpfung sind sehr unverhältnismäßig. Allgemein ist China noch auf dem Weg von Industrie 2.0 zu 3.0[171]. Gegenwärtig entwickelt sich die Hochtechnologie rasant und große Erfolge beim Aufholen werden erreicht. Allerdings verläuft Chinas Industrieentwicklung extrem ungleichmäßig. Sie glänzt in Bereichen wie der Bahnindustrie mit ihren Highspeed-Zügen und der Informations- und Kommunikationstechnologie (IKT), hinkt aber bei anderen hinterher. In vielen Industrien ist China noch weiterhin von ausländischer Technologie ggf. Schlüsseltechnologie abhängig[172].

2.2. Wahrnehmung von Industrie 4.0 in China

Das Wirtschaftswachstum verlangsamt sich. Die Löhne steigen. Die exportorientierte Strategie mit billigen Massenprodukten funktioniert nicht mehr richtig. Der 30-jährige Wirtschaftsboom in der Vergangenheit hat auch negative Effekte hinterlassen. China steht vor dem Strukturwandel. Die Realisierung eines umweltfreundlichen Wachs-

[171] Jost Wübbeke und Björn Conrad, Industrie 4.0: Deutsche Technologie für Chinas industrielle Aufholjagd? Merics China Monitor, Nr. 23/11. März 2015.
[172] Margot Schüller, Yun Schüler-Zhou, Chinas Industrie Vom Aufholen zum Überleben, Der Tagesspiegel, 16.03.2015.

tumsmodells mit unterschiedlichen Effizienzen und Qualitäten wird erhofft. Industriemodernisierung steht im Fokus.

Quelle: en. People.cn

Das deutsche Konzept „Industrie 4.0“ stellt sich als Leitfaden für Chinas Industrie dar und wird als Vorbild wahrgenommen. Vor dem Hintergrund der globalen Rückkehr zur Industrie hat China die eigene Strategie „ Made in 2025“ aufgelegt, um in der Zukunft die Führung der Industrie weltweit zu übernehmen. Die weitgehende Integration von Informatisierung und Industrialisierung bzw. die intelligente Fertigung ist der Kernpunkt dieser Strategie, was sich mit Industrie 4.0. in vielen Punkten überschneidet.

PURE ELECTRIC AND PLUG-IN HYBRID CARS

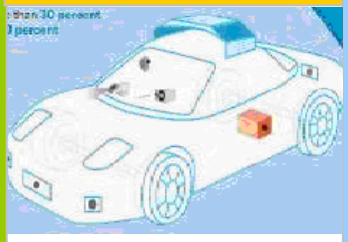
- Sales volume of pure electric and plug-in hybrid cars

  2020: 1million units
  2025: 3million units
  2014: 74,763 units
- To build star models with sales ranking in the global top 10 by 2020
- To have two carmakers' volume rank in the global top by 2025
- Overseas sales to contribute 10 percent of total volume
- Key systems, including power batteries and electric motors, to reach world- leading level by 2020
- Take 80 percent of market share
- Key systems to achieve bulk exports
- To realize informatization between car and car, car and facility by 2020.
- To test intelligent connected cars in regions by 2025

ENERGY SAVING CARS

- To lower fuel consumptions of passenger cars (including new-energy vehicles)

  2013: 7.33Liters/100km
  2020: 5Liters/100km



Made in China 2025
Strategy for Autoindustry

FUEL CELL CARS

- The production volume of fuel cell cars:

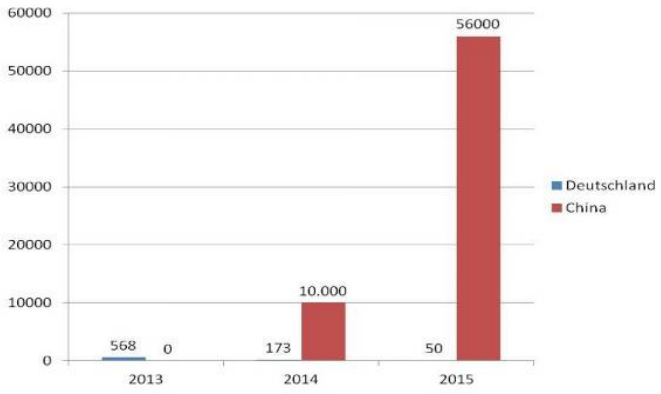
  2020: 1,000Units

INTELLIGENT CONNECTED CARS

- To reduce traffic accidents by more than 30 percent
- To reduce traffic fatalities by more than 10 percent
- To set safe autonomous driving speed at 120 km/h
- To save energy consumption by more than 10 percent
- To reduce emissions by more than 20 percent

Quelle: China Daily

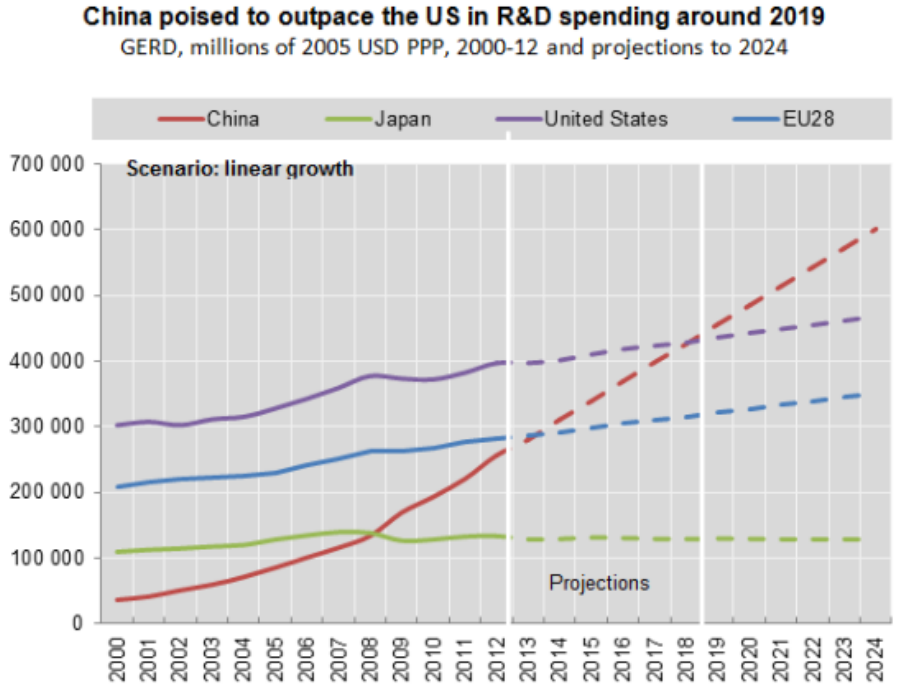
Die folgende Grafik zeigt den Verkauf des Buchs „Industrie 4.0 - Beherrschung der industriellen Komplexität mit SysLM“ von Ulrich, Sendler jeweils in Deutschland und China. Die Studie beschreibt präzise das riesige Interesse der Chinesen an Industrie 4.0 und ihre Wahrnehmung von Industrie 4.0.



Quelle: PLM Portal

2.3. Perspektive für China

China sieht die Industrie als Grundstein der Wirtschaftsentwicklung an und wird auch in der neuen Wettbewerbsrunde an der Spitze stehen. China setzt nun stark auf Innovation und Hochtechnologie. Die Ausgaben für Forschung und Entwicklung (F&E) steigen gegenwärtig kontinuierlich. Nach der Prognose von OECD wird China ca. im Jahr 2019 der größte Investor für F&E werden. Nach der Statistik von Frauenhofer ist die Anzahl der Patentanmeldung im Bereich Industrie 4.0 in China seit 2013 schon vor denen in den USA und in Deutschland.



Quelle: OECD Science, Technology and Industry Outlook 2014 - © OECD 2014

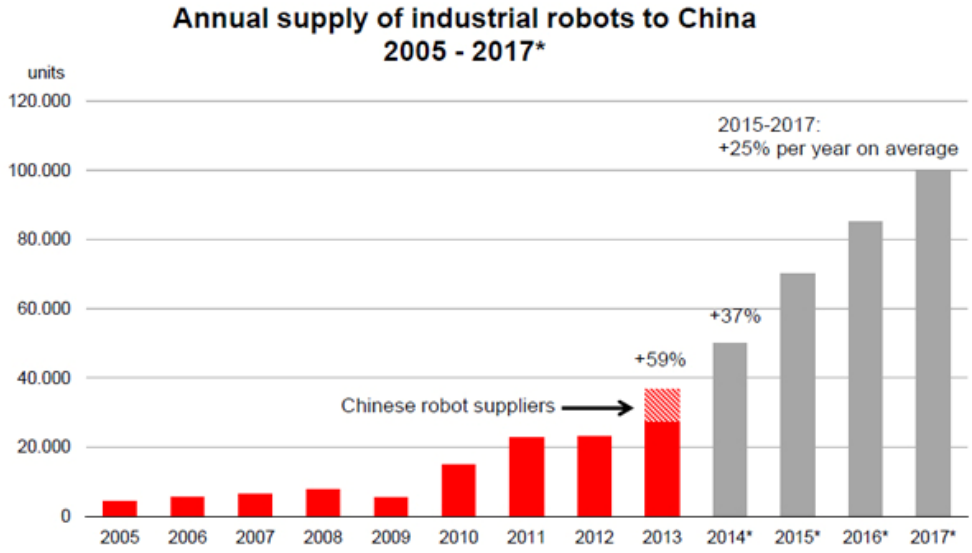
In der Strategie " Made in China 2025" hat die Regierung präzise Ziele gesetzt und verschiedene Förderungsmittel wie z.B. finanzielle und steuerliche Begünstigungen bereits vorgesehen.

Auf politischer Ebene beschlossen Deutschland und China im Bereich Industrie 4.0 bereits engere Kooperationen. Am 15.07.2015 wurde eine gemeinsame Absichtserklärung zur Kooperation beider Länder im Bereich der intelligenten Fertigung sowie der Vernetzung von Produktionsprozessen unterzeichnet, die das deutsche Konzept „Industrie 4.0" mit dem chinesischen Konzept „Made in China 2025" verbindet[173]. Es spiegelt tatsächlich die Perspektive der Zusammenarbeit beider Länder in diesem Bereich

[173] Maurice Weiss, Deutschland und China schließen engere Kooperation im Bereich Industrie 4.0, BMWi

wider. Deutschland verfügt über die führende Technologie bezüglich der Umsetzung von intelligenter und vernetzter Fertigung (Industriesoftware, Cloud Computing, Sensoren, Robotik und Funkchip usw.) und China bietet einen großen Absatzmarkt.

Für Siemens, KUKA, SAP und andere deutsche Unternehmen eröffnet diese Entwicklung große Geschäftschancen. China ist weltweit einer der wichtigsten Märkte für Automatisierungstechnik und hinter der EU der zweitgrößte für programmierbare Steuerungen. Vor diesem Hintergrund sind beispielsweise seit Februar 2013 die Siemens Electronic Works Chengdu (SEWC) in Betrieb, in denen speicherprogrammierbare Steuerungen vom Typ Simatic produziert werden. Die Fertigung bei SEWC funktioniert schon hoch automatisiert und hoch energieeffizient[174]. Aufgrund der hohen Nachfrage und des hohen Potenzials in China hat der Roboterhersteller KUKA 2014 eine neue Produktionsstätte in Shanghai geöffnet. Seit 2013 ist China in Folge der wichtigste Markt von Robotern geworden. Laut Prognose von IFR (International Federation of Robotics) und VDMA Robotics + Automation wird ein jährliches Wachstum von 25% zwischen 2015 und 2017 erwartet. SAP hat ein Projekt „SUPER“ (Share, Understand, Promote, Elaborate, Reach) zum Vorantreiben der Umsetzung der Industrie 4.0 in China ausgerufen und mit Unternehmen wie Huawei eine strategische Kooperation bezüglich Internet der Dinge und Industrie 4.0 abgeschlossen.



Quelle: IFR

[174] Ulrich Kreutzer, Digitale Fabrik: die Fabrik von morgen, http://www.siemens.com/innovation/de/home/pictures-of-the-future/industrie-und-automatisierung/digitale-fabrik-die-fabrik-von-morgen.html

2.4. Probleme bei der Umsetzung von Industrie 4.0

Im Allgemeinen ist das technologische Ausgangsniveau von China noch niedrig im Vergleich zu anderen Industrienationen wie den USA und Deutschland. China liegt auf dem Weg zur intelligenten und vernetzten Fertigung noch weit zurück. Das Niveau, das die Unternehmensgiganten wie Huawei, ZTE, Lenova, Sany und Alibaba erreicht haben, gehört momentan noch zur Ausnahme. Die erhebliche Technologielücke und der verbundene Finanzierungsbedarf zur Aufholung stellt für die Unternehmen bzw. KMU eine riesige Herausforderung dar.

Immenser Nachholbedarf zeigt sich auch bei der öffentlichen Infrastruktur. Beispielsweise sind unzureichende Breitbandanschlüsse bzw. Unternehmensanschlüsse und Internetgeschwindigkeit mögliche Hindernisse auf dem Weg zur Industrie 4.0[175]. Im Jahr 2014 lag die Internet Penetration in China bei 47,9% und in Deutschland bei 76,8%. Dem aktuellen State of the Internet Report von Akamai zufolge liegt Deutschland in Q3/2014 im Ranking der Länder mit dem schnellsten Internetzugang auf Platz 31 (durchschnittlich 8,7 Mbit/s), China hingegen auf Platz 75 (durchschnittlich 3,8 Mbit/s).

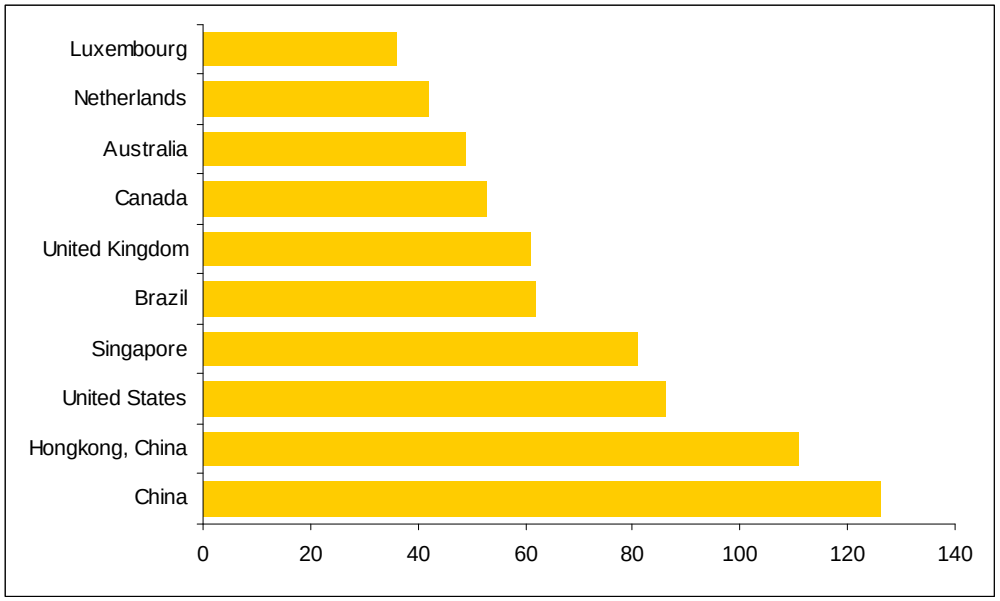
Ein anderes Hemmnis auf dem Weg zur Umsetzung der Industrie 4.0 ist die rechtliche Unsicherheit bezüglich Patent- und Datenschutz. Die kommende fortschrittliche industrielle Entwicklung wird mehr komplizierte Vernetzung bilden. Es wird die relative rückständige Gesetzgebung in China herausfordern.

3. Umfeld für Investition

3.1. Politisches und rechtliches Klima

Dem “Global Investment Trends Monitors” von der UN Welthandels- und Entwicklungskonferenz (UNCTAD) zufolge rangierte China in 2014 mit Zuflüssen von 129 Milliarden US-Dollar an der Spitze der Zielländer für ausländische Direktinvestition zum ersten Mal seit 2003. Die Wachstumsrate Chinas lag bei vier Prozent. Das Wachstum wurde vor allem von den Investitionen im Dienstleistungssektor mit Anteil von 55% getrieben. Die Investitionen im Fertigungssektor sanken auf 33%. Vor allem wurde in arbeitsintensiven Industriezweigen weniger neu investiert. Die Regierung stuft als neuen Schwerpunkt für ausländische Investitionen die Modernisierung des Fertigungssektors ein.

[175] Stefan Heng, Jan Trenczek, Industrie 4.0: „China im „ Jahr der Innovation“ auf erfolgversprechendem Weg“, Deutsche Bank Research, 26.06.2015.



Top 10 der Zielländer für ausländische Direktinvestition
Quelle: UNCAD

Die Regierung hat versprochen, sich mehr vom Markt leiten zu lassen und günstigere, fairere und transparentere Investitionsbedingungen und Marktzugänge für ausländische Investoren anzubieten. Seit 2013 wurden insgesamt vier FTZs in China gegründet, in denen die Reformfähigkeit der Wirtschaft getestet wird. Mit den Maßnahmen wie Einführung der Negativliste, Pre-Establishment National Treatment, der Ausweitung der Öffnung im Dienstleistungssektor und Vereinfachung des administrativen Verfahrens usw. werden die Bedingungen für ausländische Investitionen weiterhin gelockert. Zum Schutz des geistigen Eigentums hat China in Beijing, Shanghai und Guangzhou Sondergerichte eingerichtet.

3.2. Investitionshindernisse

Der Umfrage der EU – Handelskammer über das Geschäftsklima in China zufolge sehen trotz der hohen Zuflüsse an ausländischen Investitionen und der angekündigten Reform viele europäische Unternehmen das Geschäft in China nicht optimistisch. Schwächeres Wachstum, steigende Arbeitskosten, staatliche Lenkung und Kontrolle, Marktbarrieren und Investitionsbeschränkung, die Zensur und die rechtliche Unsicherheit sind die grundlegenden Probleme in Chinas Wirtschaftsentwicklung[176].

[176] Jonny Erling, China: EU-Firmen orten Rückfall in Protektionismus, derStandard.at; China ist für EU-Firmen weniger attraktiv, dpa; Wirtschaft: Trübe Aussichten in China: EU-Firmen treten kürzer.

3.3. Arbeitsrecht

Das Arbeitsrecht in China ist sehr arbeitnehmerfreundlich. Der Arbeitsvertrag unterscheidet zwischen befristeten, unbefristeten und projektbezogenen Arbeitsverträgen. Ein schriftlicher Arbeitsvertrag ist obligatorisch. Sollte kein schriftlicher Vertrag innerhalb eines Jahres nach Aufnahme der Arbeit abgeschlossen werden, wird dieses Arbeitsverhältnis zum Schutz des Arbeitnehmers in einen unbefristeten Arbeitsvertrag umgewandelt. Unter bestimmten Umständen darf nur ein unbefristeter Vertrag abgeschlossen werden, beispielsweise wenn der Arbeitnehmer schon über 10 Jahre bei demselben Arbeitgeber tätig ist oder wenn der befristete Vertrag schon zwei Mal verlängert wurde. Nach regulärer Beendigung eines befristeten Arbeitsvertrags soll der Arbeitgeber an den Arbeitsnehmer eine Abfindung zahlen, es sei denn, dass der Arbeitnehmer ein Verlängerungsangebot des Arbeitgebers mit denselben oder besseren Bedingungen abgelehnt hat. Die Höhe der Abfindung beträgt beispielsweise für einen fünfjährigen Arbeitsvertrag 5 Monatslöhne. Der monatliche Lohn ist der Durchschnittwert der letzten 12 Monate vor der Beendigung des Vertrags. Als Monatslohn wird höchstens der dreifache lokale Durchschnittslohns zugrunde gelegt, auch wenn der konkrete Monatslohn des Arbeitnehmers diesen Durchschnittssatz übersteigt. In unterschiedlichen Kündigungsfällen soll der Arbeitgeber auch eine Abfindung leisten. Die Abfindung ist auch dann zu leisten wenn sich beide Parteien auf die Aufhebung des Vertrags geeinigt haben. Es empfiehlt sich für die Unternehmen, eine eigene Personalstrategie aufzubauen.

3.4. Geistiges Eigentum

Der Schutz geistigen Eigentums findet sich in verschiedenen Gesetzen: Urhebergesetz, Patentgesetz (Erfindung, Gebrauchsmuster und Geschmacksmuster), Markengesetz, Gesetz gegen den unlauteren Wettbewerb (Geschäfts- und Betriebsgeheimnisse). China hat versucht, sich den internationalen Standards mehr anzunähen, die Qualität der Patente zu erhöhen, den Prozess zu beschleunigen und insgesamt die Rechtsicherheit zu verbessern. In 2014 wurde beschlossen, dass Sondergerichte für gewerblichen Rechtschutz in Beijing, Shanghai, Guangzhou eingerichtet werden, um in der Zukunft die Fragen des gewerblichen Rechtsschutzes durch fachlich qualifiziertes Personal zügig und effizient lösen zu können.

Die ausländischen Investoren legen trotzdem immer großen Zweifel daran, ob China ihr geistiges Eigentum richtig schützen kann/ will. Die hohe Anzahl von Patenten mit geringerer Qualität ist auch ein kritischer Kernpunkt aus Sicht des Marktwettbewerbs. Dies stellt für die KMU auch eine große Herausforderung dar, weil die bisherige Anmeldeflut bei neuen Anmeldungen in der Zukunft Schwierigkeiten nach sich ziehen wird. Es empfiehlt sich für Unternehmen, eigene Strategien zum Schutz geistigen Ei-

gentums in China im Vorfeld sorgfältig aufzubauen und die Patente, Marken und Werke unbedingt in China schnellstmöglich anzumelden[177].

4. Informationen und Daten

4.1. Datenschutz

Für eine lange Zeit in der Vergangenheit war der Begriff „ persönliche Daten“ für die meisten Chinesen eher fremd. Ebenso schwach war der Datenschutz. In der Zeit des Internets werden die Daten so schnell wie noch nie verbreitet. Der Anspruch auf den Schutz persönlicher Daten ist entstanden.

Am 01.02.2013 wurde der erste nationale Standard zum Datenschutz (GB/Z 28828-2012) in China eingeführt. Die persönlichen Daten werden in zwei Kategorien unterteilt: die allgemeinen und die sensiblen persönlichen Daten. Für die Erhebung und Verwertung der sensiblen persönlichen Daten ist eine ausdrückliche Genehmigung der Dateninhaber notwendig. Während der Datenerhebung, der Datenbearbeitung und des Datentransfers muss die Person umfassend informiert werden. Die Daten müssen unverzüglich gelöscht werden, sobald der bei der Erhebung informierte Zweck erreicht wird.

Der Standard hat acht grundlegende Prinzipien zur Verarbeitung von persönlichen Daten erfasst:

- Prinzip des Klaren Zwecks
- Minimalprinzip
- Prinzip der klaren Auskunft
- Prinzip der Genehmigung
- Prinzip der Qualität
- Prinzip der Sicherheit
- Prinzip von Treu und Glauben
- Prinzip der klaren Haftung

Insgesamt hat der Standard eine klare Leitlinie zum Datenschutz gezogen. Allerdings mangelt es an der Rechtsverbindlichkeit, da es sich lediglich um einen technischen Standard handelt. Ohne klare Rechtsfolge ist der Standard schwer umzusetzen. China, insbesondere die Bevölkerung, legt nun mehr Wert auf Datenschutz. Eine einheitliche und durchführbare Gesetzgebung – ein Datenschutzgesetz für personenbezogene Daten – und obligatorische Standards werden von der Theorie und Praxis erwartet.

[177] IPR-Schutz in China wird zum Wettbewerbsinstrument, GTAI, 16.02.2015.

4.2. Datensicherheit

Heutzutage sind die Daten das wichtigste Kapital eines Unternehmens geworden. Das Grundprinzip der Datensicherheit in China ist der Schutz nach Stufen. Die Schutzintensivität der Datensysteme wird nach ihrer Wichtigkeit und den Schadensstufen abgestuft. Die Prüfungskriterien von Produkte, die Datensicherheit gewähren sollen, werden auch dementsprechend abgestuft.

Das verletzte Objekt	Schadenstufen		
	leicht	schwer	sehr schwer
Interesse der Bürger, juristischen Personen und anderen Organisationen	Stufe 1	Stufe 2	Stufe 2
Gesellschaftsordnung und öffentliches Interesse	Stufe 2	Stufe 3	Stufe 4
Staatliche Sicherheit	Stufe 3	Stufe 4	Stufe 5

Schutz-stufen	Beteiligte und Regelungen	Technische Anforderungen an IT System(GB 17859-1999)
Stufe 1	Selbstschutz nach nationalen Standards	user's discretionary protection level
Stufe 2	Selbstschutz nach nationalen Standards unter Anweisung der Aufsichtsbehörde für Datensicherheit	system audit protection level
Stufe 3	Selbstschutz nach nationalen Standards unter Aufsicht und Prüfung der Aufsichts-behörde für Datensicherheit	security label protection level
Stufe 4	Selbstschutz nach nationalen Standards unter zwingender Aufsicht und Prüfung der Aufsichtsbehörde für Datensicherheit	structured protection level
Stufe 5	Selbstschutz nach nationalen Standards unter Sonderaufsicht von Sonderbehörde	access verification protection level

Eine Reihe von nationalen Standards bezüglich der Datensicherheit wurde erstellt. Ein großer Teil davon sind freiwillig anwendbare Standards. Viele große Chinesische Unternehmen haben sich dafür entschieden, ein eigenes DLP (Data Leakage Protection) System aufzubauen und aktiv eigene Daten zu schützen. Allerdings ist für KMU, deren

Datensysteme als Stufe 1 eingestuft werden und unter Selbstschutz liegen, die Verstärkung der Maßnahmen zur Datensicherheit noch zu erwarten.

4.3. Datenherrschaft und Datenverwendung

Der Staatsrat hat am 15.08.2015 die „Leitlinie zur Förderung der Entwicklung der Big Data“ veröffentlicht. Daten werden als grundlegende strategische Ressource eingestuft. Laut der Leitlinie sollte China die Verwertung der Big Data systematisch vertiefen. Allerdings muss zuvor, bevor die Daten genutzt werden, geklärt werden, wem die Daten eigentlich gehören. Diese Eigentumsfrage wird bisher noch nicht klar definiert. Daher kommen der Missbrauch der Daten und der Streit um die Daten häufig vor. In der Literatur wird die herrschende Meinung vertreten, dass die persönlichen/originären Daten den Personen / Unternehmen gehören, die die Daten original erzeugt haben. Die Daten/Datenbank, die vom Datenerheber vollständig anonymisiert und bearbeitet werden, gehört dann unter bestimmten Voraussetzungen den Datenerhebern. Ob und wie weit die erhobenen Daten benutzt werden dürfen, ist noch von der Zustimmung der originären Dateninhaber abhängig. Das Persönlichkeitsrecht darf nicht durch die Anwendung der Daten verletzt werden[178].

Ohne rechtliche Klarheit empfiehlt es sich für die Unternehmen, eine vertragliche Vereinbarung zu den Daten detailliert zu treffen.

5. Technikrecht

5.1. Produktsicherheit und Produkthaftung

Die Produkthaftung in China ist mit dem Begriff Produktqualität eng verbunden und unterscheidet zwischen vertraglicher Haftung und deliktischer Haftung. Die Rechtsgrundlage der vertraglichen Haftung ist der jeweils abgeschlossene Vertrag. Wenn die erbrachte Leistung den vereinbarten Qualitätsanforderungen nicht entspricht, hat der Käufer Gewährleistungsrechte. Im Hinblick auf Verbraucherschutz ist eine Haftungsbeschränkung nur in einem gewissen Umfang individualvertraglich möglich.

Nach dem Produktsqualitätsgesetz kann sowohl der Hersteller als auch der Händler deliktisch haftbar sein. Nach der herrschenden Meinung in der Literatur ist Hersteller im Sinne des Produktsqualitätsgesetzes nur der Hersteller des Endprodukts. Die Herstellerhaftung ist eine strikte Haftung, unabhängig von dem Verschulden der Hersteller (Gefährdungshaftung). Das Gesetz sieht auch unter Umständen die Einwendungsmöglichkeiten für den Hersteller vor, wenn 1) der Hersteller Produkt nicht in den Verkehr

[178] Rong Wang, Discussion on the core question of the data ownership in bid data trade, Big Data Reserch, 2015018.

gebracht hat; 2) der Mangel beim Inverkehrbringen noch nicht besteht oder 3) der Mangel beim Inverkehrbringen nach dem Stand von Wissenschaft und Technik noch nicht erkennbar war. Der Käufer/ Geschädigte trägt die Beweislast für die Fehlerhaftigkeit des Produktes und der Hersteller trägt die Beweislast für die oben genannten Einwendungen. Bei der Händlerhaftung kommt es grundsätzlich auf ein Verschulden des Händlers an (Delikthaftung). Hat er dies zu vertreten, haftet er mit dem Hersteller gesamtschuldnerisch.

Außer der zivilrechtlichen Haftung sind die verwaltungs- und strafrechtlichen Haftungen und die branchenbezogenen Regelungen und Standards zu beachten. Beispielsweise hat der „ Motor Vehicle Recall Regulations“ die grundlegende Pflichten und Rechtsfolgen für fehlerhafte Automobilprodukte definiert. Der Prozess des verpflichtenden / freiwilligen Rückrufs wird genau vorgeschrieben.

5.2. Normenwesen und Zertifizierung

Standardization Administration of the People's Republic of China (“SAC”) ist die zuständige Behörde für Standards. Die Standards in China unterscheiden nach Stufen ihrer Effekte zwischen nationalen Standards (GB), branchenbezogenen Standards, lokalen Standards (DB) und Unternehmensstandards (Q/). Die nationalen und branchenbezogenen Standards unterscheiden jeweils zwischen obligatorisch und freiwillig anwendbaren Normen. Die lokalen Standards, die Produktsicherheit und Hygiene berühren, sind verbindlich im gesamten Gebiet.

In China ist das Zertifizierungssystem „China Compulsory Certification (CCC)” seit 2003 eingeführt. Die Produkte, die im CCC-Produktkatalog stehen (zurzeit 175 Produkte in 17 Produktkategorien), sind zertifizierungspflichtig. Die CCC-Zertifizierung gilt sowohl für die chinesischen Produkte als auch für die Produkte, die nach China importiert werden. Ohne CCC- Zertifizierung dürfen die zertifizierungspflichtigen Produkte nicht nach China importiert, in China verkauft und in Geschäftsaktivitäten in China verwendet werden. CCC-Zertifizierung ist keine Qualitätszertifizierung, sondern eine fundamentalste Sicherheitszertifizierung. Die CCC-Zertifizierung orientiert sich ausschließlich an den chinesischen Standards. Die anderen Zertifizierungen, die auf dem Markt vorhanden sind, sind von den Unternehmen grundsätzlich freiwillig anzuwenden, es sei denn, dass eine obligatorische Zertifizierung gesetzlich vorgesehen wird, z.B. GSP-Zertifizierung für Medikamente. Die internationalen Zertifizierungen wie z.B. die ISO-Zertifizierung sind von den Unternehmen freiwillig anzuwenden.

Heutzutage sehen sich Unternehmen einer unüberschaubaren Anzahl an nationalen und internationalen Normen gegenüber. In der Zeit der Industrie 4.0, wenn Unternehmen weltweit bei der Fertigung so eng wie noch nie miteinander vernetzt arbeiten, werden sich die unterschiedlich durchgeführten Normen als ein Hindernis darstellen. Es empfiehlt sich daher, dass Deutschland und China bei der Standardsetzung hinsicht-

lich Industrie 4.0 engere Kooperationen beschließen[179]. Im Mai 2015 hat die deutsch- und chinesische Normungskommission bereits vereinbart, eine neue Arbeitsgruppe "Intelligente Fertigung - Industrie 4.0“ einzurichten, um die nationale Normierung international zu verzahnen[180].

+ + +

[179] Jost Wübbeke und Björn Conrad, Industrie4.0: Deutsche Technologie für Chinas industrielle Aufholjagd? Merics China Monitor, Nr. 23/11. März 2015.
[180] Deutschland und China kooperieren bei Standards für Industrie 4.0, BMWi. 09.06.2015.

Industrie 4.0 in Russland

Elena Duwensee, Juristin (Russland), Master of Law (Ru)
Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover

1. Allgemeine wirtschaftliche Lage in Russland

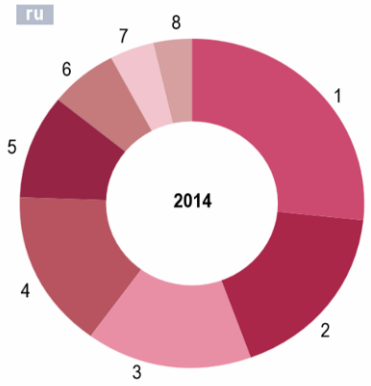
Nach der Erholung von der Krise 1998 war die russische Wirtschaft eine der am schnellsten wachsenden großen Volkswirtschaften der Welt, mit einem durchschnittlichen jährlichen Wachstum von fast 7%. Doch die internationale Finanzkrise im Jahr 2008 traf Russland wieder sehr stark. Auf ein negatives Wirtschaftswachstum bis zum Jahr 2009 folgten 2010-2012 wieder Zuwachsraten von über 4 %. Getragen wird das Wachstum von hohen Rohstoffpreisen, aber auch wachsender Beschäftigung und steigender Industrieproduktion. Aufgrund der Konjunkturschwäche im Euro-Raum und der weltweit gesunkenen Rohstoffpreise kam es 2013 nur zu einem leichten Wachstum von 1,3%.
Strukturdefizite, Finanzierungsprobleme und Handelseinschränkungen durch westliche Sanktionen wegen der Ukraine-Krise bremsten das Wirtschaftswachstum 2014. Die rückläufigen Investitionen und die Fokussierung staatlicher Finanzhilfen auf prioritäre Bereiche verstärkten diesen Trend. Seit Anfang 2014 hat der Rubel mehr als ein Drittel seines Wertes im Vergleich zum Euro verloren, was unter anderem an den Sanktionen und dem fallenden Ölpreis liegt. Durch den Währungsverfall sind die Preise für Verbraucher erheblich gestiegen. Die Inflation betrug seit Anfang des Jahres 2015 11,21%. 2015 geriet die russische Wirtschaft in die Rezession.

2. Industrie 4.0 in Russland

2.1. Wirtschaftsstruktur

Russland ist einer der größten Energieproduzenten der Welt und verfügt mit 16,8% der Weltgasreserven, 5,5% der Weltölreserven und den zweitgrößten Kohlereserven (17,6%) über bedeutende Ressourcen.
Das Bruttoinlandsprodukt nach sektoraler Entstehung ist auf der folgenden Grafik gut überschaubar:

BIP nach sektoraler Entstehung (in Prozent)



	2012	2013	2014
1 Handel, Gastgewerbe und Verkehr	28,5	27,8	26,9
2 Finanzierung, Vermietung und Dienstleistungen	16,5	17,1	17,7
3 Öffentliche und private Dienstleister	14,7	15,4	15,6
4 Verarbeitende Industrie	15,0	14,9	15,6
5 Förderung von Bodenschätzen	11,1	10,9	10,1
6 Baugewerbe	6,8	6,5	6,5
7 Land- und Forstwirtschaft, Fischerei	4,0	4,0	4,2
8 Strom, Gas und Wasser	3,4	3,4	3,4

Handel und Dienstleistungen sind das Rückgrat der russischen Wirtschaft – so liest sich das Bruttoinlandsprodukt nach sektoraler Entstehung. Dadurch bleibt verborgen, dass sich die Hälfte des russischen Haushaltes durch Einnahmen aus dem Erdölexport speist.

181

Die Industrieproduktion ist von Januar bis August 2015 um 3,2% gesunken. Der Output ist in der Verarbeitenden Industrie im Vergleich zum Vorjahreszeitraum um 5,2% geschrumpft. Die Erzeugung von Maschinen und Anlagen ist in den ersten acht Monaten um 14% eingebrochen, die von Fahrzeugen um 18%. Dafür legte der Chemiesektor um 6% zu.

2.2. Wahrnehmung von Industrie 4.0 in Russland

Führende Industrieländer bereiten sich auf den globalen Wettbewerb vor und schaffen neue Entwicklungsprogramme für ihre Industrien. Die Ziele sind die Intellektualisierung der Produktion und die weitere Erhöhung des Automatisierungsgrades. Was passiert derzeit in diesem Bereich in Russland?
Der Begriff „Industrie 4.0“ ist im Land natürlich aufgrund der engen wirtschaftlichen Beziehungen zwischen Deutschland und Russland bekannt. Dies zeigte auch das letzte russische Industrieforum „Innoprom 2015“, das im Juli 2015 in Jekaterinburg stattfand. Im Jahr 2011 wurde die *Strategie der innovativen Entwicklung der Russischen Föderation für den Zeitraum bis zum Jahr 2020* genehmigt. Und wie die Zeitung „Vedomosti“ in Verbindung mit Industrie 4.0 im Oktober 2015 berichtete, begann Russland somit, eine neue Strategie (mit zeitlichen Rahmen bis 2030) zu diskutieren. Damit muss sich Russland das erste Mal in der nationalen Geschichte nicht nur mit den Realitäten von heute, sondern auch mit dem zukünftigen technologischen Wandel auseinandersetzen.

2.3. Perspektive für Russland

Industrie 4.0 ist ohne Zweifel eine große Chance für Russland wieder in die Reihe der führenden Industrienationen einzusteigen. Das Land blieb während der postsowjeti-

[181] Deutsch-Russische Auslandshandelskammer, Russland in Zahlen. URL: http://russland.ahk.de/publikationen/russland-in-zahlen/

schen Zeit zurück und schloss die Lücken nur in einigen Richtungen in den letzten Jahren.
Beim Präsidenten der Russischen Föderation wurde im Jahr 2012 der Rat für die Modernisierung der Wirtschaft und innovative Entwicklung Russlands als ein Beratungsgremium für Zusammenarbeit der Bundesorgane gegründet. Die Regierung arbeitet verschiedene Programme aus, um Innovationen im Land zu fördern. Das allerletzte Beispiel ist die *„Nationale Technologische Initiative" (2014)* – ein Maßnahmenprogramm zur Unterstützung der Entwicklung von Zukunftsbranchen in Russland, die in den nächsten 20 Jahren die Grundlage für die Weltwirtschaft werden könnten. Für die Entwicklung wurden 9 Schlüsselmärkte im Rahmen der Initiative ausgewählt: AeroNet, AutoNet, EnergyNet, FinNet, FoodNet, HealthNet, MariNet, NeuroNet und SafeNet. Auf diesen Märkten werden die Unternehmer und Führungskräfte gesucht und höchstmöglich vom Staat gefördert. Es geht u.a. um unbemannte Luftfahrzeuge und Autos, intelligente Verkehrssysteme, erneuerbare Energien, neue persönliche Sicherheitssysteme und Big Data. Ziel ist Wachstum des russischen High-Tech-Exports bis zum Jahr 2035.

In Russland existieren außerdem Zentren für Technologien und Innovationen, die in Verbindung mit Hochschulen und mit staatlicher Unterstützung arbeiten. Als erstes Beispiel sei das Innovationszentrum „Skolkovo" (russische Silicon Valley) genannt. Laut Dmitri Medwedew, Ministerpräsident der Russischen Föderation, unterstützen - neben "Skolkovo" - auch andere wie z.B. „Russian Venture Company" (Staatsfond und Entwicklungsinstitut der Russischen Föderation), „Rusnano" (Russische Korporation für Nanotechnologien) und eine Reihe von anderen Institutionen innovative Projekte. Der Gesamtbetrag der jährlichen staatlichen Unterstützung für die zivile Forschung und Entwicklung beträgt mehr als 370 Milliarden Rubel.

Darüber hinaus entwickeln sich andere Formate der Zusammenarbeit zwischen den Teilnehmern des Innovationsprozesses, z.B. Technologieplattformen und innovative territoriale Cluster. Es existieren zurzeit insgesamt mehr als 30 Plattformen und 25 Cluster.

Unterschiedliche Foren, so wie das oben genannte Industrieforum „Innoprom", das Forum und die Technologie Show „Open Innovations" erlauben den Teilnehmern ihre Erfahrungen und Entwicklungen auszutauschen und neue, auch ausländische Partner für Zusammenarbeit zu finden.

2.4. Probleme bei der Umsetzung

Allerdings sind die Schwierigkeiten auf dem Weg Russlands zu einer führenden Industrienation jetzt schon absehbar.

Die russische Wirtschaft ist grundsätzlich öl- und gasorientiert. Bei 80% der russischen Exporte handelt es sich um Rohstoffe, womit der Staatshaushalt zur Hälfte finanziert wird. Nach der Auflösung der Sowjetunion war es leichter und günstiger von Naturressourcen zu leben, als in neue Technologien und Märkte zu investieren. Das Land verfolgte in den letzten Jahren die Politik technologischer Entlehnung.

Die Korruption ist nach wie vor das Hauptproblem des Landes. Im Korruptionsindex von Transparency International landete Russland 2014 auf Platz 136 - hinter Ländern wie Pakistan und Iran. Die Skandale rund um das Innovationszentrum „Skolkovo“, bei denen die Hauptvorwürfe die Veruntreuung von Haushaltsmitteln waren, bestätigten die häufige Ineffizienz der staatlichen Investitionen.

Die Politik und Maßnahmen der russischen Regierung während der ukrainischen Krise verschlechterten das Investitionsklima im Land. Die später eingeführten Sanktionen gegen Russland zwangen das Land den Weg der Importsubstitution auszuwählen. Die Aufrechterhaltung der Importsubstitution mit Waren und Produkten, die auf dem Weltmarkt nicht wettbewerbsfähig sind, wird nur das Potenzial des Landes untergraben.

Wie glauben die Menschen, die hinter der Umsetzung der „Nationalen Technologischen Initiative“ stehen, das ungelöste Hauptproblem ist heute der Weg von der Grundlagenforschung zu den globalen Märkten. Es gibt ein Mangel an Koordinierung und Kohärenz zwischen Forschung und Wirtschaft. Auch an den Universitäten gibt es Strömungen, die Innovation und Potenziale zu eng sehen. Nicht alle Unternehmer erkennen die Bedeutung und Notwendigkeit von Investitionen in Innovationsprojekte. Zugleich legen die Bürokratie und Regulierungsbehörden neuen Entwicklungen Hindernisse in den Weg.

Die „Nationale Technologische Initiative“ selbst kann man als weitere Initiative in einer Reihe von vielen anderen der russischen Regierung bezeichnen. In Russland hält die Abwanderung von Wissenschaftlern, hochqualifizierten Fachkräften und Unternehmern unverändert an. Die neue Strategie sollte nicht auf Fehlern der Vergangenheit basieren, daher sind Privatinvestitionen unbedingt notwendig. Die "technologischen Patrioten", die an einen technologischen Durchbruch Russlands glauben, und die auch im Land bleiben, werden als die Triebkraft der Innovationsentwicklung angesehen.

2.5. Beispiel eines Unternehmensprojektes

Als Beispiel im Bereich „Industrie 4.0“ kann man den Gewinner der russischen Nationalen Auszeichnung "Industrie" nennen. 2015 ist der Gewinner das Unternehmen „TAVRIDA ELECTRIC“. Tavrida Electric ist ein Spezialist in der Entwicklung und Herstellung von Mittelspannungsschaltanlagenprodukten für Innenraum- und Freiluftanwendungen. Vor nahezu 20 Jahren war Tavrida Electric das erste Unternehmen, welches einen

Vakuumleistungsschalter mit Magnetantrieb vorstellte. Durch tiefgreifende Forschung an Magnetaktuatoren, Vakuumschaltern und dazugehörigem Isolationsdesign, gelang es Tavrida Electric den wohl kleinsten, leichtesten und zuverlässigsten Leistungsschalter im Markt zu entwickeln. Heutzutage exportiert das Unternehmen seine Produkte in 80 Länder weltweit.

Auch zahlreiche Start-Ups, die vom Innovationszentrum „Skolkovo“ Unterstützung bekommen, können als Beispiele dienen: Kintech Lab, SuperOx company, Plasmic Sources und andere.
Leider stimulieren die niedrigen Lohnsätze die Unternehmer nicht, den Automatisierungsgrad ihrer Fabriken zu erhöhen.

3. Umfeld für Investitionen

3.1. Politisches und rechtliches Klima

Die Russische Föderation ist eine föderale Republik mit präsidialem Regierungssystem. Am 12. Juni 1991 erklärte sie ihre staatliche Souveränität. Die Verfassung der Russischen Föderation wurde am 12. Dezember 1993 verabschiedet.

Der Staatspräsident der Russischen Föderation verfügt über sehr weitreichende exekutive Vollmachten, insbesondere in der Außen- und Sicherheitspolitik. Seine Amtszeit beträgt, seit der Verfassungsänderung von 2008, sechs Jahre. Amtsinhaber ist seit dem 7. Mai 2012 erneut Wladimir Putin, der bereits zwei Amtszeiten als Staatspräsident von 2000-2008 innehatte.

Das russische Parlament besteht aus zwei Kammern, der Staatsduma (Volksvertretung) und dem Föderationsrat (Vertretung der Föderationssubjekte). Mit 238 von 450 Sitzen verfügt die Partei „Einiges Russland“ über eine absolute Mehrheit in der Staatsduma. Bei den Wahlen 2012 war Wladimir Putin der Präsidentschaftskandidat von „Einiges Russland“.

Seit Mai 2012 wird eine stete Zunahme autoritärer Tendenzen beklagt. Menschenrechtsaktivisten legen der Regierung mangelhafte Unabhängigkeit von Justiz und Gerichten, die weiterhin verbreitete Korruption sowie gestiegenen Druck auf die kritische Zivilgesellschaft und Opposition zur Last.

Die ständigen Rechtsreformen und Gesetzesänderungen schaffen auch im Hinblick auf ausländische Investitionen keine rechtliche Stabilität. Manche Experten sehen wachsende Rechtssicherheit in Russland und nennen erfolgreiche Klagen ausländischer Unternehmen gegen russische Behörden als Merkmale.

3.2. Protektionismus, Abschottung, Öffnung des Landes

Der Ukraine-Konflikt, die westlichen Wirtschaftssanktionen und russischen Gegensanktionen verschlechterten natürlich die Rahmenbedingungen für die Investitionen in Russland gründlich. Mit dem Kurs auf die Importsubstitution und die Umorientierung der Regierung zu Ländern, die keine Sanktionen erlassen haben, droht eine wirtschaftliche und politische Abwendung Russlands von westlichen Investoren.

Zu den strukturellen Problemen Russlands neben der Diversifizierung der Wirtschaft gehört ebenfalls die Dominanz des Staates in der Wirtschaft, was den Wettbewerb verzerrt. Trotz der Privatisierungsversuche der russischen Regierung steigt der Anteil des russischen Staates an Unternehmen.

Allerdings hat sich Russland als Investitionsstandort in den vergangenen Jahren eindeutig positiv entwickelt. Das bestätigt auch „Ease of doing business ranking“ 2016 der Weltbank. Russland liegt mittlerweile auf Platz 51. Noch vor sechs Jahren belegte das Land Platz 120.

Das Land braucht auf jeden Fall Investitionen um notwendige Reformen durchzuführen. Deswegen wird die Infrastruktur für die neue Werke (nicht nur innerhalb der neuen Industriecluster) verbessert; den Investoren wird Befreiung von Gewinn- und Vermögensteuer über mehrere Jahre, Zulagen für Forschungs- und Entwicklungsausgaben, für Arbeitsplätze und für Energiekosten angeboten; von der föderalen Ebene wurden bis heute zahlreiche Sonderwirtschaftszonen ins Leben gerufen.

3.3. Beschäftigung und Arbeitsrecht

Das ausgebildete russische Personal kann man in heutigen Krisenzeiten leichter und aufgrund der Entlassungswelle zu relativ niedrigen Kosten finden. Die ausländischen Spezialisten arbeiten in Russland unter Sonderregelungen. Darunter haben die hochqualifizierten Spezialisten ein erleichtertes und kürzeres Verfahren zum Erhalt von Arbeitsgenehmigungen ohne Quoten. Die völlige Abschaffung der gegenseitigen Visa-Pflicht mit europäischen Ländern ist aber noch nicht in Sicht.

Die Hauptquelle des Arbeitsrechts ist in Russland das Arbeitsgesetzbuch von 2001.

3.4. Schutz geistigen Eigentums

2008 startete in Russland die große Reform des Zivilrechts. Teil 4 des Zivilgesetzbuchs wurde verabschiedet. Er enthält die Rechtsnormen im Bereich des geistigen Eigen-

tums: zu finden sind das Urheberecht, das Datenbankherstellerrecht, das Recht auf Know-how, Technologie und so weiter.

Innovative Unternehmen in Russland können zusammen mit dem rechtlichen Schutz von Erfindungen, Gebrauchsmuster und Geschmacksmuster auch Computerprogramme, Datenbanken und Topographien integrierter Schaltkreise staatlich eintragen, sowie das Know-how als Geschäftsgeheimnis schützen. Die staatliche Registrierung bietet die Möglichkeit, das Recht auf Computerprogramme, Datenbanken und Topographien integrierter Schaltkreise auf Lizenzbasis zu erteilen. Die interne Prozedur im Umgang mit dem Geschäftsgeheimnis für das Know-how ermöglicht es, dieses in der gleichen Weise wie alle anderen Objekte des geistigen Eigentums in den zivilrechtlichen Verkehr zu integrieren.

4 Informationen und Daten

4.1. Datenschutz (personenbezogene Daten)

Die Regulierung des Schutzes personenbezogener Daten findet in der Russischen Föderation auf der Bundesebene statt. Aus Bundesgesetzen können folgende ausgesondert werden: das Bundesgesetz "Über die Ratifizierung des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" und das Bundesgesetz "Über persönliche Daten" (Datenschutzgesetz). Außerdem ist ein Kapitel des Arbeitsgesetzbuchs der Russischen Föderation dem Schutz personenbezogener Daten von Arbeitnehmern gewidmet. In diesem Bereich gibt es auch Durchführungsbestimmungen in der Form von Regierungsverordnungen, Präsidentenerlasse und Normativakte der einzelnen Fachorgane.

Das Datenschutzgesetz interpretiert den Begriff der personenbezogenen Daten sehr weit. Laut dem Gesetz sind personenbezogene Daten „beliebige Informationen, die in einem direkten oder indirekten Verhältnis zu einer bestimmten oder bestimmbaren natürlichen Person stehen“. Die für den Schutz personenbezogener Daten zuständige Aufsichtsbehörde ist der Föderale Dienst für die Aufsicht im Bereich der Kommunikation, Informationstechnologie und Massenkommunikation (Roskomnadzor). Im Register von Roskomnadzor sind zurzeit mehr als 337 000 natürliche und juristische Personen sowie Regierungsbehörden registriert, die mit personenbezogenen Daten arbeiten. Sie sind als Betreiber von persönlichen Daten definiert. Es ist gesetzlich festgestellt, dass die Betreiber notwendige Schritte unternehmen sollen, um die Daten vor unberechtigtem Zugriff und fehlerhaften Verarbeitungsprozeduren zu schützen. Auf der legislativen Ebene sind die Mindestanforderungen für den Schutz von Informationen festgelegt. Es existieren auch Anforderungen für die Verarbeitung biometrischer Daten, die in den Regierungsverordnungen festgeschrieben sind.

Die personenbezogenen Daten müssen unverzüglich gelöscht oder anonymisiert werden, sobald der Zweck der Bearbeitung erreicht oder hinfällig geworden ist.

Die letzte wichtigste Änderung im Bereich des Datenschutzes ist am 1. September 2015 in Kraft getreten. Die Neuregelung sieht vor, dass bei der Verarbeitung personenbezogener Daten russischer Staatsbürger das verarbeitende Unternehmen verpflichtet ist, diese Daten auf Servern innerhalb der Russischen Föderation zu speichern (so genannte *„Data-Localization-Rule"*). Es gibt Ausnahmen im Gesetz, die an die internationalen Verpflichtungen Russlands, die Justizverwaltung, die Arbeit der Behörden oder die wissenschaftlichen, künstlerischen und journalistischen Tätigkeiten anknüpfen.

Diese Änderungen im Datenschutzgesetz verursachten Kontroversen in der Rechtsgemeinschaft in Bezug auf seinen Geltungsbereich. Auf Grund der systematischen Auslegung und der Unzulässigkeit unbegründeter Exterritorialität der Wirkung von Rechtsvorschriften meinen manche Experten, dass die Anforderungen des Gesetzes über personenbezogene Daten nur für russische Unternehmen und für in der Russischen Föderation registrierte Niederlassungen und Repräsentanzen ausländischer juristischer Personen gelten. Ebenfalls sollen von der neuen Speicherpflicht nur personenbezogene Daten russischer Staatsbürger, die in Russland ihren Wohnsitz haben, erfasst werden. Andere Experten sind nicht so optimistisch und befürchten, dass jedes Unternehmen betroffen ist, das personenbezogene Daten russischer Staatsangehöriger selbst erhebt und speichert. Sie glauben, es sei unerheblich, ob der Sitz des Unternehmens in Russland liege oder nicht.

Laut den Kommentaren der Staatsorgane wird die Frage, unter welchen Bedingungen die Anforderungen des Gesetzes für ausländische Organisationen ohne physische Präsenz in Russland gelten, auf der Grundlage des Kriteriums der Ausrichtung der Tätigkeit auf das Territorium Russlands entschieden (wie in der bestehenden europäischen Praxis). Das Vorhandensein dieser Ausrichtung kann beispielsweise durch die Verwendung des Domain-Namens, der mit der Russischen Föderation verbunden ist, oder durch die Anwesenheit der russischen Version der Website hindeuten. Bei Nichteinhaltung des Datenschutzgesetzes durch einen Eigentümer, der seinen Wohnsitz in einem fremden Land hat, können die Internet-Ressourcen gesperrt werden.

In Bezug auf die grenzüberschreitende Übermittlung personenbezogener Daten russischer Bürger gibt es keine Änderungen. Die internationalen Verpflichtungen laut dem Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bleiben vorrangig. Gemäß der Datenschutzkonvention darf Russland die grenzüberschreitende Übermittlung personenbezogener Daten weder verbieten noch sich Sondergenehmigungen dafür ausbedingen. Es ist wichtig, alle bereits bestehenden Auflagen für grenzüberschreitenden Datentransfer laut dem Datenschutzgesetz zu erfüllen und die Primärdatenbank in Russland zu lokalisieren. Laut Roskomnadsor können die Datenbanken mit personenbezogenen Daten

russischer Bürger im Ausland entweder als eine gleichwertige Kopie der russischen Datenbank oder nur als ein Teil davon aufbewahrt werden.

Das Datenschutzgesetz sieht vor, dass personenbezogene Daten von Bürger in andere Länder geschickt werden können, die Parteien der Datenschutzkonvention sind, sowie in die Länder, die nicht Vertragspartei des Übereinkommens sind, aber einen angemessenen Schutz der persönlichen Daten gewährleisten. Roskomnadzor genehmigt die Liste solcher ausländischen Staaten. Die grenzüberschreitende Übermittlung personenbezogener Daten in die Länder, die keinen angemessenen Schutz der persönlichen Daten angeben, ist dann auch möglich, wenn z.B. die Einwilligung des Subjektes der persönlichen Daten vorliegt oder in Fällen, die durch internationale Verträge der Russischen Föderation festgelegt sind.

Insgesamt gesehen können das Datenschutzgesetz und seine letzten Änderungen sehr weit ausgelegt werden. Höchstwahrscheinlich werden noch Durchführungsbestimmungen erlassen, die das Gesetz auslegen und ergänzen werden. Vieles wird deutlicher nach den ersten Fällen der Anwendung der neuen Version des Gesetzes.

4.2. Datensicherheit (gegen unbefugten Zugriff)

Wenn es um Datensicherheit geht, spricht man in Russland über die Informationssicherheit. Es existieren die Informationssicherheitsdoktrin der Russischen Föderation und die Nationale Sicherheitsstrategie der Russischen Föderation bis zum Jahr 2020. Diese konzeptionellen Dokumente definieren die allgemeine Haltung und Politik des Staates in diesem Gebiet und dienen als Grundlage für die Erstellung von Rechtsvorschriften.

Laut dem Bundesgesetz "Über Information, Informationstechnologien und Informationsschutz", sind Informationen Angaben (Nachrichten, Daten) unabhängig von der Form der Darstellung. Dieses Gesetz teilt die Informationen (je nach Kategorie vom Zugang) auf:

- Öffentlich zugängliche Information
- Information, zu der der Zugang durch Bundesgesetz beschränkt ist (eingeschränkte Information),

Die beschränkte Information ist wiederum unterteilt in

- Staatsgeheimnis sowie
- vertrauliche Information

Vertrauliche Informationen umfassen sodann die Gruppen personenbezogene Daten; Geschäftsgeheimnis; Informationen über Erfindungswesen /vor der offiziellen Veröf-

fentlichung; Berufsgeheimnis wie z.B. Arztgeheimnis, Berufsgeheimnis des Notars, Anwaltsgeheimnis, Dienstgeheimnis und Ermittlungsgeheimnis und Geheimnis von Gerichtsverfahren.

Für die Tätigkeit von Wirtschaftsunternehmen sind die ersten drei Kategorien der vertraulichen Information interessant. Die Fragen diesbezüglich sind: Gibt es gesetzliche Anforderungen diese Informationen zu schützen? Hat der Staat Zugriffsrechte in Bezug auf diese Informationen?

Im Allgemeinen bedürfen technische Schutzmaßnahmen sowie Entwicklung und Produktion der Schutzmittel vertraulicher Information einer Erteilung von Lizenzen in Russland. Ebenfalls sind die Aktivitäten zur kryptographischen Datenverschlüsselung lizenzpflichtig. Wahrscheinlich deswegen ist der Datenschutz mit nicht kryptografischen Methoden die am weitesten verbreitete Art beim Erstellen von sicheren Informationssystemen. Im Bereich des technischen Informationenschutzes sind die entscheidenden Behörden der Föderale Sicherheitsdienst Russlands (FSB) und der Föderale Dienst für Technische und Ausfuhrkontrolle Russlands (FDTA). Der FSB arbeitet auf dem Gebiet des kryptographischen Schutzes von Informationen und der FDTA auf dem Gebiet des technischen Schutz von Informationen mit nicht kryptographischen Methoden. Die Lizenzierung technischer Schutzmaßnahmen sowie Entwicklung und Produktion der Schutzmittel vertraulicher Information führt der FDTA durch.

Neben der Lizenzierung ist in der Gesetzgebung der Russischen Föderation Konformitätsbewertung (und Zertifizierung als eine Art der Konformitätsbewertung) von Informationsschutzmitteln und Attestierung von Objekten der Informatisierung vorgesehen. Allerdings sind die Verwendung von zertifizierten Schutzmitteln und die Attestierung nur für staatliche Einrichtungen pflichtig.

Hinsichtlich personenbezogener Daten sieht das Datenschutzgesetz die Verwendung von Mitteln des Informationsschutzes vor, die das Konformitätsbewertungsverfahren in der vorgeschriebenen Weise bestehen müssen. In der Gemeinschaft der Sicherheitsexperten wird diskutiert, ob das Konformitätsbewertungsverfahren immer in der Form der Zertifizierung – so sieht es FDTA- sein muss. Viele antworten auf diese Frage negativ. Das Konformitätsbewertungsverfahren in einer anderen Form ist auch für Unternehmer günstiger als zertifizierte Produkte. Die Lösung dieses Streits ist abhängig von der Vorbereitung und die Rechtfertigung der Position des Betreibers personenbezogener Daten.

In Bezug auf das Geschäftsgeheimnis sieht das Gesetz das Recht aber nicht die Pflicht des Inhabers vom Geschäftsgeheimnis vor, die Mittel und Methoden des technischen Schutzes der Vertraulichkeit dieser Informationen falls erforderlich anzuwenden. Als zwingend beschreibt das Gesetz organisatorische Maßnahmen (Dokumente, Verfahren, Geheimhaltungsstufen und so weiter), um wirtschaftlich sensible Informationen zu schützen. Die Regelung der Beziehungen in Verbindung mit der Nutzung von Ge-

schäftsgeheimnissen wird mit den Mitarbeitern auf der Grundlage von Arbeitsverträgen und mit den Geschäftspartnern auf der Grundlage von zivilrechtlichen Verträgen durchgeführt.

Allgemein ist in Russland nur Sicherheit von personenbezogenen Daten stark gesetzlich geregelt. Andere Geheimnisse dürfen die Unternehmer nach eigenem Ermessen schützen.

Die Frage, ob der Staat Zugriffsrechte in Bezug auf vertrauliche Informationen von Unternehmen hat, kann positiv beantwortet werden. Im Gesetz sind die Bereitstellung von Informationen, die ein Geschäftsgeheimnis bilden, den Staatsorganen ausdrücklich vorbehalten, sowie die Haftung des Inhabers bei Nichtvorlage der Informationen. Die Praxis zeigt, dass eine große Anzahl von Behörden in Russland das Recht hat, Informationen vertraulicher Art zu erhalten. Das passiert aber nur in streng gesetzlich geregelten Fällen. Der Anspruch muss begründet sein. Die allgemeinen Formulierungen sind nicht erlaubt. Im Fall der Ablehnung kann die Information durch Gerichte angefordert werden. Die Behörden haben ebenfalls ihre Verantwortung. Sie müssen die Bedingungen schaffen, um die Vertraulichkeit der übermittelten Informationen zu gewährleisten. Außerdem wurde im Jahr 2008 gegen der Willkür von staatlichen Behörden bei Kontrollen von Unternehmen ein Gesetz in Russland verabschiedet, in dem die Anforderungen während geplanter und vor allem außerplanmäßiger Kontrollmaßnahmen deutlich verschärft wurden und der Schutz der Rechte von Unternehmern während dieser Maßnahmen verbessert wurde.

4.3. Datenherrschaft, Datenverwendung

Das Problem des rechtlichen Schutzes von Informationen (oder Daten) liegt in vielen Ländern, darunter in Russland, darin, dass das Eigentumsrecht traditionell ein materielles Objekt (eine Sache) hat. Information ist aber kein materielles Objekt und kann nur mit einem materiellen Objekt verbunden sein.

In Russland änderte sich die Betrachtungsweise auf die Information als ein Objekt der Zivilrechte. Noch im Wortlaut des Bürgerlichen Gesetzbuches 2007 war die Information ausdrücklich als Gegenstand der Zivilrechte erwähnt. Auf dieser Norm basierten die Bestimmungen des Bundesgesetzes "Über Information, Informationstechnologien und Informationsschutz". Doch trat am 1. Januar 2008 eine neue Version des Bürgerlichen Gesetzbuches in Kraft, in der die Information unter den Objekten der Zivilrechte nicht erwähnt wurde. Folge ist ein Konflikt zwischen dem Gesetzbuch und den Bestimmungen des Bundesgesetzes. Manche Experten sind der Ansicht, die Information an sich sei zivilrechtlich nur insofern geschützt, als sie ein schutzfähiges Ergebnis der intellektuellen Tätigkeit ist. Insgesamt führte das Herausnehmen der Information aus der Liste der Objekte der Zivilrechte nicht zu ihrem Ausschluss aus den anderen Rechtsnormen, die Rechtsverhältnisse in den verschiedenen Rechtsgebieten regeln, auch nicht aus dem

Zivilrecht. Als Ergebnis können die Parteien basierend auf dem Prinzip der Vertragsfreiheit, das im Bürgerlichen Gesetzbuch verankert ist, Verträge über Information unter Berücksichtigung der zwingenden Normen abschließen (z.B. Kaufvertrag von Information unter Berücksichtigung des Verbots der Übertragung von Geschäftsgeheimnis an Dritte ohne das Wissen des Inhabers). In der Zwischenzeit streiten sich die Anwälte und Theoretiker weiterhin darüber, ob die Information ein unabhängiges Objekt der Zivilrechte sein kann.

In Bezug auf Datenherrschaft erhalten die Gesetze nur die Begriffe der Datenbesitzer (Datenbesitzer und Besitzer eines Geschäftsgeheimnisses). Den Begriff des Dateneigentümers konnte man früher im Gesetz und in einem staatlichen Standard (GOST) von 1996 finden, der Empfehlungscharakter hatte. Der neue Standard, der 2008 in Kraft trat, definiert nur die Begriffe „Datenbesitzer“ und „Datennutzer“:

- Datenbesitzer:
  eine Person, die selbst die Information erstellt oder die gemäß einem Gesetz oder Vertrag das Recht bekommt, den Zugang zu der Information zu erlauben oder beschränken, und diese Information kann aufgrund ihrer Eigenschaften erkannt werden (Den gleichen Begriff findet man auch im Gesetz.);

- Datennutzer
  ein Subjekt, das die Information von ihrem Eigentümer, Besitzer oder Mittelsperson erhält, und sie in Übereinstimmung mit den Rechten und Regeln für den Zugang zur Information oder mit ihren Verletzungen benutzt (Diese Definition fehlt im Gesetz.).

Einige Autoren meinen, dass der Gesetzgeber den Begriff "Dateneigentümer" aus dem Gesetz gerechtfertigt ausschließe, weil die Verwendung von der traditionellen Terminologie in Bezug auf die Information falsch wäre.

5. Technikrecht

5.1. Produktsicherheit, Produkthaftung

Fragen der Produkthaftung sind insbesondere im Zivilgesetzbuch der Russischen Föderation und auch in einem speziellen Verbraucherschutzgesetz geregelt. Das Recht der Verbraucher auf die Sicherheit von Waren ist im Verbraucherschutzgesetz verankert. Die verbindlichen Anforderungen zur Sicherheit von Waren werden in den staatlichen Standards, Normen und Vorschriften zur Hygiene, Bauvorschriften und in anderen regulatorischen und technischen Dokumenten festgelegt. Pflicht des Herstellers ist es, die Sicherheit von Waren während der angegebenen Betriebsdauer oder Geltungsdauer von Waren zu gewährleisten. Für den Fall, dass der Hersteller keine Betriebsdauer für seine Waren festlegt, wird er bedingungslos verpflichtet, die Sicherheit von Waren

innerhalb von zehn Jahren ab dem Zeitpunkt ihrer Lieferung zu gewährleisten und in Fällen von Lebens-, Gesundheits- oder Vermögensschäden Schadensersatz zu bezahlen. Zusätzlich zur Entschädigung für materielle Schäden und Verluste hat der Verbraucher Recht auf Entschädigung für immaterielle Schäden.
Die Waren, die Leben, Gesundheit der Verbraucher oder Umwelt in Gefahr bringen können, unterliegen der obligatorischen Zertifizierung. Der Hersteller ist verpflichtet, solche Produkte zu zertifizieren, um ihre Sicherheit für die Verbraucher zu bestätigen. Eine Liste solcher Waren wird von der Regierung der Russischen Föderation genehmigt. Die Freigabe dieser Waren ohne entsprechendes Dokument (Zertifikat) ist verboten.

Das Gesetz sieht die Pflicht der Hersteller vor, die Produktion von Waren bis zur Beseitigung der Ursachen von Schäden auszusetzen, wenn festgestellt wird, dass sogar die richtige Verwendung und Lagerung dieser Produkte Schäden für die Verbraucher verursachen werden oder können. Gegebenenfalls muss der Hersteller geeignete Maßnahmen ergreifen, um die Produktion von diesen Waren auszusetzen oder sie auch aus dem Verkehr zu ziehen. Wenn der Hersteller sich weigert, diese Pflicht zu erfüllen, wird die Rücknahme und Rückruf des Produkts von einem zuständigen Bundesorgan durchgeführt, das mit der staatlichen Kontrolle der Qualität und Sicherheit von Produkten betraut ist.

5.2. Normenwesen, Zertifizierung

Da es zwischen Russland und der EU kein Abkommen für die gegenseitige Anerkennung von Zertifikaten gibt, müssen die Produkte bei Import nach Russland gemäß den russischen Normen überprüft und zertifiziert werden. In der Praxis erleichtert die Vorlage von europäischen Zertifikaten diesen Prozess.

Das System der Zertifizierung wird grundsätzlich durch das Bundesgesetz „Über technische Regulierung“ geregelt. Mit diesem Gesetz wurde in Russland 2003 auf die globalen Anforderungen der Wirtschaft reagiert. Das Ziel war, die technische Gesetzgebung und die technische Regulierung den Normen von internationalen und europäischen Standards anzupassen. Das Gesetz sieht zwei Arten von Zertifizierung vor: Pflichtzertifizierung und freiwillige Zertifizierung von Waren. Als Ergebnis bekommt man heutzutage das neue TR-Zertifikat (früher GOST-R-Zertifikat).

Im Jahre 2010 beschloss die Russische Föderation, Weißrussland und Kasachstan ein einheitliches System der technischen Regulierung einzuführen. Für diesen Zweck wurden durch die Kommission der Einheitlichen Zollunion (auch Euroasiatische Zollunion genannt) insgesamt mehr als 30 verschiedene Reglements bestimmt und eingeführt. Diese technischen Regelwerke (TR TS oder TR CU) sind für alle drei Länder gültig. Die ausländischen Unternehmer, die bereits in einem von drei Märkten aktiv sind, können auch leichten Zugang zu anderen Staaten innerhalb der Union bekommen und davon profitieren.

Industrie 4.0 in Indien

Dr. Jona Aravind Dohrmann, Rechtsanwalt
HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH, Hannover

1. Allgemeine wirtschaftliche Lage in Indien

Seit mehr als 20 Jahren ist Indien in einem Wettstreit mit seinem großen Nachbarn China, wer den größeren Anteil an der globalen Produktion an sich zieht. Wie ungleich dieser Wettkampf war, zeigt sich an der Tatsache, dass der Beitrag der industriellen Produktion am indischen BIP lediglich bei ca. 15 % liegt, wohingegen dieser Wert in China stolze 30 % aufweist. Eine konventionelle Aufholjagd, was den Produktionsanteil am BIP angeht, wird Indien wohl nicht mehr gewinnen können. Legt man zugrunde, dass jede industrielle Revolution schneller vonstattengeht, als ihre jeweilige Vorgängerin, könnte Indien unter dem Banner einer Industrie 4.0 zur „Digital Factory“ oder digitalen Werkbank der Welt werden. Verbindet man die Ansätze von Industrie 4.0 mit der indischen Investitionsinitiative „Make in India“, könnte Indien Chinas Stand in 20 Jahren überholt haben.

2. Industrie 4.0. in Indien

2.1. Ausgangslage

Analysten sind der Meinung, dass Indien ein paar Schritte unternehmen müsste, um von einer vierten industriellen Revolution zu profitieren. Dazu gehöre zu allererst das Wachstum des Internets der Dinge (Internet of Things = IoT). Zu diesem Zweck sind wiederum eine Förderung von Fachkräften, ein Technologiefortschritt sowie die Investition in Forschung und Entwicklung unabdingbar, damit der lokale Markt wächst.

Während das Internet der Dinge das Rückgrat der Industrie 4.0 ist, muss eine zu schaffende angemessene Datenschutzumgebung das geistige Eigentum sichern helfen. Datenschutzregelungen müssen daher von Anfang an in die neue Architektur einer smarten Fabrikanlage integriert werden. Unterstützt werden müssten die vorgenannten technologischen Ansätze durch eine möglichst frühzeitig an den Universitäten ansetzende Ausbildung im Bereich dieser hochtechnologisierten Produktionsmethode.

Bezüglich der notwendigen Veränderung im Bereich der Produktion wissen sich Indien und Deutschland Seite an Seite, wie man spätestens seit der Teilnahme Indiens als

Partnerland an der Hannover-Messe 2015 weiß. Wenn auch aus unterschiedlichen Gründen: Deutschland möchte seine Marktführerschaft im Bereich industrieller Produktion wahren, Indien möchte genau eine solch herausgehobene Stellung im Wettstreit mit dem ewigen Widersacher China erst noch erreichen.

2.2. Perspektive für Industrie 4.0

Die Zuwendung zur Industrie 4.0 könnte für den indischen Subkontinent immense Vorteile bergen, wie fortschrittsorientierte Unternehmer immer wieder betonen. Zwar besitzt Indien schon eine herausgehobene Stellung in der Produktion dank seines Binnenmarktes. Jedoch ist der Weltmarkt einem raschen Wechsel unterworfen, bei dem die Lebenszeit der Produkte immer kürzeren Zyklen folgt und sich die Arbeitskosten, die Ansprüche an Qualität sowie an die Individualität des Produkts rapide wandeln. Daher benötigt Indien smarte Lösungen, um die Produktion im Land zu halten bzw. verloren gegangene wieder aus noch billiger produzierenden Ländern zurückzugewinnen. Denn immerhin sind 40 % der weltweiten Produktion in den Schwellenländern verankert.

Pierre Leretz, Vorstandsvorsitzender der ABB Process Automation India, Middle East and Africa sieht in Industrie 4.0 ein großes Potential, da sich die Entwicklung in der von ihm betreuten Region überschlägt, was die Entwicklung von Infrastruktur in den Städten und in der Industrie selbst angeht. Dies sei ein fruchtbarer Nährboden für intelligente Industrien. Mit der Verfolgung einer Strategie zur Implementierung von Industrie 4.0 könnte Indien zudem den Trend von einer produktions- zu einer serviceorientierten Gesellschaft zu seinem eigenen Vorteil nutzen. Indische Unternehmer nehmen sehr wohl wahr, dass etwa die deutschen Automobilhersteller ca. 50 % ihres Umsatzes aus den sog. Aftersales Services generieren.

3. Umfeld für Investitionen

3.1. Politische Ziele

Der Anteil der indischen Produktion von ca. 15 % am BIP bedeutet im globalen Kontext einen Anteil von lediglich 2 %. Dieser Sektor bietet knapp 60 Millionen Menschen eine Arbeit, welches 12 % der Arbeitskräfte weltweit in diesem Bereich sind. Allerdings sieht sich der indische Staat vor die Herausforderung gestellt, wie in den nächsten 15 Jahren ca. 250 Millionen Menschen in den Arbeitsmarkt integriert werden sollen. Daher sind riesige Umwälzungen in der Produktionslandschaft notwendig, was Investitionen, Infrastruktur und Technologie angeht.

Unter dem Banner der neuen “Make in India”- Initiative möchte die indische Regierung ihren “Produktions-Fußabdruck” deutlich vergrößern. Neben den üblichen Zielsetzungen wie der Schaffung von Arbeitsplätzen, der Minimierung von Importen und dem Ausbau von Exporten soll nicht zuletzt eine der technischen Evolution zuträgliche Umgebung geschaffen werden. Auch wenn im indischen Kontext momentan mehr Fragen als Antworten vorhanden sind, beschäftigen sich immer mehr Unternehmen in Indien mit den Fragen der Industrie 4.0 und begreifen die jüngste und bevorstehende industrielle Revolution als Chance für den indischen Markt, wenn Unternehmen und die Glieder einer Wertschöpfungskette die Vorzüge dieser Entwicklung begreifen und sich den neuen Herausforderungen stellen. Frost & Sullivan, die gemeinsam mit ihren Kunden Wachstumsstrategien entwickeln, sehen ein großes Potential in den Möglichkeiten der Industrie 4.0. Dazu müssten aber Zulieferer ihre Prozesse neu definieren, Unternehmen mit neuartigen Ansätzen hätten eine Chance, sich auf dem sich neu entwickelnden Markt zu etablieren, andere Unternehmen würden vermutlich den Wandel nicht überleben. Die Wachstumsstrategen sind der Ansicht, dass Industrie 4.0 zwar deutscher Herkunft ist, jedoch einen weltweiten Widerhall gefunden hat – auch in Indien. Sie sind der Ansicht, dass Industrie 4.0 ein integraler Bestandteil der Debatte um die Wirtschaftsinitiative „Make in India“ werden muss, wenn Indien mit als Industriestandort an internationale Standards und Exzellenz anknüpfen will.

3.2. Indien und die HANNOVER MESSE 2015

Auf der HANNOVER MESSE 2015 ist es Indien mit einem frischen Auftritt im Rahmen seiner „Make in India“- Initiative gelungen, sich eindrucksvoll als aufstrebende Industrienation darzustellen, wie Dr. Jochen Köckler, Vorstand Deutsche Messe, lobte.

So könnte der positive Eindruck, den der indische Auftritt auf der HANNOVER MESSE 2015 hinterlassen hat, in Verbindung mit der deutschen Industrie 4.0 -Initiative genau den Nerv in Indien treffen, den das Land benötigt, um den Sprung von einer zwar aufstrebenden, jedoch ins Hintertreffen geratenen Industrienation zu einer führenden Wirtschaftsmacht mit innovativen Technologien zu schaffen.

3.3. Beschäftigung und Arbeitsrecht

Das indische Arbeitsrecht basiert auf kolonialen Wurzeln. In Britisch- Indien wurden zunächst Arbeitsgesetze erlassen, die die Angelegenheiten einzelner Industriezweige regelten (Industrie, Bergbau, Plantagen). Diese Struktur ist auch heute noch weitestgehend sichtbar geblieben. Es sind jedoch etliche Spezialgesetze hinzugekommen, wie das Mindestlohngesetz (*Minimum Wages Act*, 1948), das Gesetz zu variablen Vergütungsanteilen (*Payment of Bonus Act*, 1965) oder ein Gesetz zur Regelung von Arbeitskämpfen (*Industrial Disputes Act*, 1947). Ähnlich wie in Deutschland gibt es jedoch kein übergreifendes, einheitliches Arbeitsgesetzbuch. Ansätze zur vereinheitlichten Kodifi-

zierung arbeitsrechtlicher Belange scheiterten in Indien ebenso wie in Deutschland. Da die indischen Länder qua Verfassung (*Constitution of India*) in großen Teilen gesetzgeberisch für das Arbeitsrecht zuständig sind, existieren als Folge dieser konkurrierenden Gesetzgebung zahlreiche ähnliche Gesetze auf Bundes- und Länderebene. Nach der Unabhängigkeit Indiens wurde viel Wert gelegt auf die gesetzliche Ausprägung des in der indischen Verfassung enthaltenen Sozialstaatsprinzips, die vor allem in Kapitel IV der Verfassung im Rahmen der Staatszielbestimmungen ihren Niederschlag finden. Dies führte über die Jahre zu einer Überregulierung mit teils sehr starren überkommenen arbeitsrechtlichen Vorschriften.

Grundsätzlich können Arbeitsverträge formfrei abgeschlossen werden. Im sog. organisierten Sektor sind jedoch schriftliche Arbeitsverträge mittlerweile die Regel (*Letter of Appointment*), die meist in größeren Unternehmen durch sog. *Standing Orders,* ähnlich den Betriebsordnungen im deutschen Recht, ergänzt werden.

Arbeitsverträge werden in der Regel unbefristet abgeschlossen und beinhalten eine drei- bis sechsmonatige Probezeit. Es besteht jedoch auch die Möglichkeit der Befristung.

Ausländer benötigen zur Aufnahme einer Arbeit in Indien ein Arbeitsvisum (*Employment Visa*), das üblicherweise mit der Vorlage eines Angebotes eines Arbeitsvertrages beantragt wird.

Die tägliche Arbeitszeit beträgt 9 Stunden, die wöchentliche Arbeitszeit soll 48 Stunden nicht übersteigen. Büroangestellte arbeiten in der Praxis 40 bis 45 Stunden in der Woche, Fabrikarbeiter meist 48 Stunden.

Das Arbeitsverhältnis kann einseitig unter Einhaltung der Kündigungsfrist oder unter besonderen Umständen außerordentlich beendet werden. Grundsätzlich ist eine ordentliche Kündigung schriftlich und unter Einhaltung einer Mindestfrist von einem Monat zu erklären. Ob weitere Vorgaben z. B. zu einer vorherigen Abmahnung oder Kündigungsgründen bestehen, muss im Einzelfall geprüft werden. Besonders strenge Kündigungsvorschriften gelten in Betrieben mit 100 oder mehr Arbeitnehmern.

3.4. Geistiges Eigentum

Hauptsorge vieler Investoren in Indien ist der befürchtete schwache Schutz geistigen Eigentums. Im Zuge der Liberalisierung des indischen Marktes hat sich auf diesem Gebiet jedoch einiges gebessert. Indien hat die wichtige Rolle des Schutzes geistigen Eigentums erkannt. Seit dem 1.1.2005 verfügt Indien über ein reformiertes Patentrecht. Als Neuerung wurde unter anderem die Patentfähigkeit von pharmazeutischen und lebensmitteltechnischen Produkten festgeschrieben. Software bleibt ebenso wie in der EU nach wie vor nicht patentfähig, ist jedoch urheberrechtlich geschützt. Ein eingetra-

genes Patentrecht entfaltet Schutzwirkung für einen Zeitraum von 20 Jahren. Eine erneute Überarbeitung des Patentgesetzes befindet sich im Gesetzgebungsverfahren.

Das Markenrecht findet seine Rechtgrundlage im *Trade Marks Act*, 1999 und den *Trade Marks Rules*, 2002. Die Schutzdauer für Warenzeichen beträgt zunächst zehn Jahre und kann für je weitere zehn Jahre erneuert werden. Mit Wirkung zum 8.7.2013 ist Indien dem Madrider Markenprotokoll beigetreten. Damit entfalten von diesem Zeitpunkt an Markenanmeldungen unter dem Madrider Markensystem auch in Indien Wirkung.

Muster und Modelle werden durch den *Design Act*, 2000, in Kraft getreten 2001 geschützt. Die Schutzdauer beträgt zehn Jahre ab der Registrierung; es besteht eine Verlängerungsmöglichkeit von weiteren fünf Jahren.

Urheberrechte unterliegen dem 1999 zuletzt überarbeiteten *Copyright Act*. Allerdings liegt dem Parlament ein Reformentwurf vor, der unter anderem die Rechte von Musikschaffenden gegenüber Produzenten stärken soll.

Indien ist Mitglied u. a. folgender internationaler Übereinkommen:

- der Weltorganisation für geistiges Eigentum (WIPO/OMPI);
- der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums (PVÜ);
- des Vertrages über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT);
- des Budapester Vertrages über die internationale Anerkennung der Hinterlegung von Mikroorganismen für die Zwecke von Patentverfahren.

Durch den Beitritt zur WTO und dem TRIPS-Agreement (*Trade Related Aspects of Intellectual Property Rights*) zum 1. Januar 1995 war Indien darüber hinaus gezwungen, den Verpflichtungen aus diesem Beitritt nachzukommen und entsprechende Standards zum Schutze geistigen Eigentums zu verabschieden.

Kernproblem ist jedoch meist die Durchsetzung von gewerblichen Schutzrechten. Indische Gerichte sind sich dieser Problematik zunehmend bewusst und gewähren häufig einstweiligen Rechtsschutz im Wege von Arrest- und Sicherungsverfügungen.

4. Informationen und Daten

4.1. Datenschutz (personenbezogene Daten)

In Indien gibt es kein spezifisches Gesetz zum Datenschutz, wie man es in Deutschland etwa vom Bundesdatenschutzgesetz her kennt. Dennoch gibt es kodifizierte Schutzme-

chanismen zum Schutz von elektronischen Daten. Diese sind im *Information Technology Act*, 2000, niedergelegt. Der Schutz elektronischer Daten umfasst dabei auch nicht-elektronische Informationen, welche elektronisch verarbeitet wurden oder werden sollen. Gemäß der vom indischen Ministerium für Informationstechnologie (*IT Ministry*) erlassenen Durchführungsbestimmungen (*Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information*] *Rules*), auch *Privacy Rules* genannt, verlangen von Unternehmen, die persönliche Daten (inkl. besonders sensibler persönlicher Daten) sammeln, verarbeiten oder speichern, bestimmten Standards zu entsprechen. Die Unterscheidung zwischen den '*personal information*' und '*sensitive personal information*', geschieht folgendermaßen:

Die *Privacy Rules* definieren 'personal information' als jegliche Informationen, die eine natürliche Person betreffen, welche entweder mittelbar oder unmittelbar oder in Verbindung mit anderen Informationen, die für ein Unternehmen verfügbar sind, die Identifizierung einer Person ermöglichen.

Als 'sensitive personal data or information' bezeichnen die *Privacy Rules* folgende Informationen:

- Passwörter
- Finanzielle Informationen zu Bankverbindungen, Kredit- und Bankkarten oder anderen Zahlungsinstrumenten
- Physische, physiologische oder psychologische Zustandsinformationen
- Sexuelle Orientierung
- Krankenakten und -geschichten
- Biometrische Daten

Informationen, die jedoch in der *public domain* frei zugänglich sind, sind von der vorstehenden Definition ausgenommen.

Das indische *Ministry of Communications and Information* stellte in einer sog. 'Press Note' klar, dass indische Outsourcing-Provider, welche Dienstleistungen im Bereich der Datensammlung, -verarbeitung und -speicherung bezogen auf personenbezogene Daten oder besonders sensible persönliche Daten aufgrund von Dienstleistungsverträgen anbieten, dann nicht dem indischen Datenschutzrecht unterliegen, wenn sie nicht unmittelbar in Kontakt mit den Personen stehen, deren Daten verarbeitet werden. Das gilt für Verträge mit indischen wie mit ausländischen Vertragspartnern.

Jedes Unternehmen, das sensible persönliche Daten sammelt, muss einen Datenschutzbeauftragten ernennen (*Grievance Officer*), damit mögliche Beschwerden an ihn gerichtet werden können.

4.2. Datensicherheit (gegen unbefugten Zugriff)

Ein Unternehmen, das sensible persönliche Informationen besitzt, damit handelt oder diese verarbeitet, ist verpflichtet, angemessene Sicherheitspraktiken und –verfahren zur Sicherung der Daten gegen unbefugten Zugriff anzuwenden. Die Sicherheitsvorkehrungen können etwa vertraglich zwischen den betreffenden Parteien vereinbart werden. Die *Privacy Rules* verlangen ferner, dass in Abwesenheit einer solchen Vereinbarung dennoch Sicherheitsvorkehrungen getroffen werden müssen, die mindestens dem IS/ISO/IEC 27001 Standard oder den sog. *Codes of best practices for data protection* entsprechen, die staatlicherseits anerkannt wurden.

Der indische Staat hat außerdem einen Krisenstab eingerichtet, der Datenverarbeitungsmanipulationen und Verletzung der IT-Sicherheit dokumentieren, analysieren, über die festgestellten Sicherheitslücken aufklären und geeignete Gegenmaßnahmen ergreifen oder koordinieren soll. Dieser Stab nennt sich *Computer Emergency Response Team (Cert-In)*. Die dazugehörigen Durchführungsbestimmungen, genannt *Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules)*, verpflichten Service Provider, Subunternehmer, und Unternehmen auf bestimmte Hinweispflichten, wenn bestimmte sicherheitsrelevante Ereignisse (‘*cyber security incidents’*) auftreten.

Strafzahlungen in Höhe von bis zu umgerechnet knapp 700.000 EUR können erhoben werden, wenn die Datensicherheit nicht gewährleistet werden kann. Schadensersatzleistungen in einem zivilprozessualen Verfahren können weit über dem vorgenannten Betrag liegen. Verfehlungen können auch mit Gefängnisstrafen von bis zu drei Jahren oder mit einer Geldbuße von bis zu knapp 7.000 EUR geahndet werden.

4.3. Datenherrschaft und Datenverwendung

Die vorgenannten *Privacy Rules* verlangen im Rahmen der Datenherrschaft und Datenverwendung, dass jedes Unternehmen oder dessen Vertreter, welches sensible persönliche Informationen verarbeitet, eine schriftliche Zustimmung in Briefform, durch E-Mail oder FAX vorweisen können muss. Zuvor muss dieses Unternehmen seine konkreten Datenschutzregelungen offen legen und zur Kenntnis bringen, wie es mit den verarbeiteten Daten umgeht. Darüber hinaus muss das Unternehmen bezogen auf die von einer Person gesammelten Daten zur Zeit der Sammlung dieser Daten auf Folgendes hinweisen:

- dass die Daten gesammelt werden,
- den Zweck der Sammlung dieser Daten,
- den beabsichtigten Empfänger dieser Daten und
- den Namen und die Adresse des sammelnden Unternehmens.

Sensible persönliche Daten dürfen nur für einen rechtlich zulässigen Zweck gesammelt werden. Das Unternehmen muss sicherstellen, dass es die sensiblen persönlichen Daten nicht länger aufheben darf als für den intendierten Zweck notwendig ist.

Diejenigen Personen, die die Informationen zur Verfügung stellen, haben ein Recht darauf, die gespeicherten Daten zu prüfen und ggfs. zu korrigieren und sogar ihre Zustimmung zur Verarbeitung zu widerrufen (*right to opt out*).

Unternehmen dürfen sensible persönliche Daten nicht an Dritte weiterleiten, die nicht dieselben Standards gemäß dem *Information Technology Act* erfüllen wie das weiterleitende Unternehmen.

5. Technikrecht

5.1. Produktsicherheit, Produkthaftung

Unter dem Begriff Produkthaftung versteht man die Haftung des Herstellers für Folgeschäden aus der Benutzung seiner Produkte. In Indien ist diese Haftung im *Consumer Protection Act*, 1986 geregelt (CPA). Dort wird der Verbraucher vor fehlerhaften Produkten, mangelhaften Dienstleistungen und Produkten, bei denen den Informationspflichten bezüglich Inhalt, Verhalten und Auswirkung des Produkts nicht nachgekommen wurde, geschützt (Chapter I, 2. (c) ii, iii, 2(v) CPA).

Ein Produkt ist fehlerhaft, wenn es Fehler, Unvollkommenheit oder Unzulänglichkeit bezüglich Qualität, Menge, Stärke, Reinheit und Standard aufweist (Chapter I, 2. (f) CPA). Aber auch dann, wenn es bei bestimmungsgemäßem Gebrauch das Leben oder das Eigentum des Verbrauchers gefährdet (Chapter II, 6. (a) CPA). Eine Dienstleistung ist mangelhaft, wenn sie fehlerhaft, unvollkommen, unzulänglich ist oder ein Missverhältnis in der Qualität und Art und Weise ihrer Erbringung aufweist (Chapter I, 2. (g) CPA). Beim Vorliegen der vorstehend genannten Fälle hat der Verbraucher die Möglichkeit, gegen den Hersteller zu klagen. Dazu wurde ein dreistufiges Verbrauchergerichtssystem eingerichtet. Welches Gericht zuständig ist, hängt von der Höhe der Reklamation und den eventuellen Schadensersatzansprüchen ab. Gerichtsgebühren fallen nicht an. Hersteller ist gemäß S.2(j) CPA, wer

- Produkte oder nur Teile davon herstellt oder
- keine Produkte oder nur Teile davon herstellt, aber Teile zusammensetzt, die von Anderen hergestellt wurden und das Endprodukt als von ihm hergestellt ausgibt oder

- sein eigenes Kennzeichen an Produkte anbringt oder anbringen lässt, die von anderen hergestellt wurden und diese Produkte als von ihm selbst hergestellt ausgibt.
- Filialen eines Herstellers werden nicht als selbständiger Hersteller angesehen.

Liegt tatsächlich ein fehlerhaftes Produkt oder eine mangelhafte Dienstleistung vor, muss der Hersteller gem. S.14 (1a) CPA z. B.

- den Fehler beseitigen,
- eine neues fehlerfreies Produkt/Dienstleistung anbieten,
- das Geld für die erworbene Ware/Dienstleistung zurückgeben und/oder
- Schadensersatz leisten.

Die Verjährungsfrist beträgt gem. S.24A CPA zwei Jahre. Sie kann verlängert werden, wenn der Kläger beweisen kann, dass es ihm unmöglich war, die Klage innerhalb der Frist einzureichen.

5.2. Normenwesen, Zertifizierung

Indien hat ein umfassendes System der Produktzertifizierung, welches gesetzlich geregelt ist. Die Zertifikate werden von unterschiedlichen Institutionen betreut. Manche Zertifizierungen sind zwingend für Produkte, die in Indien hergestellt oder vertrieben werden sollen. Andere hingegen haben lediglich informatorischen Charakter. Alle Industriestandards und industriellen Produktzertifizierungen werden vom *Bureau of Indian Standards* geprüft. Alle anderen (z. B. für landwirtschaftliche Produkte werden von anderen staatlichen Ämter entwickelt und geprüft.

Die staatlicherseits geprüften und durchgesetzten Zertifizierungen sind gegenwärtig:

- ISI mark:
  für industrielle Produkte, Zertifizierung der Einhaltung von Standards, die vom *Bureau of Indian Standards* vorgegeben werden.[182]

- FPO mark:
  Zwangszertifizierung notwendig für alle Produkte, in denen Früchte verarbeitet sind. Zertifizierung der Herstellung eines Produkts in hygienischer und „lebensmittelsicherer“ Umgebung.

- Agmark:
  für alle landwirtschaftlichen Produkte.

[182] https://en.wikipedia.org/wiki/Certification_marks_in_India - cite_note-1

- Non Polluting Vehicle Mark
  für Fahrzeuge, die die Konformität mit indischen Emissionsstandards zertifiziert (Bharat Stage emission standards).

- BIS hallmark:
  zertifiziert die Reinheit von Goldschmuck.

- India Organic certification mark:
  für biologisch hergestellte, landwirtschaftliche Produkte. Zertifiziert, dass das Produkt den Spezifizierungen der *National Standards for Organic Products*, 2000 entspricht.[183]

- Ecomark:
  ist ein Öko-Label für unterschiedliche Produkte, welche vom *Bureau of Indian Standards* bestimmt werden. Dieses Label ist freiwillig und soll verkaufsfördernden Charakter haben.

[183] https://en.wikipedia.org/wiki/Certification_marks_in_India - cite_note-5

Indy4

Die Indy4 Gruppe

Mit der aufkommenden Bedeutung von Industrie 4.0 hat sich in Hannover eine Gruppe von Experten aus verschiedenen Fachbereichen und mit unterschiedlichem Hintergrund gebildet, um sich mit den verschiedenartigen Auswirkungen dieser technologischen Entwicklung auseinanderzusetzen. Das besondere verbindende Element ist die räumliche Konzentration mit dem Schwerpunkt in Niedersachsen.

Die Mischung der Gruppe aus Wissenschaft und Praxis ergibt ein lebendiges und vielschichtiges Bild des Phänomens Industrie 4.0. Die Erkenntnisse sollen zum einen Arbeiten in Forschung und Entwicklung anregen, zum anderen aber ganz praktische Fragestellungen in den Unternehmen identifizieren und dazu Lösungen erarbeiten.

Die Indy4 Gruppe arbeitet in Form von Arbeitspapieren und Diskussionsrunden, bei denen unmittelbar inhaltliche Vernetzungen entstehen – in der Art eines Think Tanks. Gerade die interdisziplinäre Zusammensetzung von Indy4 ermöglicht und generiert Erkenntnisse, die in einem auf einheitliche Fachgebiete konzentrierten Kreis so nicht erzielbar sind.

Indy4 spiegelt damit das notwendige Blickfeld und das breite Entscheidungsspektrum der Geschäftsführung von Unternehmen wider.

Die Lösungen werden dem interessierten Publikum zugänglich gemacht, in Form von Publikationen, Seminaren, Workshops, Konferenzen und im Internet.

Die Arbeit von Indy4 fügt sich in das Engagement des Landes Niedersachsen über das Innovationszentrum mit dem Netzwerk Industrie 4.0 ein, und trägt zum Programm des Mittelstand 4.0 – Kompetenzzentrums Hannover (für Norddeutschland) bei. Indy4-Mitglieder sind dort verantwortliche Mitglieder und Indy4 insgesamt ist über Herfurth & Partner mit dem Themenbereich „Ökonomie und Recht in der Digitalen Wirtschaft“ engagiert. Weitere Felder der Zusammenarbeit liegen bei der Industrie- und Handelskammer, Verbänden und der Deutschen Messe AG.

Mit ihrer übergreifenden Arbeit will Indy4 einen über die regionale Wahrnehmung hinausgehenden Beitrag zur Entwicklung von Unternehmen in diesem Feld von Technologie und Wirtschaft leisten: Industrie 4.0.

Indy4 - Beteiligte

Management	
Prof. Dr. Klaus Fischer	FHDW Fachhochschule für die Wirtschaft Hannover
Dr. Michael Koch	Arleon GmbH / C-PLUS M Unternehmensentwicklung
Christian Grotebrune	UNITY AG, Büren
Uwe Claaßen	Nds. Ministerium für Inneres und Sport-Abteilung 5
Produktionsplanung, Automation	
Dr. Georg Ullmann	IPH - Institut für Integrierte Produktion Hannover GmbH
Prof. Dr.-Ing. Lorenz Däubler	Hochschule Hannover
IT und Security	
Prof. Dr.-Ing. Wolfgang Nebel	OFFIS e.V. Institut für Informatik
Prof. Dr.- Ing . Karl-Heinz Niemann	Hochschule Hannover
Antonius Sommer	TÜV Informationstechnik GmbH / TÜV Nord
Prof. Dr. Matthias Schumann	Georg-August-Universität Göttingen
Frank Knischewski	Hannover IT e.V.
Jörg Peine-Paulsen	Nds. Ministerium für Inneres und Sport-Abteilung 5
Harald Bunte	Nds. Ministerium für Inneres und Sport-Abteilung 5
Marketing	
Gisela Strnad	Strnad Marketing
Personal	
Prof. Dr. Wolfgang Krüger	Fachhochschule des Mittelstands (FHM) Hannover
Lilia Flat	Arleon GmbH / Flat Coaching
Finanzen	
Prof. Dr. Niels Angermüller	Hochschule Harz
Axel Bergmann	Arleon GmbH Unternehmensentwicklung
Günter Stuff	Herfurth & Partner / Steuerberatung
Recht	
Ulrich Herfurth	Herfurth & Partner Rechtsanwaltsgesellschaft mbH
Dennis Jlussi	Herfurth & Partner Rechtsanwaltsgesellschaft mbH
Joachim Gerstein	Gramm, Lins & Partner Patentanwälte
Sebastian Aisch	Gramm, Lins & Partner Patentanwälte
Ausland	
Uzunma Bergmann	Herfurth & Partner, USA Desk
Sabine Reimann	Herfurth & Partner, Brazil Desk
Xiaomei Zhang	Herfurth & Partner, China Desk
Elena Duwensee	Herfurth & Partner, Russia Desk
Dr. Jona Aravind Dohrmann	Herfurth & Partner, India Desk

Autoren

Sebastian Aisch ist Diplom-Informatiker und Patentanwalt bei Gramm Lins und Partner Patent- und Rechtsanwälte. Er verfügt über besondere Erfahrung im Patentrecht auf dem Gebiet der computerimplementierten Erfindungen und Softwarepatente.

Uzunma Bergmann ist als US-Anwältin bei Herfurth & Partner tätig. Sie verfügt über einen Master in Intellectual Property und Informationstechnologie und arbeitete in New York im internationalen Vertragsrecht, Urheber- und Markenrecht, E-Commerce und Outsourcing. Ihre Erfahrungen umfassen Produktionsverträge und Registrierungsverfahren für internationale Copyrights. Sie ist als Attorney at Law (USA) und Solicitor (England & Wales) zugelassen.

Marc-André Delp arbeitet als Rechtsanwalt bei Herfurth & Partner im nationalen und internationalen Handelsrecht und Wirtschaftsrecht. Seine Schwerpunkte liegen im Vertragsrecht, Export, Verfahrensrecht und Forderungsmanagement. Er ist dazu regelmäßig als Referent für Kammern und Verbände tätig.

Dr. Jona Aravind Dohrmann ist als Rechtsanwalt bei Herfurth & Partner für den Bereich Indien verantwortlich. Er war mehrere Jahre in Indien tätig und verfügt über juristische und praktische Erfahrungen im Aufbau und der Führung von Organisationen im Land. Die Schwerpunkte seiner Arbeit liegen im Vertragsrecht, Immobilienrecht und Gesellschaftsrecht.

Elena Duwensee ist russische Juristin mit zwei Masterabschlüssen im internationalen Recht. Bei Herfurth & Partner betreut sie das Dezernat Russland, Ukraine und GUS. Ihr Fachgebiet ist Zivil- und Wirtschaftsrecht. Sie hat mehrere Jahre als Unternehmensjuristin in Russland mit Schwerpunkten im russischen und internationalen Gesellschafts-, Vertrags- und Steuerrecht gearbeitet.

Joachim Gerstein ist Diplom-Ingenieur und Patentanwalt bei Gramm Lins und Partner Patent- und Rechtsanwälte. Er hat langjährige Erfahrung im Patentrecht für Automatisierung und Kommunikationstechnik, der Konfliktlösung bei standardessentiellen Patenten und der Führung internationaler Patentverletzungsprozesse.

Martin Heitmüller ist als Rechtsanwalt und französischer Jurist bei Herfurth & Partner in den Bereichen Zivil- und Handelsrecht tätig. Sein Schwerpunkt liegt im Vertriebsrecht, eCommerce und Wettbewerbsrecht. Er hat mehrere Jahre in Paris als Anwalt gearbeitet betreut das Länderreferat Frankreich.

Antonia Herfurth ist Rechtsreferendarin in München. Sie hat an der Ludwig-Maximilian-Universität (LMU) in München mit dem Schwerpunkt Europarecht studiert und ist als Redakteurin Mitglied des Redaktionsteams von Herfurth & Partner und für die Alliuris Group tätig.

Ulrich Herfurth ist Seniorpartner von Herfurth & Partner und Chairman der internationalen Kanzleigruppe ALLIURIS. Der Schwerpunkt seiner Tätigkeit liegt in der strategischen Rechtsberatung von Unternehmen zu Unternehmensentwicklung, Märkten und Technologie, unter anderem zu Unternehmensnachfolge, M&A, Management und internationalen Transaktionen.

Dennis Jlussi arbeitet als Rechtsanwalt bei Herfurth & Partner im Bereich des IT- und Internetrechts; er verfügt über Erfahrung aus dem Institut für Rechtsinformatik der Universität Hannover, aus juristischer Tätigkeit im Silicon Valley und als Inhouse Counsel einer bekannten deutsch-amerikanischen Social Network Plattform im Wissenschaftsbereich.

Sabine Reimann ist als Rechtsanwältin bei Herfurth & Partner für das Ressort Personal und Arbeit und das Länderdezernat Brasilien und zuständig. Dabei stehen internationaler Personaleinsatz und die Anforderungen an Beschäftigung und Arbeit unter Industrie 4.0 im Vordergrund. Sie verfügt über Erfahrungen aus dem Bildungssektor und im Management und hat mehrere Jahre in Brasilien gelebt und gearbeitet.

Günther Stuff ist als Steuerberater bei Herfurth & Partner verantwortlich tätig, insbesondere im Bereich der nationalen und internationalen Steuergestaltung für Unternehmen. Er verfügt über langjährige Erfahrung als Abteilungsleiter in der internationalen Steuerabteilung der früheren Preussag AG.

Prof. Dr. Christiane Trüe ist Counsel bei Herfurth & Partner und arbeitet in den Bereichen öffentliches Wirtschaftsrecht, Europäisches und nationales Wettbewerbs- und Kartellrecht, Vergaberecht, Umweltrecht, Energierecht und Europarecht. Sie ist als Hochschulprofessorin an der Universität Bremen auf den Bereich des öffentlichen Wirtschaftsrechts konzentriert.

Xiaomei Zhang ist chinesische Juristin mit einem deutschen Magisterabschuss. Bei Herfurth & Partner arbeitet sie im Zivil- und Wirtschaftsrecht und betreut das Dezernat China im Handels- und Gesellschaftsrecht, insbesondere bei Gründungen und Umstrukturierungen von Unternehmen.

Literatur

Baumbach, Adolf/ Hopt, Klaus J., HGB, 36. A.
BGH, GRUR 2004, 495 – Signalfolge.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom), Rechtliche Aspekte von Industrie 4.0, Leitfaden der Bitkom, Stand 01. April 2016

Bräutigam, Peter / Klindt, Thomas, in: Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung, BDI und Noerr, November 2015, S. 14.

Bundesamt für Aussenwirtschaft (BAFA), Technologietransfer und Non-Proliferation, Informationsblatt der BAFA, 2016,
http://www.bafa.de/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_technologietransfer_non_proliferation.pdf

Bundeskartellamt: Arbeitpapier „Marktmacht von Plattformen und Netzwerken“ Bundeskartellamt: 86 – 113/15, Arbeitspapier, Marktmacht von Plattformen und Netzwerken, Juni 2016.

http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Meldungen%20News%20Karussell/2016/09_06_2016_ThinkTank.html.

http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Meldungen%20News%20Karussell/2016/09_06_2016_ThinkTank.html.

Bundesministerium für Wirtschaft und Technologie: Deutschland und China kooperieren bei Standards für Industrie 4.0, BMWi. 09.06.2015

Bundesministerium für Bildung und Forschung: Zukunftsprojekt Industrie 4.0, [https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html]

Bundesregierung: Digitale Agenda 2014-2017, [https://www.digitale-agenda.de/Webs/DA/DE/Home/home_node.html], (zuletzt aufgerufen am: 07.04.2016).

Bundesverfassungsgericht, Beschluss vom 14.03.2006, Az. 1 BvR 2087/03 (www.bundesverfassungsgericht.de).
Cornelius, Kai, Vertragsabschluss durch autonome elektronische Agenten, in: MMR 2002, 353, 355

Deutsch-Russische Auslandshandelskammer, Russland in Zahlen. URL: http://russland.ahk.de/publikationen/russland-in-zahlen/

Dölling, Dieter / Duttge, Gunnar / Rössner, Dieter (Hrsg.): Gesamtes Strafrecht, Handkommentar, Baden-Baden 3. Auflage 2013.

Dorner, Michael, Big Data und „Dateneigentum", CR 2014, 617ff.

Duisberg, Alexander, in: Müller-Tauber, Industrie 4.0 und Recht.

Ehmer, Philipp, Strukturwandel in China, Deutsche Bank Research , 28.01.2011.

Eisele, Jörg: Computer- und Medienstrafrecht, München 2013. Zitiert als: *Eisele*
Engländer, Armin: Examens-Repetitorium Strafprozessrecht, Heidelberg 5. Auflage 2011.

Erling, Jonny: China: EU-Firmen orten Rückfall in Protektionismus, derStandard.at.
Europäisches Amt, Bundeskriminalamt: Cybercrime, Bundeslagebild 2014, [abrufbar unter:
http://www.bka.de/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/internetKriminalitaet__node.html?__nnn=true]

Europäische Kommission: http://ec.europa.eu/germany/news/kartellrecht-geoblocking-laut-sektoruntersuchung-der-eu-weit-verbreitet_de.

Europäisches Parlament: Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 (ABl. L 77/20) über den rechtlichen Schutz von Datenbanken
Europäisches Parlament: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1.

Europäischer Rat, Verordnung (EU) Nr. 833/2014 des Rates vom 31. Juli 2014 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, Abruf am 22.08.2016, Verzeichnis der für allgemeinverbindlich erklärten Tarifverträge Stand: 1. Juli 2016.

Fidor Bank AG (AGB) bezüglich des Angebots der Vermittlung von Bitcoins auf der Plattform www.bitcoin.de Februar 2015), § 6.3,, www.bitcoin.de /de/AGB/Fidor,

Fischer, Thomas: Strafgesetzbuch mit Nebengesetzen, Beck'sche Kurzkommentare, Band 10, München 63. Auflage 2016,

Grünwald, Andreas/Nüßing, **Christoph**, Mashine To Mashine (M2M)-Kommunikation, MMR 2015, 378, 379f.

Germany Trade and Invest (GTAI): IPR-Schutz in China wird zum Wettbewerbsinstrument, 16.02.2015.

Härting, Nico, Internetrecht, 5. Aufl. 2014.

Heintschel-Heinegg, Bernd von (Hrsg.): Beck'scher Online Kommentar StGB, München 30. Edition 2016.

Heng, Stefan / Trenczek, Jan: Industrie 4.0: „China im „ Jahr der Innovation" auf erfolgversprechendem Weg", Deutsche Bank Research, 26.06.2015.

Hilgendorf, Eric; Roboter haften nicht, Interview von Jutta Witte mit Professor Eric Hilgendorf, 15.11.2013, Ausgabe 46.

Hochstrat, Sarah / Wirtz, Markus Antonius / Staufenbiel, Christian: Rechtliche Aspekte von Industrie 4.0, http://winfwiki.wi-fom.de/index.php/Rechtliche_Aspekte_von_Industrie_4.0

Hoeren, **Thomas**, MMR 2013, S. 486.

Hohmann, Harald: Exportrechtliche Grenzen des Technologietransfers, http://www.exportmanager-online.de/2011/ausgabe-4-2011/exportrechtliche-grenzen-des-technologietransfers/

Hornung, Gerrit / Goeble, Thilo, „Data ownership" im vernetzten Automobil , CR 2015, 265ff.

Hötitzsch, Sven, Industrie 4.0 - Rechtliche Perspektiven der Smart-Factory, www.heise.de, Abruf vom 10.11.2015 mit Verweis auf Jochen Hanisch, Zivilrechtliche Haftungskonzepte für Roboter, in: Hilgendorf / Günther, Robotik und Gesetzgebung, Nomos-Verlag 2013, S. 109 ff.

IG Metall, „Mensch mit Maschine", vom 06.01.2015, https://www.igmetall.de/neue-herausforderungen-fuer-den-betrieblichen-gesundheitsschutz-15064.htm

IHK München, Rechtlich smart in die Zukunft in Wirtschaft – Das IHK-Magazin für München und Oberbayern 5/2015, www.muenchen.ihk.de/de/WirueberUns/Publikationen/magazin

Joecks, Wolfgang / Miebach, Klaus (Hrsg.): Münchener Kommentar zum StGB.

Jost Wübbeke, Jost / Conrad, Björn, „Industrie 4.0: Deutsche Technologie für Chinas industrielle Aufholjagd?" Merics China Monitor, Nr. 23/11. März 2015.

Kaessmann, Werner, ADAC-Generalsyndikus, in: 80 für alle? Christof Henn, ADAC Motorwelt 3/2015, S. 42.

Krüger, Angela, DGUV, „Zukunft der Arbeit“, http://www.arbeit-und-gesundheit.de/3/2164

Lober, Andreas u.a. „Industrie 4.0 und Arbeitnehmerdatenschutz“, in Personalwirtschaft, Sonderheft 10/2015, S. 19, www.personalwirtschaft.de

Mansdörfer, Marco: Industrie 4.0 und die Gefahren durch Cybercrime, [https://www.youtube.com/watch?v=S-j5BDz24KI&feature=youtu.be], (zuletzt aufgerufen am: 15.04.2016).

Matzat, Lorenz: Kommentar: Zur Zukunft der Arbeit hat die Digitale Agenda nichts zu sagen, Berlin 25.08.2014, [https://netzpolitik.org/2014/kommentar-zur-zukunft-der-arbeit-hat-die-digitale-agenda-nichts-zu-sagen/], (zuletzt aufgerufen am: 15.04.2016).
Memorandum der Plattform Industrie 4.0, S. 11, http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/memorandung-industrie-4-0,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, Abruf am 23.11.2015
Näheres zum Thema *Datenschutz und Industrie 4.0* im entsprechenden Beitrag des Autors.

Rayermann, Marcus / Zimmer, Mathias, Rechtliche Grundlagen des M-Commerce, in Gora / Röttger-Gerick, Handbuch Mobile Commerce, S. 112.

Scharen in Benkard, Patentgesetz, 11. Aufl. 2015, § 9 Rn. 31.

Schüller, Margot, / Schüler-Zhou, Yun: „Chinas Industrie vom Aufholen zum Überleben, Der Tagesspiegel, 16.03.2015.

Spath, Dieter u.a. Studie „Produktionsarbeit der Zukunft – Industrie 4.0“, Frauenhofer-Institut für Arbeitswirtschaft und Organisation IAO, S. 43, S.71.

Spickhoff, Andreas (Hrsg.): Medizinrecht, Beck’sche Kurzkommentare, Band 64, München 2. Auflage 2014.

Spindler, Gerald, Rechtsprobleme Industrie 4.0 – Einführung und Überblick vom 15. April 2016.

Steiner, Falk: Kommentar zur Digitalen Agenda: Leere Phrasen statt politischer Entscheidungen, Berlin 20.08.2014, [http://www.heise.de/newsticker/meldung/Kommentar-zur-Digitalen-Agenda-Leere-Phrasen-statt-politischer-Entscheidungen-2297601.html], (zuletzt aufgerufen am: 15.04.2016)

Tuleweit, Sören, „Folgen für die Arbeitsorganisation“, IG BCE, vom 23.10.2015, https://www.igbce.de/aib-arbeitsrecht-im-betrieb-digitalisierung/116344?highlightTerms=industrie,4.0&back=#

Velten, Jens, „Übersicht über den Persönlichkeitsschutz im digitalen Umfeld in Brasilien und in Deutschland“ in DBVJ-Mitteilungen 2/ 2015,

Vocke, Jörg, in: Müller-Tauber, Industrie 4.0 und Recht – Rechtlich smart in die Zukunft in Wirtschaft – Das IHK-Magazin für München und Oberbayern 5/2015, www.muenchen.ihk.de/de/WirueberUns/Publikationen/magazin

Verein Deutscher Ingenieure (VDI): www.vdi-nachrichten.com/Technik-Wirtschaft/Roboter-haften nicht

Wang, Rong: Discussion on the core question of the data ownership in big data trade, Big Data Reserch, 2015018.

Zapf, Ines, in IAB Forschungsbericht 03/2012, Flexibilität am Arbeitsmarkt durch Überstunden und Arbeitszeitkonten

+++