eLF
NOVEMBER 2017

RESCRIPTUM

MÜNCHNER STUDENTISCHE RECHTSZEITSCHRIFT

Industrie 4.0

Zwischen Selbstregulierung und staatlicher Intervention

Lukas Hufeld

Trotz der noch jungen Geschichte von Industrie 4.0 gehen die Meinungen über Regulierung und ihre Steuerungskraft weit auseinander. Einig ist man sich allenfalls darin, dass herkömmliche hoheitliche Intervention nicht ausreicht, um Industrie 4.0 zu beherrschen. Das geltende Recht stellt Lösungen bereit, muss sich jedoch auch neuen Herausforderungen stellen.

Digitalisierung! Kein anderer Begriff bringt den technischen Fortschritt des 21. Jahrhunderts besser auf den Punkt. Er beschreibt die Überführung analoger Daten in digitale Form und damit die Vernetzung der realen mit der virtuellen Welt. Diese Vernetzung stellt einen Kulturbruch dar und verändert bis heute das Alltagsleben der Menschen auf allen Ebenen. Wie wir kommunizieren, arbeiten, lernen, konsumieren oder wohnen. Selbstfahrende Autos, ferngesteuerte Kühlschränke, E-Commerce oder E-Learning sind heute Realität. Die rasant zunehmende Digitalisierung von Gesellschaft und Wirtschaft zwingt auch die Industrie zu einem Strukturwandel. Mit der Digitalisierung der Produktion, gemeinhin als Industrie 4.0 bezeichnet, wird der Schritt in die vollständig digital vernetzte Welt für die Fertigung vollzogen. Wer hieraus schlussfolgert, Industrie 4.0 betreffe nur den Produktionssektor, greift zu kurz. Denn die Digitalisierung von Produkten und der Produktion hat Auswirkungen auf Bereiche der Gesellschaft und des Lebens, die auf den ersten Blick gar nichts mit Industrie zu tun haben. Vieles, was wir im täglichen Leben nutzen, wird industriell entwickelt und hergestellt. Dadurch beeinflusst Industrie 4.0 insgesamt Angebot und Nachfrage. Aber auch Verkehr, Versicherungen, Gesundheitssysteme oder die Stadtverwaltung sind von diesem strukturellen Wandel betroffen.[1]

Angesichts der wirtschaftlichen, gesellschaftlichen und politischen Relevanz[2] stellt sich die Frage nach der Notwendigkeit externer Einflussnahme auf Industrie 4.0. Bedarf es staatlicher Regulierung und gesetzlicher Grenzen oder ist es im Interesse aller Akteure, dass sich die Industrie selbst reguliert?

I. Industrie 4.0 – Eine Begriffsbestimmung

Industrie 4.0 steht für die vierte industrielle Revolution. Anfang des 19. Jahrhunderts war es die Einführung von Wasser- und Dampfkraft zur Unterstützung mechanischer Produktion, die zur ersten industriellen Revolution führte. Ein knappes Jahrhundert später charakterisierte sich die zweite Revolution durch die Möglichkeit der Band- und Massenproduktion mittels elektrischer Energie. Ab den 1970er startete die dritte Revolution, die sich durch die Automatisierung der Produktion dank IT und

Der Verfasser studiert Rechtswissenschaften an der LMU München und dankt Herrn Prof. Dr. Matthias Leistner sowie Herrn Wiss. Mit. Thomas Sagstetter für die Durchsicht und die wertvollen Hinweise.

1 *Sendler*, in: Sendler (Hrsg.), Industrie 4.0 grenzenlos, 2016, Vorwort S. 6.

2 So fand im April 2017 erstmalig ein Treffen der G20-*Digitalminister* statt. Mehr dazu: https://www.bmwi.de/Redaktion/DE/Veranstaltungsarchiv/20170406-digitalisation-policies-for-a-digital-future.html (Stand: 01.09.17).

Elektronik auszeichnete.[3] Mit dem 2011 im Rahmen der High-Tech Strategie durch die Bundesregierung ins Leben gerufenen Zukunftsprojekt „Industrie 4.0“[4] war es eine deutsche Initiative, die den Anspruch erhob, der vierten industriellen Revolution einen Namen zu geben. Das übergeordnete Ziel sollte sein, die Wettbewerbsfähigkeit des Standorts Deutschland zu stärken und die internationale Spitzenposition Deutschlands in der produzierenden Industrie auszubauen.[5] Heute bezeichnet Industrie 4.0 einen weltweiten Trend, der zuerst in Deutschland begrifflich erfasst wurde.[6]

Kennzeichnend für diesen Trend ist die Kombination vernetzter und kommunizierender Systeme mit der Produktions- und Automatisierungstechnik. So soll eine weitestgehend selbstorganisierte Produktion möglich werden, in der Menschen, Maschinen, Anlagen, Logistik und Produkte direkt miteinander kommunizieren und kooperieren.[7] Durch diese Vernetzung liegen alle relevanten Informationen in Echtzeit vor, anhand derer zu jedem Zeitpunkt der optimale Wertschöpfungsfluss gemanagt werden kann. Ideales Ergebnis soll eine intelligente Wertschöpfungskette sein, die alle Phasen des Lebenszyklus eines Produkts einschließt: Von der Idee eines Produkts über die Entwicklung, Fertigung, Nutzung und Wartung bis hin zum Recycling.[8] Technische Grundlage hierfür bilden sogenannte cyber-physische Systeme (CPS), welche Software- und Hardwaresysteme zu einem komplexen und intelligenten Verbund kombinieren, in dem jedes einzelne physische Objekt eine eigene Cyber-Identität besitzt.[9] CPS ermöglichen eine Reihe von neuartigen Funktionen, Diensten und Eigenschaften, die weit über die bisherigen integrierten Systeme hinausgehen.[10] So wird die – im Mittelpunkt von Industrie 4.0 stehende – „Smart Factory“ durch weitere „smarte“ Infrastrukturen ergänzt. Hierzu gehören insbesondere „Smart Logistics“, „Smart Mobility“, „Smart Buildings“ und „Smart Health“.[11]

II. Mögliche Regulierungskonzepte

CPS tragen zur Entstehung einer Datenwirtschaft ganz neuer Qualität bei, die Daten nicht mehr ausschließlich als Steuerungselement von Wirtschaftsabläufen begreift, sondern auch als Güter erfasst.[12] Das Recht kann dabei zweierlei Auswirkungen auf den Datenmarkt haben. Einerseits können regulatorische Eingriffe den freien Datenverkehr einschränken. Instrumentarien dafür sind insbesondere im Datenschutz, aber auch im Immaterialgüterrecht zu verorten. Andererseits kann das Recht aber auch dazu beitragen, einen Datenverkehr zu ermöglichen – sei es durch klare regulierende „Spielregeln“, das Vertragsrecht, oder das Wettbewerbsrecht.[13] Ziel darf es also nicht sein, den Rechtsrahmen zu mini- oder maximieren, sondern geeignete rechtliche Rahmenbedingungen zu schaffen, welche die Digitalisierung der Produktion flankieren.[14]

Dabei stellt das vielschichtige und schwer überschaubare Anwendungsfeld von Industrie 4.0 gängige Regulierungskonzepte vor große Herausforderungen. Bei der Suche nach einer geeigneten Regulierungsform müssen eine hohe Innovationsgeschwindigkeit[15], heterogene Verbrauchererwartungen[16] und das Charakteristikum grenzüberschreitender Produktion und Nutzung[17] maßgeblich berücksichtigt werden. Die möglichen Regulierungsansätze lassen sich drei Grundtypen zuordnen, wobei im Hinblick auf die Besonderheiten von Industrie 4.0 im Folgenden Stärken und Schwächen dieser Konzepte ausgelotet werden.

1. Staatliche Regulierung

Bei der staatlichen Regulierung greift der Staat direkt in Marktabläufe ein und beeinflusst das Verhalten von Unternehmen durch Vorschriften. Damit will der Staat bestimmte, im Allgemeinen Interesse stehende Ziele erreichen.[18] Dabei sollen nur jene hoheitlichen Verhaltensbeschränkungen erfasst werden, welche die Gewerbe- und Vertragsfreiheit der Wirtschaftssubjekte (Art. 2 Abs. 1, 9, 12, 14 GG) über allgemeingültige Normen einschränken.[19] Die Regulierung erfolgt dabei durch die staatlichen Organe der Legislative, Exekutive und Judikative sowie durch Institutionen, die den staatlichen Organen gegenüber weisungsgebunden sind. Hierzu zählen insbesondere Behörden wie das Bundeskartellamt oder das Bundesministerium des Innern. Die erlassenen Regelungen sind für alle Akteure verbindlich. So können sektorübergreifende Regelungen getroffen werden, an die sich alle zu halten haben. Die Vollstreckungsgewalt der spezialisierten Aufsichtsbehörden gewährleistet überdies ein Sanktionsregime, das die Einhaltung der Rege-

3 *Kaufmann*, in: *ders.,* Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge – Der Weg vom Anspruch in die Wirklichkeit, 2015, S. 4.

4 Siehe auch Website der Hightech-Strategie: http://www.hightech-strategie.de/ (Stand: 01.09.17).

5 Plattform Industrie 4.0, Was ist Industrie 4.0?, http://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html (Stand: 01.09.17).

6 *Sendler* (Fn. 1), S. 10 f.

7 Plattform Industrie 4.0 (Fn. 5).

8 Bitkom e.V./VDMA e.V./ZVEI e.V. (Hrsg.), Umsetzungsstrategie Industrie 4.0, 2015, S. 10.

9 *Siepmann*, in: Roth (Hrsg.), Einführung und Umsetzung von Industrie 4.0 – Grundlagen, Vorgehensmodell und Use Cases aus der Praxis, 2016, S. 23.

10 Geisberger/Broy (Hrsg.), agendaCPS. Integrierte Forschungsagenda Cyber-Physical Systems (acatech STUDIE), 2012, S. 19; *Fleisch/Mattern*, Das Internet der Dinge, 2005, S. 3 f.

11 Bitkom e.V. (Hrsg.), Rechtliche Aspekte von Industrie 4.0, 2016, S. 8 f.; Geisberger/Broy (Fn. 10), S. 256.

12 *Zech*, in: Körber/Immenga (Hrsg.), Daten und Wettbewerb in der digitalen Ökonomie, 2017, S. 36.

13 Ebd.

14 Ebd.; *Talidou*, Regulierte Selbstregulierung im Bereich des Datenschutzes, 2005, S. 29.

15 *Huber*, in: Sendler (Hrsg.), Industrie 4.0 grenzenlos, 2016, S. 233 f.

16 *Spindler/Thorun*, Eckpunkte einer digitalen Ordnungspolitik, 2015, S. 19 f.

17 Ebd.

18 Bundeszentrale für politische Bildung, Das Lexikon der Wirtschaft, Stichwort „Regulierung“: http://www.bpb.de/nachschlagen/lexika/lexikon-der-wirtschaft/20504/regulierung (Stand: 01.09.17).

19 *Latzer et al.*, Selbst- und Ko-Regulierung im Mediatiksektor, 2002, S. 31; bei der europaweiten Regulierung sind die Art. 15-17 GRCh als europäisches Pendant zu Art. 2 Abs. 1, Art. 9, 12, 14 GG maßgeblich.

lungen überprüft.[20] Um diese Regeln jedoch rechtsstaatlich zu legitimieren, bedarf es zunächst eines demokratischen Verfahrens. Hierbei ist das vorgeschriebene Gesetzgebungs- oder Verwaltungsverfahren einzuhalten, bevor Gesetze, Verordnungen oder Verwaltungsakte (etwa Allgemeinverfügungen) erlassen werden können.[21] Dadurch genießt die staatliche Regulierung zwar eine hohe demokratische Legitimation und ist in der Lage, auch politisch umstrittene Regelungen zu treffen. Allerdings ist der demokratische Entscheidungsprozess nicht selten langwierig, was dazu führen kann, dass der Gesetzgeber den immer neu entstehenden Rechtsproblemen nur hinterherläuft.[22] Zudem weisen Kritiker der staatlichen Regulierung auf Wissens- und Kompetenzdefizite der staatlichen Entscheidungsträger hin, was zur Verfehlung der Problemlösung und ungewollten Nebenwirkungen führen kann.[23] So könne staatliche Regulierung unter anderem dazu beitragen, Eigeninitiative, Innovation und Verantwortungsbewusstsein der Steuerungsobjekte zu hemmen und Widerstände auszulösen.[24] Diese Widerstände können darin bestehen, Ausweichstrategien und Schlupflöcher zu suchen oder politischen Druck gegen die Regulierungsinitiativen zu mobilisieren, indem beispielsweise mit der Gefährdung von Arbeitsplätzen argumentiert wird.[25]

2. Selbstregulierung

Die Alternative zur staatlichen Regulierung ist die Selbstregulierung. Da der Staat hier davon ausgeht, dass die Steuerungsziele durch gesellschaftliches Handeln selbst erfüllt werden, enthält er sich jeder Regulierung.[26] So entwirft bei der Selbstregulierung eine Einzelperson, eine private Organisation (z.B. ein Unternehmen) oder eine Gruppe (z.B. ein Branchenverband) selbst eine Regelung[27], der sie sich freiwillig unterwirft und dessen Einhaltung und Durchsetzung eigenständig überwacht wird.[28] Ein Paradebeispiel für Selbstregulierung ist das Konzept der *Corporate Social Responsibility* (CSR). Dabei setzen sich Unternehmen eigene Standards in Bezug auf soziale und ökologische Belange, die dann in Form von Verhaltenskodizes verbindliche Wirkung für die teilnehmenden Akteure entfalten.[29] Im Hochtechnologiebereich von Industrie 4.0 spielt neben derartigen Verhaltensregeln zur Unternehmensethik und Moral insbesondere das Setzen technischer Standards eine herausragende Rolle.[30] Solche Akte der Selbstregulierung erhalten ihre Legitimation aus der Privatautonomie der Sich-Bindenden.[31] Mit der Unterzeichnung eines Verhaltenskodex wird eine Selbstbindung im Sinne der Begründung eines Pflichtenprogramms eingegangen. Dieses Pflichtenprogramm unterscheidet sich beispielsweise von einem Kaufvertrag über eine Maschine dahingehend, dass es neue, nicht im Gesetz konkretisierte Verhaltenspflichten schafft, die wiederum von einer Vielzahl an Unternehmen aufgegriffen werden können.[32]

a) Vorteile

Selbstregulierung hat viele Vorteile gegenüber der staatlichen Regulierung. Neben einem hohen Maß an Flexibilität und Geschwindigkeit[33] sind insbesondere die Professionalität und Sachnähe[34] privater Akteure zu nennen. So wird eine schnelle und präzise Anpassung an neue Verhältnisse einer sich stetig verändernden Informations-, Produktions- und Kommunikationsgesellschaft ermöglicht.[35] Zudem können Kreativität, Eigeninitiative und Innovationsfähigkeit der betroffenen Marktteilnehmer stimuliert werden.[36] Dadurch, dass die aufgestellten Vorschriften aus Überzeugung freiwillig befolgt werden, steigt die Akzeptanz der Regulierung und die freiheitliche-demokratische Grundordnung wird gestärkt.[37] Ein weiterer Vorteil ist in der grenzüberschreitenden Einbindung privater Marktakteure zu verorten. Im Bereich von Industrie 4.0 ist dies von maßgeblicher Bedeutung, da die modernen Informations- und Kommunikationstechnologien zu einer Globalisierung von Verbindungen und international tätigen Unternehmen geführt haben.[38] Hier versagt staatliche Regulierung, da es an der zentralen Autorität fehlt, die unterschiedlichen Rechts- und Sozialnormsysteme aufeinander abzustimmen. Private Selbstregulierungsakte, an deren Einhaltung die einzelnen Akteure interessiert sind, können diese Grenzen überwinden.[39]

b) Nachteile

Kritiker warnen davor, dass durch die Selbstregulierung demokratische Prozesse umgangen und lediglich eigene, dem wirtschaftlichen Interesse entsprechende „Spielregeln" gesetzt würden.[40] So entsteht die Gefahr, dass Industrieinteressen zu Lasten Dritter oder des öffentlichen Interesses durchgesetzt werden. In diesem Zusammenhang wird eben-

20 *Spindler/Thorun* (Fn. 16), S. 23.
21 *Reip*, Die Selbstregulierung im Internet: unter besonderer Betrachtung der Standardsetzung und des Domain- Name-Systems, 2002, S. 36.
22 Ebd.; *Dahlhaus*, rescriptum 2017, 47 (48, 52 f.).
23 *Spindler/Thorun* (Fn. 16), S. 27.
24 Ebd.
25 *Schulz/Held*, Regulierte Selbstregulierung als Form modernen Regierens, 2002, S. A-10.
26 *Schulz/Held* (Fn. 25), S. A-3; *Buck-Heeb/Dieckmann*, Selbstregulierung im Privatrecht, 2010, S. 20.
27 Die Regelung kann beispielsweise als Selbstverpflichtungsabkommen, als Verhaltenskodex, als Gesellschaftsvertrag oder als Satzung ausgestaltet sein.
28 *Spindler/Thorun* (Fn. 16), S. 26; *Buck-Heeb/Dieckmann* (Fn. 26), S. 32.
29 *Hilty,* in: Hilty/Henning-Bodewig (Hrsg.), Corporate Social Responsibility. Verbindliche Standards des Wettbewerbsrechts?, 2014, S. 3 (4); *Podszun,* in: Hilty/Henning-Bodewig (Hrsg.), Corporate Social Responsibility. Verbindliche Standards des Wettbewerbsrechts?, 2014, S. 51 (53 f.).
30 *Latzer et al.* (Fn. 19), S. 15.
31 *Podszun* (Fn. 29), S. 73.
32 Ebd.
33 *Buck-Heeb/Dieckmann* (Fn. 26), S. 220 f.
34 *Eidenmüller*, ZGR 2007, 484 (488 f.).
35 *Buck-Heeb/Dieckmann* (Fn. 26), S. 220 f.
36 *Schulz/Held* (Fn. 25), S. A-8.
37 *Podszun* (Fn. 29), S. 78.
38 *Buck-Heeb/Dieckmann* (Fn. 26), S. 226 f.
39 *Latzer et al.* (Fn. 19), S. 49; *Buck-Heeb/Dieckmann* (Fn. 26), S. 226.
40 *Podszun* (Fn. 29), S. 79; *Latzer et al.* (Fn. 19), S. 52.

falls moniert, dass Regeladressaten und Verbraucher bei privater Regulierung gerade nicht durch rechtsstaatliche Prinzipien wie Transparenz und hinreichendem Rechtsschutz (Art. 19 Abs. 4 GG) geschützt werden. Dies kann dazu führen, dass wesentliche Stakeholder in der Regelsetzung unberücksichtigt bleiben oder dass Regeladressaten aufgrund von Rechtsunsicherheit die Geltung der Vorschriften in Frage stellen.[41]

Auch in der mangelnden Bindungswirkung privater Regulierung wird ein Kritikpunkt gesehen. Zwar kann aufgrund eines Vertragsschlusses Verbindlichkeit für die jeweiligen Parteien erzeugt werden, Dritte hingegen sind nicht an diese Regeln gebunden.[42] Auch die Anwendung von Normen, die von organisierten privaten Institutionen wie dem Deutschen Institut für Normung (DIN) auf nationaler, dem Comité Européen de Normalisation (CEN) auf europäischer sowie der International Organization for Standardization (ISO) auf internationaler Ebene erlassen und durchgesetzt werden, ist freiwillig, sofern die Normen nicht ausdrücklich in Gesetzesbezug genommen werden.[43] Aus diesem Grund wird selten eine vollständige Branchenabdeckung erreicht. Hinzu kommt ein Defizit bei der Überwachung und Durchsetzbarkeit privater Vorschriften, da es meist an wirksamen Sanktionen bei Verstößen, einem Beschwerdemechanismus und einer systematischen und unabhängigen Evaluation fehlt.[44] Im Ergebnis führen diese Defizite dazu, dass Ansätze der Selbstregulierung oft als „symbolische Politik" abgetan werden, deren einziges Ziel es sei, einschränkende Gesetzgebung zu verhindern.[45]

Es bleibt festzustellen, dass weder die Selbstregulierung noch die staatliche Regulierung allen Besonderheiten von Industrie 4.0 angemessen Rechnung tragen kann. Um die jeweiligen Stärken dieser Regulierungskonzepte zu nutzen und gleichzeitig die Nachteile auszugleichen, bedarf es möglicherweise einer Kombination aus staatlichen und privaten Arrangements.[46]

3. Regulierte Selbstregulierung

Die regulierte Selbstregulierung, auch Ko-Regulierung genannt[47], stellt ein solches kooperatives Konzept dar.[48] Dabei findet die Selbstregulierung privater Akteure innerhalb eines gesetzlichen Rahmens bzw. auf rechtlicher Grundlage statt.[49] Die Einflussnahme des Staates kann dabei ganz unterschiedlicher Natur sein. So können staatliche Institutionen Regulierungsziele gesetzlich vorgeben und deren Einhaltung überprüfen oder selbst an der Ko-Regulierung mitwirken, indem sie Mindestanforderungen für die Standardsetzung und -durchsetzung definieren. Charakteristisch dafür ist die Kombination staatlich bindender Rechtsetzungs- und Regelungstätigkeit mit Maßnahmen der Hauptbeteiligten unter Nutzung ihrer praktischen Erfahrungen.[50] Ein Beispiel für regulierte Selbstregulierung ist die Entwicklung des Datenschutzkodex der Versicherungsunternehmen, der in gemeinsamer Zusammenarbeit von dem Gesamtverband der Deutschen Versicherungswirtschaft, den deutschen Datenschutzbehörden sowie der Verbraucherzentrale Bundesverband erarbeitet wurde.[51]

Derartige Kombinationen hören sich verlockend an. Private Akteure können auf dynamischen Märkten sektorspezifische und sachgerechte Regelungen schaffen, während der Staat den rechtlichen Rahmen festlegt und darauf achtet, dass Transparenz, öffentliche Interessen und Dritte nicht zu kurz kommen. Dennoch mangelt es zu großen Teilen an strukturellen Voraussetzungen, die eine erfolgreiche Ko-Regulierung garantieren können. Unklar ist zum Beispiel, welche Anforderungen an Entwicklungsprozess und Inhalt von privat gesetzten Regeln zu stellen sind und welche rechtlichen Wirkungen sie im Falle einer Anerkennung entfalten. Vor dem Hintergrund struktureller Hindernisse müssen deshalb klare Anforderungen an die allgemeinen Rahmenbedingungen einer Ko-Regulierung formuliert werden.

a) Exklusive Anreize

Das Kernproblem der Selbstregulierung liegt darin, dass sich nicht alle Unternehmen einem privat beschlossenen Kodex anschließen wollen (sog. Free-Rider-Dilemma)[52]. Zum einen, weil sie es mangels Bindungswirkung nicht müssen, zum anderen, weil die positiven Auswirkungen selbstregulatorischer Maßnahmen (etwa das Verhindern „harter" staatlicher Regulierung oder ein branchenübergreifender Reputationsgewinn) nicht ausschließlich den Unternehmen zugute kommen, die die Maßnahmen auch befolgen.[53] Da Selbstregulierung oft mit beachtlichen Kosten verbunden ist, bedarf es deshalb exklusiver Anreize für all diejenigen, die sich den Regeln unterwerfen. Um ein umfassendes und transparentes Verfahren der Regelaufstellung zu fördern, könnte der Staat beispielsweise mit finanziellen Fördermitteln zur Seite stehen oder öffentliche Plattformen zum Austausch von Stakeholdern einrichten.[54] Eine echte

41 *Buck-Heeb/Dieckmann* (Fn. 26), S. 235.
42 *Buck-Heeb/Dieckmann* (Fn. 26), S. 230.
43 *Makowski*, in: Mestmäcker/Möschel/Hellwig (Hrsg.), Wirtschaftsrecht und Wirtschaftspolitik, Band 212, 2007, S. 54 f.; DIN e.V./DKE, Deutsche Normungs-Roadmap. Industrie 4.0, Version 2, 2015, S. 11; Podszun (Fn. 29), S. 60.
44 *Bachmann*, Private Ordnung: Grundlagen ziviler Regelsetzung, 2006, S. 54.
45 OECD, Report: Alternatives to traditional regulation, 2006, S. 40; *Latzer et al.* (Fn. 19), S. 52.
46 *Latzer et al.* (Fn. 19), S. 48; Schulz/Held (Fn. 25), S. A-3.
47 Begriff nicht ganz unstrittig. *Makowski* (Fn. 43), S. 21, vermeidet ihn und fasst die damit bezeichneten Gestaltungsformen unter den Selbstregulierungsbegriff; so auch *Buck-Heeb/Dieckmann* (Fn. 26), S. 24; *Podszun* (Fn. 29), 76 f., hingegen spricht von „Meta-Regulierung".
48 *Talidou* (Fn. 14), S. 27.
49 *Reip* (Fn. 21), S. 22; *Schulz/Held* (Fn. 25), S. A-5.
50 *Spindler/Thorun* (Fn. 16), S. 25.
51 Zum Datenschutzkodex siehe: http://www.gdv.de/2013/09/versicherungsunternehmen-treten-datenschutzkodex-bei/ (Stand: 01.09.2017).
52 Zum „Free-Rider-" oder auch „Trittbrettfahrerbegriff" siehe *Spindler/Thorun* (Fn. 16), S. 34; *Buck-Heeb/Dieckmann* (Fn. 26), S. 231.
53 *Spindler/Thorun* (Fn. 16), S. 53.
54 *Spindler/Thorun* (Fn. 16), S. 51.

Grundlage für eine branchenabdeckende Implementierung privater Regelsetzung wäre allerdings ein umfassendes System zur Anerkennung bestimmter Verhaltenskodizes[55] durch staatliche Institutionen (z.B. durch das Bundesamt für Verbraucherschutz). Wer sich etwa bei der Aufstellung von Standards an gesetzliche Anforderungen hält (hierzu gehört insbesondere, dass alle interessierten Kreise am Normsetzungsverfahren gleichwertig beteiligt werden[56]), kann dann einen Anspruch auf Genehmigung eines Kodex geltend machen. Durch die Einführung von Gütesiegeln dürften entsprechende Kodizes werblich verwendet werden und dem Kunden signalisieren, dass auf freiwilliger Basis überdurchschnittliche Anforderungen eingehalten wurden. Im Rahmen des Wettbewerbsrechts (UWG) könnte die unzulässige Verwendung derartiger Gütesiegel dann als Wettbewerbsverstoß in Gestalt irreführender Werbung geahndet werden.[57]

b) Rechtliche Wirkung von Standards

Darüber hinaus können in Verhaltenskodizes festgeschriebene branchen- und funktionsspezifische Standards vor Gericht Beachtung finden, indem sie Generalklauseln ausfüllen oder zur Konkretisierung unbestimmter Rechtsbegriffe beitragen.[58] So dienen technische Standards im Produktsicherheitsbereich oft zur Quasi-Konkretisierung der im Verkehr üblichen Sorgfalt (§ 276 Abs. 2 BGB). Die Rechtsprechung sieht DIN-Normen in besonderer Weise als geeignet an, da sie anerkannte Regeln der Technik wiedergeben.[59] Dennoch sind sie nicht in der Lage, eine Bindungswirkung für Gerichte zu entfalten. Zum einen können sie bereits bei Erlass durch technische Entwicklungen überholt sein. Zum anderen dienen technische Normen – im Gegensatz zu CSR-Standards – in erster Linie einer Standardisierung zum Nutzen von Wirtschaft und Technik und weniger dem Rechtsgüterschutz und der Sicherheit. Den Anforderungen, die etwa an die Neutralität und Unvoreingenommenheit gerichtlicher Sachverständiger zu stellen sind, genügen sie deshalb nicht. Aus diesen Gründen kommt den Normen nur eine Indizwirkung zu.[60] Im Bereich des Produktsicherheitsrechts kann der Hersteller zusätzlich nach § 4 Abs. 2 ProdSG das Privileg einer sogenannten Konformitätsvermutung für sein Produkt in Anspruch nehmen. Hierfür muss das Produkt einer von den nationalen Normungsorganisationen (DIN) erlassenen „Spiegelnorm" entsprechen, die europäisch harmonisierte Normen umsetzt.[61] Daraufhin darf das Unternehmen davon ausgehen, dass zumindest im Wege des ersten Anscheins (Prima-facie-Beweis) ein Gericht oder eine Behörde von gesetzeskonformem Verhalten ausgeht.[62] Diese Regelungstechnik der „normkonkretisierenden Verweisung" vermittelt eine beachtliche Zwangswirkung, die in der Praxis einen wirksamen Anreiz zur Normbefolgung setzt.[63] Um Rechtssicherheit zu gewährleisten und dem „Free-Rider-Dilemma"[64] entgegenzuwirken, sollte diese Vermutungswirkung branchenübergreifend gesetzlich verankert werden.

c) Förderung der Regelsetzungsprozesse

Der Staat ist dazu angehalten, die – Interoperabilität ermöglichende – Vereinheitlichung technischer Standards und die Eröffnung eines offenen Wettbewerbs bereits im Standardsetzungsprozess zu fördern.[65] Dazu gehört eine globale oder zumindest regionale Harmonisierung anerkannter Normen (wie etwa durch die EU-Harmonisierungsrichtlinien oder die Produktsicherheitsverordnungen), die Definition eines einheitlichen Vokabulars und einer einheitlichen Softwaresprache sowie Vereinbarungen hinsichtlich der Qualitätsanforderungen an technische Standards.[66] Da Standards zwangsläufig auch Berührungspunkte mit Grundrechten wie der Privatsphäre, dem Recht auf Eigentum oder der persönlichen Freiheit haben, ist der Staat zudem angehalten, politische Ansprüche an die Standardsetzung zu stellen. Um gleichzeitig nicht das Innovationspotential von Industrie 4.0 zu hemmen, müssen Industrie, Forschungsinitiativen, Normungsgremien und staatliche Kontrollinstanzen eng zusammenarbeiten und Standards und Kodizes kontinuierlich überprüfen und evaluieren.[67]

III. Rechtliche Herausforderungen

1. Datenschutz

Einen Schwerpunkt der rechtlichen Herausforderungen im Zusammenhang mit Industrie 4.0 bildet der Datenschutz. Grundsätzlich gilt, dass die Preisgabe personenbezogener Daten einer Einwilligung (§§ 4, 4a BDSG) bedarf. Andernfalls liegt ein nicht gerechtfertigter Eingriff in die informationelle Selbstbestimmung vor.[68] Die Einwilligung dient jedoch nur insoweit als tragfähige Rechtsgrundlage, wie Zweck und Reichweite der Verarbeitung zuvor festgelegt wurden. Im Kontext von Industrie 4.0-Szenarien mit einer Vielzahl an Datenvorgängen und potenziell Betroffenen ist es praktisch unmöglich, eine entsprechende Einwilligung einzuholen.[69]

Da Unternehmen bestrebt sind, die hohen Anforderungen des Bundesdatenschutzgesetzes zu vermeiden, zeigt sich bereits, dass zunehmend Konzepte in den Vordergrund treten, bei denen die Verarbeitung von Daten in einer Art und

55 Siehe § 2 Abs. 1 Nr. 5 UWG zur Definition von „Verhaltenskodex".
56 *Buck-Heeb/Dieckmann* (Fn. 26), S. 167, 279 f.; vgl. BGH NJW 1987, 2222 – *Komposthäcksler*.
57 *Buck-Heeb/Dieckmann* (Fn. 26), S. 96.
58 *Griss*, in: Hilty/Henning-Bodewig (Fn. 29), S. 271 ff.
59 BGH NJW 2004, 1449 (1450); BGH NJW 2001, 2019 (2020); s.a. *Dahlhaus*, rescriptum, 2017, 47 (49).
60 *Franzius*, in: Hoffman-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. I, 2006, S. 195, Rn. 30; BVerwGE 77, 285 (291 f.); 79, 254 (265); BGHZ 139, 16 (19).
61 *Menz*, in: Klindt (Hrsg.), ProdSG, 2. Aufl. 2015, § 4 Rn. 5 ff.
62 *Franzius* (Fn. 60); *Buck-Heeb/Dieckmann* (Fn. 26), S. 164 f.
63 *Röthel*, JZ 2007, 755 (759).
64 Vgl. Fn. 53.
65 EU-Kommission, Building a european data economy, 2017, S. 16.
66 EU-Kommission, ICT Standardisation Priorities for the Digital Single Market, S. 11.
67 EU-Kommission (Fn. 66), S. 3; *Spindler/Thorun* (Fn. 16), S. 56.
68 *Ronellenfitsch*, InTeR 2015, 13 (14); *Lüdemann*, ZD 2015, 247 (253).
69 *Lüdemann*, ZD 2015, 247 (253); *Bräutigam/Klindt*, NJW 2015, 1127 (1140).

Weise erfolgt, die eine Identifizierung von Personen nur mit großem Aufwand zulässt.[70] Ein zeitgemäßer Datenschutz zeichnet sich daher insbesondere durch in die Technik integrierte Datenschutzfunktionen aus, die eine Anonymisierung oder Pseudonymisierung von Daten ermöglichen.[71] Da der informationellen Selbstbestimmung Grundrechtsrang zukommt (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), ist es Aufgabe des Gesetzgebers, Eckpunkte und ein Mindestschutzniveau festzulegen.[72] So sieht die 2016 verabschiedete EU-Datenschutzgrundverordnung (DSGVO) in Art. 25 erstmalig verbindlich die Grundsätze „Privacy by Design" (Datenschutz durch Technik) und „Privacy by Default" (Datenschutz durch datenschutzfreundliche Voreinstellungen) vor.[73]

In Anbetracht der Besonderheiten von Industrie 4.0 hat die DSGVO jedoch auch die Instrumente der Selbstregulierung erheblich ausgeweitet und detailliert geregelt. Art. 40 DSGVO ermöglicht es Verbänden oder anderen Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftraggebern vertreten, der gemäß Art. 55 DSGVO zuständigen Aufsichtsbehörde Verhaltensregeln vorzulegen und so die wirksame Anwendung der VO zu erleichtern.[74] Die Behörde prüft daraufhin die Verhaltensvorschrift auf Vereinbarkeit mit der DSGVO. Ist dies der Fall und bieten die Verhaltensregeln „ausreichend geeignete Garantien" i.S.v. Art. 40 Abs. 3 DSGVO, erfolgt eine Aufnahme in das Verzeichnis für Verhaltensregeln und eine Veröffentlichung (Art. 40 Abs. 6 DSGVO). Daneben spielen Marktanreize in Form von Zertifikaten, Gütesiegeln und Audits eine entscheidende Rolle. Art. 42 Abs. 1 DSGVO sieht ein explizites, durch die EU-Mitgliedstaaten, die Aufsichtsbehörden, den Ausschuss und die EU-Kommission gefördertes Zertifizierungsverfahren vor. So kann eine effiziente Datenschutzkontrolle ermöglicht und eine nach der DSGVO ordnungsgemäße Datenverarbeitung nachgewiesen werden.[75] Zwar können auch zertifizierte Unternehmen jederzeit von behördlichen Kontrollen betroffen werden, allerdings dürfte sich eine Zertifizierung positiv auf einen risikoorientierten Prüfungsansatz einer Behörde auswirken.[76] Zusätzlich soll bei der Verhängung von Geldbußen gemäß Art. 83 Abs. 2 lit. j DSGVO die Einhaltung eines genehmigten Zertifizierungsverfahrens oder einer genehmigten Verhaltensregel gebührend berücksichtigt werden. So wurde erstmals ein finanzieller Anreiz für selbstregulierungswillige Stellen geschaffen, der angesichts des drastisch gestiegenen Bußgeldrahmens im Vergleich zum BDSG zu einer Minderung von „Free-Rider-Mitnahmeeffekten" führen dürfte.[77]

Aus den genannten Gründen können Verhaltenskodizes und Zertifikate maßgeblich zur Stärkung des Datenschutzes beitragen. Die Formulierung konkreter Rechtsfolgen oder eine verstärkte Integration der Datenschutz-Aufsicht bereits in der Entwicklungsphase von Verhaltensregeln oder Prüfkatalogen von Zertifizierungsverfahren wurde zwar verpasst. Die durch die DSGVO erstmals klare Ausgestaltung sowohl von Zertifizierungsprozessen als auch von Verhaltensregeln ist jedoch ein klarer Schritt in die richtige Richtung.[78] Angesichts dessen, dass jegliche Form der eigenen datenschutzrechtlich relevanten Standardsetzung und -durchsetzung durch Unternehmen und Vereinigungen die unabhängigen Aufsichtsbehörden einbeziehen muss, ist im Bereich des Datenschutzes nur eine Ko-Regulierung erfolgsversprechend.

2. IT-Sicherheit

Der Datenschutz ist eingebettet in die IT-Sicherheit. Wegen des unüberschaubaren Gefährdungspotenzials im Bereich von Industrie 4.0 liegt hier ein hoher Forschungsbedarf. Dabei gilt es zwischen Informationssicherheit und Betriebssicherheit zu unterscheiden. So bezeichnet Informationssicherheit den Schutz von Daten und Diensten in digitalen Systemen gegen Missbrauch (unbefugten Zugriff, Veränderung oder Zerstörung).[79] Ziel der Betriebssicherheit hingegen ist es, Gefährdungen für Menschen und Umgebung zu reduzieren, die von technischen Systemen ausgehen.[80] Denn auch in der künftigen Smart Factory bleibt der Mensch der entscheidende Produktionsfaktor. Als übergeordnete Steuerungseinheit ist er in den Produktions- und Steuerungsprozess integriert und bildet die letzte Entscheidungsinstanz auf Basis der über Big Data- und Analytics-Dienste aggregierten Daten.[81]

Diese immer stärkere Vernetzung von Systemen, Menschen und Produktionsanlagen führt zu einer signifikanten Erhöhung der Bedrohungslage im Cyberraum.[82] Bei der Umsetzung von IT-Sicherheit geht es dabei im Wesentlichen um vier anerkannte Grundwerte: Schutz der Verfügbarkeit (Gewährleistung der Funktionalität von IT-Systemen), der Integrität (Verhinderung von Manipulationen an Informationen), der Vertraulichkeit (Zugang zu Daten und Informationen nur für entsprechend Befugte) und der Authentizität (Sicherstellung der Quelle).[83] Mit dem 2015 in

70 *Krings/Mammen*, RDV 2015, 231 (231).
71 *Krings/Mammen*, RDV 2015, 231 (232).
72 *Lüdemann*, ZD 2015, 247 (254).
73 *Vander/Kinting*, Fachbereich IT-Recht: Rechtliche Aspekte im Zusammenhang mit der Digitalisierung der Wirtschaft (Überblick), 2016, S. 7.
74 *Paal*, in: ders. (Hrsg.), Datenschutz-Grundverordnung, 2017, Art. 40 DSGVO, Rn. 3.
75 *Krings/Mammen*, RDV 2015, 231 (231); *Schwartmann/Weiß*, RDV 2016, 240 (242).
76 *Schwartmann/Weiß*, RDV 2016, 68 (72).
77 Ebd.
78 *Krings/Mammen*, RDV 2015, 231 (236); *Schwartmann/Weiß*, RDV 2016, 240 (245).
79 Kagermann et al. (Hrsg.), Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Abschlussbericht des Arbeitskreises Industrie 4.0, 2013, S. 51.
80 Ebd.
81 *Siepmann* (Fn. 9), S. 69.
82 Siehe hierzu auch das vom BKA herausgegebene Bundeslagebild Cybercrime 2015, abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html (Stand: 01.09.2017).
83 *Wilmer*, in: Bräutigam/Klindt (Hrsg.), Digitalisierte Wirtschaft/Industrie 4.0, 2015, S. 107.

Kraft getretenen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) wurden diese Grundwerte erstmals im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) verankert. So sind die Betreiber kritischer Infrastrukturen nach § 8a Abs. 1 BSIG verpflichtet, ein Mindestniveau an IT-Sicherheit einzuhalten, das den Bestand dieser vier Grundwerte sicherstellt.[84] Daneben ermöglicht § 8a Abs. 2 BSIG den Betreibern und ihren Branchenverbänden, dem Bundesamt branchenspezifische Sicherheitsstandards vorzuschlagen, um die Grundwerte zu gewährleisten. Ist dies der Fall, erfolgt eine „Feststellung" durch das BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde.

Eine explizite Vermutungswirkung hat das BSIG für „festgestellte" Standards nicht statuiert, allerdings kann die Einhaltung technischer Standards wie der IEC 62443[85] bei haftungsrechtlichen Fragen an Bedeutung gewinnen. Gerade im Deliktsrecht können sich aus ihnen Art und Umfang der Herstellerpflichten ergeben. Aber auch die vertragliche Haftung wird von Standards beeinflusst. So kann die Tatsache, dass ein Produkt nach anerkannten technischen Normen oder Standards entwickelt wurde, eine taugliche Beschaffenheitsvereinbarung (§ 434 Abs. 1 S. 1 BGB) darstellen.[86] Zur Entwicklung derartiger Standards empfiehlt die Begründung zu § 8a Abs. 2 BSIG explizit die Einbeziehung des DIN als nationale Normungsorganisation. Dabei ist zu beachten, dass IT-Sicherheit immer relativ ist und gerade die Umsetzung technischer Standards wie der IEC 62443 oder ISO 27000[87] enorm aufwendig ist. Für kleine und mittlere Unternehmen ist dies in aller Regel nicht zu bewältigen.[88] Daher ist es wichtig, diese Unternehmen im Standardsetzungsprozess zu beteiligen und offene, kompatible Standards für Verschlüsselungstechniken von Daten und Informationen einzuführen, an die sich alle halten können. Auch das BSIG sieht, ähnlich wie die DSGVO, eine rechtliche Kontrolle derartiger Ko-Regulierung in Form von Zertifizierungen und Sicherheitsaudits vor (§ 8a Abs. 3 BSIG).

Mit diesen regulatorischen Bemühungen ist die Richtung für die IT-Sicherheit vorgegeben. Die Selbstregulierung soll gestärkt und ihre rechtliche Verankerung ausgebaut werden. Angesichts der im Zusammenhang mit Industrie 4.0 völlig neuen Verflechtung von Produktion und IT dürfte eine rechtlich abgesicherte Vermutungswirkung für Standards, wie im Produktsicherheitsrecht, auch im IT-Recht sinnvoll sein. Daneben ist zu beachten, dass das IT-Sicherheitsgesetz nur für Betreiber kritischer Infrastrukturen Geltung beansprucht. Dazu zählen namentlich die für die Gesellschaft bedeutsamen Versorgungssysteme, etwa aus den Sektoren Energie, Informationstechnik, Telekommunikation, Gesundheit und Wasser.[89] Da es außerhalb des Anwendungsbereichs des IT-Sicherheitsgesetzes bei den allgemeinen und wenig konkreten Vorgaben im Kontext von Organisationspflichten und Schutzmaßnahmen im Sinne des Datenschutzrechts bleibt, ist es wünschenswert, das IT-Sicherheitsgesetz mit entsprechenden Modifikationen auszubauen und so eine Anwendung auf kleinere Unternehmen zu ermöglichen. Den ersten Schritt für einen einheitlichen Mindeststandard geht die 2016 in Kraft getretene europäische NIS-Richtlinie, deren Vorgaben im BSIG zu großen Teilen schon vorweggenommen wurden. Da die IT-Sicherheit einen der entscheidenden Faktoren für den Erfolg von Industrie 4.0 darstellt, bedarf es jedoch einer stetigen Weiterentwicklung gesetzlicher und technischer Mindeststandards, um das nötige Vertrauen in digitale Systeme aufzubauen.[90]

IV. Zusammenfassende Schlussbetrachtung

Abschließend lässt sich feststellen, dass das geltende Recht durchaus Lösungsansätze bereitstellt, um die wichtigsten Herausforderungen von Industrie 4.0 zu bewältigen. Ko-Regulierung soll staatliche Regulierung daher nicht ersetzen, sondern vielmehr eine Ergänzung in ausgewählten und insbesondere untergesetzlichen Bereichen darstellen und dabei helfen, Regelungen besser durchzusetzen. Dabei ist ein Spalt zwischen der progressiven technischen Entwicklung und den Rechtsregeln nicht nur unvermeidbar, sondern auch notwendig, um das Innovationspotential von Industrie 4.0 nicht auszubremsen. Die Wahl eines technikneutralen Rechtsrahmens, der angemessen auf Entwicklungen der Technik reagieren kann, ist geboten.[91] Dem damit regelmäßig verbundenen Problem der Rechtsunsicherheit gilt es im Wege kluger Ko-Regulierung zu begegnen. Mindestanforderungen an Verfahren, Beteiligung und Transparenz von Regulierungsprozessen, eine starke Einbindung der Aufsichtsbehörden und die Definition einer eindeutigen Rechtswirkung von Verhaltenskodizes müssen europaweit hergestellt werden. Gerade Unternehmensjuristen wünschen sich daher weniger neue Regelungen als eine stärkere Harmonisierung nationaler Regulierung.[92] Gerade in den Bereichen des Datenschutzes und der Datensicherheit haben die etablierten Dienstanbieter längst begriffen, dass es keine Bürde sein muss, Regeln und wirtschaftlich faires Verhalten einzuhalten, sondern dass dies im eigenen Interesse als Marketinginstrument funktionieren kann. Ein gelungenes Wechselspiel zwischen staatlicher Einflussnahme und Selbstregulierung ist daher auch ein Liberalisierungsprogramm, das den Wirtschaftssubjekten mehr Freiheiten gibt und den Staat entlastet.

84 *Wilmer* (Fn. 83), S. 110.

85 Die IEC 62443 „Industrial Communication Networks – Network and System Security" ist die internationale Normreihe zur IT-Sicherheit in industriellen Automatisierungssystemen. Sie baut auf der ISO/IEC-Normenreihe 27000 auf und legt zusätzliche Anforderung für kritische Infrastrukturen fest; DIN e.V./DKE (Fn. 43), S. 47.

86 *Rockstroh/Kunkel*, MMR 2007, 77 (78 f.).

87 Siehe Fn. 86.

88 *Tschohl*, e&i 2014, 219 (221).

89 *Vander/Kinting* (Fn. 73), S. 10.

90 EU-Kommission (Fn. 66), S. 8.

91 EU-Kommission (Fn. 66), S. 3; *Reip* (Fn. 21), S. 25; *Latzer et al.* (Fn. 19), S. 48.

92 BDI/Noerr LLP (Hrsg.), Industrie 4.0 – Rechtliche Herausforderungen der Digitalisierung. Ein Beitrag zum politischen Diskurs, 2015, S. 9.

HERAUSGEBER
rescriptum - Akademischer Verein für rechtswissenschaftliche Publikation e.V.
Registernummer: VR 204487
Registergericht: Amtsgericht München
Vertreten durch die 1. Vorsitzende Katharina Baudisch (V.i.S.d.P.)
Stellv. Vorsitzende: Dominik Dahlhaus, Martin Heidebach, Robin Leick, Michael Rapp, Quirin Weinzierl

KONTAKT
redaktion@rescriptum.org
www.rescriptum.org

POSTADRESSE
rescriptum
Ludwig-Maximilians-Universität München
Juristische Fakultät
Prof.-Huber-Platz 2
80539 München

ABONNEMENT/ BESTELLUNG
Bestellungen richten Sie bitte an:
verkauf@rescriptum.org. Der Abopreis beträgt 6 € pro Jahr (inkl. Versand).

DRUCK
Lichtpunkt Medien
Lothstrasse 78a
80797 München

AUFLAGENHÖHE
500 Exemplare

ERSCHEINUNGSWEISE
rescriptum erscheint zweimal jährlich, jeweils im Mai und November.

EINSENDEN VON BEITRÄGEN
rescriptum veröffentlicht Beiträge von Studierenden und jungen WissenschaftlerInnen. Exposés können stets an *inhalte@rescriptum.org* eingesandt werden. Wir bitten um Beachtung der Formalia (siehe *www.rescriptum.org*).

ISSN : 2195-3120

Gegründet von Katharina Baudisch, Florian Knerr und Quirin Weinzierl.

In freundlicher Kooperation mit