PLATTFORM INDUSTRIE 4.0
WISSENSCHAFTLICHER BEIRAT

Industrie 4.0 und das Recht: Drei zentrale Herausforderungen

Prof. Dr. Gerrit Hornung, LL.M. / Kai Hofmann, Universität Kassel

Impressum

Herausgeber
acatech – Deutsche Akademie
der Technikwissenschaften
Geschäftsstelle
Karolinenplatz 4
80333 München

Gestaltung und Produktion
PRpetuum GmbH, München

Bildnachweis
chombosan – iStock (Titel),
PhonlamaiPhoto – iStock (S. 2),
vschlichting – Fotolia (S. 4),
science photo – Fotolia (S. 10),
zapp2photo – Fotolia (S. 16)

Stand
April 2017

Druck
omb2 Print GmbH, München

Plattform Industrie 4.0

acatech – Deutsche Akademie
der Technikwissenschaften

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

Inhalt

1 Industrie 4.0: Innovationsschub und Rechtsfragen ... 2
1.1 CPS als soziotechnische Innovation der Fabrik der Zukunft ... 2
1.2 Neue rechtliche Herausforderungen ... 3
1.3 Rechtliche Handlungsempfehlungen ... 3

2 Datengetriebene Geschäftsmodelle – Datenhoheit ... 4
2.1 Anwendungen und Interessen ... 4
2.2 Daten als Schutzgegenstand ... 5
2.3 Datenhoheit nach bestehendem Recht ... 5
2.3.1 Verfügbarkeit und Zugang ... 6
2.3.2 Integrität ... 6
2.3.3 Vertraulichkeit ... 6
2.3.4 Verwertung ... 7
2.4 Änderung des Rechtsrahmens ... 8

3 M2M-Kommunikation – Neujustierung der Verantwortlichkeit ... 10
3.1 Anwendungen und Interessen ... 10
3.2 Intelligentes Handeln – Schäden innerhalb der Wertschöpfungskette ... 11
3.2.1 Verschuldenshaftung ... 11
3.2.2 Rechtsgeschäftliches Handeln ... 12
3.2.3 Möglichkeiten der Haftungsbegrenzung ... 13
3.2.3.1 Grenzen der vertraglichen Gestaltung ... 13
3.2.3.2 Eigenständige Haftung als elektronische Person? ... 13
3.3 Verteiltes Handeln – Beweis und Zurechnungsprobleme ... 14
3.4 Schäden durch ein in der Industrie 4.0 gefertigtes Produkt ... 15

4 Wertschöpfungsnetzwerke – Rechtliche Grenzen der Vernetzung ... 16
4.1 Arbeit in der „Smart Factory“ ... 16
4.1.1 Beschäftigtendatenschutz ... 16
4.1.1.1 Gezielter Personenbezug – Assistenzsysteme ... 17
4.1.1.2 Ungezielter Personenbezug – Maschinendaten ... 17
4.1.2 Neue flexible Organisationsformen ... 18
4.2 Zentrale und dezentrale Akteure – Plattformregulierung ... 18
4.2.1 Anwendung und Interessen ... 19
4.2.2 Wettbewerbsrechtliche Beschränkungen ... 19
4.2.3 Haftung des Plattformbetreibers ... 19

1 Industrie 4.0: Innovationsschub und Rechtsfragen

Die rasant fortschreitende Digitalisierung von Wirtschaft und Gesellschaft verändert die Art und Weise, wie in Deutschland produziert und gearbeitet wird. Industrie 4.0-Lösungen verzahnen die Produktion mit modernster Informations- und Kommunikationstechnik und schaffen „intelligente" Wertschöpfungsketten. Dies wird bestehende Geschäftsmodelle verändern, etablierte Marktstrukturen verschieben und hergebrachte unternehmensinterne Abläufe in Frage stellen.

1.1 CPS als soziotechnische Innovation der Fabrik der Zukunft

Der disruptive Wandel, der die vierte Stufe der Industrialisierung einläutet, basiert vor allem auf der Veränderung bisheriger Muster der Automatisierung. Statt auf einer zentral gesteuerten, im Vorhinein festgelegten und optimierten Abfolge von Schritten basieren neue Automatisierungskonzepte auf der laufenden Selbstoptimierung zunehmend dezentral gesteuerter Abläufe.[1] Der Schlüssel hierzu liegt in einer möglichst durchgängigen Informationsverarbeitung, durch die neue sowie bestehende, bislang aber getrennte Informationsquellen miteinander verbunden werden.[2] Technisch soll dies durch den Einsatz von Cyber-Physical Systems (CPS) gewährleistet werden.[3] Auf diese Weise ausgerüstete Produktionsressourcen (Produktionsmaschinen, Roboter, Förder- und Lagersysteme, Betriebsmittel) verfügen zusätzlich zu ihren primären Eigenschaften über die Fähigkeit, Daten zu erfassen, zu verarbeiten und untereinander, mit den Planungs- und Steuerungssystemen oder in der Interaktion mit dem Menschen auszutauschen.[4]

1 *Hirsch-Kreinsen*, AP-SOZ 38/2014, S. 6; *ten Hompel/Kerner*, Informatik-Spektrum 2015, S. 176 ff.; *Spath* (Hrsg.)/*Ganschar/Gerlach/Hämmerle/Krause/Schlund*, Produktionsarbeit der Zukunft, 2013, S. 95 ff.

2 *Schlick/Stephan/Loskyll/Lappe*, in: Bauernhansl/ten Hompel/Vogel-Heuser, Industrie 4.0 in Produktion, Automatisierung und Logistik, 2014, S. 57, 59.

3 *Hirsch-Kreinsen*, AP-SOZ 38/2014, S. 7.

4 *acatech/Forschungsunion*, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, S. 24, https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf; *Bauernhansl*, in: Bauernhansl, et al. (Fn. 2), S. 15 ff.

Ziel der Industrie 4.0 ist es, den Grad der Automatisierung insgesamt zu steigern und die Produktion dadurch flexibler, individueller, störungsunempfindlicher und ressourceneffizienter zu machen. Die Unternehmen sollen in der Lage sein, ihre Produktion schneller den sich wandelnden Anforderungen des Absatzmarktes anzupassen und insbesondere auch speziellen Kundenwünschen in geringen Losgrößen bis hin zur Einzelanfertigung rentabel entsprechen zu können. Die umfassende Verfügbarkeit von Informationen soll die Entscheidungsfindung in der Planung und der Produktion erleichtern und der dezentrale Steuerungsansatz soll es erlauben, die zunehmende Komplexität[5] der Produkte und Prozesse zu bewältigen.[6] Insgesamt soll die Industrie 4.0 so Unternehmen in die Lage versetzen, sich weiterhin unter den verschärften Bedingungen des Wettbewerbs behaupten zu können.

1.2 Neue rechtliche Herausforderungen

Der Wandel zur Industrie 4.0 wirft eine Fülle von Rechtsfragen auf. Während viele dieser Fragen an die rechtlichen Probleme früherer soziotechnischer Innovationen anschließen, sind andere grundlegender Natur, weil sie an Paradigmenwechsel im Wirtschaftssystem anknüpfen, die mit der Industrie 4.0 einhergehen.

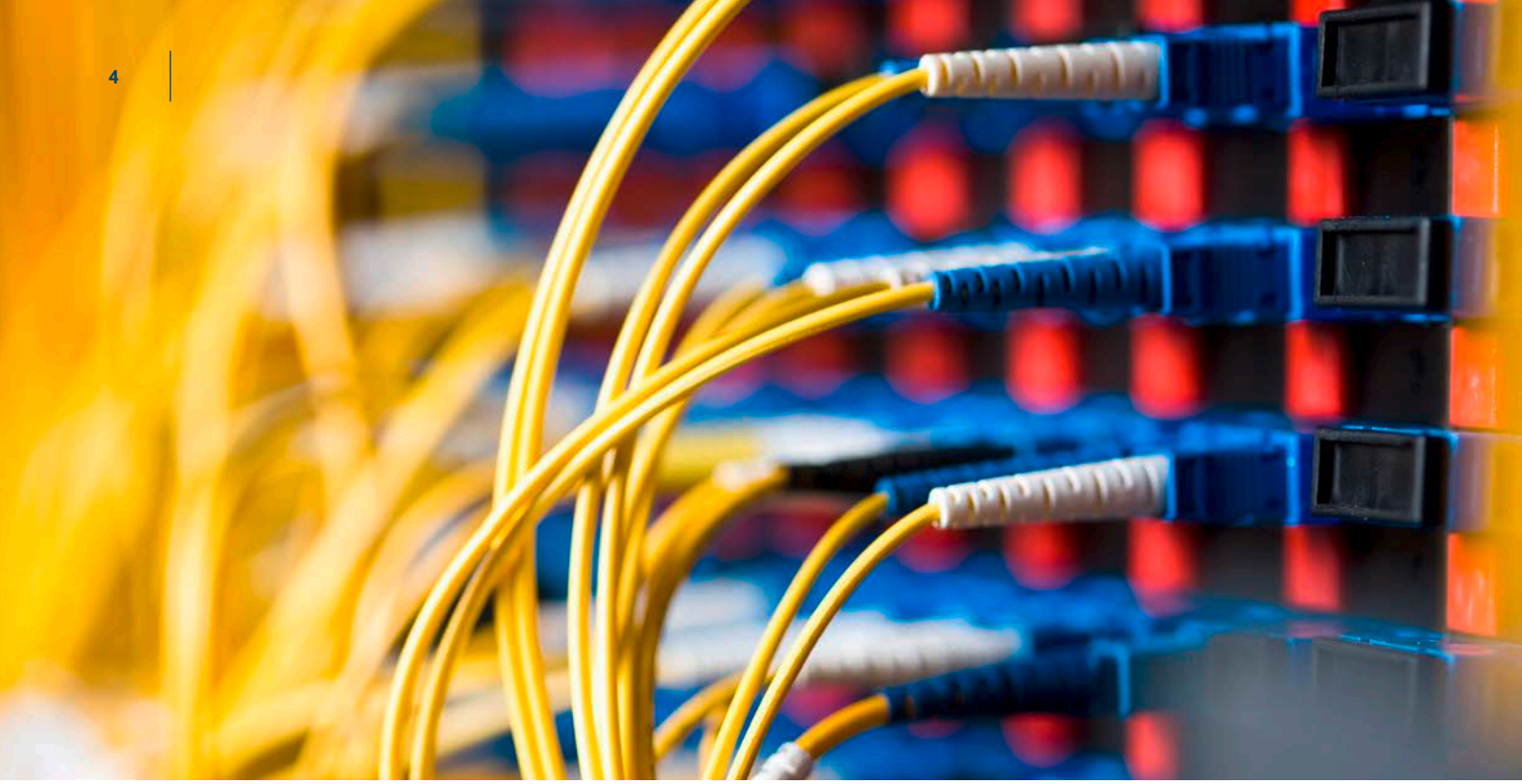
Dementsprechend fokussiert dieser Text auf drei fundamental neue Charakteristika der produzierenden Industrie der Zukunft: datengetriebene Wirtschaft, M2M-Kommunikation, Wertschöpfungsnetzwerke. So heterogen nämlich die aufgeworfenen Rechtsprobleme wirken, beruhen sie doch überwiegend auf einigen für die Industrie 4.0 spezifischen Phänomenen, die zu ähnlichen Fragestellungen in den jeweiligen Bereichen des Rechts führen. Die juristische Diskussion soll darum anhand dieser Phänomene strukturiert werden.

1.3 Rechtliche Handlungsempfehlungen

Eine solche Strukturierung erscheint besonders geeignet, um die Rechtsfragen nicht nur zu erfassen und wissenschaftlich zu durchdringen, sondern sie auch in Handlungsempfehlungen für die Politik und die betriebliche Praxis zu überführen. Dabei geht es nicht nur um den rechtskonformen Betrieb der jeweiligen Industrie 4.0-Lösungen. Die Handlungsempfehlungen sollen auch darauf gerichtet sein, die notwendigen Voraussetzungen für die Akzeptanz bei kleinen und mittleren Unternehmen sowie den betroffenen Beschäftigten zu schaffen, ohne die die Industrie 4.0 insgesamt keinen Erfolg haben kann. Ziel der folgenden Ausführungen ist es, diesen Prozess durch eine Zusammenfassung der einschlägigen wissenschaftlichen Diskussion anzustoßen und zu erleichtern.

5 *ten Hompel/Kerner*, Informatik-Spektrum 2015, S. 176 f.

6 Zu den Zielen insgesamt *acatech/Forschungsunion* (Fn. 4), S. 19 f.; *Hirsch-Kreinsen*, AP-SOZ 38/2014, S. 6.



2 Datengetriebene Geschäftsmodelle – Datenhoheit

2.1 Anwendungen und Interessen

Der Einsatz von CPS ermöglicht es, die damit realisierten Prozesse durchgehend und in Echtzeit transparent zu gestalten. In dem Maße, wie Ereignisse, Lasten und Zustände erfasst werden, entsteht bei entsprechender Analyse und Auswertung dieser Daten ein permanent aktuelles virtuelles Abbild der Fabrik und der darin ablaufenden Prozesse.[7] Dies bildet die Grundlage für eine Reihe neuer, datengetriebener Anwendungen, die helfen können, die Entwicklung, Produktion und Logistik zu optimieren.

Ein Beispiel hierfür ist die zustandsbasierte Wartung, die anstatt nach festen Intervallen anhand der tatsächlichen, aus den Daten abgeleiteten Wartungsbedürftigkeit durchgeführt wird. Hierdurch lassen sich die Ausfallzeiten der Maschine bei sinkenden Wartungskosten minimieren.[8] Neben diesem Mehrwert für den Betreiber der Maschine ließen sich den Daten aber womöglich auch Informationen entnehmen, die der Hersteller zur Produktentwicklung, zur Marktbeobachtung oder zur Einschätzung von Gewährleistungsansprüchen nutzen könnte.[9] Da solche Auswertungen umso aussagekräftiger geraten, je betreiber- und herstellerübergreifender sie angelegt sind,[10] könnten sie auch von einem externen Dienstleister durchgeführt werden.

Der intensive Datenaustausch birgt für die Beteiligten aber nicht nur Chancen, sondern auch Risiken. Dies betrifft zum einen die durch autonome Systeme gesteuerte Produktion und Logistik selbst. Je stärker sie auf den nahtlosen Datenaustausch von Maschine zu Maschine setzt, desto anfälliger wird sie auch für die Störung oder Manipulation dieser Daten. Darüber hinaus können Maschinendaten einen ungewollt tiefen Einblick in Unternehmensinterna wie Konstruktionsdetails oder angewandte Produktionsmethoden[11] sowie die Auftragslage oder erzielte Absätze geben.[12]

7 *Bauernhansl* (Fn. 4), S. 16.

8 *acatech/Forschungsunion* (Fn. 4); *Bosch Rexroth AG,* Das Fitness-Programm für Ihre Maschine – Remote-Condition-Monitoring, http://www.boschrexroth.com/various/utilities/mediadirectory/download/index.jsp?object_nr=R911336114; *Schöning/Dorchain*, in: Bauernhansl, et al. (Fn. 2), S. 545.

9 *Ensthaler*, NJW 2016, S. 3473, 3474; *Roßnagel*, NJW 2017, S. 10; *Schwartmann/Hentsch,* PinG 2016, S. 117, 118.

10 *Roßnagel*, NJW 2017, S. 10.

11 *Peschel/Rockstroh*, MMR 2014, S. 571, 574.

12 So ähnlich das Beispiel in *EU-Kommission*, Commission staff working document on the free flow of data and emerging issues of the European data economy, COM(2017) 9 final, S. 27.

Durch die datengetriebenen Anwendungen könnte ein Daten- und Informationsmarkt entstehen, auf dem z. B. der Maschinenbetreiber die Daten einem Dienstleister bereitstellt, der diese analysiert und die so gewonnenen Informationen wiederum dem Betreiber (z. B. Ausfallprognosen), möglicherweise aber auch dem Hersteller (z. B. häufige Fehlerquellen) oder anderen Dritten anbietet.[13] Diese Austauschbeziehungen werden überwiegend über Verträge gestaltet sein. Der Wert der ihnen zugrundeliegenden Daten bestimmt sich dabei aber nicht nur nach deren Optimierungs- und Risikopotential. Entscheidend wird auch sein, inwiefern die sich hieraus ergebenden Interessen gesetzlich geschützt sind.[14] Diese sind: die Verfügbarkeit und der Zugang (2.3.1), die Integrität (2.3.2), die Vertraulichkeit (2.3.3) und die Verwertung (2.3.4) der bzw. zu den Daten.

2.2 Daten als Schutzgegenstand

Wenn von Daten als Schutzgegenstand die Rede ist, muss zunächst der Begriff geschärft werden.[15] Daten betreffen die Zeichenebene; diese ist nach „oben" von der Bedeutungsebene (Informationen) und nach unten von der Stoffebene (Datenträger) zu unterscheiden.

Für den Schutz von Daten kommen mit dem Sacheigentum (bzw. einem hieraus abgeleiteten „Dateneigentum") und dem geistigen Eigentum zwei Konzepte in Betracht, die grundverschiedene Schutzrichtungen verfolgen.[16] Maßgeblich ist die Unterscheidung zwischen den rivalen und nicht-rivalen Nutzungen des Schutzgegenstands. Körperliche Gegenstände können nur rival genutzt werden, d. h. so, dass jede Nutzung durch den einen die potentielle Nutzbarkeit der Sache für den anderen einschränkt. Um die Übernutzung zu vermeiden, weist das Sacheigentum dem oder den Inhaber(n) diese rivalen Nutzungen exklusiv zu. Die Nutzung immaterieller Güter ist nicht mit solchen Beeinträchtigungen verbunden; sie ist nicht-rival. Statt um Übernutzung geht es beim geistigen Eigentum darum, ausschließlich dem oder den Berechtigten die Früchte seiner bzw. ihrer Arbeit zu gönnen.[17]

Daten sind sowohl rivaler als auch nicht-rivaler Nutzung zugänglich.[18] Sie können einerseits leicht vervielfältigt und so einer Vielzahl von Nutzern zugänglich gemacht werden. Die dadurch mögliche ungestörte Parallelnutzung ist nicht-rival.[19] Die umfassende Verwertung, insbesondere die Nutzung von Kopien und die Analyse von Daten wäre damit dem geistigen Eigentum zuzuordnen. Andererseits könnten Daten in ihrer Fixierung auf einen Datenträger aber auch in ihrer Integrität und Verfügbarkeit betroffen sein,[20] indem sie etwa gelöscht, geändert oder unzugänglich gemacht werden. Ein am Sacheigentum angelehntes „Dateneigentum" würde dem Inhaber nur solche rivalen Nutzungen zuweisen.[21]

2.3 Datenhoheit nach bestehendem Recht

Die Diskussion um die Datenhoheit hat aufgezeigt, dass sich Daten durch die anerkannten gesetzlichen Instrumente nur lückenhaft schützen lassen. Das liegt in erster Linie daran, dass „rohe" Maschinendaten außerhalb der Schutzbereiche der bestehenden Immaterialgüterrechte liegen und insofern gemeinfrei sind.[22]

Da Maschinendaten zudem üblicherweise keinen Personenbezug aufweisen, findet auch der Datenschutz keine Anwendung. Die dortige Paralleldiskussion zum „Dateneigentum"[23] spielt für die Industrie 4.0 darum nur eine

13 *Roßnagel/Jandt/Marschall*, in: Vogel-Heuser/Bauernhansl/ten Hompel, Handbuch Industrie 4.0, 2016, S. 1, 23.

14 *Ensthaler*, NJW 2016, S. 3473, 3474.

15 So *Grützmacher*, CR 2016, S. 485, 486; *Zech*, CR 2015, S. 137, 138; ähnlich *Hoeren/Völkel*, in: Hoeren, Big Data und Recht, 2014, S. 11, 12; *Specht*, CR 2016, S. 288, 290; *Wiebe*, GRUR Int 2016, S. 877, 881 f.

16 Siehe dazu *Berberich/Golla*, PinG 2016, S. 165, 168 f.

17 Zum Ganzen *Berberich/Golla*, PinG 2016, S. 165, 168 f.

18 *Berberich/Golla*, PinG 2016, S. 165, 169; in Beiträgen, die sich hauptsächlich mit Verwertungsrechten befassen, wird dagegen der nicht-rivale Charakter betont, *Kerber*, GRUR Int 2016, S. 989, 992 f.; *Zech*, CR 2015, S. 137, 139.

19 *Zech*, CR 2015, S. 137, 139.

20 *Härting*, CR 2016, S. 646, 647.

21 *Berberich/Golla*, PinG 2016, S. 165, 169; *Härting*, CR 2016, S. 646, 647.

22 *Dorner*, CR 2014, S. 617, 622; *Ensthaler*, NJW 2016, S. 3473 f.; für einen urheberrechtlichen Schutz fehlt es Maschinendaten zudem am notwendigen menschlichen Einfluss bei ihrer Entstehung, *Wiebe*, GRUR Int 2016, S. 877, 879; *Zech,* CR 2015, S. 137, 141.

23 Dazu z. B. *Hornung/Goeble*, CR 2015, S. 265 ff.; *Schwartmann/Hentsch*, RDV 2015, S. 221 ff.; *Specht/Rohmer*, PinG 2016, S. 127 ff..

untergeordnete Rolle. Angesichts seiner persönlichkeitsrechtlichen Fundierung könnte es ein wirtschaftlich ausgerichtetes Recht an Daten aber ohnehin nur begrenzen und nicht begründen.[24]

Nichtsdestotrotz genießen Daten in wesentlichen Punkten gesetzlichen Schutz. Dieser gliedert sich wie folgt.

2.3.1 Verfügbarkeit und Zugang

Aus Sicht des Maschinenbetreibers sind vor allem solche Systemgestaltungen problematisch, in denen die Daten ausschließlich extern gespeichert und/oder ausgewertet werden. Will er sie selbst oder von einem anderen Dienstleister analysieren lassen, muss er die Daten vom alten Dienstleister herausverlangen können.

Hierzu könnte nach dem Vorbild des strafrechtlichen Schutzes von Daten, insbesondere von § 303a StGB, ein „Dateneigentum" analog zu § 903 BGB konstruiert,[25] und der Herausgabeanspruch auf § 985 analog gestützt werden.[26] Dieses „Dateneigentum" soll demjenigen zustehen, der den sog. Skripturakt vornimmt, d.h. die Speicherung der Daten unmittelbar bewirkt.[27] Wie dies genau zu bestimmen ist, ist umstritten.[28] Da aber jedenfalls ein weisungsfrei agierender Dienstleister selbst „Skribent" wäre, dürfte das „Dateneigentum" nur eine untergeordnete Rolle spielen.

Ein anderer Ansatz besteht darin, Daten als Nutzungen (§ 100 BGB) einer Maschine einzustufen und sie deren Eigentümer oder berechtigtem Besitzer zuzuweisen.[29] Dies bezöge sich aber nur auf die Nutzung des Messgeräts[30] und die dabei erzeugten Daten – nicht aber auf deren Kopie bei einem externen Dienstleister.[31]

Eine allgemeine Pflicht des Dienstleisters oder Herstellers, anderen Dienstleistern Daten zugänglich zu machen oder Schnittstellen offenzulegen, ist im geltenden Recht nicht verankert. Ein kartellrechtlicher Ansatz wird aufgrund der sehr engen Voraussetzungen als untauglich bewertet.[32]

2.3.2 Integrität

Verfälschte oder unbrauchbare Daten gefährden die Qualität der hierauf beruhenden Anwendungen. Ein umfassender deliktischer Schutz hiergegen ist jedoch bisher nur für den Eigentümer oder berechtigten Besitzer des gleichsam betroffenen Datenträgers anerkannt. Die Daten selbst sind lediglich strafrechtlich (§§ 303a ff. StGB) sowie zivilrechtlich als Teil des Gewerbebetriebs und darum nur gegen gezielte Eingriffe geschützt. Eine im Vordringen begriffene Meinung will darum ein Recht am Datenbestand als sonstiges Recht nach § 823 Abs. 1 BGB anerkennen, das auch gegen fahrlässige Schädigungen schützen würde.[33]

2.3.3 Vertraulichkeit

Vor allem Maschinenhersteller und -betreiber werden den Abfluss von Know-how verhindern wollen. Dabei geht es nicht um die – dem Dienstleister freiwillig übermittelten –

24 *Berberich/Golla*, PinG 2016, S. 165, 167; *Grützmacher*, CR 2016, S. 485, 486; *Specht/Rohmer*, PinG 2016, S. 127, 131 f.

25 *Hoeren*, MMR 2013, S. 486 ff.; *Hoeren/Völkel* (Fn. 15); *Zech*, GRUR 2015, S. 1151, 1159; ablehnend *Berberich/Golla*, PinG 2016, S. 165, 171 f.; *Dorner*, CR 2014, S. 617, 626; *Ehlen/Brandt*, CR 2016, S. 570, 571; *Härting*, CR 2016, S. 646, 649; *Heun/Assion*, CR 2015, S. 812, 814; *Kraus*, in: Taeger, Big Data & Co, 2014, S. 377, 381; *Wiebe*, GRUR Int 2016, S. 877, 881.

26 *Hoeren*, MMR 2013, S. 486, 490; *Hoeren/Völkel* (Fn. 15), S. 35 f.

27 *Hoeren*, MMR 2013, S. 486, 487.

28 Für die Zuordnung zum Arbeit-/Auftragnehmer: OLG Nürnberg v. 23.01.2013 – 1 Ws 445/12, ZD 2013, S. 282, 283; *Hoeren*, MMR 2013, S. 486, 487; *Hoeren/Völkel* (Fn. 15), S. 36; für den Arbeit-/Auftragnehmer: *Popp*, juris PR-ITR 7/2013, Anm. 3; *Zech*, GRUR 2015, S. 1151, 1159.

29 *Assion*, CR 2015, S. 84, 85; *Heun/Assion*, CR 2015, S. 812, 818; *Heymann*, CR 2016, S. 650, 651. Für die Einordnung als Rechtsfrüchte i.S.v. § 99 Abs. 3 BGB, *Grosskopf*, IPRB 2011, S. 259, 260; allg. BGH v. 17.12.2010 – V ZR 45/10, GRUR 2011, S. 323, 324 f.; BGH v. 1.3.2013 – V ZR 14/12, GRUR 2013, S. 623, 624 f.

30 *Zech*, CR 2015, S. 137, 142; so wohl auch *Härting*, CR 2016, S. 646, 647; *Heun/Assion*, CR 2015, S. 812, 818; a.A. wohl *Specht*, CR 2016, S. 288, 292.

31 I.E. *Härting*, CR 2016, S. 646, 647; vgl. zum Eigentumserwerb nach § 950 BGB analog durch Speicherung *Hoeren*, MMR 2013, S. 486, 490.

32 *Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblytė/Wiedemann*, Ausschließlichkeits- und Zugangsrechte an Daten, S. 11 ff., http://hdl.handle.net/11858/00-001M-0000-002B-42CF-4; *Surblytė*, Data as a Digital Resource, S. 25 ff., http://ssrn.com/abstract=2849303.

33 *Bartsch*, in: Conrad/Grützmacher, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 297, 301 f.; *Berberich/Golla*, PinG 2016, S. 165, 170 ff.; *Faust,* Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, 2016, S. 72 ff.; *Grützmacher,* CR 2016, S. 485, 489 f.; *Meier/Wehlau*, NJW 1998, S. 1585, 1588 f.; *Spindler*, JZ 2016, S. 805, 812 ff.

Daten selbst; ihr Schutz stellt keine neue Herausforderung dar. Entscheidend ist vielmehr die Vertraulichkeit der in den Analyseergebnissen enthaltenen Informationen.

Die Vertraulichkeit von Daten wird in erster Linie[34] durch den Schutz von Betriebs- und Geschäftsgeheimnissen nach § 17 UWG sichergestellt, unter den angesichts ihres Werts für datengetriebene Anwendungen grundsätzlich auch Maschinendaten fallen können.[35] Der Geheimnisschutz soll primär die direkte Offenbarung von Informationen verhindern und läuft darum bei gezieltem Datenaustausch leer. Es ist aber gemäß § 17 Abs. 2 Nr. 2 UWG ebenfalls verboten, Informationen zu verwerten, die man sich sonst unbefugt verschafft hat. Besteht eine ausdrückliche Nutzungsvereinbarung über die geheimen Daten, ist auch die davon abweichende Analyse als unbefugtes Sichverschaffen einzustufen.[36] Eine ähnliche Regelung findet sich auch in Art. 4 Abs. 2 RL 2016/943/EU.

Berechtigt ist jedoch nur derjenige, der die Geheimhaltung der Daten – faktisch oder vertraglich vermittelt[37] – kontrolliert;[38] über wen die Daten Informationen enthalten, spielt keine Rolle.[39] Wo die Kontrolle der Daten nicht aufrechterhalten werden kann, weil etwa der Maschinenbetreiber dem -hersteller nicht auf Augenhöhe begegnen kann, bietet der gesetzliche Geheimnisschutz keine Hilfe.[40] Mehr noch: Gelingt es dem Hersteller einer Maschine, die von ihr erzeugten Daten vor dem Betreiber geheim zu halten, sind sie ihm, dem Hersteller, zugeordnet.[41]

2.3.4 Verwertung

Die eigentliche „Veredelung" der Daten zu werthaltigen Informationen findet bei dem auf die Analyse spezialisierten Akteur statt. Üblicherweise wird das ein Dienstleister oder der Hersteller selbst sein. Die Parteien, die diesen letzten Akt nicht kontrollieren können, haben darum ein Interesse, an der Verwertung wirtschaftlich beteiligt zu werden.

Dies kann teilweise über den skizzierten Geheimnisschutz erreicht werden. Eine entsprechende Nutzungsvereinbarung vorausgesetzt, kann derjenige, der die Daten für die Analyse bereitstellt, die Verwertung des Analyseergebnisses ganz oder teilweise verbieten. Diese Kombination aus tatsächlicher Exklusivität und vertraglichen Regelungen ist bisher die Grundlage für den Handel mit Daten,[42] ohne aber eine eigenständige Zuweisung zu bewirken.[43]

Eine davon unabhängige Verwertungsmöglichkeit bietet das Leistungsschutzrecht an Datenbanken nach §§ 87a ff. UrhG. Danach hat der Datenbankhersteller das alleinige Recht, die Datenbank[44] – gemeint ist der Inhalt, nicht die u. U. schöpferische Struktur – zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Diese Nutzungshandlungen müssen jedoch – auf einmal oder sukzessive – mindestens wesentliche Teile der Datenbank betreffen. Die einfache Datenbankabfrage bleibt darum frei; einzelne Daten sind für sich genommen schutzlos. Die Analyse des Datenbestands fällt darum nur in den Schutz der Datenbank, wenn die damit verbundene Speicherung der Daten diese Wesentlichkeitsschwelle überschreitet. Das dürfte regelmäßig nicht der Fall sein.[45]

34 Zum Vertraulichkeitsschutz über § 823 Abs. 1 BGB und dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (BVerfGE 120, S. 274) s. *Faust* (Fn. 33), S. 74 f.; *Spindler*, JZ 2016, S. 805, 813. Es ist fraglich, inwiefern dieses persönlichkeitsrechtlich geprägte Grundrecht auf Unternehmen übertragen werden kann, s. *Hofmann,* JurPC Web-Dok. 158/2015, Rn. 18 ff.

35 *Zech,* GRUR 2015, S. 1151, 1156; i.E. *Roßnagel,* NJW 2017, S. 10, 12; *Specht*, CR 2016, S. 288, 291; dazu skeptisch *EU-Kommission* (Fn. 12), S. 20.

36 *Peschel/Rockstroh,* MMR 2014, S. 571, 574, denen zufolge eine solche Nutzungsvereinbarung nicht aus stets bestehenden vertraglichen Nebenpflichten zur Geheimhaltung entnommen werden kann. Zustimmend *Roßnagel,* et al. (Fn. 13), S. 7; *Roßnagel*, NJW 2017, S. 10, 12. Ein stillschweigendes Verwertungsverbot lehnt auch *Żdanowiecki,* in: Bräutigam/Klindt, Digitalisierte Wirtschaft/Industrie 4.0, 2015, S. 19, 23, ab.

37 *Dorner*, CR 2014, S. 617, 623; i.E. auch *Peschel/Rockstroh,* MMR 2014, S. 571, 574.

38 *Wiebe,* GRUR Int 2016, S. 877, 880; *Zech*, GRUR 2015, S. 1151, 1155, unter Verweis auf Art. 39 Abs. 2 TRIPS. In Art. 2 Nr. 2 der Geschäftsgeheimnis-RL 2016/943/EU wurde dieses Kriterium übernommen. Für weitere Kriterien dagegen wohl *Dorner,* CR 2014, S. 617, 623.

39 *Hofmann,* JurPC Web-Dok. 158/2015, Rn. 40; *Zech,* GRUR 2015, S. 1151, 1155; a.A. *Dorner*, CR 2014, S. 617, 623.

40 Zum Ganzen *Zech*, GRUR 2015, S. 1151, 1156.

41 *Zech,* GRUR 2015, S. 1151, 1155.

42 *Drexl*, et al. (Fn. 32), Rn. 7; *Heun/Assion,* CR 2015, S. 812, 814; *Specht*, CR 2016, S. 288, 289 f.

43 *Dorner,* CR 2014, S. 617, 623; *Grützmacher,* CR 2016, S. 485, 489; *Zech*, GRUR 2015, S. 1151, 1155.

44 Zu den niedrigen Voraussetzungen für deren Schutz *Ensthaler*, NJW 2016, S. 3473, 3474 f.; *Wiebe,* GRUR Int 2016, S. 877, 879.

45 *Ehlen/Brandt*, CR 2016, S. 570, 573; *Spindler,* GRUR 2016, S. 1112, 1114; *Triaille*, Study on the legal framework of text and data mining (TDM), S. 79, http://ec.europa.eu/internal_market/copyright/docs/studies/1403_study2_en.pdf; *Zieger/Smirra*, MMR 2013, S. 418, 420.

Hinzu kommt, dass das Leistungsschutzrecht demjenigen zusteht, der die wesentliche Investition in die Beschaffung, Überprüfung und Darstellung der Daten tätigt; das Erzeugen der Daten bleibt unberücksichtigt.[46] Berechtigter ist darum allein derjenige, der das wirtschaftliche Risiko für den Betrieb der Datenbank trägt[47] – in der Regel also der Analyse-Dienstleister.[48] Hersteller und Betreiber der Maschine bleiben außen vor.

Ob ein Verwertungsrecht durch richterliche Rechtsfortbildung geschaffen werden könnte, ist umstritten.[49] Zumindest für ein absolutes Recht wird dies einhellig verneint.[50] Entsprechend bewirken weder das „Dateneigentum"[51] noch die Einordnung als Nutzungen (§ 100 BGB)[52] oder die Anerkennung eines sonstigen Rechts am Datenbestand (§ 823 Abs. 1 BGB)[53] eine Zuweisung der nicht-rivalen Nutzungen wie der Vervielfältigung oder der Analyse.

2.4 Änderung des Rechtsrahmens

Um den Herausforderungen einer digitalisierten Wirtschaft gerecht zu werden, erwägen sowohl der europäische als auch der deutsche Gesetzgeber den gegenwärtigen Rechtsrahmen – auch, aber nicht nur im Hinblick auf die Datenhoheit – zu ändern.[54] Im Mittelpunkt der Diskussion steht dabei die Schaffung eines neuen Ausschließlichkeitsrechts an Daten. Hierzu schlägt Zech vor, dem wirtschaftlich verantwortlichen Datenerzeuger ein auf nur wenige Jahre beschränktes Leistungsschutzrecht an Messdaten zu gewähren, dem zufolge er allein diese Daten gewerblich verwerten dürfte.[55] Im Gegenzug hierfür könnten Zugangsrechte für den Maschinenhersteller, Behörden oder die Wissenschaft festgeschrieben werden.[56]

In der Literatur wird die Einführung eines solchen Rechts überwiegend abgelehnt; es erreiche keines der mit seiner Schaffung verfolgten Ziele:[57]

- Codierungsanreiz[58]: Daten seien technisch leicht zu erzeugen, ein bisher fehlender Anreiz darum nicht erkennbar.

- Datenmarkt[59]: Daten würden bereits auf Basis ihrer faktischen Exklusivität gehandelt. Ein Recht an Daten könne den bestehenden Markt darum allenfalls ordnen[60] und um nichtgeheime Daten erweitern, wofür aber kein Bedarf bestehe. Im Gegenzug drohten Marktzugangsschranken zu entstehen.

46 EuGH, ECLI:EU:C:2004:695, Rn. 31; EuGH, ECLI:EU:C:2004:696, Rn. 24; kritisch dazu *Wiebe*, GRUR Int 2016, S. 877, 879; *Zech,* GRUR 2015, S. 1151, 1158.

47 *Peschel/Rockstroh,* MMR 2014, S. 571, 573; *Wulf/Burgenmeister,* CR 2015, S. 404, 408; *Żdanowiecki* (Fn. 36), S. 22; a.A. *Hornung/Hofmann,* in: Reinhart, Handbuch Industrie 4.0, 2017, S. 191, 195, die auch die Kosten der Sensorik zur Messung der Daten berücksichtigen wollen.

48 *Dorner*, CR 2014, S. 617, 622; *Ehlen/Brandt,* CR 2016, S. 570, 575; *Kraus* (Fn. 25), S. 382.

49 Dazu eingehend *Dorner,* CR 2014, S. 617, 620 f.

50 *Berberich/Golla*, PinG 2016, S. 165, 173; *Wiebe,* GRUR Int 2016, S. 877, 883.

51 *Hoeren*, MMR 2013, S. 486, 488; *Hoeren/Völkel* (Fn. 15), S. 36.

52 I.E. *Härting,* CR 2016, S. 646, 647; in die Richtung wohl auch *Heymann,* CR 2016, S. 650, 651; *Specht/Rohmer,* PinG 2016, S. 127, 132; *Zech*, CR 2015, S. 137, 142; a.A. *Heun/Assion*, CR 2015, S. 812, 818.

53 *Berberich/Golla*, PinG 2016, S. 165, 170 ff.; *Wiebe,* GRUR Int 2016, S. 877, 880.

54 *86. Konferenz der Justizministerinnen und Justizminister der Länder*, Beschluss TOP I.8 Digitaler Neustart, Rn. 4, https://www.justiz.nrw.de/JM/leitung/jumiko/beschluesse/2015/fruehjahrskonferenz_15/TOP-I_8---Digitaler-Neustart-_oA_.pdf; *EU-Kommission* (Fn. 12), S. 30 ff.

55 *Zech*, CR 2015, S. 137, 144 ff.; *Zech*, GRUR 2015, S. 1151, 1159 f.; zustimmend *Ensthaler*, NJW 2016, S. 3473, 3476 f. Dazu eingehend *Becker*, in: Büscher/Glöckner/Nordemann/Osterrieth/Rengier, Marktkommunikation zwischen geistigem Eigentum und Verbraucherschutz, 2016, S. 815, 824 ff.

56 *EU-Kommission* (Fn. 12), S. 33 ff.

57 Ausführlich *Kerber*, GRUR Int 2016, S. 989 ff.

58 *Dorner,* CR 2014, S. 617, 626; *Heymann*, CR 2016, S. 650, 653; *Kerber,* GRUR Int 2016, S. 989, 992 f.; *Wiebe*, GRUR Int 2016, S. 877, 881; das räumt aber auch Zech ein, *Zech,* CR 2015, S. 137, 144 f.

59 *Cattaneo/Micheletti/Woodward/David/Osimo*, Data Ownership and Access to Data – Key Emerging Issues, S. 29 f., https://idc-emea.app.box.com/s/7oimpbwf0k0tinlugjbxpoxazr5k7fc1; *Drexl*, et al. (Fn. 32), Rn. 6 f.; *Kerber,* GRUR Int 2016, S. 989, 994 f.; skeptisch in Bezug auf das Funktionieren des Marktes *EU-Kommission* (Fn. 12), S. 34.

60 Zur Ordnungsfunktion *Wiebe,* GRUR Int 2016, S. 877, 881; *Wiebe,* CR 2017, S. 87, 91.

- Zuordnung des Datennutzens[61]: Eine interessengerechte Verteilung des Nutzens lasse sich – gerade in Wertschöpfungsnetzwerken – über vertragliche Lösungen besser bewerkstelligen. Die erlaubte Parallelerzeugung von Daten erschwere überdies die Zuordnung.[62]

- Negative Effekte[63]: Das Recht droht Informationen zu monopolisieren, Transaktionskosten zu steigern und so datengetriebene Geschäftsmodelle zu verhindern.

Alternative Ansätze zielen darauf, die faktische Kontrolle über die Daten als Grundlage der Verwertung zu stärken – also eher den „Datenbesitz" als das „Dateneigentum".[64] Hierzu sollen z. B. Know-how als geistiges Eigentum anerkannt,[65] die Umgehung technischer Schutzmaßnahmen sanktioniert[66] oder bestimmte – ggf. durch den Gesetzgeber zu konkretisierende – Eingriffe in die unternehmerische Sphäre als unlauter verboten werden.[67]

Handlungsbedarf wird noch am ehesten beim Zugang zu Daten gesehen.[68] Hier werden kontext- oder sektorspezifische Regelungen nach dem Vorbild der Datenportabilität nach Art. 20 Datenschutz-Grundverordnung (2016/679/EU) für möglich gehalten.[69] Die EU-Kommission erwägt hier die Einführung eines dem Wettbewerbsrecht entlehnten, aber unterhalb der dort geltenden Schwellen angesiedelten eigenständigen Zugangsrechts für Akteure auf Sekundärmärkten in Form einer „Zwangslizenz".[70]

61 *Kerber*, GRUR Int 2016, S. 989, 995 f.; *Sahl,* PinG 2016, S. 146, 149 f.; *Wiebe*, CR 2017, S. 87, 90.

62 *Wiebe*, GRUR Int 2016, S. 877, 882 f.; a. A. *Ensthaler,* NJW 2016, S. 3473, 3477 f.

63 *Dorner*, CR 2014, S. 617, 625 f.; *Drexl,* et al. (Fn. 32), Rn. 6; *Kerber,* GRUR Int 2016, S. 989, 996 f.; *Plattform Industrie 4.0,* Industrie 4.0 – wie das Recht Schritt hält, S. 22, http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/i40-wie-das-recht-schritt-haelt.pdf; *Wiebe*, GRUR Int 2016, S. 877, 882; *Wiebe*, CR 2017, S. 87, 91.

64 *EU-Kommission* (Fn. 12), S. 33 ff.

65 *McGuire*, GRUR 2016, S. 1000, 1003; ähnlich *Specht*, CR 2016, S. 288, 294.

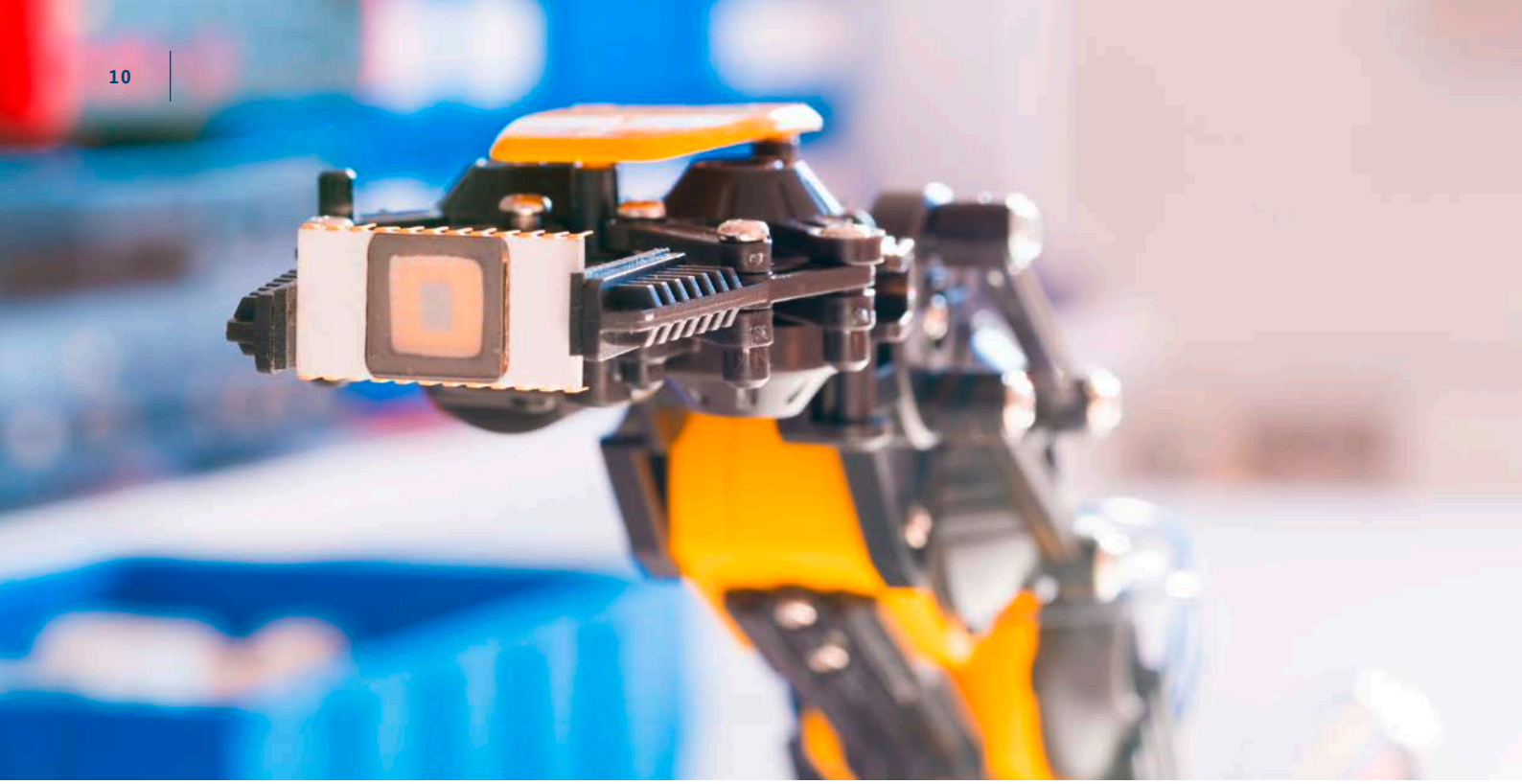
66 *Specht*, CR 2016, S. 288, 295; *Wiebe,* GRUR Int 2016, S. 877, 883; zum bisherigen Schutz *Grützmacher,* CR 2016, S. 485, 492 ff.; dazu allgemein *Specht,* ZGE 2016, S. 289 ff.; zur technischen Betrachtung *Hoppen,* CR 2015, S. 802 ff.

67 *Drexl,* et al. (Fn. 32), S. 7; *Hofmann*, InTeR 2013, S. 210, 216; *Kerber,* GRUR Int 2016, S. 989, 998; *Schefzig*, K&R Beilage 2015, S. 3, 4; *Wiebe,* GRUR Int 2016, S. 877, 879; zu Big Data allgemein *Zieger/Smirra*, MMR 2013, S. 418, 421.

68 *Becker* (Fn. 55), S. 824; *Kerber,* GRUR Int 2016, S. 989, 998.

69 *Drexl,* et al. (Fn. 32), Rn. 39.

70 *EU-Kommission* (Fn. 12), S. 36 ff., dazu *Wiebe,* CR 2017, S. 87, 92 f.; ähnlich auch *Surblytė* (Fn. 32), S. 27 ff.



3 M2M-Kommunikation – Neujustierung der Verantwortlichkeit

3.1 Anwendungen und Interessen

Die Entwicklung zur Industrie 4.0 wird wesentlich durch einen Paradigmenwechsel in der Automatisierung getrieben, der sich vor allem durch einen Wandel von einer zentralen zu einer dezentralen Steuerung durch autonome Systeme zeigt.[71] Dazu kommen in der Produktion zunehmend CPS mit sog. (Software-)Agenten[72] zum Einsatz. Diese autonomen intelligenten Systeme kennen ihre Fähigkeiten und Ziele und sind in der Lage, selbstständig mit ihrer Umwelt zu interagieren.[73] Das Werkstück „weiß" also, wie es bearbeitet werden[74] und zu welcher Stelle in der Fabrik es gelangen[75] muss. Umgekehrt „weiß" die Produktionsmaschine, welche Bearbeitungsschritte sie vornehmen, und das Transportsystem, zu welchem Punkt es Dinge befördern kann.[76] Der Prozess wird nun so gesteuert, dass die daran beteiligten CPS selbstständig Dienstleistungen anbieten oder nachfragen und so ihr Verhalten gegenseitig beeinflussen, ohne dass es einer zentralen Instanz bedürfte.[77] Dies geht so weit, dass CPS selbstständig oder voneinander lernen, indem sich z. B. Fahrzeuge über den Standort von Lagerplätzen austauschen und so die Transportwege selbstständig optimieren[78] oder Systeme ihr Verhalten im Sinne einer Regelauswahl ändern können.[79]

Durch diesen Ansatz, ein Problem in eine Vielzahl einfacher, von CPS lokal zu lösender Teilprobleme zu zerlegen, können Gesamtsysteme realisiert werden, die in ihrer Komplexität durch einen zentralen Ansatz nicht bewältigt werden könnten.[80] Insofern haben alle Beteiligten ein

71 *acatech/Forschungsunion* (Fn. 4), S. 24 f.; *Felix*, Industrie 4.0 Magazin 2015, S. 32, 33; *Günthner/Klenk/Tenerowicz-Wirth*, in: Bauernhansl, et al. (Fn. 2), S. 300 f.; *ten Hompel/Kerner*, Informatik-Spektrum 2015, S. 176, 177; *Spath, et al.* (Fn. 1), S. 98.

72 Näher *Gitter*, Softwareagenten im elektronischen Geschäftsverkehr, 2007, S. 48; *Kirn/Müller-Hengstenberg*, MMR 2014, S. 225 ff., m.w.N.

73 Zu „selbstständig veränderlichen Systemen", *Wendt/Oberländer,* InTeR 2016, S. 58 f.

74 *acatech/Forschungsunion* (Fn. 4), S. 23; *Vogel-Heuser*, in: Bauernhansl, et al. (Fn. 2), S. 42.

75 *Bauernhansl* (Fn. 4), S. 22.

76 *Frenz*, WRP 2016, S. 671, 672.

77 *Kerkmann*, Revolution in den Fabrikhallen, http://www.handelsblatt.com/9715564.html.

78 *ten Hompel/Kerner*, Informatik-Spektrum 2015, S. 176, 177.

79 *Kirn/Müller-Hengstenberg*, MMR 2014, S. 225, 229.

80 *ten Hompel/Kerner,* Informatik-Spektrum 2015, S. 176, 178 f.

Interesse an derartigen Lösungen. Sie führen aber zu Folgeproblemen, die sich daraus ergeben, dass das Verhalten dieser Systeme weder genau vorhergesagt, noch genau nachvollzogen werden kann. Dabei ist zwischen verschiedenen Schadensszenarien zu unterscheiden.

3.2 Intelligentes Handeln – Schäden innerhalb der Wertschöpfungskette

Durch das Einbinden einer Vielzahl von CPS in den Produktions- und Materialflussprozess steigt auch die Anzahl der Stellglieder im System stark an. Die dabei entstehenden Daten bilden die Grundlage für die oben beschriebenen datengetriebenen Dienste (2.1), mit deren Hilfe die Prozesssteuerung verbessert werden kann. In der Folge kommt es aber auch zu Wechselwirkungen zwischen den Teilsystemen, die zwar gewissen Gesetzmäßigkeiten unterliegen, welche aber wiederum so komplex sind, dass das Verhalten des Systems praktisch nicht mehr in jedem Fall vorhergesehen werden kann.[81]

Die Betreiber haben dadurch nicht nur keine unmittelbare Kontrolle über das – aus autonomen Teilsystemen bestehende – System; sie können sein Verhalten auch nicht mehr sicher, sondern nur noch mit einer gewissen Wahrscheinlichkeit vorhersagen. In diesem Zusammenhang ist darum von stochastischen Systemen die Rede, die sich deterministisch chaotisch verhalten.[82]

3.2.1 Verschuldenshaftung

Das spezifische Neue der Industrie 4.0 liegt darin, dass zu den bekannten neue, „kommunikationsbezogene" Schadensszenarien hinzutreten, in denen CPS fehlerhaft im Verbund agieren. Die daraus resultierenden Probleme betreffen im Wesentlichen Sach- und Vermögensschäden bei den beteiligten Unternehmen. Personenschäden bei Arbeitnehmern unterfallen dem Sonderregime der gesetzlichen Unfallversicherung.

Der Anknüpfungspunkt der Haftung bleibt auch bei „intelligenten" Systemen stets menschliches Handeln.[83] Die Schadenersatzpflicht des Betreibers oder Herstellers der CPS hängt dabei – sowohl nach den Regeln einer etwaigen vertraglichen als auch der deliktischen Haftung – grundsätzlich von deren Verschulden ab.[84] Innerhalb eines Wertschöpfungsnetzwerks wird die Haftung in der Regel durch vertragliche Vereinbarungen modifiziert bzw. überlagert werden; ähnlich wie bei der Datenhoheit (s. 2.1) bildet die gesetzliche Ausgangslage aber die Verhandlungsbasis für derartige Abweichungen.

Für die Verschuldenshaftung ist entscheidend, welcher Sorgfaltsmaßstab an den Einsatz der Systeme anzulegen ist. In Bereichen, in denen wie bei der Autonomik Rechtsvorschriften fehlen und sich im Rechtsverkehr noch keine festen Vorstellungen von dem jeweils erlaubten Risiko gebildet haben, ist hierfür auf eine Interessenabwägung abzustellen, die auf der Grundlage einer Kosten-Nutzen-Analyse durchgeführt wird.[85] Insofern wird auch zu berücksichtigen sein, dass es sich hier lediglich um potentielle Sach- und Vermögensschäden von Unternehmen handelt, die sich bewusst für den Einsatz autonomer Systeme entscheiden und die damit verbundenen Vorteile genießen. Es wird darum ein Sorgfaltsmaßstab anzulegen sein, bei dem das unvorhersehbare Verhalten eines Systems im Einzelfall dazu führen kann, dass dessen Betreiber oder Hersteller kein Verschulden trifft.[86]

Im System der deliktischen Haftung besteht sowohl für den Betreiber als auch für den Hersteller eine Reihe von Verkehrspflichten, durch die auch die Risiken autonomer

81 *ten Hompel/Kerner*, Informatik-Spektrum 2015, S. 176, 179; *Kirn/Müller-Hengstenberg*, MMR 2014, S. 225, 229 f.

82 *ten Hompel/Kerner*, Informatik-Spektrum 2015, S. 176, 179; zu Multiagentensystemen allgemein *Kirn/Müller-Hengstenberg,* MMR 2014, S. 225, 230.

83 *Spindler*, CR 2015, S. 766, 767. Eine unbedingte Zurechnung des maschinellen Handelns analog § 278 BGB scheidet darum aus, s. *Horner/Kaulartz*, CR 2016, S. 7; *John,* Haftung für künstliche Intelligenz, 2007, S. 248 f.; *Schulz,* Verantwortlichkeit bei autonom agierenden Systemen, 2015, S. 138 ff., i.E. auch *Grützmacher*, CR 2016, S. 695, 697; a.A. *Schirmer*, JZ 2016, S. 660, 664 f.

84 Die Gefährdungshaftung nach § 1 Abs. 1 ProdHaftG (dazu 3.4) ist aufgrund des darin enthaltenen Ausschlusses von Schäden an gewerblich genutzten Sachen für die Haftung zwischen Unternehmen nicht relevant.

85 *Horner/Kaulartz,* CR 2016, S. 7, 8; *Wendt/Oberländer*, InTeR 2016, S. 58, 60; *Zech,* in: Gleß/Seelmann, Intelligente Agenten und das Recht, 2016, S. 161, 181.

86 S. zum Einsatz von Agenten im E-Commerce *John* (Fn. 83), S. 253 f., 330. Zum autonomen Fahren *Grützmacher*, CR 2016, S. 695, 697; *Horner/Kaulartz*, CR 2016, S. 7, 8; *Riehm,* ITRB 2014, S. 113, 114; *Sosnitza,* CR 2016, S. 764, 769; *Wendt/Oberländer*, InTeR 2016, S. 58.

87 *Borges*, CR 2016, S. 272, 275; *Spindler*, CR 2015, S. 766, 769; *Wendt/Oberländer*, InTeR 2016, S. 58, 61; *Zech* (Fn. 85), S. 177 ff.

Systeme hinreichend erfasst werden können.[87] Im Einzelnen kann sich deren Bedeutung aber verschieben. So werden auf Seiten der Betreiber Bedienfehler kaum noch eine Rolle spielen, die richtige Festlegung des Einsatzgebietes und die Überwachung des Systems dafür aber umso mehr.[88] Auf Seiten des Herstellers wird die Unvorhersehbarkeit des Systemverhaltens nicht per se einen Konstruktionsfehler darstellen.[89] Im Gegenzug werden aber verschärfte Produktbeobachtungspflichten gefordert,[90] die sich insbesondere auf die Lernfähigkeit des Produkts,[91] nicht aber auf sämtliche Fehler bei der Interaktion mit fremden CPS beziehen sollen.[92]

Insgesamt zeigt sich, dass die Haftungsrisiken innerhalb des Wertschöpfungsnetzwerks mit den bestehenden Instrumenten beherrscht werden können.[93] Für die Einführung einer (strikten) Gefährdungshaftung des Betreibers[94] oder des Herstellers[95] autonomer Systeme, die allgemein schon kontrovers diskutiert wird, besteht in diesem speziellen Bereich darum wohl kein Bedarf.

3.2.2 Rechtsgeschäftliches Handeln

Die Kommunikation von CPS (bzw. deren Softwareagenten) beschränkt sich nicht auf das Auslösen rein faktischen Verhaltens, sondern kann auch rechtsgeschäftliche Erklärungen beinhalten. Nach der gängigen Lesart werden solche Erklärungen, die von einem IT-System automatisiert abgegeben werden, dessen Nutzer als eigene Erklärung zugerechnet.[96] Es genügt, das System willentlich in Betrieb zu nehmen. Bei deterministischen Systemen folgt dies bereits aus der Tatsache, dass sie lediglich die vordefinierten Anordnungen des Betreibers ausführen.[97] Bei autonomen Systemen erscheint dieser Ansatz zweifelhaft. Letztlich sind aber auch hier die Erklärungen der Risikosphäre des Nutzers zuzuordnen.[98] Nach dieser Logik trägt er das Risiko einer unbewussten Falschübermittlung und muss sich grundsätzlich die gesamte Erklärungstätigkeit des Systems zurechnen lassen. Eine Anfechtungsmöglichkeit bei Systemfehlern wird bisher nur anerkannt, wenn sich die fehlerhafte Übernahme der Vorgaben des Betreibers im Wortlaut der Erklärung niederschlägt.[99]

Anders als im Bereich der Verschuldenshaftung kann sich der Betreiber bei der Zurechnung von Willenserklärungen nicht darauf berufen, das konkrete Verhalten der Maschine sei für ihn nicht vorhersehbar gewesen. Zukünftig könnte die Zurechnung aber durch die Ausweitung der Anfechtungsmöglichkeit auf alle fehlerhaften Erklärungen gelockert werden.[100] Eine andere Möglichkeit bestünde in der Anwendung der Regeln der Stellvertretung, nach denen

88 *Grützmacher*, CR 2016, S. 695, 697; *Horner/Kaulartz,* CR 2016, S. 7, 8 f.; *Schulz* (Fn. 83), 137 f., 143 f.; *Spindler*, CR 2015, S. 766, 768.

89 *Klindt/Wende/Burrer/Schaloske/Żdanowiecki,* in: Bräutigam/Klindt (Fn. 36), S. 87; *Sosnitza*, CR 2016, S. 764, 769 f.; *Spindler*, CR 2015, S. 766, 768 ff.; ähnlich zur Produkt- und Produzentenhaftung *Grützmacher*, CR 2016, S. 695, 696; a.A. *Zech* (Fn. 85), S. 192.

90 *Grützmacher*, CR 2016, S. 695, 696; *Klindt,* et al. (Fn. 89), S. 85; *Schulz* (Fn. 83), S. 171; *Sosnitza*, CR 2016, S. 764, 769; *Spindler*, CR 2015, S. 766, 769; *Wendt/Oberländer*, InTeR 2016, S. 58, 63.

91 *Zech* (Fn. 85), S. 193 f.

92 Zu entsprechend eingeschränkten Produktbeobachtungspflichten des Herstellers *Sosnitza*, CR 2016, S. 764, 769; *Spindler*, CR 2015, S. 766, 769; a.A. *Grützmacher*, CR 2016, S. 695, 696; *Schulz* (Fn. 83), S. 172.

93 *Plattform Industrie 4.0* (Fn. 63), S. 17; allgemein *Spindler*, CR 2015, S. 766, 774; *Wendt/Oberländer,* InTeR 2016, S. 58, 64.

94 Dafür *Hanisch,* in: Hilgendorf, Robotik im Kontext von Recht und Moral, 2013, S. 27, 35 f.; *Zech* (Fn. 85), S. 201 f. Für nützlich, aber nicht zwingend halten dies *Spindler*, CR 2015, S. 766, 775; *Wendt/Oberländer*, InTeR 2016, S. 58, 64. Gänzlich ablehnend *Grützmacher*, CR 2016, S. 695, 698; *Horner/Kaulartz*, CR 2016, S. 7, 14; *John* (Fn. 83), S. 282 ff. Für einen umfassenden Regulierungsanstoß *Europäisches Parlament*, Entwurf eines Berichts mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik, 2015/2103(INL).

95 *Borges*, CR 2016, S. 272, 277 ff.; zurückhaltend *Zech* (Fn. 85), S. 200.

96 BGH v. 26.01.2005 – VIII ZR 79/04, NJW 2005, S. 976.

97 OLG Frankfurt v. 20.11.2002 – 9 U 94/02, CR 2003, S. 450, 451; *Köhler*, AcP 182 (1982), S. 126, 133 f.; *Kuhn*, Rechtshandlungen mittels EDV und Telekommunikation, 1991, S. 69 f.; *Spindler*, in: Spindler/Schuster, Vorbemerkung §§ 116 ff. BGB, Rn. 6; so auch für autonome Agenten *Cornelius,* MMR 2002, S. 353, 355.

98 *Sosnitza*, CR 2016, S. 764, 767; *Wiebe*, in: Gounalakis, Rechtshandbuch Electronic Business, 2003, S. 578, Rn. 33 ff.; für die Anwendung der Grundsätze der Blanketterklärung *Gitter/Roßnagel*, K&R 2003, S. 64, 66; *John* (Fn. 83), S. 121 f.; *Schulz* (Fn. 83), S. 109 ff.; *Sester/Nitschke*, CR 2004, S. 548, 550 f.; kritisch *Bauer*, Elektronische Agenten in der virtuellen Welt, 2006, S. 78 ff.; *Schirmer*, JZ 2016, S. 660, 663 f.

99 Bei einem System zum Verkauf von Produkten wäre dies z. B. der Preis, bei einem System zum Kauf z. B. die Menge, sofern der jeweilige Parameter vom Betreiber vorgegeben und nicht vom System selbst ermittelt wird, BGH v. 26.01.2005 – VIII ZR 79/04, NJW 2005, S. 976, 977; *Spindler*, in: Spindler/Schuster, § 120 BGB, Rn. 11.

dem Vertreter (Nutzer) nur jene Erklärungen zugerechnet werden, die der Vertreter (Softwareagent) innerhalb seiner Vertretungsmacht abgibt. Neben zahlreichen offenen Detailfragen[101] scheitert dieser Ansatz aber bereits daran, dass ein IT-System kein Vermögen hat, mit dem es dem Erklärungsgegner gemäß § 179 BGB haften könnte.[102]

3.2.3 Möglichkeiten der Haftungsbegrenzung

In beiden Fällen, sowohl dem rein tatsächlichen als auch dem rechtsgeschäftlichen Handeln, wird ein dringendes Bedürfnis bestehen, handhabbare Maßstäbe festzulegen, über welche die Haftungsrisiken angemessen verteilt und ggf. auch versicherungstechnisch abgesichert werden.

3.2.3.1 Grenzen der vertraglichen Gestaltung

Hierfür bieten sich zum einen vertragliche Regelungen an. Aus der Sicht der Praxis erweist sich dabei jedoch das AGB-Recht in seiner aktuellen Ausgestaltung als hinderlich,[103] dem Verträge nur entzogen sind, soweit die konkrete Bestimmung – und nicht lediglich der Vertrag insgesamt – inhaltlich ernsthaft zur Disposition steht.[104] Greift die AGB-Kontrolle, können die wesentlichen Vertragspflichten nur aus schwerwiegenden Gründen abbedungen werden,[105] sodass Haftungserleichterungen wie die Beschränkung des Sorgfaltsmaßstabs[106] oder der Schadenshöchstsumme[107] nur noch eingeschränkt möglich sind.

Um die notwendige Flexibilität im B2B-Bereich zu gewährleisten, wird darum gefordert, die Anwendbarkeit des AGB-Rechts auf solche Fälle zu beschränken, in denen eine Partei tatsächlich keinen Einfluss auf den Vertragsinhalt nehmen konnte, oder die Indizwirkung der §§ 308 f. BGB abzuschaffen.[108]

3.2.3.2 Eigenständige Haftung als elektronische Person?

Auf rechtspolitischer Ebene wurde der Vorschlag geäußert, IT-Systeme zur „elektronischen Person“ zu erklären, mit eigener Haftungsmasse auszustatten und die Informationen darüber in einem Register zu hinterlegen.[109] Verursacht das System einen Schaden oder überschreitet es bei einer rechtsgeschäftlichen Erklärung seine Befugnisse, soll dann nicht der Betreiber, sondern es selbst für seine Handlung haften.

Im Ergebnis führt dies jedoch zu kaum lösbaren Problemen.[110] So fehlt einer Maschine, die anders als ein Mensch nicht darauf bedacht ist, ihre wirtschaftliche Existenz zu sichern, jeder Anreiz, ihre Haftungsmasse nicht willkürlich zu gefährden. Ohne diesen „Überlebenswillen“ als Schutzmechanismus für den Rechtsverkehr erscheint es aber kaum möglich, eine allgemeine gelockerte Zurechnung für autonome Maschinen einzuführen.[111] Denkbar wäre dies allenfalls für das rechtsgeschäftliche Handeln innerhalb geschlossener Systeme, in denen alle Beteiligten ein Interesse an dieser Form der Interaktion haben (s. 4.2.1).

100 Nur für den Fall, dass die Fehlerhaftigkeit für den Erklärungsgegner erkennbar ist, *Sosnitza*, CR 2016, S. 764, 768. *Schirmer,* JZ 2016, S. 660, 664 konstruiert eine Außenvollmacht, lässt den Menschen nach § 166 Abs. 1 BGB aber die Erklärungen der ihn vertretenden Maschine anfechten.

101 *Gitter* (Fn. 72), S. 178 f.; *Hofmann/Hornung*, in: Engemann/Sprenger, Internet der Dinge, 2015, S. 181, 187 f.; *Spindler*, JZ 2016, S. 805, 816.

102 *Bräutigam/Klindt*, NJW 2015, S. 1137, 1138; *Cornelius*, MMR 2002, S. 353, 354 f.; *Gitter/Roßnagel*, K&R 2003, S. 64, 66; *Sester/Nitschke,* CR 2004, S. 548, 550; *Sosnitza*, CR 2016, S. 764, 766.

103 *Klindt*, et al. (Fn. 89), S. 78 f., 82; *Plattform Industrie 4.0* (Fn. 63), S. 5 f.

104 BGHZ 200, S. 326, Rn. 27.

105 BGHZ 164, S. 11, Rn. 39.

106 BGHZ 145, S. 203, Rn. 109 ff.

107 BGHZ 145, S. 203, Rn. 50 ff.; *Cloppenburg/Mahnken*, NZBau 2014, S. 743 ff.

108 *Klindt*, et al. (Fn. 89), S. 83; *Plattform Industrie 4.0* (Fn. 63), S. 5.

109 *Beck*, in: Hilgendorf, Robotik und Gesetzgebung, 2013, S. 239, 255 ff.; *Chopra/White*, A legal theory for autonomous artificial agents, 2011, *S. 160 ff.*; *Pagallo*, in: Hildebrandt/Gaakeer, Human Law and Computer Law, 2013, S. 47, 59 ff.; *Wettig/Zehendner*, in: Proceedings of the 2nd Workshop The Law and Electronic Agents, 2003, IV.4; a.A. *Bauer* (Fn. 98), S. 45 ff.; *Hanisch* (Fn. 94), S. 40; Plattform Industrie 4.0 (Fn. 63), S. 7; *Sosnitza*, CR 2016, S. 764, 766; *Spindler*, CR 2015, S. 766, 774 f.; *Spindler*, JZ 2016, S. 805, 816.

110 Eingehend *Hofmann/Hornung* (Fn. 101), S. 189 ff.

111 A.A. wohl *Kersten*, in: Karsch/Manzeschke, Roboter, Computer und Hybride, 2016, S. 89, 97 ff.

3.3 Verteiltes Handeln – Beweis und Zurechnungsprobleme

Die künstliche Intelligenz geht in der Industrie 4.0 weniger von einem einzelnen komplexen System aus, wie dies vornehmlich bei selbststeuernden Autos und in der Robotik der Fall ist. Passender erscheint insofern ein Vergleich mit Multiagentensystemen[112], wie sie im Hochfrequenzhandel zum Einsatz kommen. Hier hat sich auch die beschriebene fehlende Vorhersehbarkeit der Systeme gezeigt, bis hin zu Resonanzkatastrophen, die auch nicht dadurch verhindert werden konnten, dass die einzelnen Agenten über eigene Sicherheitsmechanismen verfügten.[113]

Die wesentliche Schwierigkeit liegt darum in der Ermittlung und Zurechnung der jeweiligen Verursachungsbeiträge. Eine rechtssichere Dokumentation, die z. B. dadurch gewährleistet werden könnte, dass sämtliche Systemdaten etwa in einem Fehlerspeicher[114] aufgezeichnet und elektronisch signiert werden,[115] dürfte darum in der Industrie 4.0 unerlässlich sein.

Als problematisch erweisen sich jene Fälle, in denen eine solche Dokumentation ausscheidet, etwa weil sie unwirtschaftlich wäre,[116] oder bereits an konzeptionellen Schwierigkeiten scheitert.[117] Letzteres liegt zum einen daran, dass nach dem „Zerfall" eines solchen Verbunds dessen Verhalten u. U. nicht mehr nachvollzogen werden kann. Zum anderen können sich sehr viele Verursachungsbeiträge zu einem schädigenden Ereignis summieren, ohne dass einer davon klar herausstünde. In der Folge kann die Verantwortung keinem der Beteiligten klar zugewiesen werden; sie „verschwimmt" also gewissermaßen im Wertschöpfungsnetzwerk.

Die gängige Beweislastumkehr aus der vertraglichen (§ 280 Abs. 1 S. 2 BGB) und Teilen der gesetzlichen Haftung[118] bezieht sich lediglich auf das Vertretenmüssen bzw. das Verschulden. Eine Beweislastumkehr auch für die Kausalität zwischen Pflichtverletzung und Rechtsgutverletzung besteht lediglich in speziellen Regelungsbereichen wie den §§ 6 f. UmweltHG und wird für die Haftung für autonome Systeme nicht befürwortet.[119] Dies hat allerdings nicht zur Folge, dass eine Haftung in jedem Fall ausscheidet. Steht fest, dass mehrere Beteiligte einen Schaden verursacht haben, nicht aber, wie ihre jeweiligen Beiträge zu bewerten sind, weist § 830 BGB dieses „Unaufklärbarkeitsrisiko" den potentiellen Schädigern zu, die in der Folge gesamtschuldnerisch haften.[120] Im Bereich der vertraglichen Haftung können entsprechende Beweislastverteilungen vereinbart werden.[121]

Im Übrigen ist die Haftung für derart komplexes verteiltes Handeln jedoch bisher kaum diskutiert worden. Für die parallele Problematik der – vertikalen und nicht wie hier horizontalen – Abgrenzung der Verantwortlichkeitsbereiche von Maschinenhersteller und -betreiber wird eine gesamtschuldnerische Haftung vorgeschlagen, bei der für jeden Beteiligten sowohl das zurechenbare Verhalten als auch ein diesbezügliches Verschulden vermutet wird.[122]

112 S. zu Multiagentensystemen *Kirn/Müller-Hengstenberg*, MMR 2014, S. 225, 226.

113 *ten Hompel/Kerner*, Informatik-Spektrum 2015, S. 176, 179 f.

114 *Hanisch* (Fn. 94), S. 45 f.; *Klindt,* et al. (Fn. 89), S. 85; *Kröner*, in: Vieweg/Gerhäuser, Digitale Daten in Geräten und Systemen, 2010, S. 183 ff.; *Wendt/Oberländer*, InTeR 2016, S. 58, 64; zur Aufzeichnung im Fahrzeug *Sosnitza*, CR 2016, S. 764, 771.

115 *Horner/Kaulartz,* in: Taeger, Internet der Dinge, 2015, S. 510, 513; *Hornung/Hofmann*, in: acatech/Forschungsunion (Fn. 4), S. 64; *Tschohl*, e & i 2014, S. 219, 220.

116 *Grützmacher,* CR 2016, S. 695, 697; *Reichwald/Pfisterer*, CR 2016, S. 208, 211 f.

117 *Zech* (Fn. 85), S. 175.

118 In der Produzentenhaftung nach § 823 Abs. 1 BGB ist dies richterrechtlich anerkannt, BGHZ 51, S. 91, Rn. 36; BGHZ 105, S. 346, Rn. 17. Es wird vorgeschlagen, diese Grundsätze auf die Haftung des Betreibers auszuweiten, *Riehm*, ITRB 2014, S. 113, 114; *Spindler*, CR 2015, S. 766, 771 f. Für eine analoge Anwendung des § 831 BGB, bei dem ebenfalls ein Organisationsverschulden vermutet wird, *John* (Fn. 83), S. 272 ff.; a. A. *Schulz* (Fn. 83), S. 147 f.

119 *Spindler*, CR 2015, S. 766, 775.

120 *Horner/Kaulartz*, CR 2016, S. 7, 10.

121 Dazu allgemein *Horner/Kaulartz* (Fn. 115), S. 514 f.

122 *Hanisch* (Fn. 94), S. 56 f.; *Schuhr*, in: Hilgendorf (Fn. 94), S. 21.

Für das Problem des verteilten Handelns schlägt Spiecker gen. Döhmann eine „graduelle Gesamtschuldnerschaft" vor, bei der die Anteile statt nach Kausalität und Verschulden nach Merkmalen wie Investitionsleistung und Gewinnanteil verteilt werden können.[123] Dieser Ansatz ähnelt einer Billigkeitshaftung nach Marktanteilen, wie sie von der US-amerikanischen Rechtsprechung vereinzelt angewendet, aber nicht weiterverfolgt wurde.[124] Ob diese nicht am Verursachungsbeitrag, sondern am wirtschaftlichen Interesse orientierte Haftungsverteilung in allen Fällen angemessen ist, bedarf aber noch weiterer Untersuchung.

3.4 Schäden durch ein in der Industrie 4.0 gefertigtes Produkt

Als Haftungsfälle außerhalb des Wertschöpfungsnetzwerks kommen vor allem Schäden in Betracht, die etwa beim Käufer eines durch Industrie 4.0-Methoden gefertigten Produkts auftreten. Für Personenschäden und Schäden an privat genutzten Sachen, die durch den Fehler eines Produktes verursacht werden, sieht § 1 Abs. 1 ProdHaftG eine verschuldensunabhängige Haftung vor. Daneben kann stets auch auf die – z. B. auch auf Schäden an gewerblich genutzten Sachen anwendbare – allgemeine deliktische Produzentenhaftung[125] nach § 823 BGB zurückgegriffen werden.

Diese Haftungskonzepte werden durch die Industrie 4.0 nicht grundlegend in Frage gestellt.[126] Das Kernproblem besteht nämlich nicht im unvorhersehbaren Verhalten der Produkte – in der Industrie 4.0 geht es um „intelligentes" Produzieren, nicht um „intelligente" Produkte –, sondern vielmehr in der schwer zu ermittelnden Verantwortlichkeit in einem besonders arbeitsteilig organisierten Produktionsprozess. Dies geht jedoch zu Lasten des Herstellers des Endproduktes, als der gem. § 4 Abs. 1 S. 2 ProdHaftG auch gelten kann, wer sich durch die Kennzeichnung der Produkte dafür ausgibt (Quasi-Hersteller). Er haftet – gesamtschuldnerisch mit dem Hersteller der Teilprodukte oder Grundstoffe – auch für die Fehler der anderen am Prozess Beteiligten.[127] Ähnliches gilt im Deliktsrecht, dem zwar die Figur des Quasi-Herstellers fremd ist,[128] in dem sich der Hersteller aber nur von Haftung befreien kann, wenn er seine Partner sorgfältig ausgewählt und instruiert hat.[129]

123 *Spiecker gen. Döhmann*, CR 2016, S. 698, 703 f.

124 Sindell vs. Abbott Laboratories, 26 Cal. 3d 588 (1980); *Zipursky/Goldberg*, Harv. L. Rev. 123 (2010), Heft 8, S. 1919, 1920, dazu *Hanisch* (Fn. 94), S. 41 f.

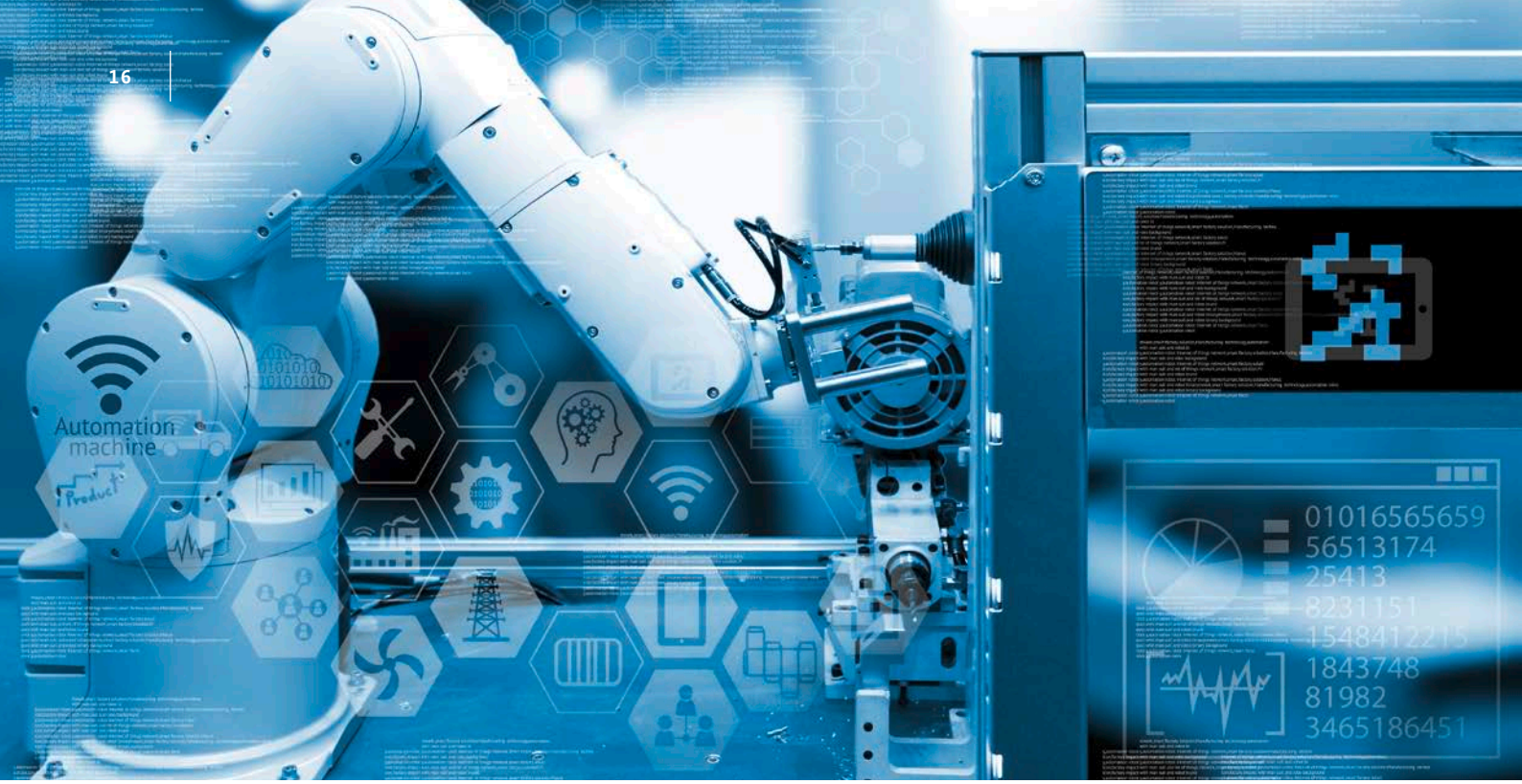
125 S. Fn. 118.

126 *Klindt*, et al. (Fn. 89), S. 84; *Spindler,* CR 2015, S. 766, 773.

127 *Riehm*, ITRB 2014, S. 113, 114; MüKo BGB/*Wagner*, § 4 ProdHaftG, Rn. 8.

128 BGH v. 14.06.1977 – VI ZR 247/75, VersR 1977, S. 839 f.

129 MüKo BGB/*Wagner*, § 823, Rn. 628 f.



4 Wertschöpfungsnetzwerke – Rechtliche Grenzen der Vernetzung

Weite Teile der aufgezeigten Vernetzung sowie der Kommunikation auf Maschinenebene werden nicht auf bilateraler Zusammenarbeit einzelner weniger beruhen, sondern in Wertschöpfungsnetzwerken realisiert werden, in die eine Vielzahl von Beteiligten mit einbezogen sein wird. Die Industrie 4.0 wird folglich durch eine besonders intensive und bereits auf unteren Hierarchieebenen einsetzende unternehmensübergreifende Zusammenarbeit geprägt sein.

Bei allen daraus resultierenden Möglichkeiten ist eine solche enge Vernetzung jedoch mit erheblichen Herausforderungen verbunden – zum einen hinsichtlich der schon aufgezeigten Risiken, zum anderen, weil Vernetzung selbst zwingenden gesetzlichen Vorgaben unterliegt. Der Schutz der Arbeitnehmer (4.1) ist dafür ein Beispiel. Ihr volles Potential wird die Vernetzung darum nur ausschöpfen können, wenn strukturiert und unter Beachtung dieser Vorgaben gestaltet wird. Hierbei kommt Plattformbetreibern (4.2) eine zentrale Rolle zu.

4.1 Arbeit in der „Smart Factory“

Die Entwicklung zur Industrie 4.0 unterzieht auch das Arbeitsumfeld der Beschäftigten einem tiefgreifenden Wandel, der nicht zuletzt den Arbeitsschutz vor neue Herausforderungen stellt.[130] Die hier im Fokus stehende enge Kooperation von Unternehmen in Wertschöpfungsnetzwerken betrifft hingegen vor allem zwei Problemfelder: den Beschäftigtendatenschutz (4.1.1) und die Erosion klassischer Organisationsformen (4.1.2).

4.1.1 Beschäftigtendatenschutz

Die datenschutzrechtlichen Fragestellungen des Internets der Dinge bzw. des Ubiquitous Computing werden seit geraumer Zeit diskutiert.[131] Demgegenüber steht die Analyse der innerbetrieblichen Anforderungen erst am Anfang.[132]

130 S. dazu z. B. *Kohte*, NZA 2015, S. 1417 – 1424; *Krause*, Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, 2016, S. 28 ff.; *Steffan,* NZA 2015, S. 1409 ff.

131 *Hansen/Thiel,* DuD 2012, S. 26 – 30; *Roßnagel*, Datenschutz in einem informatisierten Alltag, 2007; *ULD/IWI*, TAUCIS, https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf.

132 *Dehmel/Diekmann,* PinG 2016, S. 141 ff.; *Hofmann*, ZD 2016, S. 12 ff.; *Hornung/Hofmann*, in: Hirsch-Kreinsen, Digitalisierung industrieller Arbeit, 2015, S. 165 ff.

4.1.1.1 Gezielter Personenbezug – Assistenzsysteme

Am sichtbarsten wird die Frage im Bereich der datengetriebenen Assistenzsysteme, die etwa dazu dienen, den Einsatz der Arbeitnehmer zu organisieren, ihnen kontextbezogen Informationen einzublenden oder sie durch die unmittelbare Zusammenarbeit mit Robotern zu entlasten. Die Daten werden hier zwar nicht notwendigerweise zur Überwachung der Arbeitnehmer, aber doch gezielt auf einen Personenbezug hin erhoben und verarbeitet und geben nicht selten präzise darüber Aufschluss, wo sich der Arbeitnehmer wie lange aufgehalten und mit welcher Qualität und Geschwindigkeit er die ihm übertragenen Aufgaben erfüllt hat.[133]

Die Zulässigkeit dieser Datenverarbeitung bestimmt sich – unabhängig davon, ob hierfür auf den gesetzlichen Erlaubnistatbestand oder eine kollektivarbeitsrechtliche Vereinbarung[134] abgestellt wird – nach der Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses. Dabei kann der Arbeitgeber weitgehend frei darüber entscheiden, welche (gesteigerten) funktionalen Anforderungen er an die Systeme stellt, mit denen er die Arbeit organisiert. Ob die Datenverarbeitung in der Umsetzung zulässig ist, ist stets eine Frage des Einzelfalls und hängt nicht zuletzt auch von der datenschutzfreundlichen Gestaltung des Systems ab. Eine intensivere Datenverarbeitung kann aber durchaus durch eine effizientere Organisation des Betriebsablaufs gerechtfertigt werden. In jedem Fall muss sie aber transparent erfolgen, in zeitlicher und räumlicher Hinsicht kontrollfreie Bereiche wahren und Maßnahmen zur Missbrauchskontrolle vorsehen.[135]

Auch die Zulässigkeit der Datenübermittlung richtet sich nach dem Erforderlichkeitsprinzip – mit der Folge, dass Assistenzsysteme, die prinzipiell auch intern realisiert werden könnten, in der Regel nur auf der Grundlage einer Auftragsdatenverarbeitung durch Externe betrieben werden dürfen. Die Externalisierung der Datenverarbeitung wird dabei an umfangreiche Pflichten für den Arbeitgeber, insbesondere zur Kontrolle seines Auftragnehmers geknüpft. In solch übersichtlichen Verantwortungsstrukturen stellt die Industrie 4.0 keine strukturell neue Herausforderung für das Datenschutzrecht dar.[136]

4.1.1.2 Ungezielter Personenbezug – Maschinendaten

Anders als die Daten in Assistenzsystemen wird die weit überwiegende Zahl der Daten in der Industrie 4.0 keinen gezielten Personenbezug aufweisen, sondern vornehmlich schlicht maschinen- oder betriebsbezogen sein. Ein Personenbezug kann jedoch auch indirekt, durch die Verknüpfung von selbst nicht personenbezogenen Daten, hergestellt werden[137] – mit der Folge, dass alle gesetzlichen Vorgaben zu beachten sind; das Datenschutzrecht macht keinen Unterschied zwischen gezieltem und ungezieltem Personenbezug. Insbesondere große, für Big-Data-Analysen vorgesehene Datenbestände sind darum latent vom Personenbezug „bedroht“, nicht zuletzt auch, weil handhabbare gesetzgeberische oder aufsichtsbehördliche Vorgaben zur Anonymisierung fehlen.

Wird der Personenbezug bejaht, gehen damit erhebliche Beeinträchtigungen für den unternehmensübergreifenden Datenaustausch einher. Da eine Auftragsdatenverarbeitung in Wertschöpfungsnetzwerken regelmäßig ausscheidet,[138] müssen die Voraussetzungen für eine Übermittlung gegeben sein. Auch hier können Effizienzgewinne prinzipiell legitimierend wirken; es muss aber sichergestellt sein, dass die Datenverarbeitung beim Dritten die intern bestehenden Zweckbegrenzungen nicht überschreitet.[139] Um dies unter

133 *Dehmel/Diekmann*, PinG 2016, S. 141, 142.

134 Die Einführung eines technischen Systems bedarf der Mitbestimmung des Betriebsrats, wenn sie im konkreten Fall zur Überwachung objektiv geeignet ist (st. Rspr. zu § 87 Abs. 1 Nr. 6 BetrVG, BAG AP Nr. 1 zu § 87 BetrVG 1972 Überwachung; zuletzt BAGE 109, 235). Da hierdurch in der Industrie 4.0 weit mehr Systeme mitbestimmungspflichtig wären als bisher, sieht vor allem die Arbeitgeberseite an dieser Stelle Reformbedarf. Diskutiert werden z. B. ein vorläufiges Einführungsrecht des Arbeitgebers (s. *Plattform Industrie 4.0* [Fn. 63], S. 26) sowie die Beschränkung des Mitbestimmungstatbestands auf gezielte Leistungs- und Verhaltenskontrollen (*Schipp*, ArbRB 2016, S. 177, 179) oder auch auf die Auswertung dieser Daten, nicht bereits die Erhebung (*Günther/Böglmüller*, NZA 2015, S. 1025, 1027; *Hanau*, NJW 2016, S. 2613, 2615). *Krause* (Fn. 130), S. 79 f. plädiert dagegen für eine Klarstellung, dass – wie nach der BAG-Rechtsprechung – jeder Umgang mit personenbezogenen Daten unter § 87 Abs. 1 Nr. 6 BetrVG fällt.

135 *Hornung/Hofmann* (Fn. 132), S. 172 f.

136 *Hornung/Hofmann* (Fn. 47), S. 205 f.

137 *Schefzig*, K&R 2014, S. 772, 773 f.; *Skistims/Voigtmann/David/Roßnagel*, DuD 2012, S. 31, 35.

138 Schädlich ist insofern sowohl das Eigeninteresse des Empfängers der Daten (*Petri*, in: Simitis, § 11 BDSG, Rn. 23) als auch die wohl nicht durchsetzbaren Kontrollpflichten, i.E. *Plattform Industrie 4.0* (Fn. 63), S. 14.

139 *Roßnagel/Jandt/Müller/Gutscher/Heesen*, Datenschutzfragen mobiler kontextbezogener Systeme, 2006, S. 115.

den Bedingungen des automatisierten Datenaustausches zu gewährleisten, muss die Berechtigung jedes potentiellen Empfängers für jede Datenkategorie einzeln im Vorhinein festgelegt sowie dessen Vertrauenswürdigkeit und Berechtigung geprüft werden.[140] Ein Netzwerk darf also insbesondere nicht nach dem Prinzip aufgebaut sein, dass jeder Beteiligte zu jeder Zeit auf alle personenbezogenen Daten zugreifen kann.

An den darin zum Ausdruck kommenden Prinzipien der Erforderlichkeit, Transparenz und Zweckbindung der Datenverarbeitung hält auch die neue Datenschutz-Grundverordnung fest. Mit der in Art. 26 DS-GVO enthaltenen Regelung für mehrere „gemeinsam für die Verarbeitung Verantwortliche" bietet sie aber ein weiteres Instrument, diesen Anforderungen gerecht zu werden, ohne zu einer Datenübermittlung greifen zu müssen. Die Herausforderung besteht hier darin, Vertragsmodelle zu entwerfen, die eine solche gemeine Verantwortlichkeit umsetzen.

Besonders problematisch sind aus datenschutzrechtlicher Sicht internationale Fallkonstellationen. Hier bringt die Datenschutz-Grundverordnung einige Erleichterungen: Zum einen fällt das Verbot der Auftragsdatenverarbeitung außerhalb des Europäischen Wirtschaftsraums (§ 3 Abs. 8 BDSG) weg. Zum anderen erkennt die Verordnung mit den branchenweiten Verhaltensregeln und der Zertifizierung (Art. 46 Abs. 2 lit. e und f DS-GVO) weitere Instrumente an, mit denen ein unangemessenes Datenschutzniveau in dem Drittland (vor allem den USA) kompensiert werden kann.

4.1.2 Neue flexible Organisationsformen

Die intensive Vernetzung und Zusammenarbeit verschiedener Unternehmen wird dazu führen, dass die klassische Betriebsstruktur zunehmend flexiblen und dezentralen Organisationsformen weicht.[141] Die Verantwortungsbereiche für die Produktion werden zukünftig immer seltener zentral gebündelt und hierarchisch strukturiert, sondern stattdessen dezentral in spezialisierten Einheiten verankert sein.[142] In der Folge werden in zunehmenden Maße unternehmensfremde Personen das Direktionsrecht des Arbeitgebers ausüben.

Das System der Mitbestimmung orientiert sich an den hierarchischen Strukturen des Konzerns, Unternehmens und Betriebs, sodass sich hier u. U. ein Anpassungsbedarf ergeben kann.[143] Die bereits bestehenden Möglichkeiten in § 3 BetrVG, alternative Organisationsformen durch kollektivarbeitsrechtliche Regelungen zu bilden, werden jedoch als unzureichend bewertet. Sie sind darauf angelegt, die bestehenden Strukturen durch ebenso stabile Konstruktionen zu ersetzen; die alten Betriebsräte müssten demnach aufgelöst werden. Für solche langfristigen Ansätze sind die Liefer- und Kundenbeziehungen in einem Wertschöpfungsnetzwerk allerdings nach einhelliger Auffassung nicht dauerhaft genug.[144] Den insofern passenderen, als bloße Ergänzung fungierenden Arbeitsgemeinschaften nach § 3 Abs. 1 Nr. 4 BetrVG stehen jedoch keine Beteiligungsrechte zu.[145] Darum wird angeregt, die Gründung einer zusätzlichen Arbeitnehmervertretung mit diesen Rechten zu ermöglichen.[146]

4.2 Zentrale und dezentrale Akteure – Plattformregulierung

Eine zentrale Rolle beim Aufbau von Wertschöpfungsnetzwerken werden Plattformbetreiber spielen, welche die notwendige Infrastruktur für die Vernetzung bereitstellen. Aus juristischer Perspektive sind diese Betreiber aber besonders dann interessant, wenn sie darüber hinaus weitere Funktionen wahrnehmen.

140 Ein solch aufwändiger Prozess könnte aber ohnehin zum Schutz von Know-how notwendig sein. Ein solches Ziel verfolgt z. B. die Initiative „Industrial Data Space". Die Vertrauenswürdigkeit der Beteiligten könnte in beiden Fällen über Zertifikate nachgewiesen werden, *Hofmann*, in: Obermaier, Industrie 4.0 als unternehmerische Gestaltungsaufgabe, 2016, S. 171, 182.

141 *Krause* (Fn. 130), S. 89 f.; *Plattform Industrie 4.0* (Fn. 63), S. 28. Das kann so weit gehen, dass sich Arbeitgeber zusammenschließen, um sich wechselseitig Arbeitnehmer zu überlassen oder diese gleich bei einem Plattformbetreiber anzustellen, *Uffmann,* NZA 2016, S. 977, 983 f.

142 *Günther/Böglmüller*, NZA 2015, S. 1025, 1027.

143 Insgesamt zurückhaltend *Krause* (Fn. 130), S. 91 ff.

144 *Günther/Böglmüller*, NZA 2015, S. 1025, 1027; *Hanau*, NJW 2016, S. 2613, 2615; *Krause* (Fn. 130), S. 93 f.; *Oetker*, JZ 2016, S. 817, 822; *Rieble*, NZA-Beilage 2014, S. 28, 29 f.

145 *Hanau*, NJW 2016, S. 2613, 2615; *Rieble*, NZA-Beilage 2014, S. 28, 29 f.; etwas anderes gilt in Konzernunternehmen. Hier können unternehmensübergreifende Ausschüsse des Konzernbetriebsrats gegründet werden, dazu ebd. sowie *Günther/Böglmüller*, NZA 2015, S. 1025, 1026 f.

146 *Hanau*, NJW 2016, S. 2613, 2615; *Krause* (Fn. 130), S. 94.

4.2.1 Anwendung und Interessen

Plattformbetreiber können zum einen die Stellung eines Intermediärs einnehmen, der Plattformen für den Handel mit Daten und datengetriebenen Dienstleistungen[147] oder zur Abstimmung von Produktions- und Logistikprozessen[148] etabliert. In dieser Position wären sie auch in der Lage, regulatorisch tätig zu werden, und branchenspezifisch Standards vorzugeben, wie bestehende Schutzlücken in den oben beschriebenen Bereichen vertraglich zu schließen wären. Dies beträfe z. B.:

- die Datenhoheit (s. 2.), mit Regelungen zum „Herrn der Daten" oder den erlaubten Nutzungsformen;[149]
- das rechtsgeschäftliche Handeln von Agenten (s. 3.2.2), wo weitere Möglichkeiten vorgesehen werden könnten, sich von fehlerhaften Erklärungen zu lösen;[150]
- den Beschäftigtendatenschutz (s. 4.1.1) mit Verhaltensregelungen (Art. 40 DS-GVO) zur Anonymisierung bei der Datenweitergabe.

Zum anderen können die Betreiber eigene, die eigentliche Bereitstellung der Plattform flankierende Dienstleistungen anbieten. Neben der Zahlungsabwicklung wird es vor allem darum gehen, das – bei einer offenen Plattform systembedingt – niedrige Vertrauensniveau zu kompensieren. Denkbar wäre hier eine Zertifizierung der Teilnehmer im Hinblick auf die Qualität ihrer Dienstleistung oder ihren Umgang mit fremdem Know-how oder fremden Beschäftigtendaten. Damit ließen sich auch Versicherungsmodelle kombinieren.

Die Plattformbetreiber werden zunächst mit der Frage konfrontiert sein, wie sich die beschriebenen Funktionen rechtskonform umsetzen lassen. Darüber hinaus stellen sich aber auch Rechtsfragen zum Betrieb der Plattform selbst.

4.2.2 Wettbewerbsrechtliche Beschränkungen

Aus wettbewerbsrechtlicher Sicht geht es dabei vor allem um den Zugang zu der Plattform und die Bedingungen, unter denen er gewährt werden muss. Gerade Plattformen, auf denen viele Unternehmen einer Ebene zusammenarbeiten, können zu einer marktmächtigen Stellung gelangen. Würden also bspw. viele Maschinenhersteller oder -betreiber einer Branche den Zugang zu den von ihnen generierten Rohdaten nur über eine Plattform oder einen Standard gewähren, wäre dies geeignet, den Wettbewerb in dem benachbarten, hierauf angewiesenen Markt der Datenanalyse auszuschließen und dadurch letztlich Innovationen zu verhindern. Einem Unternehmen den – kostenpflichtigen – Zugang zu verweigern, wäre wettbewerbswidrig.[151]

Vor diesem Hintergrund wird auch staatliche Regulierung als problematisch angesehen, die auf ein besonders hohes Schutzniveau – z. B. im Bereich der Datenhoheit oder der IT-Sicherheit – zielt. Könnten in der Folge nur wenige Unternehmen die Anforderungen erfüllen, würde dies die Entstehung von Monopolen begünstigen.

4.2.3 Haftung des Plattformbetreibers

Ein anderer Aspekt ist die Haftung der Plattformbetreiber selbst, die umso relevanter werden dürfte, je weiter diese die Position eines neutralen Dritten verlassen.

147 *Plattform Industrie 4.0*, Fortschreibung der Anwendungsszenarien der Plattform Industrie 4.0, S. 14, http://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/fortschreibung-anwendungsszenarien.html. Ein weiteres Beispiel ist ein Technologiedatenmarkt, *acatech/Forschungsunion* (Fn. 4), S. 106.

148 *Müller,* Abschlussbericht 2010 – 2012 zum RFID-based Automotive Network, S. 4.

149 *Specht*, CR 2016, S. 288, 295 f. Der Abnehmer der Daten könnte zusätzlich verpflichtet werden, diese vertraglichen Beschränkungen entsprechend an seine Partner weiterzugeben, *Żdanowiecki* (Fn. 36), S. 26 f.

150 *Hofmann/Hornung* (Fn. 101), S. 191, schlagen dazu Regelungen nach dem Vorbild der Mistrade-Regeln an der Börse vor, welche es der Börsengeschäftsführung erlauben, Geschäfte, die aufgrund von Fehlern in technischen Systemen zu nicht marktgerechten Preisen geschlossen wurden, aufzuheben, dazu *Schäfer,* in: Assmann/Schütze, Handbuch des Kapitalanlagerechts, 4. Aufl., 2015, § 13, Rn. 40.

151 *Frenz,* WRP 2016, S. 671, 673 ff.

Eine Haftung für eigene Fehler kann z. B. dadurch begründet werden, dass die bereitzustellende Infrastruktur Fehler aufweist und dadurch Informationen zu den autonomen Systemen falsch oder gar nicht weitergeleitet werden können. Die Sorgfaltspflichten werden hier abzustufen sein, je nachdem, wie funktionswichtig die einzelnen Informationen sind. Allein die Weiterleitung falscher Informationen wirkt nicht haftungsbegründend.[152]

Daneben kommt auch eine Haftung für fremdes Handeln in Betracht. Die Haftungsszenarien reichen dabei von der bereits aus Online-Marktplätzen bekannten Haftung für rechtswidrige Angebote der Nutzer bis zu der Frage, inwieweit der Plattformbetreiber für die von ihm zertifizierten Eigenschaften der Nutzer einstehen muss. Dies würde z. B. dann relevant, wenn ein Datendienstleister das ihm übergebene Know-how missbraucht oder die datenschutzrechtlichen Anforderungen für eine Datenübermittlung nicht erfüllt.

152 *Schulz* (Fn. 83), S. 179.