November 2015

DIGITALISIERTE WIRTSCHAFT/ INDUSTRIE 4.0

Ein Gutachten der Noerr LLP
im Auftrag des BDI
zur rechtlichen Situation, zum Handlungsbedarf
und zu ersten Lösungsansätzen

Herausgegeben von
Prof. Dr. Peter Bräutigam, Noerr LLP
Prof. Dr. Thomas Klindt, Noerr LLP

BDI
Bundesverband der
Deutschen Industrie e.V.

Noerr

Vorwort

Die Digitalisierung verändert tiefgreifend und mit rasantem Tempo fast alle Bereiche von Wirtschaft, Gesellschaft und täglichem Leben. Längst gehören das Internet, mobile Kommunikation und digitale Anwendungen zum Alltag. Nun wird auch das „Internet der Dinge“ Realität: Immer mehr Produkte und Maschinen werden miteinander vernetzt. Teils evolutionär, teils disruptiv werden digitale Technologien Wertschöpfung und Innovationsprozesse verändern. Die Integration digitaler Technologien in Produkten wie Autos, Flugzeugen oder Haushaltsgegenständen, in Gebäuden und Produktion geht mit enormer Dynamik voran. Gerade die Industrie treibt diesen Wandel – und wird von ihm getrieben. Die digitale Transformation erfasst sämtliche Stufen der industriellen Wertschöpfung, von der Logistik über die Produktion bis hin zur Dienstleistung. Der industrielle Kern Deutschlands und Europas steht am Beginn einer grundlegenden Veränderung, die einen Zuwachs von 1,25 Billionen Euro an industrieller Bruttowertschöpfung und damit Wohlstand für breite Bevölkerungsschichten verheißt – oder den Verlust der Weltmarktführerschaft für deutsche und europäische Industrieunternehmen bedeuten kann.

Wenn Wirtschaft und Gesellschaft sich digitalisieren: Müssen sich dann auch die rechtlichen Rahmenbedingungen „digitalisieren“? Beeinträchtigen die Gesetze in Deutschland die Entwicklung und Nutzung digitaler Innovationen, Anwendungen und Geschäftsmodelle? Fragen wie diese rücken bei den Rechtsexperten in den Mittelpunkt der öffentlichen Diskussion. Die Anpassung des Rechtsrahmens an die Bedürfnisse der digitalisierten Wirtschaft wird von vielen als eine wesentliche Herausforderung der Digitalisierung wahrgenommen. Der BDI hat aus diesem Grund die Kanzlei Noerr damit beauftragt, in einem umfassenden Gutachten den deutschen und europäischen Ordnungsrahmen einem „Digitalisierungs-Check“ zu unterziehen. Was funktioniert gut? Welche Rahmensetzungen erweisen sich als Hindernisse? Was muss sich ändern, damit die Digitale Transformation gelingt und der Digitale Binnenmarkt in Europa Wirklichkeit wird?

Diese Publikation soll einen rechtlichen Diskurs befördern, an dem Wirtschaft und Politik, Praxis und Wissenschaft gleichermaßen teilnehmen. Ziel dieses Diskussionsprozesses muss es sein, einen wettbewerbsfähigen Rechtsrahmen für die Industrie der Zukunft zu gestalten.

November 2015

Iris Plöger
Leiterin der Abteilung
Digitalisierung und industrielle
Wertschöpfungsstrukturen, BDI

Dr. Heiko Willems
Leiter der Abteilung
Recht und Versicherung, BDI

Prof. Dr. Peter Bräutigam
Partner, Noerr

Prof. Dr. Thomas Klindt
Partner, Noerr

GLIEDERUNG

Teil 1 Executive Summary – Rechtsfragen der digitalisierten Wirtschaft, Handlungsbedarf und Lösungsansätze (*Prof. Dr. Peter Bräutigam*) 11

I. Notwendigkeit eines ständig begleitenden rechtlichen Diskurses zwischen Praxis, Politik und Wissenschaft 12
II. Notwendigkeit eines interdisziplinären Ansatzes, der nicht nur auf das Recht, sondern auf Technik, Wirtschaft und Kommunikationswissenschaften baut 12
III. Überlegungen zu etwaigen Regelungsansätzen müssen davon geleitet sein, dass sie digitale Businessmodelle zulassen und nicht Entwicklung hemmen 14
IV. Notwendigkeit internationalen, namentlich europäischen Handelns 15
V. Alle Akteure sind gefragt, neben dem Gesetzgeber insbesondere auch Behörden, Gerichte und Wirtschaft (Selbstregulierung) 16
VI. Hohes Maß an Eigenverantwortung der Unternehmen 17

Teil 2 Recht an den Daten (*Konrad Żdanowiecki*) 19

I. Daten als zentrales Wirtschaftsgut 19
1. Maschinengenerierte Daten als Kennzeichen der digitalisierten Wirtschaft 19
2. Die „Umwidmung“ und „Neuschaffung“ von Daten durch Big-Data-Verfahren 20
II. Keine klare Zuordnung unter derzeitigem Rechtsrahmen 20
1. Eigentum an Daten de lege lata (§ 90 BGB, § 823 Abs. 1 BGB [sonstiges Recht], UrhG [insb. § 87 a ff. UrhG], § 17 UWG?) 20
2. Wem gehören die Daten? 23
III. Vertragliche Gestaltungsmöglichkeiten 26
1. Relative Zuordnung der Daten durch vertragliche Regelungen 26
2. Lässt sich vertraglich eine (quasi-)absolute Zuordnung erreichen? 26
3. „Insolvenzfestigkeit“ der Zuordnung der Daten (insbesondere der Lizenz an Daten?) 27
IV. Gesetzlicher Handlungsbedarf 28
1. Rechtliche Regelung bestimmter Grundkonstellationen 28
2. Gemeinsamkeiten und Unterschiede zu bestehenden Schutzrechten 28

Teil 3 Datenschutz (*Dr. Daniel Rücker*) 30

I. Anwendbares Datenschutzrecht 30
1. International anwendbares Recht bei Anwendungen mit Auslandsbezug 30
2. Gestaltungsspielräume zur Beeinflussung des anwendbaren Rechts 31
3. Bereichs- und Sektorenspezifische Spezialregelungen 31
II. Anwendung deutschen Datenschutzrechts nur auf personenbezogene Daten 31
1. Personenbeziehbarkeit – absoluter vs. relativer Personenbezug 32
2. Anonymisierung – Anforderungen Rechtsfolgen 32
3. Pseudonymisierung: Anforderungen und Rechtsfolgen 33

III. Anwendung bestehender Grundsätze auf die digitalisierte Wirtschaft 33
1. Datenschutzrechtlich relevante Nutzungshandlungen 34
2. Verbot mit Erlaubnisvorbehalt und Rechtfertigungsmöglichkeiten 34
3. Zweckbindungsgrundsatz – Bedeutung in der digitalisierten Wirtschaft und Big Data-Konstellationen 34
4. Sonderfall Auftragsdatenverarbeitung 35
IV. Gesetzliche Rechtfertigungstatbestände 35
V. Einwilligungen: Informed Consent und systemimmenante Grenzen 36
VI. Effiziente Strukturierung datenschutzrechtlicher Rechtfertigungsmöglichkeiten 37
VII. Privacy by Design und Privacy by Default 37
VIII. Security and Data Breach Notification – Melde- und Informationspflichten bei Datenverlust 38
IX. Regulatorische Situation und Ausblick 38
1. Gestaltung von Einwilligungen 39
2. Ausweitung des Zweckbindungsgrundsatzes 39
3. Privacy by Design and Privacy by Default 39
4. Codes of Conduct 40
5. Datenschutz-Grundverordnung 40

Teil 4 Know-how-Schutz im Umfeld von Industrie 4.0 (Der Richtlinienentwurf zum Schutz von Geschäftsgeheimnissen und seine Konsequenzen für das betriebliche Vertragsmanagement) *(Sandra Sophia Redeker)*..... 41

I. Änderungen der deutschen Rechtslage aufgrund der kommenden Richtlinie zum Schutz von Geschäftsgeheimnissen 41
1. Der Begriff des Geschäftsgeheimnisses 42
2. Einheitlicher Verletzungstatbestand und Ausnahmen 43
3. Rechtsfolgen und prozessuale Geheimhaltung 43
II. Vertragliche Regelungen zum Schutz vom geheimem Know-how im Rahmen digitaler Fertigungsprozesse 44
1. Kooperationsvereinbarungen 44
2. Arbeitsverträge 45
3. Allgemeine Geschäftsbedingungen 47
III. Handlungsbedarf 47

Teil 5 Open Innovation/Kollaborationen/F&E *(Prof. Dr. Sebastian Wündisch, LL.M.)*..... 49

I. Forschung in Zeiten von 4.0 – Erscheinungsformen und Rechtsbeziehungen 49
1. Bedeutung und Erscheinungsformen 49
2. Rechtsbeziehungen 50
3. Semi-offene Innovationsprozesse 51
4. Beispiele offener Innovationsprozesse 52
II. Forschung in Zeiten von 4.0 – Rechteallokation 52
1. Exklusivität und Blockadevermeidung 53
2. Strenges Erfinder- und Schöpferprinzip und Erfordernis des abgeleiteten Erwerbs 54
III. Erfinderprinzip vs. netzwerkorientierter Eigentumsbegriff 56
IV. Schutzrechte bei Produktion nach Kundenwunsch und Verantwortung 56

V. Handlungsbedarf ... 57

Teil 6 IP-Recht in der digitalen Welt *(Sandra Sophia Redeker, Katharina Klett, LL.M., Prof. Dr. Ulrich Michel)* ... 58

I. Urheberrecht ... 58
1. Rechte an Ergebnissen aus automatisierten Prozessen (computer generated works) ... 58
2. Digital Rights Management Systeme (DRM) ... 60
3. Lizenzmodelle ... 61
4. Ausblick: mögliche Folgen aus der digitalen Agenda der EU-Kommission ... 62

II. Gewerblicher Rechtsschutz (Patentrecht, Designrecht, Wettbewerbsrecht etc.) ... 64
1. Erfinderrechte an Arbeitsergebnissen aus automatisierten Prozessen (computer generated works) ... 64
2. Standardessentielle Patente als Problem im Digitalisierungsprozess? ... 65
3. Computerimplementierte Erfindungen ... 66
4. Reformbedarf? ... 67

III. Rechtsprobleme des 3D-Drucks ... 68
1. Urheberrechtlicher Schutz ... 68
1. Gewerbliche Schutzrechte (Marken-, Design-, Patentrecht) ... 70
2. Haftung der 3D-Vorlagenportale und 3D-Druckereien ... 72
3. Reichweite des Erschöpfungsgrundsatzes bei digitalen Inhalten und Produkten ... 72
4. Bewertung des Klärungs- und Handlungsbedarfs ... 75

Teil 7 (Produkt-) Haftung/Haftung für Softwaremängel und versicherungsrechtliche Aspekte *(Prof. Dr. Thomas Klindt, Dr. Susanne Wende, LL.M., Dr. Steffen Burrer, Dr. Henning Schaloske, Konrad Żdanowiecki)* ... 76

I. Vertragliche Haftung für Software/Softwarefehler ... 76
1. Gewährleistung und Haftung bei der Lieferung/Zurverfügungstellung von Software, Maschinen und Smart Products (insbesondere im Zusammenhang mit IT-Sicherheitsmängeln) ... 76
2. Gewährleistung und Haftung für software-gestützte Dienste in der digitalisierten Wirtschaft ... 79

II. Produkthaftung ... 83
1. Maßstäbe des Produkthaftungsrechts ... 83
2. Produktsicherheit und IT-Sicherheit – Produktfehler durch Cyber-Angriffe im Produktionsprozess und durch unzureichende IT-Sicherheit am Produkt selbst ... 87
3. Risikoverteilung/Zurechnung ... 88
4. Spezielle Herausforderungen durch „Smart Products“ (Wearable computing/intelligent fashion) – neue Produktrisiken durch neue Funktionen, insbesondere bei Erfassung und Auswertung von Körperfunktionen ... 91
5. Auswirkung von Product-Lifecycle-Management-Lösungen auf die Produkthaftung ... 93
6. Die Nichtspeicherung von Funktionsdaten als Produkthaftungsfall ... 93

III. Versicherungen ... 94
1. Versicherungsbedarf infolge veränderter Risikosituation ... 94
2. Innovationsbedarf durch angepasste und neue Versicherungsprodukte ... 95

3. Kein gesetzlicher Reformbedarf ... 98
IV. Richterliche Rechtsfortbildung als alleinige Lösung? ... 99

Teil 8 Standardisierung und Produktkonformität *(Prof. Dr. Thomas Klindt, Dr. Susanne Wende, LL.M., Dr. Steffen Burrer)* ... 100

I. Standardisierung ... 100
1. Status Quo der Standardisierung und technischen Normung für die digitale Wirtschaft in Deutschland, Europa und international ... 100
2. New Approach: Rechtliche Anreizmöglichkeiten für die Entwicklung und Einhaltung technischer Standards ... 101
3. Rechtsrahmen für CEN-/CENELEC- und ETSI-Normung ... 102
II. Produktkonformitätsrecht ... 103
1. Deutscher und Europäischer Rechtsrahmen des Produktkonformitätsrechts in Zusammenschau mit der Strategie für einen digitalen Binnenmarkt in Europa ... 103
2. Werden die aktuellen Begriffe des „Herstellers“ und des „Inverkehrbringens“ den Herausforderungen der digitalisierten Wirtschaft gerecht? ... 103
3. Eignung des Konzepts der Vermutungswirkung des New Approach im Umfeld der digitalen Wirtschaft – Probleme der Normierbarkeit und der Auswahl der maßgeblichen (auch internationalen) Normen ... 105
4. Erhöhte Anforderungen an den Hersteller durch neuen Funktionsumfang von Produkten als Hindernis für die neuen Techniken, z.B. Smart Watch, Smart Textiles, Intelligent Fashion als Medizinprodukte ... 105

Teil 9 IT-Sicherheit (*Stefan Wilmer*) ... 107

I. IT-Sicherheit als determinierender Faktor der digitalisierten Wirtschaft ... 107
1. Begriff der IT-Sicherheit ... 107
2. Bedeutung in der digitalisierten Wirtschaft ... 108
II. Rechtliche Rahmenbedingungen ... 109
1. IT-Sicherheitsgesetz ... 110
2. NIS-Richtlinie der EU ... 111
3. Ausblick: Nationales Referenzprojekt zum Schutz der Produktion vor Cyberangriffen und Spionage ... 111
III. Bewertung der Rechtslage ... 112
IV. Technische Entwicklung und Gesetzgebungsprozess ... 115
1. Herausforderung ... 115
2. Denkbare Lösungswege ... 116

Teil 10 IT-Infrastruktur/Cloud (*Dr. Thomas Thalhofer*) ... 118

I. Datenschutz und Cloud ... 118
1. Das Institut der ADV – Reformbedarf für die Cloud? ... 119
2. Sonderregelungen für bestimmte Bereiche (z.B. § 203 StGB) – faktischer Ausschluss der Cloud-Nutzung? ... 122
3. Sonstige datenschutzrechtliche Hindernisse ... 124
II. Das deutsche AGB-Recht ... 127

1. Vertragliche Flexibilität als Voraussetzung für Cloud Computing – Grenzen des AGB-Recht bei Änderungen der angebotenen Leistungen 128
2. Strenge Anforderungen an Haftungsklauseln 128
III. Chancen vertraglicher Lösungen gegenüber gesetzlichen Ansätzen und konzertierter Abstimmung der Datenschutzaufsichtsbehörden 130

Teil 11 Vertragsrecht *(Tilmann Walz)*.....131

I. Vertragsschluss 131
1. „Willenserklärungen“ von autonomen Systemen 131
2. Zurechnung elektronischer Erklärungsakte zur Willenserklärung..... 131
3. Zurechnung autonomer Erklärungsakte zur Willenserklärung..... 132
4. Rechtsfähigkeit autonomer Systeme: „ePerson“ 132
II. Vertragstypen 134
1. Das Unikat als standardisiertes Produkt..... 134
2. Smart Products 136
III. Europäische Dimension 137
1. Digitale Agenda: Ausreichende Thematisierung der digitalen Produktion? 137
2. Notwendigkeit eines einheitlichen vertragsrechtlichen Rahmens? 138

Teil 12 Handelsbeschränkungen für Dual-Use-Güter (Dr. Bärbel Sachs) 140

I. Beschränkungen für den Transfer von Software und Technologie nach der EG-Dual Use VO..... 140
1. Digitalisierung der Wertschöpfungskette von der Exportkontrolle unterliegenden Gütern 140
2. Mass Customization..... 142
II. Insbesondere: Beschränkungen für Software mit kryptographischen Eigenschaften 143
1. Gelistete Kryptotechnik 143
2. Derzeitige Genehmigungserfordernisse 144
3. Lösungsansätze 145

Teil 13 Prozessrecht *(Dr. Steffen Burrer)* 146

I. Beweislast und beweisrechtliche Probleme 146
II. Zivilprozessuale Fragestellungen 147
1. Anforderungen an den substantiierten Parteivortrag bei vermuteten Fehlern in Datenverarbeitungsvorgängen 147
2. Frage der Notwendigkeit prozessualer Auskunfts-/Vorlageansprüche („e-discovery“) 148
3. Beweiswert von Datenpaketen 149
4. Auswertung von Daten durch das Gericht und Mitwirkungspflichten des Herstellers..... 149
5. Geheimnisschutz und Zeugnisverweigerungsrechte 150
6. Alternative Online-Streitbeilegung in Verbraucherangelegenheiten..... 150
7. Probleme mit nationalen Prozessregelungen angesichts internationaler Vernetzung – Internationalisierung des Prozessrechts/Stärkung der internationalen Schiedsgerichtsbarkeit..... 151

Teil 14 Kartell- und Beihilfenrecht *(Dr. Alexander Birnstiel, LL.M., Helge Heinrich, Dr. Tobias Kruis, LL.M.)*.....153

I. Digitale Wirtschaft und Kartellrecht 153
1. Herausforderungen der digitalen Wirtschaft für das Kartellrechts 154
2. Kartellrechtliche Fragen bei der Regulierung digitaler Märkte und innovativer Geschäftsmodelle 159
3. Regulierungsnotwendigkeit marktmächtiger Internetplattformen 160
II. Vernetzung der Industrie 164
1. Horizontale und vertikale Themen 164
2. Marktmacht und einseitige Wettbewerbsbeschränkungen (Standardisierung und Interoperabilität, Essential Facilities) 167
III. Big Data als neue Herausforderung des Kartellrechts 169
1. Datenschutz und Kartellrecht 169
2. Notwendigkeit veränderter Aufgreifkriterien in der Fusionskontrolle 171
3. Internet der Dinge oder „Internet of Everything 172
IV. Herausforderung der digitalen Wirtschaft für das europäische Beihilferecht 173
1. Problemaufriss 174
2. Rechtliche und politische Rahmenbedingungen 175
3. Kritikpunkte, Lösungsansätze und Perspektiven 177

Teil 15 Telekommunikationsrecht und Netzausbau *(Dr. Tobias Frevert, Dr. Michael Bergmann, Pascal Schumacher)*.....179

I. Regulatorischer Rahmen 179
II. Begrenzte Nummernressourcen 181
III. Netzneutralität 181
IV. Haftung 182
V. Netzausbau 183
VI. EU-weite Vereinheitlichung der Regulierungspraxis 184

Teil 16 Strafrecht *(Dr. Martin Schorn)*.....187

I. (Teil-)Autonome Systeme und Strafrecht 187
1. Grundüberlegungen zur strafrechtlichen Haftung bei autonomen Systemen 187
2. Besonderheiten bei der strafrechtlichen Produkthaftung 189
3. Algorithmen und Ethik: Abwägungsentscheidungen und Rechtfertigung 191
II. Strafrechtlicher Schutz gegen Angriffe in der digitalisierten Wirtschaft 193
1. Formen von Cyber-Kriminalität und Cyber-Aktivismus 193
2. Bisheriger und geplanter Rechtsrahmen 193
3. Gesetzgeberischer Handlungsbedarf 194
III. Internet der Dinge, Wearables und Augmented Reality 194
1. Kollision mit strafrechtlichem Schutz der Privatsphäre 194
2. Wearables und §§ 90, 148 TKG 195
3. Aufzeichnung von Gesundheitsdaten und deren strafrechtlicher Schutz 195

Teil 17 Gesundheitswirtschaft 4.0 (Dr. Susanne Wende, LL.M.) 196

I. Rechtliche Problemfelder im Zusammenhang mit Mobile Health Anwendungen 196

1. Unsicherheiten bei der rechtlichen Einordnung von Wearables, Health-Apps und weiteren Mobile Health-Anwendungen (als Medizinprodukte) und datenschutzrechtliche Herausforderungen im Rahmen der Anwendung 196
2. Regelungsdefizite im Rahmen der Behandlung medizinischer Software – Klassifizierung als Medizinprodukt? 201
II. Rechtliche Problemfelder im Zusammenhang mit der Gesundheits-Telematik 202
1. Interoperable IT- und Medizintechniksysteme zur Vermeidung technischer „Insellösungen“ in Krankenhäusern und Arztpraxen 202
2. Einhaltung berufsrechtlicher und vertragsarztrechtlicher Archivierungspflichten bei elektronischer Datenverwaltung und Nutzung innovativer IT- und Medizintechniksysteme (in Krankenhäusern und Praxen) 203
III. Rechtliche Hindernisse im Bereich der Telemedizin als heilberufliche Leistung 203
1. Fehlende Grundlagen der Erstattungsfähigkeit telemedizinischer Leistungen nach SGB V, EBM und GOÄ 203
2. Berufsrechtliche Hürden (MBO-Ä) und heilmittelwerberechtliche Beschränkungen (HWG) 204
IV. Der aktuelle Regierungsentwurf zum „E-Health-Gesetz“: Fortentwicklung von Telematik-Infrastruktur, Telemedizin und der elektronischen Gesundheitskarte (§ 291a SGB V) 205
1. Die elektronische Gesundheitskarte („eGK“) und Stammdatenmanagement 205
2. Telemedizin 205
3. Gesundheits-Telematik und Telematik-Infrastruktur 206
4. Datenschutzrechtliche Aspekte 207
V. Rechtsprobleme im Rahmen der Personalized Medicine – Individualisierung von Medizinprodukten (u.a. durch 3D-Druck) 207
VI. Haftungsrechtliche Aspekte der Gesundheitswirtschaft 4.0 208
1. Nichtfunktionieren als Produktfehler 209
2. Besonders hohe berechtigte Sicherheitserwartung des Patienten 209
3. Haftung bei Kombinationsrisiken 210
VII. Versicherbarkeit neuer Haftungsrisiken in der vernetzten Gesundheitswirtschaft 210
VIII. Europäische/internationale Dimension 211
1. Gesetzgebungsprozesse auf EU-Ebene: Auswirkungen der Medical Devices Regulation (MDR) auf die Gesundheitswirtschaft 4.0 211
2. Strategien auf EU-Ebene: Inhalt und Auswirkungen des Grünbuchs der Kommission zu Mobile-Health-Diensten (mHealth) und des Aktionsplans für elektronische Gesundheitsdienste 2012 – 2020 (eHealth Action Plan) 212
3. Looking abroad: Internationale Initiativen am Beispiel der US-amerikanischen FDA-Guidelines zu Mobile Medical Applications (HealthApps) sowie zu Safety and Security bei Medizinsystemen 212
4. Auswirkungen der Transatlantischen Handels- und Investitionspartnerschaft (TTIP) 213
IX. Zusammenfassung und Ausblick 214

Teil 18 Energy *(Dr. Cornelia Kermel)* 215

I. Erhebung, Verarbeitung und Nutzung von Daten 215

1. Eindeutige Regelung zur Erhebung, Verarbeitung und Nutzung aller erhobenen Daten 216
2. Mehrwertdienste müssen möglich sein 217
II. Gewährleistung der Versorgungssicherheit 218
1. Klare Abgrenzung der Verantwortungsbereiche im Zusammenhang mit dem Einbau und dem Betrieb von intelligenten Messsystemen 218
2. Schutz digitaler Energieinfrastruktur gegenüber Angriffen von außen 220
III. Verteilung der Kosten für die Digitalisierung der Energiewirtschaft 222
1. Begrenzung der Kosten für den Einbau intelligenter Messsysteme 222
2. Weitere ggf. kostenrelevante (Reform-)Vorhaben 222

Teil 1 Executive Summary – Rechtsfragen der digitalisierten Wirtschaft, Handlungsbedarf und Lösungsansätze (*Prof. Dr. Peter Bräutigam*)

Unter dem Schlagwort Industrie 4.0 wird die Vernetzung der Produktion und damit eine neue Stufe der Organisation und Steuerung der gesamten Wertschöpfungskette über den Lebenszyklus von Produkten verstanden. Diese sogenannte vierte industrielle Revolution soll nach der Erfindung der Dampfmaschine (erste Revolution), der arbeitsteiligen Fließbandproduktion (zweite Revolution) und der Automatisierung (dritte Revolution) folgen. Für das vorliegende Gutachten wurde dabei ein noch weitreichenderer Begriff herangezogen, der die Problemstellungen sämtlicher Akteure aller Wertschöpfungsstufen der digitalisierten Wirtschaft umfasst und damit auch sämtliche Anwendungen des Internets der Dinge mit einschließt.

Das Gutachten befasst sich mit den zentralen juristischen Themen der Digitalisierung. Neben der Frage der (IP-) Rechte in der digitalen Welt (Teil 2 - Recht an Daten, Teil 4 – Know-how-Schutz, Teil 5 – Open Innovation, Kollaborationen, F&E und Teil 6 – IP-Recht in der digitalen Welt) werden die wichtigen Bereiche Datenschutz (Teil 3), IT-Sicherheit (Teil 9) und IT-Infrastruktur/Cloud (Teil 10) beleuchtet. Erfasst sind weiter die intensiv diskutierten zivilrechtlichen Themen (Produkt-) Haftung einschließlich Standardisierung/Produktkonformität (Teile Teil 7 und Teil 8) und Vertragsrecht (Teil 11). Nicht zuletzt widmet sich die juristische Befassung auch den anderen Rechtsgebieten, wie Prozessrecht (Teil 13), Kartellrecht nebst den Handelsbeschränkungen für Dual-Use-Güter (Teil 14 und Teil 12), Telekommunikationsrecht (Teil 15), sowie Strafrecht (Teil 16). Abgerundet wird das Gutachten schließlich durch die nähere rechtliche Betrachtung der Situation in den ausgewählten Branchen Gesundheitswirtschaft (Teil 17) und Energy (Teil 18).

Aufbauend auf die folgende detaillierte juristische Auseinandersetzung in den verschiedenen Kapiteln lassen sich sechs Thesen aufstellen:

- *Notwendigkeit eines ständig begleitenden rechtlichen Diskurses zwischen Praxis, Politik und Wissenschaft.*
- *Notwendigkeit eines interdisziplinären Ansatzes, der nicht nur auf das Recht, sondern auf Technik, Wirtschaft und Kommunikationswissenschaften baut.*
- *Überlegungen zu etwaigen Regelungsansätzen müssen davon geleitet sein, dass sie digitale Businessmodelle zulassen und nicht Entwicklung hemmen.*
- *Notwendigkeit internationalen, namentlich europäischen Handelns.*

– *Alle Akteure sind gefragt, neben dem Gesetzgeber insbesondere auch Behörden, Gerichte und Wirtschaft (Selbstregulierung).*

– *Hohes Maß an Eigenverantwortung der Unternehmen.*

I. Notwendigkeit eines ständig begleitenden rechtlichen Diskurses zwischen Praxis, Politik und Wissenschaft

Digitalisierung fordert das Recht heraus. Es gilt, die stürmische technische Entwicklung permanent im Rahmen eines stetigen Austausches zwischen Praxis, Politik und Wissenschaft im Auge zu behalten, um rechtzeitig mit den geeigneten juristischen Instrumenten steuernd einzugreifen. Das vorliegende Gutachten ist insoweit lediglich eine Momentaufnahme , die den aktuellen Handlungsbedarf zum Status Quo identifiziert. Damit ist es jedoch für diesen unsere Zukunft massiv umgestaltenden Entwicklungsprozess nicht getan. Zu begrüßen ist deshalb die intensive Arbeit in der Arbeitsgruppe Recht der Plattform Industrie 4.0. Hier treffen Vertreter aus Politik, Wirtschaft, Wissenschaft und Gewerkschaften zusammen, damit auf allen Ebenen ein abgestimmter Entwicklungsprozess entsteht. Der genannte Arbeitskreis beschäftigt sich mit den Themen Datensicherheit und Datenschutz, Zivilrecht und Zivilprozessrecht, (Produkt-) Haftung sowie Arbeitsrecht.[1] Die Ergebnisse der Plattform sollen auf dem IT-Gipfel am 18./19.11.2015 vorgestellt werden. Auch die Universitäten sind schon längst mit Grundlagenforschung zu Aspekten der Digitalisierung befasst. Forschungsprojekte wie das DFG-Graduiertenkolleg 1681 „Privatheit“[2] an der Universität Passau, „Robot Recht“[3] an der Universität Würzburg oder das Institut für Informations-, Telekommunikations- und Medienrecht[4] der Universität Münster analysieren die rechtlichen Herausforderungen, die die digitalisierte Wirtschaft mit sich bringt. Wünschenswert wäre, die hier vorliegende Initiative des BDI, die Aktivitäten der Plattform Industrie 4.0 sowie die weiteren Initiativen[5] einzelner Bundesländer (z.B. in Baden-Württemberg, Bayern, Thüringen), der Wirtschaft und der wissenschaftlichen Forschung zusammenzuführen.

II. Notwendigkeit eines interdisziplinären Ansatzes, der nicht nur auf das Recht, sondern auf Technik, Wirtschaft und Kommunikationswissenschaften baut

Digitalisierungsprozesse zeigen dem Recht die Grenzen auf. „Die moderne, globalisierte und digitalisierte, stark fragmentierte und hochvernetzte Welt ist viel zu komplex, als dass man

---

1 http://www.plattform-i40.de/I40/Navigation/DE/Industrie40/Handlungsfelder/Rechtsrahmen/rechtsrahmen.html;jsessionid=B2C352BFAE370AB6209C2DB494554503.

2 http://www.privatheit.uni-passau.de/privatheitsforschung/ziele/.

3 http://www.jura.uni-wuerzburg.de/forschung/forschungsstelle_robotrecht/robotrecht/.

4 http://www.uni-muenster.de/Jura.itm/hoeren/.

5 http://www.plattform-i40.de/I40/Navigation/DE/In-der-Praxis/ProjekteInitiativen/projekte-und-initiativen.html.

sie mit dem staatlichen Recht vollständig durchdringen und durch staatliches Recht punktgenau steuern könnte."[6]

Recht muss deshalb offen sein für interdisziplinäre Lösungen, insbesondere mit Fachleuten aus Technik, Wirtschaft und Kommunikationswissenschaften.[7]

„Privacy by Design",[8] „Privacy by Default",[9] „(IT-)Security by Design"[10] sind prominente Schlagworte, bei denen die Realisierung des Datenschutzes oder der IT-Sicherheit durch das Recht Hand in Hand mit der Technik gesucht wird. In einem quasi symbiotischen Verhältnis normiert einerseits das Recht, das bereits im Programmierungs- und Datenverarbeitungsprozess Datenschutz bzw. Datensicherheit zu gewährleisten ist, umgekehrt wird andererseits der Datenschutz oder die Datensicherheit gerade durch bereits vorinstallierte technische Maßnahmen sichergestellt. So verweist bereits der Erwägungsgrund 46 der Datenschutzrichtlinie aus dem Jahre 1995 (Richtlinie 95/46 der Europäischen Union[11]) ebenso wie der Erwägungsgrund 61 des Entwurfs der Datenschutzgrundverordnung darauf, dass geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sowohl bei der Konzipierung der Verarbeitungsvorgänge als auch zum Zeitpunkt der Verarbeitung getroffen werden sollen.[12] Ein bekannter Anwendungsfall des *„Privacy by sign"* besteht darin, dem regelmäßig nicht versierten Endnutzer Sperr- bzw. manuelle Einstellungsmöglichkeiten an die Hand zu geben, mit denen er die Datenerhebung unterbinden kann (*„Opt-Out"*). Noch vorher greift der Ansatz *„Privacy by Default"*. Diese Methode zur Verringerung des Gefahrenpotentials für die informationelle Selbstbestimmung durch proaktive Technikgestaltung verhindert in der Ausgangsstellung, dass Daten erhoben bzw. gespeichert werden, bevor der Nutzer dies nicht ausdrücklich erlaubt (*„Opt-In"*).

Analog zu den vorgenannten Erwägungen spielt das Hand-in-Hand-Greifen von Recht und Technik auch bei der IT-Sicherheit eine große Rolle. Verfügbarkeit, Integrität der Systeme und (verschlüsselte) Verbindungen sowie die Sabotagefestigkeit (Resilienz) bei Produktion und Produkten nehmen einen fundamentalen Stellenwert ein. Auch hier sollte schon – rechtlich abgesichert – beim Entwicklungsvorgang oder weitergehend für den gesamten Lebenszyklus eines Produkts der IT-Sicherheit Beachtung geschenkt werden. Spinnt man diesen Gedanken für regulatorische Anforderungen weiter, so lässt sich durchaus über rechtliche Pflichten nachdenken, auch im Rahmen des Planungs-, Programmierungs- oder Produktionsprozesses dafür Sorge zu tragen, dass regulatorische Anforderungen „ex an-

---

6 *Volker Boehme-Neßler*, „Unscharfes Recht, Überlegungen zur Relativierung des Rechts in der digitalisierten Welt", S. 640.

7 Grundlegend hierzu *Volker Boehme-Neßler*, „Unscharfes Recht, Überlegungen zur Relativierung des Rechts in der digitalisierten Welt", S. 635 ff., insbesondere S. 642-654.

8 Gutachten, Teil 3VII. und Teil 3IX.3.

9 Gutachten, Teil 3VII., Teil 3IX.3.

10 Gutachten, Teil 9III.

11 http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:31995L0046>.

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF>; *Fraunhofer SIT*, „Entwicklung sicherer Software durch Security by Design", S. 4 ff., https://www.kastel.kit.edu/downloads/Entwicklung_sicherer_Software_durch_Security_by_Design.pdf.

te“ berücksichtigt werden. Man mag dies in Anlehnung an die obigen Schlagworte griffig *„Regulatory by Design“* nennen.

Anders als die Gesetzgebung, die auf einem langwierigen Verfahren beruht, ist die Wirtschaft prädestiniert, es im Hinblick auf Regulierung mit der rasanten technischen Entwicklung aufzunehmen. Es sind die Unternehmen selbst, die sehr dynamisch technische Innovationen vorantreiben. Sie haben deshalb die beste Ausgangslage im Zuge internationaler Zusammenarbeit, (regulierter)[13] Selbstregulierung und Teilnahme am Diskurs über juristische Normierung, Einfluss auf einen angemessenen rechtlichen Rahmen zu nehmen.

Schließlich und endlich stößt das Recht bei der Kommunikation in der digitalen Welt an seine Grenzen. Man denke nur an die langen und selbst für Juristen schwer verständlichen Einwilligungserklärungen, Informations- und Aufklärungstexte. In der Realität werden diese von Nutzern nicht gelesen, geschweige denn verstanden. Hier sollte das Recht in einer Symbiose mit den Kommunikationswissenschaften auf Visualisierung in Bildern, Trailern und kurzen Filmen und auf vereinfachende Kategorisierungen setzen, wie z.B. durch Heranziehen des Ampelsystems zum leicht fasslichen Verständnis typisierter Einwilligungen.[14]

III. Überlegungen zu etwaigen Regelungsansätzen müssen davon geleitet sein, dass sie digitale Businessmodelle zulassen und nicht Entwicklung hemmen

Es ist verständlich, dass Unternehmen, insbesondere auf europäischer Ebene, einen Rechtsrahmen fordern, der eine gleichartige Ausgangsposition für einen fairen Wettbewerb sichert (Stichworte sind Digitale Agenda,[15] Know-how-Schutz,[16] Datenschutzgrundverordnung,[17] Kartellrecht[18]). Weiter gilt es, teilweise überkommene Regelungen zu modernisieren, wie insbesondere die AGB-rechtlichen Beschränkungen im B2B-Bereich oder die stark arbeitsteilige Prozesse ignorierende Regelung des § 203 StGB, die faktisch eine Nutzung von Cloud-Diensten für berufliche Geheimnisträger rechtlich unmöglich macht.[19] Zu beachten ist aber stets, dass vielfach eher ein tastender, abwartender Ansatz nach dem Grundsatz „weniger ist mehr“ von Vorteil sein kann. Dies gilt insbesondere für den Bereich des Zivilrechts, namentlich der (Produzenten-) Haftung, aber auch der Zurechnung von Willenserklärungen und der von Verantwortlichkeiten. Hier kann auf die jahrzehntelang erfolgreiche richterliche Rechtsfortbildung gebaut werden, die auf entwickelte Grundsätze zurückgreifen und sich von Problemfeld zu Problemfeld vorarbeiten kann. Vorsichtig mit der Rechtsetzung sollte man auch bei Sachverhalten sein, in denen durch Statuierung ausschließlicher

---

13 Z.B. die Festlegung von datenschutzrechtlichen Konzepten durch Codes of Conduct, vergleiche Gutachten, Teil 3IX.4.

14 Vgl. hierzu auch *Boehme-Neßler*, „Unscharfes Recht, Überlegungen zur Relativierung des Rechts in der digitalisierten Welt“, S. 653/654, der zu Recht auf die Kraft der Bilder verweist, sowie Gutachten, Teil Teil 3IX.3.

15 Gutachten, Teil 6I.4.

16 Gutachten, Teil 4I.

17 Gutachten, Teil 3IX.5.

18 Gutachten, Teil 14.

19 Gutachten Teil 10I.2.

Schutzrechte Monopole geschaffen werden.[20] Dies gilt vor allem für die Diskussion um ein Recht an Daten allgemein; dieser Problemkreis ist noch zu wenig ausgeleuchtet und die Gefahr zu groß, faktische Zuordnungen durch gesetzliche Regelungen zu zementieren.[21]

IV. Notwendigkeit internationalen, namentlich europäischen Handelns

Digitalisierung macht nicht vor Ländergrenzen halt, sondern ist eine internationale rechtliche Herausforderung. Deshalb liegt auf europäischem Recht und europäischen Initiativen großes Gewicht. Zu nennen ist für den Datenschutz die Datenschutzrichtlinie und die Datenschutzgrundverordnung,[22] für den Know-how-Schutz die kommende Richtlinie zum Schutz von Geschäftsgeheimnissen[23] sowie für das IP-Recht in der digitalen Welt die Digitale Agenda der EU-Kommission.[24] Eine große Rolle zur Herstellung der Chancengleichheit kommt auch dem EU-Kartellrecht zu, das insoweit über hinreichend abstrakt formulierte Bestimmungen[25] verfügt, um auch die Herausforderungen der Digitalisierung (z.B. die Unentgeltlichkeit bei vielen Internetdiensten oder deren dynamische Entwicklung in unterschiedlichen Märkten[26]) zu meistern.[27] In diesem Zusammenhang steht die Diskussion der EU-weiten Vereinheitlichung der Regulierungspraxis im Bereich von Telekommunikation und Netzausbau. In Teilbereichen, wie insbesondere der Gesundheitswirtschaft, spielen die europäischen Normsetzungsinitiativen ebenfalls eine große Rolle, wie beispielsweise die Medizinprodukte-Richtlinie bei der Einordnung von Mobile Health Apps als Medizinprodukte,[28] aber auch die Bestrebungen der Kommission im Rahmen des Grünbuchs „Mobile-Health-Dienste“ und des Aktionsplans für elektronische Gesundheitsdienste 2012-2020.[29] Auch im Bereich der IT-Sicherheit ist durch die NIS-Richtlinie der EU eine europäische Vereinheitlichung der Anforderungen zu erwarten.[30] Flankierend hierzu sollten auf Ebene der europäischen Dual-Use-Verordnung Handelsbeschränkungen der für die Verschlüsselung notwendigen Kryptografie-Technik entweder de lege ferenda oder auf Behördenwege gelockert werden, um so die bestehenden Beschränkungen für den Übergang zur Industrie 4.0 abzubauen.[31]

Mit rein europarechtlichen Harmonisierungsbestrebungen ist es allerdings nicht getan, vielmehr sind letztlich globale Annäherungen, insbesondere zu Nordamerika, notwendig. Es

---

20 Gutachten, Teil 3IX.4.
21 Gutachten, Teil 2IV.2.
22 Gutachten, Teil 3IX.5, flankierend die Guidelines der Artikel-29-Gruppe, z.B. im Bereich Datenschutz und Cloud siehe Gutachten, Teil 10III.
23 Gutachten, Teil 4I.
24 Gutachten, Teil 6I.4., dabei wird es insbesondere um die Auflösung des Interessengegensatzes zwischen Nutzern und Industrie an einem gemeinsamen Single Digital Market einerseits und nationaler Kulturindustrie (insbesondere Film) andererseits gehen.
25 Vgl. Gutachten, Teil 14I.c).
26 Gutachten, Teil 14I.a).
27 Gutachten, Teil 14I., Teil 14II. und Teil 14III..
28 Gutachten Teil 17I.1.a).
29 Gutachten, Teil 17VIII.
30 Gutachten, Teil 9II.2.
31 Gutachten, Teil 12II.3.

bleibt abzuwarten, inwieweit sich die USA auf die Anforderungen einer kommenden europäischen Datenschutzgrundverordnung zubewegen werden.[32]

Von wesentlicher Bedeutung werden auch künftige, die Digitalisierung adressierende europäische und internationale Standards sein, für deren Schaffung es aber bereits ausreichende rechtliche Grundlagen gibt.[33]

Nicht zuletzt sollten international agierende Unternehmen im Bereich des Prozessrechts vorbereitet sein, Daten und Dokumentation über digitale Verfahren vorzuhalten, weil sie – namentlich im Rahmen internationaler Schiedsgerichtsbarkeit – nicht davor gefeit sind, dass dort, im Gegensatz zum deutschen Zivilprozessrecht, „Discovery"-Verfahren oder „Requests for Documents" zugelassen werden.[34]

V. Alle Akteure sind gefragt, neben dem Gesetzgeber insbesondere auch Behörden, Gerichte und Wirtschaft (Selbstregulierung)

Auch wenn die Normsetzung schwerfällig ist, sind doch für die Digitalisierung wesentliche - teilweise auch schon angestoßene – Projekte vom nationalen Gesetzgeber umzusetzen, um der Innovation bei gleichzeitiger Setzung von angemessenen Leitplanken den rechtlichen Weg zu ebnen. Wichtig ist beispielsweise die Umsetzung des neuen Energierechts (Gesetz zur Digitalisierung der Energiewende[35]). Im Bereich der Gesundheitswirtschaft ist mit dem Entwurf des E-Health-Gesetzes, der wichtige Regelungen für die Telemedizin, die Telematik-Infrastruktur und über datenschutzrechtliche Aspekte enthält, ein erster Schritt gemacht.[36] Um die Innovation bei der Software-Erstellung zu fördern, sollte über die – im internationalen Vergleich bemerkenswerte – Beschränkung der Möglichkeit der Haftungslimitierung im deutschen AGB-Recht im Verhältnis B2B nachgedacht werden.[37] Um die im Rahmen der IT-Sicherheit durchaus wichtigen Cloud-Angebote von professionellen Host-Providern für die in § 203 StGB genannten Berufsgruppen zu öffnen, ist auch die Modernisierung dieser schon längst als atavistisch zu bezeichnenden Strafrechtsnorm in Betracht zu ziehen.[38] Ausdrücklich kein gesetzlicher Regelungsbedarf besteht derzeit Im Hinblick auf die Einführung einer besonderen Rechtspersönlichkeit für künstliche Intelligenz („*ePerson*")[39] im Zivil- und Strafrecht,[40] im Hinblick auf ein „Eigentum" an Daten[41] und im Hinblick auf die Bereiche

---

[32] So kommen neue Vorschläge zu Gesetzesreformen im Bereich IT-Sicherheit und Datenschutz dem europäischen Verständnis bereits näher; https://www.datenschutzbeauftragter-info.de/obama-will-mehr-sicherheit-im-netz/.

[33] Gutachten, Teil 8I. und Teil 8II.

[34] Gutachten, Teil 13II.7.

[35] Gutachten, Teil 18I. dort mit entsprechenden Hinweisen auf Ergänzungsbedarf.

[36] Gutachten, Teil 17IV.; dort auch die Kritikpunkte am aktuellen Regierungsentwurf zum „E-Health-Gesetz".

[37] Gutachten, Teil 7I.2.

[38] Gutachten, Teil 10I.2.

[39] Gutachten, Teil 11I.4.

[40] Gutachten, Teil 16I.; die Grenze ist aber auch hier bei Sachverhalten erreicht, in denen dem Menschen keine Entscheidungshoheit wiederübergeben wird oder für diesen kein Raum mehr besteht, eine antizi-

Haftung und Haftungszurechnung.[42] Hier kann auf bewährte Grundsätze der richterlichen Rechtsfortbildung zurückgegriffen werden. Auch der Kanon der Vertragstypen im BGB muss trotz der zunehmenden Individualisierung der Produkte noch nicht erweitert werden; bis auf Weiteres kommt man hier mit dem Werklieferungsvertrag zu Rande.[43]

Eine besondere Rolle kommt dem Gesetzesvollzug, also dem Behördenhandeln und den Behördenempfehlungen zu. Dies gilt z.B. im Bereich Datenschutz für die Artikel-29-Datenschutzgruppe auf Europaebene und national für den Düsseldorfer Kreis und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Als positives Beispiel darf hier die Orientierungshilfe Cloud Computing genannt werden, die mittlerweile in einer überarbeiteten zweiten Version vorliegt und den Unternehmen einen zuverlässigen Leitfaden zur Umsetzung der rechtlichen Vorgaben bietet.[44] Behördenhandeln ist von eminenter Bedeutung im Bereich Kartellrecht[45] sowohl auf europäischer wie nationaler Ebene (In diesem Bereich wäre z.B. eine Anpassung der Leitlinien der Kommission und des Bundeskartellamtes an die neuen Herausforderungen wünschenswert.). Gleiches gilt auf dem Feld der Datensicherheit, auf dem flexibles schnelles Reagieren auf neue Bedrohungen notwendig ist.[46]

Schließlich und endlich kommt den Unternehmen selbst eine wesentliche Rolle bei der Regulierung von rechtlichen Herausforderungen der Digitalisierung zu. Dies gilt namentlich für Ansätze der Selbstregulierung (z.B. bei Audits und Zertifizierungen, wie beispielsweise nach der neuen ISO 27018, die Cloud-Anbietern die Einhaltung von Standards für Datenschutz in der Cloud bescheinigt[47]). Überhaupt trifft die Unternehmen angesichts der mit dem Instrumentarium des Rechts allein nicht befriedigend zu kontrollierenden voranstürmenden technischen Entwicklung ein hohes Maß an Eigenverantwortung.

VI. Hohes Maß an Eigenverantwortung der Unternehmen

Neben der Selbstregulierung muss es im Interesse jedes Unternehmens liegen, sich den durch die Digitalisierung redefinierten Compliance-Anforderungen zu stellen. Dies gilt namentlich für den Know-how-Schutz, für die „Lizenzierung“ von Daten als Wirtschaftsgut sowie für die Regelung der Rechteallokation bei Open Innovations, Kollaborationen und von Ergebnissen, die aus automatisierten Prozessen hervorgehen.[48] Es stellt sich die Frage, ob

---

pierte Abwägungsentscheidung zu treffen; der strafrechtliche Schutz gegen Angriffe in der digitalen Welt ist ebenfalls noch als ausreichend zu beurteilen, vgl. Teil 16II.3.

41 Gutachten, Teil 2IV.; der gleiche Befund gilt auch für Cloud-Angebote: Gutachten, Teil 10II.

42 Gutachten, Teil 7IV.; freilich wird bei Fortschreiten der Automatisierung eine Normierung (Roboterhaftung) unausweichlich sein.

43 Gutachten, Teil 11II.

44 Gutachten, Teil 10III.; die Orientierungshilfe ist abrufbar unter: http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OHCloudComputing.pdf;jsessionid=46E16F4661B02D11B6D3E7BA684453E1.1_cid329?__blob=publicationFile&v=7.

45 Gutachten, Teil 15I.

46 Gutachten, Teil 9IV.2.

47 Gutachten, Teil 10I.1.

48 Gutachten, Teil 5I., Teil 5V. und Teil 5I.3.

mit besonderem Blick auf den Mittelstand Musterklauseln für gewisse typisierte Lizenzierungssituationen geschaffen werden sollten.

Große Verantwortung obliegt den Unternehmen im Bereich IT-Sicherheit[49] und in der Regelung der arbeitsrechtlichen Bedingungen des digitalisierten Produktionsprozesses. Das vernetzte Arbeiten auch mit anderen Unternehmen erfordert es, Verantwortungsbereiche vertraglich klar abzugrenzen.

Weiter können Versicherungsunternehmen durch vermehrte Entwicklung von „Cyber-Policen“ ebenfalls zur (privatrechtlichen) Verhaltenssteuerung beitragen.[50] Nicht zuletzt haben Unternehmen angesichts des Vordringens angloamerikanischer Mechanismen wie der „Discovery“ oder des „Request for Documents“ ihre „digitale Beweislage“ abzusichern, um international, insbesondere auch vor internationalen Schiedsgerichten, prozessual gewappnet zu sein.[51] Tendenzen einer weitreichenden etwaigen Vereinheitlichung der Aufklärungs- und Mitwirkungspflichten sind dabei kritisch zu begleiten. Allenfalls bei der Beweisführung mit Datenpaketen und mit „Maschinenkommunikation“ ist an eine moderate Anpassung des Beweisrechts zu denken.[52] Schließlich erstreckt sich die Compliance auch darauf, dass die Unternehmen geeignete Schutzmaßnahmen zur Absicherung ihres geheimen Know-hows vorsehen, um die Anwendungsvoraussetzungen der europäischen Regelungen zu erfüllen.[53]

[49] Gutachten, Teil 9.
[50] Gutachten, Teil 7III.
[51] Gutachten, Teil 13II.7.
[52] Gutachten, Teil 13II.4.
[53] Gutachten, Teil 4III.

Teil 2 Recht an den Daten (*Konrad Żdanowiecki*)

I. Daten als zentrales Wirtschaftsgut

Die Digitalisierung sowohl des privaten als auch des öffentlichen Lebens wird angetrieben durch immer größere Datenübertragungskapazitäten und ständig neue Technologien zur Erfassung und Speicherung von Daten. Dies führt zu einer Explosion bei der Menge der weltweit in elektronischer Form vorhandenen Daten. Entstanden im Jahr 2005 weltweit noch 130 Exabyte,[54] so werden es 2015 voraussichtlich bereits 8.591 Exabyte und im Jahr 2020 nach aktuellen Schätzungen gar 40.026 (!) Exabyte sein.[55]

Dabei sind Daten im 21. Jahrhundert längst zu einem zentralen Wirtschaftsgut geworden. Je nach Inhalt und Kontext der in den Daten verkörperten Informationen können die Daten für denjenigen, der über sie verfügt, einen beträchtlichen wirtschaftlichen Wert darstellen. So können z.B. Messdaten zu Produktionsprozessen, Daten zum Umsatz und zur Nutzung von Produkten oder Daten zum Kundenverhalten einem Unternehmen einen entscheidenden Wettbewerbsvorteil gegenüber anderen Unternehmen verschaffen. Daher geht der Trend derzeit eindeutig zu Datengetriebenen Geschäftsmodellen („data-driven economy"). Um derartige Geschäftsmodelle zu fördern und eine EU-weite „Datenwirtschaft" zu ermöglichen, hat etwa die EU-Kommission in ihrer „Strategie für einen digitalen Binnenmarkt in Europa" die Beseitigung von entgegenstehenden technischen und rechtlichen Hemmnissen angekündigt.[56]

1. Maschinengenerierte Daten als Kennzeichen der digitalisierten Wirtschaft

Daten entstehen auch in der modernen digitalen Welt nicht aus dem Nichts. Schlägt man den Begriff „Daten" im Duden nach, so erhält man folgende Definition: *„(durch Beobachtungen, Messungen, statistische Erhebungen u. a. gewonnene) [Zahlen]werte, (auf Beobachtungen, Messungen, statistischen Erhebungen u. a. beruhende) Angaben, formulierbare Befunde*". Damit ein Datum entsteht, bedarf es somit einer Beobachtung, Messung, statistischer Erhebung oder sonstigen Aktivität, die einen Vorgang aus der Lebenswirklichkeit als Information aufnimmt und auf einem dafür geeigneten (Speicher-)Medium körperlich fixiert. In Zeiten von Smart Products und Industrie 4.0 gewinnt zunehmend die automatische Erfassung von Daten durch Maschinen und Produkte an Bedeutung. Dabei sind Maschinen etwa mit Sensoren ausgestattet, die bestimmte Vorgänge aus der Umwelt aufnehmen und diese Vorgänge mit Hilfe entsprechender Computerprogramme und Schnittstellen körperlich als elektronische Daten fixieren, entweder direkt auf einem in der Maschine integrierten Speichermedium oder auf einem separaten, über ein Netzwerk mit der Maschine verbundenen Server.

---

[54] Exabyte steht für eine Trillion Bytes, also eine Milliarde Gigabyte.

[55] http://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen.

[56] COM(2015) 192 vom 06.05.2015, Ziffer 4.2 (S. 16 f.).

Aktuelle Beispiele sind etwa Smart-Analytics-Verfahren zur Erfassung und Auswertung von Funktions- und Verbrauchsdaten von Produktionsanlagen („Smart Factory"), Telemetriedaten von Kraftfahrzeugen („Connected Car") oder auch Nutzungsdaten von internetfähigen TV-Geräten („Smart TV").

2. Die „Umwidmung" und „Neuschaffung" von Daten durch Big-Data-Verfahren

Der eigentliche Entwicklungssprung sind dabei die sog. Big-Data-Verfahren bzw. „Big Data Analytics", verstanden als Verfahren zur Analyse und Strukturierung großer Datenmengen aus unterschiedlichen Quellen mit einer hohen Verarbeitungsgeschwindigkeit zur Erzeugung wirtschaftlichen Nutzens.[57] Meistens basieren sie auf dem vom ehemaligen Yahoo-Entwickler Doug Cuttings konzipierten Hadoop-Framework, welches anhand des Dateispeichersystems HDFS[58] und des von Google entwickelten MapReduce-Algorithmus eine redundante Skalierung und parallele Verarbeitung immenser Datenmengen auf miteinander verbundenen Server-Clustern ermöglicht.

Durch Big Data Analytics können etwa die nach einzelnen Kunden oder Produktionsmaschinen erfassten Daten aus verschiedenen Quellen auf bestimmte Muster, Schnittmengen, Parallelen und Entwicklungen analysiert werden. Die erhobenen Daten werden im Rahmen der Big Data Analyse neuen Fragestellungen und Auswertungen unterworfen, z.B. zum Zwecke der Prozessoptimierung, Produktentwicklung oder dem Marketing. Durch die Sichtung der Daten auf zunächst nicht sichtbare Muster und Strukturen gewinnen die Daten einen neuen Aussagegehalt. Der vorhandenen Datenmasse werden neue Informationen entnommen, so dass letztlich neue Daten geschaffen werden.

II. Keine klare Zuordnung unter derzeitigem Rechtsrahmen

1. Eigentum an Daten de lege lata (§ 90 BGB, § 823 Abs. 1 BGB [sonstiges Recht], UrhG [insb. § 87 a ff. UrhG], § 17 UWG?)

a) Eigentum gemäß § 903 BGB?

Die umfänglichste Zuordnung der Daten zu einem Rechtssubjekt unter dem deutschen Recht wäre eine Stellung als Eigentümer. Dieser kann gemäß § 903 S. 1 BGB *„mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen"*. Das Eigentum schafft somit positiv ein umfassendes Benutzungsrecht und gleichzeitig negativ ein Verbotsrecht, mit dem der Eigentümer anderen den Zugang und die Benutzung verwehren kann.

Wie aus dem oben stehenden Zitat der Vorschrift hervorgeht, erkennt das BGB Eigentum aber nur an „Sachen" an. Gemäß § 90 BGB sind Sachen körperliche Gegenstände. Darunter fällt zwar das physische Medium auf dem die Daten gespeichert sind, z.B. die Festplatte,

---

[57] https://www.bitkom.org/Publikationen/2015/Leitfaden/Big_Data_und_Geschaeftsmodell_ Innovationen/Big_Data_und_Geschaeftsmodell_Innovationen_Leitfaden.pdf, S. 14.

[58] Hadoop Distributed Filesystem.

nach h.M. hingegen nicht die Daten selbst, verstanden als der in dem Datum zum Ausdruck kommende Informationsgehalt. Der reflexartige Schutz der Daten über die körperliche Fixierung auf einem Datenträger ist indes eher rudimentär. Zum einen stehen die Speichermedien (insb. Server) in Zeiten von Cloud Computing immer seltener im Eigentum des „Rechteinhabers" an den Daten. Zum anderen erfolgt durch das Abstellen auf den körperlichen Datenträger keine Zuweisung einer Rechtsposition an den Daten als solchen. Sobald etwa die Daten an einen Dritten übermittelt werden und dieser sie bei sich speichert, scheidet ein Substanzeingriff beim Rechteinhaber von vorneherein aus, so dass dieser gegen eine ungewollte Nutzung durch den Dritten nicht wegen einer Verletzung von §§ 823, 903 BGB vorgehen könnte.

b) Schutz als „sonstiges Recht" nach § 823 Abs. 1 BGB?

Angesichts der Digitalisierung des Wirtschaftslebens stellen Teile der Lehre die oben aufgezeigte Koppelung an körperliche Gegenstände für den Eigentumsschutz der Daten in Frage. Die Verkehrsfähigkeit der Daten, die Bedeutung dieses Wirtschaftsguts und die potentiellen Nachteile ungewollter Verarbeitung würden es rechtfertigen, das Recht an Daten als „sonstiges Recht" nach § 823 Abs. 1 BGB zu behandeln.[59] Dieser Ansatz konnte sich aber in der Rechtsprechung bisher noch nicht durchsetzen.[60]

Selbst bei den Befürwortern besteht keine Einigkeit darin, wie weit ein etwaiger Schutz nach § 823 Abs. 1 BGB gehen soll, insbesondere ob jedes einzelnen Datum geschützt ist und ob der in den Daten verkörperte Wert für die Bestimmung des Schutzbereichs maßgeblich sein soll.[61]

Fraglich wäre zudem, ob die Anerkennung als „sonstiges Recht" i.S.d. § 823 Abs. 1 BGB lediglich die negative Abwehrkomponente in Form eines Verbietungsrechts oder zugleich eine positive Nutzungsbefugnis samt Möglichkeit einer dinglich wirkenden Rechtseinräumung an Dritte beinhalten soll. In letztere Richtung gehen Überlegungen im Bereich personenbezogener Daten, wonach solche Daten ein „Splitter" des allgemeinen Persönlichkeitsrechts seien, für welches der BGH[62] eine vermögensrechtliche Stellung (samt Möglichkeit der Lizenzierung an Dritte) der betreffenden Person anerkannt hat.[63]

c) Schutz des Datenbankherstellers nach § 87a ff. UrhG

Die §§ 87 a ff. UrhG enthalten einen leistungsschutzrechtlichen Schutz einer Datenbank zu Gunsten des Datenbankherstellers. Unter einer Datenbank im Sinne des UrhG versteht § 87 a Abs. 1 S. 1 UrhG eine Sammlung von Daten, die *„systematisch oder methodisch angeord-*

---

59 So etwa *Bartsch* in Conrad/Grützmacher, Recht der Daten und Datenbanken in Unternehmen, § 22 Rn. 17 ff.; *Zech*, Information als Schutzgegenstand, 2012, 386; *Redeker,* CR 2011, 634 ff.

60 Vgl. OLG Dresden NJW-RR 2013, 27.

61 Vgl. *Bartsch* (Fn. 59), § 22 Rn. 27 ff. wonach nur *„eine Datensammlung von erheblicher Bedeutung"* geschützt sein soll.

62 BGH GRUR 2000, 709.

63 *Bräutigam,* MMR 2012, 635.

net und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert". Denkbar wäre daneben zwar grundsätzlich auch ein Schutz durch das Datenbankurheberrecht des § 4 Abs. 2 UrhG. Dieser „große Bruder" des Datenbankherstellerrechts verlangt aber ein Datenbankwerk und damit eine persönliche geistige Schöpfung im Sinne des § 2 Abs. 2 UrhG, welche bei der reinen technischen Erfassung und Aktualisierung der Daten in einem Datenbanksystem in der Regel nicht vorliegen wird

Im Hinblick auf das Datenbankherstellerrecht ist zum einen zu beachten, dass nach Ansicht der Gerichte[64] die „Beschaffung" der Daten nicht auch die Aufwände für deren Erzeugung umfasst. Deshalb sind etwa die Investitionen in die Entwicklung, die Installation und den Betrieb von Messsensoren nicht berücksichtigungsfähig, sondern erst die Einstellung und Pflege der Daten in die Datenbank sowie die Kosten für Software und Infrastruktur.

Zum anderen ist Schutzgegenstand der §§ 87 a ff. UrhG die Datenbank in ihrer Gesamtheit, nicht hingegen die einzelnen Daten. Dies verdeutlicht § 87b Abs. 1 S. 1 UrhG, wonach sich das Ausschließlichkeitsrecht des Datenbankherstellers grundsätzlich auf „*die Datenbank insgesamt oder einen nach Art oder Umfang wesentlichen Teil der Datenbank*" beschränkt. Das Wesentlichkeitsmerkmal wird nach der Rechtsprechung quantitativ wie qualitativ bestimmt. Pauschale Aussagen verbieten sich zwar, jedenfalls eine Entnahme von 10 % des Datenbankinhalts sieht der BGH nicht als „wesentlich" an.[65]

Eine Entnahme oder Weiterverwendung von unwesentlichen Teilen kann der Datenbankhersteller nur dann untersagen, „*sofern diese Handlungen einer normalen Auswertung der Datenbank zuwiderlaufen oder die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen*". Grundsätzlich kann die Nutzung einzelner Datenbankinhalte somit nicht unter Berufung auf das Datenbankherstellerrecht verhindert werden.

d) Geheimnisschutz nach §§ 17, 18 UWG

Sofern Daten Betriebs- oder Geschäftsgeheimnisse darstellen, sind sie grundsätzlich nach §§ 17, 18 UWG zivilrechtlich und strafrechtlich geschützt. Dabei handelt es sich aber zum einen wiederum nicht um eine dem Eigentum vergleichbare positive Zuordnung, sondern negativ um ein Abwehrrecht. Zum anderen setzt die Verwirklichung dieser Tatbestände auch eine subjektive Komponente auf Täterseite in Form von bestimmten Motiven voraus.[66] Darüber hinaus erfassen die betreffenden Tatbestände nicht sämtliche Arten der Datenverwendung, die der Inhaber des Betriebs- oder Geschäftsgeheimnisses möglichweise verhindern möchte.

---

[64] EuGH MMR 2005, 29 – BHB-Pferdewetten; EuGH, GRUR 2005, 252 – Fixtures-Fußballspielpläne I; EuGH, GRUR 2005, 254 – Fixtures-Fußballspielpläne II; BGH, MMR 2005, 754 – HIT BILANZ.

[65] BGH GRUR 2011, 724.

[66] Umfasst sind Handlungen „*zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen*".

So kann Täter eines Geheimnisverrats nach § 17 Abs. 1 UWG nur eine bei dem Unternehmen beschäftigte Person sein. Mitarbeiter anderer Unternehmen scheiden von vorneherein aus.

Der Tatbestand der Betriebsspionage nach § 17 Abs. 2 UWG setzt voraus, dass der Täter sich das Geschäfts- oder Betriebsgeheimnis „unbefugt verschafft oder sichert". Fraglich ist das Vorliegen eines unbefugten „Verschaffens" oder „Sicherns" etwa dann, wenn zwei Unternehmen in Produktion oder Vertrieb zusammenarbeiten und das eine Unternehmen Daten über die Produktionsanlagen oder Produkte des anderen Unternehmens selbst generiert (etwa durch Messungen mithilfe eigener Maschinen). Die Verwendung der generierten Daten zu den Produktionsanlagen des Vertragspartners für eigene Zwecke stellt wohl nicht automatisch ein unbefugtes Sich-Verschaffen oder Sichern dar.

§ 18 UWG schützt nur „*Vorlagen oder Vorschriften technischer Art, insbesondere Zeichnungen, Modelle, Schablonen, Schnitte, Rezepte*" und umfasst deswegen von vornherein viele der heutzutage wirtschaftlich relevanten Datenkategorien nicht, etwa Messdaten von Produktionsanlagen oder Big-Data-Analyseergebnisse.

e) Zwischenfazit: Kein „Eigentum" an Daten nach geltendem Recht

Es ist somit festzuhalten, dass nach herrschender Ansicht *de lege lata* weder ein Eigentum an Daten im Sinne des § 903 BGB noch ein dem Eigentum vergleichbares Recht mit absoluter (d.h. dinglicher) Wirkung gegenüber dem gesamten Rechtsverkehr besteht.

Bei Vorliegen der jeweiligen Tatbestandsvoraussetzungen können bestimmte Abwehrrechte gegen einen Zugriff auf Daten und/oder deren Verwendung gegeben sein, etwa die §§ 87 a ff. UrhG oder § 17 UWG. Diese enthalten aber keinen positiven Zuweisungsgehalt an einen bestimmten Rechtsträger und enden häufig dort, wo die Daten willentlich und wissentlich die Sphäre dieses Rechtsträgers verlassen haben oder gar von dem Dritten erzeugt wurde.

2. Wem gehören die Daten?

Die Begründung eines Eigentums oder einer eigentumsähnlichen Stellung würde voraussetzen, dass klare Regelungen und Kriterien für eine absolute Zuordnung zu einem Rechtsträger vorhanden sind. So regelt etwa das Sachenrecht konkret die Voraussetzungen für einen originären (z.B. §§ 946 ff. BGB) oder derivativen (z.B. §§ 929 ff. BGB) Erwerb von Eigentum. Immaterialgüterrechte entstehen durch Erfüllung der Tatbestandsvoraussetzungen des jeweiligen Spezialgesetzes, etwa Eintragung in das Markenregister (z.B. § 4 Nr. 1 MarkenG), Veröffentlichung im Patentblatt (§ 58 Abs. 1 S. 3 PatG), die Entstehung des Werks durch einen schöpferischen Akt (§ 2 Abs. 2 UrhG) oder die Herstellung einer Datenbank (§ 87a UrhG).

Fraglich ist, nach welchen Kriterien die rechtliche Zuordnung von erzeugten Daten erfolgen soll. Überwiegend wird dabei auf wirtschaftliche Gesichtspunkte abgestellt. Uneinigkeit herrscht indes darüber, welche wirtschaftlichen Gesichtspunkte dies sein sollen. Von den Befürwortern eines Eigentums an Daten wird wohl überwiegend auf den sog. „Skripturakt“ als den Moment der Datenerzeugung abgestellt.[67] Dies lässt aber die Frage unbeantwortet wem der Skripturakt rechtlich zugerechnet werden soll, wer mithin als der „Datenerzeuger“ gilt.

Die nachfolgenden Beispiele zeigen lediglich exemplarisch einige der denkbaren Konstellationen auf, in denen eine Zuordnung nach derzeitiger Gesetzeslage im relativen Verhältnis zwischen den Beteiligten problematisch sein kann. Dieser Konflikt würde sich noch verstärken, sofern man ein absolut gegenüber Jedermann geltendes Recht an den Daten schaffen wollte.

a) Daten werden im Rahmen der Nutzung durch Kunden aufgezeichnet; Hersteller möchte sie auswerten

So bestehen etwa unterschiedliche Auffassungen darüber, wem die bei der Benutzung eines erworbenen Produkts erzeugten Messdaten gehören sollen, z.B. bei einem Automobil oder einem Smart TV.

In der Literatur wird teilweise vertreten, dass die Erzeugung, verstanden als der Vorgang des Codierens der Informationen in einer für Maschinen lesbaren Zeichenfolge, wirtschaftlich betrachtet durch den Betreiber des Maschine – also z.B. dem Fahrzeughalter – erfolgt.[68] Daran ist richtig, dass die Kosten des Betriebs der Maschine vom Halter getragen werden. Die Hersteller der Maschine argumentieren naturgemäß oft gegenteilig und beanspruchen das Recht an den Daten für sich, mit dem Hinweis, dass sie die Herstellungs- und/oder Entwicklungskosten für die der Erfassung zugrundeliegende Technologie tragen und dass die Daten gerade das Produkt und seine Weiterentwicklung betreffen.

Folgt man der letztgenannten Auffassung, wird die Zuordnung noch komplizierter, wenn mehrere Unternehmen einen Beitrag zu den Daten erfassenden Komponenten der Maschine beigesteuert haben. Kooperiert etwa ein Automobilhersteller bei der Herstellung des „vernetzten Autos“ mit einem Anbieter von Navigationsgeräten, dürften häufig beide Unternehmen ein Interesse an den Fahrdaten des Kunden haben.

b) Mehrere Beteiligte erfassen/generieren Daten im Rahmen einer Produktions- oder Vertriebskette

Ein Unternehmen kann sich von der Entwicklung über die Produktion bis zum Vertrieb seiner Produkte zahlreicher Partner bedienen, etwa eines Zulieferers von Einzelkomponenten oder eines Distributors beim Verkauf der Produkte. Dabei können für den Hersteller des

---

[67] *Hoeren*, MMR 2013, 486, 487; *Zech*, CR, 2015, 137, 144.
[68] *Zech*, CR, 2015, 137, 144.

Gesamtprodukts (etwa eines Automobils) auf allen Stufen erzeugte Daten relevant sein. So kann es für den Hersteller etwa von Bedeutung sein, welche Zeiten bei der Produktion der einzelnen Komponenten angefallen sind und ob dabei bestimmte Probleme aufgetreten sind. Beim Vertrieb kann der Hersteller möglicherweise anhand von Lagerzeiten Optimierungspotential bei den einzelnen Vertriebskanälen erkennen. Gleichzeitig haben auch der Zulieferer und der Vertriebspartner berechtigte wirtschaftliche Interessen an einer Nutzung der Daten. So arbeitet der Distributor möglicherweise mit mehreren Herstellern zusammen und möchte wissen, wessen Produkte sich am schnellsten weitervertreiben lassen.

Ohne anderweitige vertragliche Absprache sind die Daten grundsätzlich demjenigen Beteiligten in der Kette zuzuordnen, der den wirtschaftlich-organisatorischen Aufwand für deren Erzeugung (sprich: die Kosten) trägt. Wie ist aber etwa der Fall zu beurteilen, dass das fertig produzierte Automobil über Sensoren (z.B. RFID-Chips) verfügt, die bei der An- und Auslieferung beim Distributor am Lagereingang und -ausgang über entsprechende Antennen erfasst werden?[69] Hier können gegebenenfalls sowohl Hersteller als auch Distributor Zugriff auf und ein Interesse an den erzeugten Daten haben.

c) Big-Data-Analyse von durch Dritte erfassten/generierten Daten und Schaffung neuer Aussagen/Zusammenhänge dieser Daten

Nicht ganz einfach zu beantworten ist die Frage der wirtschaftlichen Zuordnung auch in der Konstellation, dass ein Unternehmen für ein anderes Unternehmen Daten durch Analyseverfahren auswertet und dadurch Daten mit einem eigenständigen Aussagegehalt schafft (vgl. oben I. 2.). Besonders virulent wird die Thematik der Zuordnung dann, wenn der Dienstleister nicht solche Datensätze analysiert, die er vom Auftraggeber erhalten, sondern solche, die er selbst erhoben hat. Letzteres ist z.B. bei Smart-Analytics-Verfahren in Produktionsanlagen der Fall, bei denen der Dienstleister die erforderlichen Tools für die Erfassung, Speicherung und Auswertung der Messdaten zur Verfügung stellt. Hier vertreten die Dienstleister die Ansicht, dass die erzeugten Messdaten grundsätzlich ihnen als Träger der wirtschaftlichen Aufwände zustehen und sie etwa auch als Datenbankhersteller nach § 87 a UrhG anzusehen sind.[70] Auch wenn in diesem Fall in aller Regel entsprechende vertragliche Abreden zugunsten des Auftraggebers bestehen dürften, zeigt sich, dass eine wirtschaftliche Zuordnung im Rahmen der Diskussion um ein „Recht an Daten“ häufig zu schwierigen Abgrenzungsfragen führt.

Trotz des Auftragscharakters solcher Dienstleistungen wären insbesondere nach Vertragsbeendigung ohne explizite vertragliche Regelung Herausgabeansprüche des Auftraggebers gegen den Auftragnehmer nicht völlig unproblematisch. Zwar wäre an einen Anspruch aus § 667 BGB (analog) zu denken, allerdings umfasst diese Regelung von ihrem Wortlaut her

[69] Beispiel nach *Hofmann*, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, 729.
[70] *Peschel/Rockstroh* in Big Data & Co, Tagungsband DSRI-Herbstakademie 2014, 309, 313.

nur das, was der Auftragnehmer im Rahmen der Auftrags „erhält“ oder „erlangt“ hat. Von Auftragnehmer selbst generierte Daten fallen nicht darunter.[71]

III. Vertragliche Gestaltungsmöglichkeiten

1. Relative Zuordnung der Daten durch vertragliche Regelungen

Nach derzeitiger Gesetzeslage kann ein effektiver Schutz der Daten nur durch hinreichend eindeutige vertragliche Regelungen zwischen den an der Datenerzeugung, -verarbeitung und -nutzung Beteiligten erreicht werden. Dies ermöglicht eine rechtlich verbindliche Zuordnung zwischen demjenigen der die Daten durch Initiierung des konkreten Erfassungsvorgangs erzeugt und demjenigen der (ebenfalls) ein wirtschaftlicher Interesse an der Verwertung hat. Dies gilt gleichermaßen auf den nachgelagerten Stufen zwischen verschiedenen an der wirtschaftlichen Nutzung der Daten Beteiligten.

Dabei sollte eindeutig festgelegt werden, welcher Vertragspartner über welche Nutzungsrechte verfügen soll und welche Verwertungshandlungen explizit ausgeschlossen sind, insbesondere ob und mit welchen Dritten die Daten geteilt werden dürfen. Da aber faktisch nicht alle aktuell oder zukünftig denkbaren Verwertungshandlungen vertraglich erfasst werden können, sollte der Vertrag eine grundsätzliche Aussage darüber treffen, welche der Vertragsparteien im Innenverhältnis als „Herr der Daten“ anzusehen ist.

Bei einer entsprechenden kommerziellen Bedeutung sollte der jeweilige „Herr der ten“ erwägen, etwaige Verstöße der Gegenseite gegen ihre zentralen Vertragsverpflichtungen durch adäquate Vertragsstrafen zu sanktionieren. Dies auch deshalb, weil Verstöße gegen Datenorientierte Vertragspflichten, etwa Geheimhaltung und Sicherheit, für das betroffene Unternehmen immense Nachteile mit sich bringen können, bei denen sich aber die konkrete Schadensberechnung häufig schwierig gestaltet (z.B. Offenbaren von Betriebsgeheimnissen, Imageschäden).

2. Lässt sich vertraglich eine (quasi-)absolute Zuordnung erreichen?

Grundsätzlich gilt der Grundsatz von der Relativität des Schuldverhältnisses. Das bedeutet, dass vertragliche Regelungen auch nur zwischen den beteiligten Vertragsparteien wirken. Daher kann eine nicht gestattete Nutzung der Daten durch nicht am Vertrag beteiligte Dritte nur durch etwaige gesetzliche Ansprüche (s.o. bei II.), nicht aber auf Basis des Vertrags, unterbunden werden.

Durch eine Kombination aus der faktischen Möglichkeit zum Schutz von nicht öffentlich zugänglichen Daten, etwa durch entsprechend technisch-organisatorische Maßnahmen, sowie entsprechenden vertraglichen Maßnahmen (s.o.), kann man aber ggf. zumindest in Grenzen faktisch eine quasi-dingliche Wirkung durch die Verhinderung des Zugangs durch unbefugte Dritte erzielen.

---

[71] *Grützmacher*, ITRB 2004, 260, 262.

Je länger aber die Vertragskette der an der Verwertung Beteiligten wird, desto mehr kommen die Daten dadurch in „Umlauf“. Eine Kontrolle wird dem „Herrn der Daten“ dadurch zunehmend erschwert. Daher sollte der Vertragspartner stets darauf verpflichtet werden, die vertraglichen Beschränkungen zur Nutzung und Weitergabe in der Vertragskette (etwa an Subunternehmer) durchzureichen. Wichtig kann in diesem Zusammenhang eine Kontrolle der Datennutzung durch den Vertragspartner bzw. die weiteren Datenempfängen sein. Der Vertrag sollte dazu entsprechende Auditrechte enthalten.

3. „Insolvenzfestigkeit“ der Zuordnung der Daten (insbesondere der Lizenz an Daten?)

Gewährt ein Unternehmen einem anderen Unternehmen auf vertraglicher Basis eine Lizenz zur Nutzung bestimmter Daten, kann sich die Frage stellen, welche Auswirkungen die Insolvenz des Lizenzgebers auf das Nutzungsrecht des Lizenznehmers hat. Hier dürfte zu unterscheiden sein:

Sofern das Nutzungsrecht zeitlich beschränkt gewährt wurde, wird dies als Miete oder Pacht, in jedem Fall aber als ein Dauerschuldverhältnis, einzustufen sein. In dieser Konstellation trifft den Lizenzgeber während der Vertragsdauer die fortlaufende Plicht, dem Lizenznehmer die Datennutzung zu gestatten und zu ermöglichen. Somit handelt es sich um einen noch nicht beiderseits erfüllten Vertrag, für den dem Insolvenzverwalter das Wahlrecht des § 103 InsO zusteht. Wählt der Insolvenzverwalter die Nichterfüllung, endet das Nutzungsrecht des Lizenznehmers.

Anders kann dagegen der Fall zu bewerten sein, dass dem Lizenznehmer die Daten dauerhaft überlassen werden. Parallel zur dauerhaften Überlassung von Software ist in dieser Konstellation von einem Kaufvertrag über die betreffenden Daten (bzw. genauer: über eine Kopie dieser Daten) auszugehen. Sind die Daten übergeben und hat der Lizenznehmer den Kaufpreis vollständig entrichtet, könnte man den Vertrag durchaus bereits als beiderseitig erfüllt ansehen. Zu berücksichtigen ist jedoch, dass bereits das Bestehen von noch nicht erfüllten Nebenpflichten zu einer Anwendbarkeit des § 103 InsO führen kann. Dazu können etwa Pflichten zur Vornahme von Maßnahmen zur Datensicherheit oder zur Anbringung von Urheberrechtsvermerken gehören. Hält man § 103 InsO für anwendbar, wäre zu erwägen, ob die Rechtsprechung des BGH[72] und des OLG München[73] zu Softwarelizenzen entsprechend anwendbar ist, wonach die Nichterfüllung nach § 103 InsO nicht dazu führt, dass vor der Insolvenzeröffnung eingeräumte Nutzungsrechte erlöschen. Einerseits bezieht sich das Urteil ausweislich seiner Begründung auf einen „dinglichen Rechtsübergang“, welcher bei Daten mangels entsprechender Rechtsstellung des Lizenzgebers gerade nicht vorliegt. Andererseits sind die beiden Konstellation aus wirtschaftlichen Gesichtspunkten durchaus vergleichbar, was für ein Fortbestehen des Datennutzungsrechts beim Lizenznehmer sprechen würde.

---

[72] BGH GRUR 2006, 435.
[73] OLG München GRUR 2013, 1125.

Unabhängig davon stellt sich die Frage, welche Konsequenzen eine Weiternutzung der Daten durch den (ehemaligen) Lizenznehmer bei einem Fortfall der Lizenz hätte. Anders als bei einer Lizenz für Software oder für sonstige Immaterialgüterechte bestehen keine spezialgesetzlichen Ansprüche wegen des unberechtigten Eingriffs in das Immaterialgüterrecht, etwa auf Unterlassung und Schadensersatz nach § 97 UrhG. Sofern man das Recht an Daten nicht als „sonstiges Recht" gemäß § 823 BGB anerkennen möchte (s.o.), bleibt dem Lizenzgeber als Abwehranspruch nur § 17 UWG. Hier wäre dann im Einzelfall näher zu prüfen, ob die Verwendung der Daten durch den Lizenznehmer nach dem Ende des Lizenzvertrags ein unberechtigtes „Sich-Verschaffen" darstellen kann.

IV. Gesetzlicher Handlungsbedarf

Die Frage, ob gesetzgeberischer Handlungsbedarf im Hinblick auf ein „Recht an Daten" besteht, wird allgemein sehr unterschiedlich beurteilt. Teilweise wird eine gesetzliche Ausgestaltung eines Rechts des Datenerzeugers[74] gefordert. Andere verneinen das Bedürfnis nach der Schaffung gesetzlicher Vorschriften für ein Dateneigentum oder vergleichbarer absolute Rechtsstellungen.[75]

1. Rechtliche Regelung bestimmter Grundkonstellationen

Es ist zweifelhaft, ob der Gesetzgeber die zahlreichen Konstellation im Zusammenhang mit der Zuordnung von Daten befriedigend lösen könnte. Ein spezielle Regelung für einzelne konkrete Datenerzeugungsvorgänge, etwa speziell für die Messdaten bei Fahrzeugen oder Produktionsanlagen, würde nicht das Problem der grundsätzlichen Zuordnung von Daten lösen und wäre zudem möglicherweise durch die technische Entwicklung nach kurzer Zeit wieder überholt.

2. Gemeinsamkeiten und Unterschiede zu bestehenden Schutzrechten

Ob generell ein umfassendes „(Geistiges) Eigentum an Daten" geschaffen werden sollte, ist eine rechtspolitische Frage. Da es sich letztlich um den Schutz eines Immaterialguts handeln würde, wäre sehr sorgfältig zu prüfen, ob sich ein solches „(Geistiges) Eigentum an ten" in die Systematik der bestehenden Schutzrechte innerhalb der deutschen Rechtsordnung einfügt.

Bestimmte Gemeinsamkeiten sind nicht von der Hand zu weisen. Den in den Daten verkörperten Informationen kann eine große wirtschaftliche Bedeutung zukommen. In gewissen Konstellationen mag es angemessen erscheinen, einem Unternehmen, welches substantielle Aufwendungen für die Erzeugung der Daten aufgewandt hat, gemäß dem urheberrechtlichen Gedanken des Partizipationsinteresses einen Schutz vor Ausbeutung zu gewähren.

---

[74] Vgl. etwa *Zech*, CR, 2015, 137, 146.
[75] Vgl. etwa *Dorner*, CR 2014, 617, 626.

Dennoch sind auch signifikante Unterschiede zu den *de lege lata* geschützten Immaterialgütern nicht zu verkennen: Wie bereits dargestellt, fehlt ein einheitliches Verständnis darüber, welcher Akt für die Entstehung und Zuordnung eines solchen Ausschließlichkeitsrechts maßgeblich sein soll. Die oben beschriebenen Beispiele zeigen exemplarisch, dass insbesondere die Frage der wirtschaftlichen Zuordnung nicht einfach zu beantworten ist (s.o. bei II.2.). In jedem Fall dürfte durch ein solches Dateneigentum auch nicht der immaterialgüterrechtliche Grundsatz angetastet werden, wonach allgemein zugängliche Informationen gemeinfrei bleiben und nicht monopolisiert werden.

Die juristische Diskussion zu rechtlich schützenswerten Interessen an Daten ist im Fluss und wird auch durch die immer neuen technischen Möglichkeiten dynamisch beeinflusst. Hier sollten statische Zuordnungen jedenfalls nicht vorschnell durch eine gesetzliche Regelung zementiert werden.

Teil 3 Datenschutz (*Dr. Daniel Rücker*)

I. Anwendbares Datenschutzrecht

Die Vernetzung von Maschinen und Prozessen sowie Big Data Anwendungen machen im Zeitalter der Globalisierung keinen Halt an Landesgrenzen. Auch aus datenschutzrechtlicher Sicht stellt sich damit schon die Frage, welches nationale Recht überhaupt anwendbar ist.

1. International anwendbares Recht bei Anwendungen mit Auslandsbezug

a) Aktuelle deutsche Rechtslage

Innerhalb der Europäischen Union ist das Datenschutzrecht bereits heute in weiten Teilen harmonisiert.[76] Dabei gilt im Grundsatz das sog. Territorialitätsprinzip, wonach das Recht desjenigen Landes anwendbar ist, in dessen Territorium die betroffene Erhebung, Verarbeitung oder Nutzung personenbezogener Daten stattfindet.[77] Erhebt, verarbeitet oder nutzt also beispielsweise ein US-Unternehmen ohne Sitz in der EU personenbezogene Daten in Deutschland, so gilt hierfür deutsches Datenschutzrecht.[78] Abweichend hiervon findet zur Abgrenzung des anwendbaren Datenschutzrechts für innerhalb der EU ansässige Unternehmen das sog. Sitzlandprinzip Anwendung. Danach ist das Datenschutzrecht desjenigen EU-Mitgliedsstaates anwendbar, in dem das betroffene Unternehmen seinen Sitz hat, auch wenn es personenbezogene Daten in anderen EU-Mitgliedsstaaten erhebt, verarbeitet oder nutzt.[79] Hat aber das betroffene Unternehmen in dem EU-Mitgliedsstaat, in dem die Erhebung, Verarbeitung oder Nutzung stattfindet, auch eine Niederlassung, so gilt wieder das Territorialitätsprinzip. Es findet damit das Recht des EU-Mitgliedsstaates Anwendung, in dem die Erhebung, Verarbeitung oder Nutzung stattfindet (und nicht etwa das Recht des EU-Mitgliedsstaates, in dem das Unternehmen seinen Hauptsitz hat).[80]

b) Auswirkungen der geplanten Europäischen Datenschutz-Grundverordnung

Erhebliche Änderungen bei der Bestimmung des anwendbaren Rechts wird die derzeit in Entstehung befindliche Europäische Datenschutz-Grundverordnung mit sich bringen. Anders als die bisherigen Europäischen Richtlinien zum Datenschutz findet diese Verordnung direkte Anwendung, bedarf also keiner Umsetzung in die nationalen Rechtsordnungen der Mitgliedsstaaten. Nach dem aktuellen Verhandlungsstand[81] zum Entwurf der Datenschutz-

---

[76] Grundlage der europäischen Harmonisierung ist die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (*„EU-DSRL“*).

[77] Art. 4 EU-DSRL , § 1 Abs. 5 BDSG.

[78] Art. 4 Abs. 1 lit. c) EU-DSRL, § 1 Abs. 5 S. 2 BDSG.

[79] Art. 4 Abs. 1 lit. a) S. 1 EU-DSRL, § 1 Abs. 5 S. 2 Hs. 1 BDSG.

[80] Art. 4 Abs. 1 lit. a) S. 2 EU-DSRL, § 1 Abs. 5 S. 2 Hs. 2 BDSG.

[81] Hierzu der Vorschlag der Kommission vom 25.01.2012, der Beschluss des Europäischen Parlaments vom 12.03.2014 und zuletzt der Vorschlag des Rates vom 15.06.2015 für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (*„DS-GVO-E“*).

Grundverordnung soll zudem das sog. „Marktortprinzip“ gelten, so dass Europäisches Datenschutzrecht auch dann gilt, wenn ein Unternehmen weder eine Niederlassung in der EU hat, noch Daten innerhalb der EU erhebt, verarbeitet oder nutzt. Vielmehr führt das Marktortprinzip schon dann zu einer Anwendung der Europäischen Datenschutz-Grundverordnung, wenn ein Unternehmen Daten verarbeitet, um „Personen in der Union Waren oder Dienstleistungen anzubieten.“[82]

Mittelfristig würden danach die Datenschutz-Grundverordnung und das Marktortprinzip die derzeit noch geltenden Regeln des Territorialitäts- und Sitzlandprinzips verdrängen. Wann die Datenschutz-Grundverordnung genau in Kraft tritt, ist derzeit noch offen und insbesondere vom Fortschritt der Verhandlungen der hiermit befassten Gremien abhängig. Der aktuelle Entwurf sieht für die verbindliche Geltung zudem eine Übergangsfrist von zwei Jahren ab Inkrafttreten vor.[83]

2. Gestaltungsspielräume zur Beeinflussung des anwendbaren Rechts

Insbesondere nach der oben skizzierten aktuellen Rechtslage innerhalb der EU bestehen durchaus gewisse Gestaltungsspielräume, ein konkret gewünschtes Recht zur Anwendung zu bringen, etwa durch die gezielte Wahl des Sitzes von Unternehmen und/oder des Ortes, an dem die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten stattfindet. Innerhalb der EU wird sich dies aber mit Inkrafttreten der geplanten EU-Datenschutz-Grundverordnung und dem dann geltenden Marktortprinzip ändern.[84]

3. Bereichs- und Sektorenspezifische Spezialregelungen

Selbst wenn man nach der noch aktuellen Rechtslage zur Anwendung deutschen Datenschutzrechts kommt, sind nicht alle datenschutzrechtlichen Vorschriften zentral im Bundesdatenschutzgesetz (BDSG) geregelt, sondern vielmehr auf zahlreiche bereichsspezifische Spezialregelungen verteilt, etwa im Telekommunikationsgesetz (TKG) für telekommunikationsspezifische Datenschutzvorschriften oder im Telemediengesetz (TMG) für bestimmte in Zusammenhang mit der Nutzung von Telemedien (z.B. Online-Plattformen) anfallende Daten.

II. Anwendung deutschen Datenschutzrechts nur auf personenbezogene Daten

Nur personenbezogene Daten unterfallen dem Anwendungs- und Schutzbereich deutschen Datenschutzrechts.[85] „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffe-

---

82 Art. 3 Abs. 2 lit. a) DS-GVO-E.

83 Art. 91 Abs. 2 DS-GVO-E.

84 Siehe dazu Teil 3I.1. des Gutachtens.

85 Anders verhält es sich etwa in Österreich: Das österreichische Bundesgesetz über den Schutz personenbezogener Daten (DSG 2000) unterstellt auch nicht auf Menschen bezogene Informationen dem Datenschutzrecht, insbesondere Informationen über juristische Personen, vgl. § 4 Nr. 3 DSG 2000.

ner)",[86] im Wesentlichen also alle Informationen über Menschen, wobei es hier noch nicht drauf ankommt, wie interessant oder sensibel diese Informationen sein mögen. Damit hat gerade die Frage, ob und wie lange bestimmte Daten einen der datenschutzrechtlichen Regulierung unterfallenden Personenbezug haben, essentielle Bedeutung. Eng verknüpft hiermit ist die Folgefrage, welche Maßnahmen erforderlich sind, um einen Personenbezug zu vermeiden oder aus vorhandenen Datensätzen zu entfernen, um der datenschutzrechtlichen Regulierung zu entgehen.

1. Personenbeziehbarkeit – absoluter vs. relativer Personenbezug

Nach einer weniger strengen „relativen Theorie" des Personenbezugs soll es nur darauf ankommen, ob die datenschutzrechtlich verantwortliche Stelle auf Grundlage der bei ihr vorhandenen Daten einen Bezug zu einer individualisierbaren Person herstellen kann. Danach käme es nur auf das bei der jeweiligen konkreten verantwortlichen Stelle vorhandene Wissen an. Nach der von den Datenschutzbehörden bislang überwiegend vertretenen[87] strengeren „absoluten Theorie" sind Informationen schon dann personenbezogen, wenn zwar die verantwortliche Stelle auf Grundlage bei ihr vorhandener Informationen nicht das für die Herstellung eines Personenbezuges erforderliche Wissen hat, wenn aber Dritte dieses Zusatzwissen haben. Dies soll selbst dann gelten, wenn dieser Dritte sein Zusatzwissen nicht weitergeben darf.[88]

2. Anonymisierung – Anforderungen Rechtsfolgen

Ist ein Personenbezug nicht herstellbar, spricht man von anonymen Daten, auf die das Datenschutzrecht keine Anwendung findet. Damit hat gerade die Frage der Anforderungen an eine Anonymisierung erhebliche Bedeutung bei der Planung und Realisierung von Big Data- und Industrie 4.0-Prozessen. Eine Anonymisierung bisher personenbezogener Daten ist nur dann gegeben, wenn der Personenbezug *„nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft*"[89] herstellbar ist. Spiegelbildlich zur Definition personenbezogener Daten stellt sich auch hier wieder die Frage, ob nur auf die Möglichkeiten der jeweiligen verantwortliche Stelle abzustellen ist,[90] oder ob auch etwaiges Zusatzwissen Dritter zu berücksichtigen ist.[91]

Zweifel an einer hinreichenden Anonymisierung bestehen insbesondere dann, wenn ein vergleichsweise detaillierter Datensatz vorliegt und schon die Kombination der darin ent-

---

86 § 3 Abs. 1 BDSG.

87 So in Hinblick auf IP-Adressen das gemeinsame Gremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis") in seinem Beschluss vom 26./27.11.2009 (Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten) sowie die Artikel-29-Datenschutzgruppe in ihren Stellungnahmen WP 136, S. 19, WP 148, S. 9 und WP 150, S. 6.

88 Für einen Überblick über den Theorienstreit etwa *Gola/Klug/Körffer* in Gola/Schomerus, 12. Aufl. 2015, § 3, Rn. 10 sowie *Bergt*, ZD 2015, 365 jeweils m. w. N.

89 § 3 Abs. 6 BDSG.

90 So die relative Theorie (vgl. oben Teil 3II.1. des Gutachtens).

91 So die absolute Theorie (vgl. oben Teil 3II.1. des Gutachtens).

haltenen Einzelinformationen Schlüsse auf die Identität des Betroffenen zulässt, etwa die Kombination von Geburtsdatum, Postleitzahl und Geschlecht von Personen.

In der Praxis bietet die Anonymisierung von Daten durchaus die Möglichkeit, dem Anwendungsbereich des Datenschutzrechts zu entgehen. Allerdings ist hier im jeweiligen Einzelfall kritisch zu hinterfragen, ob tatsächlich eine ausreichende Anonymisierung vorliegt oder nicht. In der Praxis zunehmend wichtiger werden damit Verfahren, die eine Anonymisierung hinreichend zuverlässig sicherstellen, so dass niemand mehr in der Lage ist, die entsprechend bearbeiteten Informationen einer konkreten Person zuzuordnen.

3. Pseudonymisierung: Anforderungen und Rechtsfolgen

Die Pseudonymisierung lässt zwar anders als die Anonymisierung von Daten deren Personenbezug und die Anwendbarkeit des Datenschutzrechts nicht entfallen,[92] ist aber insbesondere gegenüber dem Umgang mit Klarnamen der Betroffenen datenschutzrechtlich weniger invasiv.[93] Pseudonymisieren ist *„das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“.*[94] Eine Pseudonymisierung schließt die unmittelbare Erkennbarkeit der betroffenen Personen für solche Verarbeitungsvorgänge aus, bei denen der (direkte) Personenbezug nicht erforderlich ist.

Da die Verwendung pseudonymisierter Daten gegenüber der Verwendung insbesondere mit Klarnamen der Betroffenen versehenen Daten weniger invasiv ist, kann die Verwendung pseudonymisierter Daten tendenziell auch einfacher gerechtfertigt werden, etwa im Rahmen der Verarbeitung von Nutzungsprofilen zu Werbezwecken.[95] Damit ist auch die Pseudonymisierung ein wichtiger Baustein bei der datenschutzkonformen und -freundlichen Planung und Realisierung von Big Data- und Industrie 4.0-Prozessen.

III. Anwendung bestehender Grundsätze auf die digitalisierte Wirtschaft

Die bestehenden Vorschriften des Datenschutzrechts sind auch auf neue Prozesse und Geschäftsmodelle der immer weiter vernetzten digitalen Wirtschaft anwendbar. Allerdings gerät das bestehende Konzept des europäischen und deutschen Datenschutzrechts hierbei zunehmend an systembedingte Grenzen.

---

92 Vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, S. 21; Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, S. 3 f. Zu den Herstellungsvarianten von Pseudonymen siehe *Scholz* in Simitis, 8. Aufl. 2014, § 3 BDSG, Rn. 220 ff.

93 Vgl. auch *Scholz* in Simitis, 8. Aufl. 2014, § 3 BDSG, Rn. 219d; siehe auch *Gola/Klug/Körffer* in Gola/Schomerus, 12. Aufl. 2015, § 28, Rn. 11 zu pseudonymisierten *„Konsumentendossiers*“.

94 § 3 Abs. 6a BDSG.

95 Ausdrücklich gestattet etwa § 15 Abs. 3 TMG die Erstellung von Nutzungsprofilen für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung von Telemedien bei Verwendung von Pseudonymen, sofern der Nutzer dem nicht widerspricht.

1. Datenschutzrechtlich relevante Nutzungshandlungen

Das BDSG differenziert bei den datenschutzrechtlich relevanten Handlungen begrifflich zwischen den Hauptkategorien der Erhebung, Verarbeitung und Nutzung personenbezogener Daten.[96] Unterkategorien der Verarbeitung sind die Speicherung, Übermittlung, Veränderung, Sperrung und Löschung.[97] Die Nutzung ist als Auffangtatbestand jede sonstige Verwendung personenbezogener Daten.[98]

Damit unterfällt die gesamte Wertschöpfungskette der Verwendung personenbezogener Daten der datenschutzrechtlichen Regulierung, von der Erhebung bis zur Löschung. Gerade komplexe Big Data- und Industrie 4.0-Prozesse sind damit von vornherein unter Berücksichtigung datenschutzrechtlicher Vorgaben zu durchdenken und zu planen.

2. Verbot mit Erlaubnisvorbehalt und Rechtfertigungsmöglichkeiten

Bestimmendes Grundprinzip deutschen und europäischen Datenschutzrechts ist das Verbot mit Erlaubnisvorbehalt.[99] Danach ist jede Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten grundsätzlich erst einmal verboten, soweit sie nicht durch das BDSG oder eine andere Rechtsvorschrift erlaubt ist oder eine Einwilligung des Betroffenen vorliegt. Gesetzliche Rechtfertigungstatbestände erlauben die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur in vergleichsweise engen Grenzen. Jenseits dieser Grenzen delegiert der Gesetzgeber die Entscheidung über die Reichweite der Datennutzung an den Betroffenen und trägt damit dem in Deutschland sogar verfassungsrechtlich abgesicherten Recht auf informationelle Selbstbestimmung Rechnung.[100]

3. Zweckbindungsgrundsatz – Bedeutung in der digitalisierten Wirtschaft und Big Data-Konstellationen

Auch der datenschutzrechtliche Zweckbindungsgrundsatz[101] hat essentielle Bedeutung bei der Planung von Big Data- und Industrie 4.0-Prozessen. Danach erstreckt sich jede gesetzliche Rechtfertigung oder Einwilligung in die Verwendung von Daten grundsätzlich nur auf einen zugrundeliegenden Verwendungszweck. Die Verwendung einmal vorhandener Daten zu anderen Zwecken oder eine Zusammenführung von Daten mit Daten aus anderen Quellen, mithin eine Zweckänderung bei der Datenverwendung, bedarf grundsätzlich einer neuen zusätzlichen Rechtfertigung.[102] Insbesondere dürfen für einen konkreten Zweck erhobe-

---

96 Hierzu § 3 Abs. 3-5 BDSG.
97 § 3 Abs. 4 BDSG.
98 § 3 Abs. 5 BDSG.
99 § 4 Abs. 1 BDSG.
100 Siehe hierzu erstmals BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83, NJW 1984, 419.
101 Art. 6 Abs. 1 lit. b) EU-DSRL; im deutschen Datenschutzrecht ist der Grundsatz der Zweckbindung nicht einheitlich an einer Stelle normiert, er kommt jedoch in verschiedenen Regelungen zum Ausdruck, etwa in § 4a Abs. 1 S. 2 BDSG, wonach der Betroffene bei Einwilligung auf den vorhergesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen ist, oder § 28 Abs. 1 S. 2 BDSG, wonach die Zwecke, für die die Daten verarbeitet oder genutzt werden „konkret festzulegen“ sind.
102 *Heckmann* in jurisPK-Internetrecht, 4. Aufl. 2014, Kap. 9 Rn. 53.

ne Daten nicht zu beliebigen anderen Zwecken genutzt werden, soweit diese anderen Zwecke nicht auch von einer gesetzlichen Rechtfertigung oder einer Einwilligung des Betroffenen abgedeckt sind. Gerade bei komplexen Big Data- und Industrie 4.0-Prozessen werden Daten aber regelmäßig aus ihrem ursprünglichen Zweckzusammenhang gerissen, zusammengeführt, umstrukturiert und analysiert und damit im Ergebnis neuen Nutzungen zugeführt. Dabei erfordert der Zweckbindungsgrundsatz im Rahmen der datenschutzrechtlichen Konzeption die Berücksichtigung aller innerhalb dieser Prozesse relevanten unterschiedlichen Datenverwendungen und Verwendungszwecke. Die Auslegung der konkreten Anforderungen des Zweckbindungsgrundsatzes befindet sich jedoch gerade auch im Hinblick auf dessen sehr unterschiedliche Umsetzung in den einzelnen EU-Mitgliedsstaaten in einer steten Diskussion und Fortentwicklung. Insbesondere für Big Data-Anwendungen und Industrie 4.0-Prozesse obliegt der Rechtsprechung und Literatur die Entwicklung und Konturierung übergreifender Maßstäbe für die Zulässigkeit vor dem Hintergrund des Zweckbindungsgrundsatzes.[103]

4. Sonderfall Auftragsdatenverarbeitung

Ein wichtiges datenschutzrechtliches Instrument bei Konzeption und Planung auch von neuen Geschäftsmodellen ist die sogenannte Auftragsdatenverarbeitung.[104] Im Kern ermöglicht es die Auftragsdatenverarbeitung, außerhalb der datenschutzrechtlich verantwortlichen Stelle stehende Dritte in einer Weise einzubinden, dass diese Dritten datenschutzrechtlich wie eine interne Abteilung des Auftraggebers behandelt werden. Dies setzt voraus, dass die verantwortliche Stelle als Auftraggeberin den Dritten vertraglich so eng bindet, dass der Dritte gleichsam als verlängerter Arm der verantwortlichen Stelle ohne eigene Entscheidungsmöglichkeiten in Bezug auf die Verwendung der betroffenen personenbezogenen Daten ist.

Die Auftragsdatenverarbeitung hat den Vorteil, dass die Einbindung des außenstehenden Dritten keine zusätzliche datenschutzrechtliche Rechtfertigung erfordert. Ferner werden die Handlungen des Auftragsdatenverarbeiters grundsätzlich dem Auftraggeber als datenschutzrechtlich verantwortliche Stelle zugerechnet, mit der Folge einer nur sehr eingeschränkten datenschutzrechtlichen Verantwortlichkeit des als Auftragsdatenverarbeiter eingesetzten Dritten.

IV. Gesetzliche Rechtfertigungstatbestände

Gesetzliche Rechtfertigungstatbestände haben in der Praxis ganz erhebliche Bedeutung, weil sie die Erhebung und Verwendung personenbezogener Daten gestatten, unter der zusätzlichen Voraussetzung der bloßen Information des Betroffenen über die Details der Erhebung, Verarbeitung und Nutzung seiner Daten, jedoch ohne dass eine Einwilligung des Betroffen erforderlich wäre. Allerdings gestattet der Gesetzgeber nur ein Mindestmaß der

[103] So auch *Helbing*, K&R 2015, 145.
[104] § 11 BDSG.

Erhebung und Verwendung personenbezogener Daten von vornherein und überlässt die Entscheidung über die Reichweite der Datennutzung im Übrigen den hiervon Betroffenen.

Gerade bei neuen digitalen Geschäftsmodellen, die eine intensive und oft komplexe Nutzung auch personenbezogener Daten mit sich bringen, geraten gesetzliche Rechtfertigungstatbestände schnell an Grenzen. Hinzu kommt, dass viele Details der Auslegung und Anwendung gesetzlicher Rechtfertigungstatbestände umstritten und nicht abschließend geklärt sind. Weitere Rechtsunsicherheiten ergeben sich daraus, dass einige gesetzliche Rechtfertigungstatbestände auch auf der Abwägung von Interessen der Beteiligten basieren und damit vergleichsweise offen formuliert sind.

V. Einwilligungen: Informed Consent und systemimmenante Grenzen

Gerade bei komplexen und datennutzungsintensiven digitalen Geschäftsmodellen spielen datenschutzrechtliche Einwilligungen in der Praxis eine wichtige Rolle, nicht zuletzt infolge der engen Grenzen der von gesetzlichen Rechtfertigungstatbeständen ausgehenden Erlaubnissen zur Datennutzung. Allerdings stellt insbesondere das deutsche Datenschutzrecht auch an die Wirksamkeit von Einwilligungen vergleichsweise hohe Anforderungen.[105]

Eine Einwilligung ist nur dann wirksam, wenn sie auf hinreichend informierter Grundlage erklärt wurde, wenn also der Betroffene bei Erklärung der Einwilligung auch genau erkennen konnte, wer welche konkret ihn betreffenden Daten zu welchen konkreten Zwecken erhebt, verarbeitet oder nutzt. Gerade bei sehr komplexen und vielschichtigen Datenverarbeitungen kann es in der Praxis schwierig sein, dem Nutzer ein hinreichend differenziertes Bild über die konkrete Verwendung seiner Daten zu geben. Dabei gilt es einerseits, technisch sehr komplexe Themen in der Darstellung so zu vereinfachen, dass deren Beschreibung nicht schon ob ihrer technischen Komplexität für den durchschnittlichen Adressaten unverständlich wird. Andererseits darf die Vereinfachung nur soweit reichen, dass der Betroffene immer noch ein hinreichend klares und differenziertes Bild darüber hat, was mit seinen Daten passiert, so dass er die Reichweite der Verwendung seiner Daten als maßgebliche Grundlage für seine Entscheidung über die Erteilung einer Einwilligung beurteilen kann. Gleichzeitig sind auch Einwilligungen regelmäßig an strengen AGB-rechtlichen Anforderungen[106] zu messen, insbesondere mit Blick auf ihre Länge und die Transparenz der Darstellung. Dabei kann auch ein besonders großer Umfang einer vorformulierten Einwilligungserklärung deren Intransparenz begründen, ebenfalls mit der Folge der Unwirksamkeit der Einwilligung.

Je komplexer und datenintensiver digitale Geschäftsmodelle und Prozesse werden, so etwa bei vielen Big Data-Anwendungen, desto stärker gerät auch das datenschutzrechtliche Konzept der informierten Einwilligung an die vorstehend skizzierten systemimmanenten Grenzen. Hinzu kommt, dass der Betroffene einmal erklärte Einwilligungen grundsätzlich jeder-

[105] Vgl. § 4a BDSG zu den grundsätzlichen Anforderungen an die Einwilligung.
[106] §§ 305 ff. BGB.

zeit widerrufen kann, wenn er die durch seine Einwilligung legitimierte Verwendung seiner personenbezogenen Daten mit Wirkung für die Zukunft unterbinden möchte. Im Widerrufsfall muss die verantwortliche Stelle auch technisch und organisatorisch sicherstellen, dass die von der Einwilligung umfasste Datenverwendung beendet wird und ein entsprechendes Einwilligungsmanagement implementieren.

VI. Effiziente Strukturierung datenschutzrechtlicher Rechtfertigungsmöglichkeiten

In der Praxis gilt es regelmäßig, die unter den bestehenden datenschutzrechtlichen Rahmenbedingungen in Betracht kommenden Rechtfertigungsmöglichkeiten umfassend und effizient nutzbar zu machen. Soweit gesetzliche Rechtfertigungstatbestände zur Verfügung stehen, sollten diese genutzt werden. In Teilbereichen gestattet das BDSG die Verwendung personenbezogener Daten der Betroffenen soweit sie für die Anbahnung und Erfüllung eines Vertrages mit dem Betroffenen erforderlich ist.[107] Insbesondere unter diesem Aspekt kann auch die geschickte Gestaltung der einer Datenverwendung zugrunde liegenden vertraglichen Beziehungen mit dem Betroffenen die Nutzbarkeit gesetzlicher Rechtfertigungstatbestände optimieren.

Nur soweit gesetzliche Rechtfertigungstatbestände nicht greifen, sollte auf Einwilligungen zurückgegriffen werden. Dies reduziert den Umfang von Einwilligungen auf das unvermeidbare Mindestmaß und erhöht indirekt auch die Transparenz der Einwilligung. Gleichzeitig entfällt im Falle eines Widerrufs der Einwilligung die datenschutzrechtliche Legitimation nur für die von der Einwilligung umfassten Datenverwendungen.

VII. Privacy by Design und Privacy by Default

Eine Befassung mit den hier skizzierten datenschutzrechtlichen Anforderungen zeigt, dass diese schon bei der Konzeption von neuen digitalen Prozessen oder Geschäftsmodellen zu berücksichtigen sind und einen integralen Bestandteil von deren Planung bilden, sog. *„Privacy by design“*.[108]

Insbesondere unter dem Gesichtspunkt der Datensparsamkeit[109] sollte dabei der Datenschutz gleichsam als systemseitige Standardeinstellung integriert werden, mit dem Ziel, die Erhebung, Verarbeitung und Weitergabe personenbezogener Daten von Beginn der Datenverarbeitung an auf das erforderliche Mindestmaß zu begrenzen, sog. „*Privacy by default*“.[110]

---

[107] § 28 Abs. 1 S. 1 Nr. 1 BDSG.
[108] Hierzu *Schulz,* CR 2012, 204.
[109] § 3a BDSG.
[110] Hierzu *Schulz,* CR 2012, 204 sowie in *Wolff/Brink*, Beck'scher Online-Kommentar Datenschutzrecht, Stand: 01.11.2014, § 3a, Rn. 66 ff.

Diese Gedanken von *„Privacy by design“ und „Privacy by default“* finden auch im aktuellen Entwurfsstand der Datenschutz-Grundverordnung Berücksichtigung.[111]

VIII. Security and Data Breach Notification – Melde- und Informationspflichten bei Datenverlust

Datenschutzrechtlich sind Unternehmen verpflichtet, bei begründetem Verdacht des Abhandenkommens bestimmter Arten personenbezogener Daten oder der unberechtigten Kenntnisnahme Dritter die zuständige Datenschutz-Aufsichtsbehörde sowie die Betroffenen unverzüglich zu informieren.[112]

Entsprechende Melde- und Informationspflichten stehen unter dem Vorbehalt, dass schwerwiegende Beeinträchtigungen der Rechte oder schutzwürdigen Interessen der Betroffenen drohen, wofür die Umstände des jeweiligen Einzelfalls entscheidend sind.[113] Wann diese Schwelle jeweils konkret überschritten ist, ist in der Praxis oft nur schwer abzugrenzen. Ist die Benachrichtigung der Betroffenen nicht möglich oder würde sie einen unverhältnismäßigen Aufwand erfordern, insbesondere wegen einer besonders hohen Zahl an Betroffenen, so kommt stattdessen die Information der Öffentlichkeit in Betracht, etwa im Wege hinreichend großer und deutlicher Anzeigen in mehreren überregional erscheinenden Tageszeitungen.[114]

Verstöße gegen diese Melde- und Informationspflichten können als Ordnungswidrigkeit[115] oder, unter entsprechenden qualifizierten Voraussetzungen, auch als Straftat[116] geahndet werden. Viel schlimmere Folgen können insbesondere Imageverluste der von Security- und Data-Breaches betroffenen Unternehmen sein.

IX. Regulatorische Situation und Ausblick

Es ist festzuhalten, dass das derzeitige Datenschutzrecht durchaus einen Rahmen vorgibt, unter den auch neue digitale Geschäftsmodelle subsumierbar sind. Allerdings stößt das bisherige Instrumentarium zur Rechtfertigung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten mit zunehmender Komplexität der Geschäftsmodelle an Grenzen, insbesondere bei vielschichtigen Big Data-Anwendungen. Dabei kommen verschiedene Ansätze in Betracht, um auch das bestehende rechtliche Instrumentarium für datenschutzrechtlich komplexe Geschäftsmodelle besser nutzbar zu machen.

---

[111] Vgl. Erwägungsgrund 61 DS-GVO-E.

[112] § 42a BDSG; ähnliche spezialgesetzliche Informationspflichten finden sich in § 15a TMG, §§ 93 Abs. 3, 109a TKG sowie in § 83a SGB X für Sozialdaten.

[113] Maßgebliche Kriterien sind die Art der betroffenen Daten und die potenziellen Auswirkungen der Kenntniserlangung durch Dritte auf die Betroffenen (etwa materielle Schäden bei Kreditkarteninformationen oder soziale Nachteile einschließlich des Identitätsbetrugs).

[114] § 42a S. 5 BDSG.

[115] § 43 Abs. 2 Nr. 7 BDSG.

[116] § 44 Abs. 1 BDSG.

1. Gestaltung von Einwilligungen

Gestaltungsspielräume bleiben dabei etwa bei der Einwilligung.[117] Die konkreten Anforderungen an die Transparenz und Detaillierung einer hinreichend informierten Einwilligung sind gleichzeitig Ansatzpunkte für eine Fortentwicklung des Datenschutzrechts.[118] Hier gilt es, Alternativen zu schaffen zu ellenlangen und schon aufgrund ihrer Länge intransparenten Einwilligungserklärungen. Denkbar sind hierbei etwa für bestimmte Anwendungen und Arten von Geschäftsmodellen standardisierte Einwilligungen bei gleichzeitiger klarer Benennung und Hervorhebung etwaiger Abweichungen von diesen Standards. Dies würde die Vergleichbarkeit und Transparenz erhöhen. Ebenso denkbar ist es, die Transparenz und Verständlichkeit durch Ampelsysteme zu erhöhen, die den Grad der Beeinträchtigung des Rechts auf informationelle Selbstbestimmung intuitiv verständlich anzeigen. Ebenso in Betracht kommt der unterstützende Einsatz audiovisueller Informationen, wobei hier zur Vermeidung von Medienbrüchen insbesondere die von Betroffenen ohnehin genutzten Medien verwendet werden sollten, z.B. Mindmaps, Videos oder Chats, in denen Fragen des Betroffenen direkt beantwortet werden. Weitere Unterstützung könnten konkrete Beispiele leisten, was in welchen Situation mit den Daten geschieht. All diese Maßnahmen könnten die Transparenz und Verständlichkeit von Einwilligungen erhöhen und dazu führen, dass der betroffene Nutzer bewusster und freier über den Grad der Beeinträchtigungen seines Recht auf informationelle Selbstbestimmung entscheiden kann, den er zulassen möchte.

2. Ausweitung des Zweckbindungsgrundsatzes

Ein weiterer Gesichtspunkt, der in der Rechtsprechung noch weitestgehend ungeklärt ist und einer stetigen Diskussion und Fortentwicklung durch die Literatur unterliegt, ist der **Zweckbindungsgrundsatz.**[119] Hier stellt sich im Kern die Frage, inwieweit eine weitere Interpretation des Zweckbindungsgrundsatzes die Möglichkeit schafft, auch dem eigentlichen Zweck ähnliche Datenverwendungen unter eine einheitliche Zweckbestimmung zu subsumieren und so zu rechtfertigen.

3. Privacy by Design and Privacy by Default

Weitere Ansatzpunkte sind die Berücksichtigung datenschutzrechtlicher Anforderungen und die datenschutzrechtlich möglichst minimalinvasive Gestaltung von Angeboten und Systemen bereits bei deren Konzeption. Solche Maßnahmen zum Schutz der Interessen der Betroffenen wirken sich auch auf die Nutzbarkeit gesetzlicher Rechtfertigungstatbestände aus,[120] insbesondere soweit diese auf eine Interessenabwägung erfordern, indem sie die Interessenabwägung positiv beeinflussen.

---

[117] Hierzu oben Teil 3III.2.

[118] So auch die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme WP 223 vom 16.10.2014, in der sie ausdrücklich neue Konzepte und Formen zur Einholung von Einwilligungen fordert.

[119] Hierzu oben Teil 3III.3.

[120] Siehe oben Rechtfertigungstatbestände.

4. Codes of Conduct

Einen Ansatzpunkt zur Abstimmung neuartiger Konzepte mit den Datenschutzbehörden sind Codes of Conduct, die in § 38a BDSG bereits vorgesehen sind. Zwar sind in diesem Zusammenhang geäußerte Einschätzungen der Behörden nicht letztverbindlich[121] erreichen diese Einwilligungsarten damit keine rechtliche Verbindlichkeit. Dennoch wirken sie wie eine Art behördliches „Gütesiegel“ [122] und dienen so der Reduzierung von Rechtsunsicherheit und der Vermeidung rechtlicher Auseinandersetzungen. Daneben ist schon derzeit die Vorlage von Vorschlägen für Codes of Conduct auf europaweiter Ebene an die Artikel-29-Datenschutzgruppe möglich.[123] Vergleichbare Möglichkeiten sowohl auf nationaler als auch auf Unionsebene soll es auch in der Datenschutzgrundverordnung geben.[124]

5. Datenschutz-Grundverordnung

Gleichzeitig sind die Tage nationaler Datenschutzgesetze mit Blick auf die derzeit entstehende Datenschutz-Grundverordnung gezählt, die dann für alle EU-Mitgliedsstaaten einheitlich und unmittelbar gelten soll. Die Datenschutz-Grundverordnung wird dabei soweit ersichtlich an den bestehenden Grundsätzen nur wenig ändern, insbesondere am datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt. Gleichzeitig unterstreicht sie die Bedeutung der Einhaltung des datenschutzrechtlich zulässigen Rahmens, nicht zuletzt durch die gegenüber der aktuellen Rechtslage drastisch verschärften Sanktionen.

Es ist festzuhalten, dass das derzeitige Datenschutzrecht durchaus einen Rahmen vorgibt, unter den auch neue digitale Geschäftsmodelle subsumierbar sind. Allerdings ist festzustellen, dass das bisherige Instrumentarium zur Rechtfertigung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten mit zunehmender Komplexität der Geschäftsmodelle an Grenzen stößt, insbesondere bei vielschichtigen Big Data-Anwendungen.

Gestaltungsspielraum eröffnet dabei der Umstand, dass gerade im Bereich Big Data und Industrie 4.0 wesentliche Aspekte der datenschutzrechtlichen Rechtfertigung, wie etwa die konkreten Voraussetzungen an die Gestaltung der informierten Einwilligung,[125] in der Rechtsprechung noch weitestgehend ungeklärt sind und einer stetigen Diskussion und Fortentwicklung durch die Literatur unterliegen. Insbesondere eröffnet die aktuelle Diskussion über die konkreten Anforderungen und Ausprägungen des Zweckbindungsgrundsatzes[126] die Möglichkeit aktiver Mitgestaltung der maßgeblichen rechtlichen Rahmenbedingungen.

---

[121] Als begünstigender Verwaltungsakt bindet die Anerkennung der Verhaltensregeln die Datenschutzbehörden und andere Behörden, vgl. *Petri*, in Simitis, BDSG, § 32a, Rn. 25.

[122] *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 38a, Rn. 1.

[123] Art. 27 Abs. 3 EU-DSRL.

[124] Vgl. dazu Art. 38 DS-GVO-E, der insoweit keine Änderungen durch das Europäische Parlament und den Rat erfahren hat.

[125] Hierzu oben Teil 3III.2.

[126] Hierzu oben Teil 3III.3.

Teil 4 Know-how-Schutz im Umfeld von Industrie 4.0 (Der Richtlinienentwurf zum Schutz von Geschäftsgeheimnissen und seine Konsequenzen für das betriebliche Vertragsmanagement) *(Sandra Sophia Redeker)*

Die vierte industrielle Revolution bietet für Unternehmen diverse Möglichkeiten, mittels intelligenter Maschinen und Produkte Geschäftsprozesse entlang der gesamten Wertschöpfungskette zu optimieren. Gleichzeitig birgt die fortschreitende digitale Vernetzung zusätzliche Gefahren für das unternehmenseigene Know-how: Je höher die Anzahl der Beteiligten bei der Schaffung und Nutzung des Know-hows, desto größer ist die Konfliktgefahr bezüglich bestehender Rechte und die Gefahr des unberechtigten Zugriffs auf das Know-how durch Dritte. Die Europäische Kommission ist im Rahmen ihrer Wachstumsstrategie Europa 2020 bestrebt, eine Innovationsunion zu schaffen, die einen verbesserten und einheitlichen Know-how-Schutz gewährleistet. Im Zuge dessen hat sie ihren Richtlinienentwurf zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen COM (2013) 813 vorgestellt, der sich derzeit in der EU-parlamentarischen Diskussion befindet.[127] Ein verbesserter Know-how-Schutz wird deutschen Unternehmen im Zuge der fortschreitenden Digitalisierung der Wirtschaft zu Gute kommen. Jedoch resultiert daraus auch Handlungsbedarf für die Unternehmen, wie nachfolgend gezeigt wird.

I. Änderungen der deutschen Rechtslage aufgrund der kommenden Richtlinie zum Schutz von Geschäftsgeheimnissen

Der Know-how-Schutz gilt in Deutschland noch immer als das Stiefkind des Geistigen Eigentums, wohl auch aufgrund der historisch bedingten Einordnung im Bereich der strafrechtlichen Vorschriften der §§ 17 ff. UWG. Dabei steht die wirtschaftliche Bedeutung betrieblicher Geheimnisse derjenigen von Immaterialgüterrechten im Unternehmensalltag in Nichts nach. Der Know-how-Schutz greift zum einen immer dann ein, wenn sich Unternehmen bewusst für eine Geheimhaltung und gegen eine Anmeldung zu einem zeitlich begrenzten immaterialgüterrechtlichen Schutzrecht entschließen. Zum anderen ist ein effektiver Know-how-Schutz erforderlich, wenn Informationen, wie etwa Kundenlisten oder kaufmännisches Wissen, nicht den gewerblichen Schutzrechten zugänglich sind. Dies kann insbesondere auch dann relevant werden, wenn und solange die bestehenden gesetzlichen Instrumentarien des Immaterialgüterrechts Schutzlücken im Hinblick auf aktuelle Phänomene aufweisen, die durch das Thema Industrie 4.0 entstehen. Die EU-Gremien widmen nunmehr Geschäfts- und Betriebsgeheimnissen die rechtliche Aufmerksamkeit, die ihrer wirtschaftlichen Bedeutung gerecht wird. Unternehmer dürfen sich insoweit auf einige Verbesserungen ihrer Rechtsposition freuen. Gleichzeitig enthält die neue Richtlinie voraussichtlich auch

[127] Der Kommissionsentwurf wurde durch einen Kompromissvorschlag des Rates der Europäischen Union vom 26.05.2014 (Dok. 7039/14), ergänzt. Der Rechtsausschuss des Europäischen Parlaments hat hierzu seinen Bericht mit Änderungsvorschlägen am 22.06.2015 veröffentlicht, vgl. www.europarl.europa.eu/meetdocs/2014_2019/documents/juri/pr/1048/1048388/1048388de.pdf. Die erste Lesung im Europäischen Parlament ist für den 08.03.2016 geplant.

Bestimmungen, die Geheimnisinhaber dazu zwingt, aktiv(er) zu werden, wenn sie auch in Zukunft rechtlichen Schutz für ihre Geschäftsgeheimnisse in Anspruch nehmen wollen.

1. Der Begriff des Geschäftsgeheimnisses

Die Definition des Begriffs des Geschäftsgeheimnisses in Art. 2 Abs. 1 des Richtlinienentwurfs übernimmt den Wortlaut des Art. 39 Abs. 2 TRIPS und setzt voraus, dass eine Information (a) geheim, (b) von kommerziellem Wert und (c) Gegenstand von angemessenen Geheimhaltungsmaßnahmen ist. Der Begriff entspricht nur eingeschränkt der zu § 17 UWG entwickelten Definition des Geschäftsgeheimnisses.[128] Zwar ist es zutreffend, dass die ersten beiden Tatbestandsmerkmale im Wesentlichen dem bisherigen deutschen Verständnis des Geschäftsgeheimnisses entsprechen, das Merkmal der angemessenen Geheimhaltungsmaßnahmen bringt hingegen eine wesentliche Änderung der Rechtslage mit sich. Im Rahmen des bisherigen Lauterkeitsrechts ist lediglich ein subjektiver Geheimhaltungswille erforderlich, der anhand von objektiven Umständen erkennbar wird, damit eine Information als Geschäftsgeheimnis anerkannt werden kann. An einen derartigen Willen werden in der Praxis jedoch keine besonderen Anforderungen gestellt, denn im Ergebnis wird er für alle nicht offenkundigen Betriebsinterna vermutet.[129]

Wie genau das neue Merkmal der angemessenen Geheimhaltungsmaßnahmen auszulegen ist, wird die Rechtsprechung klären müssen, die Richtlinie selbst enthält keine weiteren Erläuterungen. Der Terminus „angemessene Geheimhaltungsmaßnahmen“ lässt jedoch bereits erkennen, dass ein subjektiver Wille allein nicht ausreicht. Vielmehr muss der Geheimnisinhaber objektive, geeignete und den Umständen nach adäquate Handlungen vornehmen, um die Geheimhaltung seines Know-hows sicherzustellen.[130] Das bedeutet, dass er diese Maßnahmen im Zweifelsfall vor Gericht auch darlegen und beweisen können muss, um in einem späteren Verletzungsprozess gegen Dritte erfolgreich sein zu können. Welche Art von Maßnahmen dabei im Einzelfall als „angemessen“ gelten, werden die nationalen Gerichte sowie in letzter Instanz der EuGH beurteilen. Ein Blick auf die US-amerikanische Judikatur, deren Gesetze[131] das Merkmal der angemessenen Geheimhaltungsmaßnahmen bereits heute kennen, zeigt jedoch, dass Gerichte physische Zugangsbeschränkungen, rechtliche Vertragsklauseln und IT-Maßnahmen überprüfen, um zu beurteilen, ob der Inhaber Vorkehrungen für eine angemessene Geheimhaltung getroffen hat. So wurde beispielsweise untersucht, ob Fabrikeingänge ausreichend bewacht, wirksame Verschwiegenheitsklauseln in Arbeitsverträgen vereinbart oder eine Firewall eingerichtet worden war.[132] Demnach ist es zu erwarten, dass Unternehmen nach neuer Rechtslage deutlich höhere An-

---

[128] Anders *Gärtner*, NZG 2014, 650 (651).

[129] *Köhler*, in Köhler/Bornkamm, UWG, 32. Auflage 2014, § 17 Rn. 10.

[130] *Gärtner*, NZG 2014, 650 (651); zu Art. 39 II TRIPS *McGuire/Joachim/Künzel/Weber*, GRURInt 2010, 829 (830).

[131] Es handelt sich um Vorschriften der einzelnen Bundesstaaten, die überwiegend den Uniform Trade Secrets Act aus dem Jahre 1979 übernommen haben.

[132] Überblick über Entscheidungen der US-Judikatur bei *Redeker/Pres/Gittinger*, WRP 2015, 681 (684).

forderungen zu erfüllen haben, als dies bisher der Fall war, um geltend machen zu können, dass ihr Know-how ein geschütztes Geschäftsgeheimnis im Sinne der Richtlinie darstellt.

2. Einheitlicher Verletzungstatbestand und Ausnahmen

Weiterhin enthält der Richtlinienentwurf in Artikel 3 einen einheitlichen Verletzungstatbestand und Ausnahmeregeln in Artikel 4. Aus deutscher Perspektive hervorzuheben ist hier die Änderung der Rechtslage im Hinblick auf eine künftige generelle Zulässigkeit des Reverse Engineerings: Wie schon im anglo-amerikanischen Rechtsraum üblich (in Deutschland aber bislang verpönt), wird es mit Inkrafttreten der Richtlinie europaweit generell erlaubt sein, auf dem Markt frei erhältliche Produkte der Konkurrenz zu erwerben, zu analysieren und nachzubauen, soweit und solange sie nicht durch ein Sonderschutzrecht, insbesondere ein Patent oder Gebrauchsmuster, geschützt sind. Dies stellt insbesondere für technologieintensive Unternehmen einen weiteren Anreiz dar, für firmeneigenes Know-how, soweit möglich, gewerbliche Schutzrechte zu erwerben. Ob die Zulässigkeit des Reverse Engineerings vertraglich ausgeschlossen werden kann, wie es der Kompromissvorschlag des Rates ermöglichen will, wird sich erst noch im Laufe des europäischen Gesetzgebungsverfahrens entscheiden.

3. Rechtsfolgen und prozessuale Geheimhaltung

Wird das geheime Know-how eines Unternehmers durch Dritte unbefugt entwendet, stehen dem Geheimnisinhaber nach Art. 11 bis 13 diverse Ansprüche, insbesondere auf Beseitigung, Unterlassung, Schadensersatz sowie Rückruf und Vernichtung rechtsverletzender Produkte zu. Der durch den Richtlinienentwurf vorgesehene Umfang der Rechtsfolgen kommt mithin demjenigen bei Verletzung von Immaterialgüterrechten gleich. Will der Geheimnisinhaber allerdings seine Rechte prozessual geltend machen, erwies sich die bisherige prozessuale Situation als unbefriedigend. Das deutsche Zivilprozessrecht zwingt nach aktuellem Stand dazu, Geschäftsgeheimnisse im Prozess derart genau zu beschreiben, dass der Kläger (und Verletzte) befürchten muss, sein sensibles Know-how dem Prozessgegner durch die Klageschrift auf dem Silbertablett zu servieren.[133] Dies kann dazu führen, dass geschädigte Unternehmen von vornherein auf einen Verletzungsprozess verzichten, um nicht noch weiteres geheimes Wissen offenbaren zu müssen. Auch diese Problematik hat die Kommission erkannt und will zukünftig effektive Maßnahmen zur Geheimhaltung des Know-hows im Prozess schaffen. Ob dies letztendlich zur Einführung eines In-camera-Verfahrens unter Ausschluss der Parteien führt, bei dem lediglich das Gericht und allenfalls die anwaltlichen Prozessvertreter von den sensiblen Informationen Kenntnis erlangen, bleibt abzuwarten.[134]

---

[133] *Rojahn*, in FS Loewenheim 1. Aufl. 2009, 251, 254; *Götz*, Der Schutz von Betriebs- und Geschäftsgeheimnissen im Zivilverfahren, 1. Aufl. 2014, S. 251 f.

[134] Der Kompromissvorschlag des Rates der Europäischen Union vom 26.05.2014 (Dok. 7039/14) bleibt in diesem Punkt deutlich hinter den weitreichenden Vorschriften des Kommissionsvorschlages zurück, sodass zum jetzigen Zeitpunkt unklar ist, wie umfassend der Geheimnisschutz im Prozess ausgestaltet

II. Vertragliche Regelungen zum Schutz vom geheimem Know-how im Rahmen digitaler Fertigungsprozesse

Die Kommission will mit der Richtlinie ein angemessenes Schutzniveau für betriebliches Know-how garantieren und Unternehmen wirksame Rechtsbehelfe für den Fall, dass ihre Geschäftsgeheimnisse gestohlen oder missbräuchlich verwendet werden, an die Hand geben.[135] Es bleibt jedoch weiterhin ureigene Aufgabe der Unternehmen, ihre Betriebsgeheimnisse zu schützen. Dies gilt insbesondere auch im Rahmen von digitalen Fertigungsprozessen und der Produktion mit Kundenbeteiligung, bei denen aufgrund der technischen Möglichkeiten und der potenziell höheren Anzahl der Beteiligten die Gefahr eines unbefugten Zugriffs durch Dritte besonders hoch ist. Die Notwendigkeit eines umfassenden Schutzes resultiert zum einen daraus, dass angemessene Geheimhaltungsmaßnahmen erforderlich sind, damit eine Information als Geschäftsgeheimnis im Sinne der Richtlinie gilt, zum anderen daraus, dass lediglich effektive Schutzmechanismen den Diebstahl und Missbrauch durch Dritte verhindern und den Wert eines Geschäftsgeheimnisses erhalten können. Ein wesentlicher Eckpfeiler einer solchen Schutzstrategie für betriebliches Know-how sind für den Einzelfall passende vertragliche Regelungen, die den Verlust geheimen Wissens verhindern sollen. In der Praxis finden sich allzu häufig keine, unwirksame oder ineffektive Regelungen in den einschlägigen Verträgen, die im Ergebnis keine angemessene Geheimhaltung nach der Definition der kommenden Richtlinie gewährleisten.

1. Kooperationsvereinbarungen

Eine wirksame Kooperation erfordert es, dass die Beteiligten ihr Know-how im gewissen Rahmen mit dem Kooperationspartner teilen. Gleichzeitig begründet dies die Gefahr, dem Gegenüber zu weitreichende Einblicke in eigene Geschäftsgeheimnisse zu gewähren, die dieser dann nach Beendigung der Kooperation zum eigenen Vorteil nutzen kann. Know-how-Schutzklauseln in Kooperationsverträgen müssen deshalb je nach Einzelfall den Umfang, aber auch die erforderlichen Ausnahmen[136] der Geheimhaltungsverpflichtung festlegen. Darüber hinaus ist insbesondere der zeitliche Faktor zu beachten; eine unbefristete Geheimhaltungsverpflichtung kann sich aus verschiedenen Gründen als inadäquat erweisen.[137]

Detaillierterer Regelungsbedarf ergibt sich u.a. auch je nach den individuellen Umständen im Hinblick auf die zugriffsberechtigten Personenkreise sowie auf den Umgang mit den Daten. Von besonderer Relevanz ist ferner die Frage, wie mit Ergebnissen der Kooperation umgegangen werden soll. Während eine Geheimhaltung von Forschungsergebnissen während der Kooperation unproblematisch zulässig ist, ist eine nachvertragliche Schweige-

---

werden wird. Ein Überblick über bereits im deutschen Recht bzw. der Verfahrenspraxis der Gerichte vorhandene Lösungsansätze findet sich bei *Redeker/Pres/Gittinger*, WRP 2015, 821ff.

[135] Pressemitteilung der Europäischen Kommission vom 28. November 2013, abrufbar unter: http://europa.eu/rapid/press-release_IP-13-1176_de.htm.

[136] Üblich sind insbesondere Öffnungsklauseln für den Fall, dass geheimes Know-how auf andere Weise öffentlich und eine weitere Geheimhaltung demnach sinnlos geworden ist.

[137] *Maume*, in: Ann/Loschelder/Grosch, Praxishandbuch Know-how-Schutz, 1. Aufl. 2010, Kap. 4 Rn. 56.

pflicht aus kartellrechtlicher Sicht kritisch zu beurteilen und nur in gewissen Konstellationen zulässig.[138]

2. Arbeitsverträge

In der betrieblichen Praxis begründen eigene Mitarbeiter immer noch eine weitaus größere Gefahr für betriebseigenes Know-how als etwa die Industriespionage durch Dritte.[139] Daher kommt insbesondere der Vereinbarung von Know-how-Schutzklauseln in Arbeitsverträgen eine herausragende Bedeutung zu.

a) Vertragliche und nachvertragliche Geheimhaltungsklauseln

Während des Arbeitsverhältnisses ist der Arbeitnehmer bereits durch die arbeitsvertragliche Treuepflicht daran gehindert, Betriebs- und Geschäftsgeheimnisse zu offenbaren.[140] Zur Konkretisierung der Verschwiegenheitspflicht und deren Erstreckung auch auf die Dauer nach Beendigung des Arbeitsverhältnisses , sind Verschwiegenheitsklauseln in den Arbeitsvertrag aufzunehmen. Nach der Rechtsprechung des BAG können sich Verschwiegenheitsklauseln aber nicht auf alle denkbaren betrieblichen Angelegenheiten erstrecken. Dies ergibt sich aus §§ 134, 138, 242 BGB und durch die gesetzlichen Vorgaben bei Allgemeinen Geschäftsbedingungen.[141] Anderenfalls dürfte der Arbeitnehmer überhaupt nichts mehr über den Betrieb erzählen. Dies würde sein Persönlichkeitsrecht verletzen. Zu weit gefasste Verschwiegenheitsklauseln sind daher unwirksam. [142]

Besonders sensibel und bedeutsam sind nachvertragliche Verschwiegenheitsverpflichtungen. Denn oftmals besteht die Gefahr, dass ehemalige Mitarbeiter betrieblich erworbenes Wissen im Rahmen einer neuen Tätigkeit für die Konkurrenz fruchtbar machen. Die Möglichkeit des Arbeitgebers, dies zu verhindern und die vertragliche Verschwiegenheitspflicht über die Dauer des Arbeitsverhältnisses hinaus zu verlängern, ist durch die arbeitsgerichtliche Rechtsprechung jedoch stark beschnitten worden.[143] Nach ständiger Rechtsprechung des Bundesarbeitsgerichts darf der ehemalige Mitarbeiter sein redlich erlangtes, im Gedächtnis gespeichertes Erfahrungswissen auch beim neuen Arbeitgeber verwenden; dies ist

---

138 *Maume*, in: Ann/Loschelder/Grosch, Praxishandbuch Know-how-Schutz, 1. Aufl. 2010, Kap. 4 Rn. 58.

139 Das Bundesamt für Verfassungsschutz geht davon aus, dass die Innentäter 70% der Fälle des Informationsdiebstahls ausmachen: Faltblatt „Sicherheitslücke Mensch – Der Innentäter als größte Bedrohung für die Unternehmen“, abrufbar unter: http://www.verfassungsschutz.de/de/download-manager/_faltblatt-2014-04-sicherheitsluecke-mensch.pdf.

140 BAG, 25.08.1966 – 5 AZR 525/65, NJW 1967, 125 (126).

141 *Rolfs* in Preis, Der Arbeitsvertrag, 5. Auflage [2015], II V 20 Rz. 33; LAG Rheinland-Pfalz, Urt. v. 21. 02. 2013 - 2 Sa 386/12, ZD 2013, 460; BAG, Urt. v. 19. 05. 1998 – 9 AZR 394/97, BB 1999, 212.

142 Ständige Rechtsprechung; vgl. statt vieler LAG Hamm, Urt. v. 05.10.1988 – 15 Sa 1403/88; Preis in Erfurter Kommentar, 15. Auflage [2015], § 611 BGB Rn. 714; Rolfs in Preis, Der Arbeitsvertrag, 5. Auflage [2015], II V 20 Rz. 34.

143 Überblick zur Entwicklung der Rechtsprechung bei: *Gaugenrieder/Unger-Hellmich*, WRP 2011, 1364, 1373 ff.

von Art. 12 Abs. 1 GG erfasst, der das Recht auf ein berufliches Fortkommen schützt.[144] Umso wichtiger ist die vertragliche Ausgestaltung von einerseits zwar möglichst umfänglichen, andererseits aber auch interessengerechten Verschwiegenheitsverpflichtungen, um deren Wirksamkeit zu gewährleisten. Soweit eine nachvertragliche Verschwiegenheitsverpflichtung praktisch wie ein nachvertragliches Wettbewerbsverbot wirkt, sind die insofern geltenden Grenzen einzuhalten.[145]

Bei Selbstständigen, externen Dienstleistern oder Personal, das nicht dem Unternehmen angehört, in dem es eingesetzt ist, muss die Verschwiegenheitspflicht vertraglich genau geregelt werden, und zwar sowohl während als auch nach Ende der Tätigkeit.

b) Wettbewerbsverbote

Zu unterscheiden sind vertragliche und nachvertragliche Wettbewerbsverbote. Während der Dauer des Arbeitsvertrages ist es dem Arbeitnehmer bereits als Nebenpflicht untersagt, in Wettbewerb mit dem Arbeitgeber zu treten und somit dessen Interessen zu schädigen. Nach Beendigung des Arbeitsverhältnisses ist der Arbeitnehmer grundsätzlich frei, Wettbewerb zu betreiben. Will der Arbeitgeber dies verhindern, kann er bis zur Dauer von maximal zwei Jahren ein nachvertragliches Wettbewerbsverbot unter Zahlung einer Karenzentschädigung von mindestens der Hälfte der bisherigen vertraglichen Bezüge vereinbaren. Einzelheiten ergeben sich aus §§ 74 ff. HGB. Nachvertragliche Wettbewerbsverbote sind also teuer. Der Arbeitgeber muss genau überlegen, mit welchen Arbeitnehmern er dies vereinbaren wird; im Regelfall werden dies nur Schlüsselpersonen mit besonderen Kenntnissen sein.

Bei Geschäftsführern/Vorständen, Selbstständigen, externen Dienstleistern oder Personal, das nicht dem Unternehmen angehört, müssen Wettbewerbsbeschränkungen ebenfalls explizit vertraglich geregelt werden.

c) Abwerbeverbote

Insbesondere im US-amerikanischen Raum sind Verbote zwischen zwei Unternehmen, sich gegenseitig Arbeitnehmer abzuwerben (sog. Non-Solicitation-Klauseln), Standard in vielen Vertragswerken. Sie bieten Unternehmen die Möglichkeit, dem Konkurrenzkampf auf dem Arbeitsmarkt entgegenzuwirken und gleichzeitig dem Verlust wichtiger Mitarbeiter und sensiblen Know-hows vorzubeugen. Hierzulande ist der Spielraum für solche Vereinbarungen durch § 75f HGB stark begrenzt; Abwerbeverbote werden von der Rechtsprechung nur unter strengen Voraussetzungen und zeitlich befristet auf maximal zwei Jahre zugelassen[146]

---

[144] BAG, Urt. v. 15.12.1987 – 3 AZR 474/86, NZA 1988, 502 (503) – Kundenschutzabrede; BAG, Urt. v. 15.06.1993 – 9 AZR 558/91, NZA 1994, 502 (505) – Titandioxid.

[145] BAG, Urt. v. 19. 05. 1998 – 9 AZR 394/97, BB 1999, 212; vgl. auch *Redeker/Pres/Gittinger*, WRP 2015, 681 (686).

[146] § 75f HGB gilt nicht nur für Einstellungsverbote, sondern auch für Abwerbeverbote und findet zugleich Anwendung auf jeden Arbeitnehmer. Zu den eingeschränkten Voraussetzungen von Abwerbeverboten:

3. Allgemeine Geschäftsbedingungen

Geheimhaltungsverpflichtungen in Allgemeinen Geschäftsbedingungen (AGB) bieten den Vorteil, dass sie standardisiert für eine Vielzahl von Konstellationen angewendet werden können. Dabei unterliegen sie jedoch – auch im B2B-Bereich – der Wirksamkeitskontrolle nach § 307 BGB. Es ist grundsätzlich ratsam, eine wechselseitige Geheimhaltungsverpflichtung zu vereinbaren, wobei je nach Interessenlage – insbesondere in Konstellationen, in denen nur eine Partei ihr Know-how offenlegen muss – auch eine einseitige Verpflichtung zulässig sein dürfte.[147] Bei der Produktion mit Kundenbeteiligung (sog. Customizing) beispielsweise wird meist nicht nur der Unternehmer, sondern auch der Kunde gewisses Know-how offenbaren, um ein Produkt zu erhalten, welches optimal auf seine Vorstellungen abgestimmt ist. Mithin bergen nur einseitige Verpflichtung des Kunden zur Geheimhaltung des herstellereigenen Know-hows das Risiko der Unangemessenheit und damit Unwirksamkeit. Gleichermaßen kann sich eine unangemessene Benachteiligung durch Non-Disclosure-Klauseln in AGB ergeben, wenn keine zeitliche Begrenzung oder Ausnahmetatbestände enthalten sind, die den Gegenüber von seiner Verpflichtung zur Verschwiegenheit entbinden. Schließlich ist zu bedenken, dass die üblicherweise enthaltene Vertragsstrafe für den Fall der Verletzung der Geheimhaltungsvereinbarung sich auch im Einzelfall als angemessen erweisen muss.

III. Handlungsbedarf

Der Entwurf der Richtlinie zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen bringt für den wirtschaftlich relevanten Bereich des Know-how-Schutzes entscheidende Änderungen mit sich. Wollen Unternehmer auch zukünftig im Falle von Industriespionage beispielswiese gegen den unrechtmäßigen Verlust von firmeneigenen Betriebsgeheimnissen rechtlich vorgehen, werden sie nachweisen müssen, dass sie angemessene, d.h. wirksame und effektive Maßnahmen zum Schutz ihres Know-hows ergriffen haben. Durch die fortschreitende Digitalisierung und Vernetzung werden die Risiken des Verlustes von Betriebsgeheimnissen weiter zunehmen, was damit gleichzeitig auch für die erforderlichen Schutzmaßnahmen gilt, die einem solchen vorbeugen sollen. Im Hinblick auf Arbeitsverträge sollten die Unternehmen verstärkt darauf achten, wirksame Verschwiegenheitsklauseln und Wettbewerbsverbote mit speziellen identifizierten Arbeitnehmern abzuschließen. Die bestehenden Arbeitsverträge sind zu überprüfen, da sie häufig überholte oder unwirksame Klauseln enthalten. Aber auch in diversen anderen Konstellation ihrer betrieblichen Praxis, wie bei einer F&E-Kooperation oder dem Abschluss standardisierter Geschäfte mittels AGB, sind Unternehmer nunmehr verstärkt gehalten, die Wirksamkeit der Geheimhaltungsregelungen zu hinterfragen. Denn nur eine Information, die auch in ver-

---

BGH, Urt. v. 30.04.2014 – I ZR 245/12, BB 2014, 2897 – Abwerbeverbot; s. zum früheren Streitstand *von Hoyningen-Huene*, in: MüKoHGB, 3. Aufl. 2010, § 75f Rn. 5.

[147] Vgl. zu dieser Problematik bei Einkaufsbedingungen *Graf von Westphalen*, Vertragsrecht und AGB-Klauselwerke, 36. Ergänzungslieferung März 2015, Teil „Vertragsrecht“ X. Geheimhaltungsgebote – Wettbewerbsverbote Rn. 81; *Christensen* in Ulmer/Brandner/Hensen, AGB-Recht, 11. Aufl. 2011, Teil 2, (11) Einkaufsbedingungen Rn. 9.

traglicher Hinsicht entsprechenden Schutz genießt, kann im Falle des rechtswidrigen Verlusts den Schutz eines Geschäftsgeheimnisses genießen und Ansprüche gegen Dritte begründen.

Teil 5 Open Innovation/Kollaborationen/F&E *(Prof. Dr. Sebastian Wündisch, LL.M.)*

I. Forschung in Zeiten von 4.0 – Erscheinungsformen und Rechtsbeziehungen

1. Bedeutung und Erscheinungsformen

Die Bedeutung von Forschung und Entwicklung („F&E“) als Wachstumsmotor und Schlüssel zur Wettbewerbsfähigkeit kann nicht hoch genug eingeschätzt werden.[148] Die sich stetig verkürzenden Produktlebens- und Innovationszyklen, die zunehmende Komplexität von Produkten, Systemen und Technologien,[149] die steigenden Kosten im Bereich Forschung und Entwicklung, die zunehmende Globalisierung und der damit einhergehende Innovationsdruck[150] stellen gerade große Industrienationen vor die Herausforderung, Standortnachteile vor allem gegenüber Niedrigkostenländern durch ihren Wissensvorsprung zu kompensieren.[151]

Zur Steigerung ihrer Innovationskraft sind Unternehmen daher schon im vergangenen Jahrzehnt zunehmend dazu übergegangen, auf externe Wissensquellen zurückzugreifen. In der Wissenschaft wird dieses Phänomen unter dem Begriff „Open Innovation“ diskutiert, welches sich durch die Öffnung des betrieblichen Innovationsprozesses gegenüber externen Akteuren charakterisieren lässt.[152] Hintergrund ist die Erkenntnis, dass die *„Quelle, wo Wissen kreiert wird, nicht zwingend der Innovationsquelle entsprechen muss [und beide...] auch nicht notwendigerweise innerhalb des Unternehmens entspringen [müssen]“*.[153] Diese Abkehr von den klassischen internen Innovationsprozessen, die sich weitgehend im Unternehmen abspielen, hin zu einem offenen und vielschichtigen Such- und Lösungsprozess zwischen verschiedenen Akteuren (wie z.B. Lieferanten, Forschungsinstituten, Kunden, komplementären Partnerunternehmen etc.) über die Unternehmensgrenzen hinaus, hat damit einen griffigen, gleichwohl auch schillernden Titel bekommen.[154] Maßgeblich getrieben und potenziert wird diese Entwicklung nicht zuletzt von den Möglichkeiten, welche die Vernetzung bietet, indem sie eine einfache, kostengünstige und ortsunabhängige Basis zur Verfügung stellt, um die verschiedenen Akteure zusammen zu bringen.[155]

Die für Industrie 4.0 prägende Automatisierung der Fertigungstechnik und der Logistik mit dem Ziel von „intelligenten Fabriken“ (Smart Factories), welche sich durch Modularität, Ressourceneffizienz sowie die Integration von Kunden und Geschäftspartnern in Geschäfts- und Wertschöpfungsprozesse auszeichnen,[156] stellt daher eine entscheidende Komponente

---

148 *Wurzer*, GRUR 2008, 577 (578).
149 *Gerybadze*, in Eifert/Hoffmann-Riem (Hrsg.), Geistiges Eigentum und Innovation, S. 165 (166).
150 *Gassmann/Enkel*, zfo 3/2006, 132 (132, 137); *Reichwald/Piller*, Interaktive Wertschöpfung, 1 Aufl., S. 95.
151 *Reichwald/Piller*, Interaktive Wertschöpfung, 1 Aufl., S. 95.
152 *Chesbrough*, Open Innovation, 2003.
153 *Gassmann/Enkel*, zfo 3/2006, 132 (137).
154 *Reichwald/Piller*, Interaktive Wertschöpfung, 1 Aufl., S. 95.
155 Vgl. in diese Richtung auch *Reichwald/Piller*, Interaktive Wertschöpfung, 1 Aufl., S. 178.
156 Zum Begriff: https://de.wikipedia.org/wiki/Industrie_4.0, abgerufen am 31.08.2015.

und am Ende sogar zwingende Voraussetzung für diese modernen Innovationsformen dar: Die Automatisierung von Innovation in Form der Selbstoptimierung, Selbstkonfiguration, Selbstdiagnose und Kognition setzt als Basis die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen sowie die Fähigkeit, aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten, voraus.

Vor diesem Hintergrund überrascht es nicht, wenn das Modell der Open Innovation durch neue Schlagwörter wie DevOps und Hyperinnovation weiterentwickelt und ausdifferenziert wird. DevOps – als Kunstwort aus Development und Operations – steht für die enge Zusammenarbeit und Vernetzung von Entwicklungsteams und Anwendern zur Erleichterung von Kommunikation und Zusammenarbeit zur Erhöhung der Auslieferung neuer Entwicklungen.[157] Hyperinnovation umfasst demgegenüber die durch Digitalisierung, weltweite Vernetzung und vor allem mächtige Endgeräte gekennzeichnete umfassende digitale Rekombination und damit vor allem die Einbindung von Endanwendern in den Innovationsprozess, wie er auch durch die sog. Schwarmintelligenz vorangetrieben und bereits seit vielen Jahren durch die Open Source Bewegung praktiziert wird.

2. Rechtsbeziehungen

Das Konzept der „Open Innovation" lässt sich auf verschiedenstem Wege rechtlich umsetzen, wobei im Hinblick auf die Rechtsbeziehungen zwei wesentliche Gruppen zu unterscheiden sind:

- **Semi-offene Innovationsprozesse** sind gekennzeichnet durch einen **vorab festgelegten bzw. zumindest bestimmbaren Teilnehmerkreis**. Hierzu zählt bereits die innerbetriebliche Open Innovation z. B. durch die Vernetzung von Abteilungen, die klassische Auftrags- oder Kooperationsforschung unter Beteiligung von Dritten, beispielsweise Hochschulen und Forschungseinrichtungen, institutionellen Einrichtungen wie Standardisierungsorganisationen, Patentpools oder Innovationsnetzwerken. Rechtlich werden semi-offene Innovationsnetzwerke durch Vertrag oder sogar gesellschaftsrechtliche Strukturen zwischen allen Beteiligten nebst Festlegung von Rechten und Pflichten umgesetzt, die nicht zuletzt die Teilnehmer definieren und damit wesensimmanent zu einer Zugangsbeschränkung für oder sogar zum Ausschluss von Dritten führen.

- **Offene Innovationsprozesse** zeichnen sich dagegen durch einen **vorab unbestimmten Teilnehmerkreis** ohne Zugangsbeschränkung aus. Sie sind meist web-basiert, fußen regelmäßig auf Freiwilligkeit und haben gerade keinen verpflichtenden Charakter. Umgekehrt besteht damit auch kein „Anspruch" auf Beteiligung und Mitwirkung. Das

[157] *Loukides,* What is DevOps? – Infrastructure as a Code (http://radar.oreilly.com/2012/06/what-is-devops.html).

schließt nicht aus, dass im Falle einer Beteiligung rechtliche Instrumentarien zur Festlegung von Rechten und Pflichten Anwendung finden.

3. Semi-offene Innovationsprozesse

Gerade in Industriebereichen in denen Kompetenzen aus den unterschiedlichsten Branchen erforderlich sind, lassen sich zunehmend horizontale Kooperationen zwischen teilweise sogar konkurrierenden Unternehmen sowie vertikale Forschungs- und Entwicklungsaufträge beobachten. Instrument der Umsetzung sind meist umfassende Vertragswerke, die alle wesentlichen Punkte der Zusammenarbeit vorab vertraglich regeln.[158] Hierzu zählen insbesondere die Festlegung der jeweiligen F&E-Arbeiten und Arbeitspakete, der Zeitplan, die Vergütung und Finanzierung, der Zugriff auf vorbestehendes geistiges Eigentum während und nach der Zusammenarbeit („Background"), die Allokation der entstehenden geistigen Eigentumsrechte Eigentum während und nach der Zusammenarbeit („Foreground"), Geheimhaltungsvereinbarungen, Gewährleistung und Haftung sowie Dauer und Kündigung.

Derartige Vertragswerke sehen sich einer Fülle von rechtlichen Rahmenbedingungen gegenüber. Sie reichen von allgemeinen Grundsätzen des Zivilrechts und damit des BGB bis hin zum Recht des geistigen Eigentums, Kartellrecht, Beihilfenrecht sowie Gesellschaftsrecht.[159] Da diese Verträge zumeist als Dauerschuldverhältnisse ausgestaltet sind, stehen sie im besonderen Maße stets unter dem Risiko von Vertragsstörungen, die von Pflichtverletzungen bis hin zu der Insolvenz eines der Vertragspartner reichen. Die Komplexität zeigt sich schließlich in den häufig langwierigen Verhandlungen derartiger Vertragswerke, die für die regelmäßig gewichtigen Transaktionskosten verantwortlich zeichnen.

Darüber hinaus wird die Zusammenarbeit auch durch die Etablierung eigener Rechtspersonen institutionalisiert. So bündeln Unternehmen einer bestimmten Branche beispielsweise ihr geistiges Eigentum in sog. Patentpools, zu deren Gunsten die beteiligten Partner ihr geistiges Eigentum auf den Pool übertragen und an der gemeinsamen Nutzung durch Vergütungsschlüssel beteiligt werden.[160] Die jeweiligen Bedingungen werden meist im Rahmen der Satzung geregelt. Verbreitet sind auch Standardisierungsorganisationen[161] oder die Etablierung von Joint Venture Unternehmen.

Der Transaktionsaufwand – und die damit verbundenen Kosten bei der Umsetzung von semi-offenen Innovationsprozessen durch Vertrag oder gesellschaftsrechtliche Konstruktionen – stellen die Kehrseite dieser modernen Innovationsformen dar, die von der Innovationswissenschaft nur wenig wahrgenommen werden. Die Vorteile sind nicht zuletzt auch vor diesem Hintergrund zu bewerten.

---

[158] Beispielsweise als Kooperationsvertrag oder dienst- oder werkvertraglich geprägter Forschungs- und Entwicklungsvertrag; vgl. *Wündisch* in Weise/Krauß (Hrsg.), Beck'sche Online-Formulare Vertrag, 12. 3 und 12.4.

[159] *Rosenberger*, Verträge über Forschung und Entwicklung, 2. Aufl., S. 77.

[160] *Huebner* in Eifert/Hoffmann-Riem (Hrsg.), Geistiges Eigentum und Innovation, S. 185.

[161] Vgl. hierzu *Huebner* in Eifert/Hoffmann-Riem (Hrsg.), Geistiges Eigentum und Innovation, S. 185.

4. Beispiele offener Innovationsprozesse

Offene Innovationsprozesse sehen sich demgegenüber vor die Herausforderung gestellt, dass sich weder die Beteiligten und ihr Ressourceneinsatz voraussehen, noch bindend festlegen lassen. Die offene Innovationsprozesse kennzeichnende freiwillige Betätigung einer unbestimmten Teilnehmeranzahl muss durch Anreize geweckt werden. Das gilt insbesondere dann, wenn die interaktive Beteiligung von Nutzern und Kunden in den Innovationsprozess eingebunden wird. Beispiele hierfür sind Innovationsplattformen und -wettbewerbe sowie herstellerinitiierte Communities für Open Innovation. Besondere Bedeutung hat die Open Source Software (OSS), in der eine Vielzahl von Entwicklern gemeinsam eine Software (weiter)entwickeln.[162]

In der rechtlichen Umsetzung ist zu beobachten, dass die zentralen Themen, wie sie auch für semi-offene Innovationsprozesse von Relevanz sind, auch in offenen Innovationsprozessen von entscheidender Bedeutung sind. Durch die Verwendung von vorformulierten Bedingungen versuchen die Betreiber von Innovationsplattformen ihre rechtlichen Positionen durchzusetzten, insbesondere den möglichst umfänglichen Erwerb von Rechten an den Innovationen der Teilnehmer und den möglichst weitgehenden Ausschluss eigener Verantwortung. Diese Vorgehensweise ist selbst in der Open Source-Bewegung zu erkennen: Das Modell der „freien Software“ im Sinne einer umfassenden und freien Verbreitung des Quellcodes, seine Weiterentwicklung und vergütungsfreie Nutzung durch jedermann wird durch detaillierte Lizenzbedingungen auf Grundlage des der Software immanenten Urheberrechts durchgesetzt.[163] Verstöße gegen diese Lizenzbedingungen stellen daher regelmäßig Urheberrechtsverletzungen dar.

Im Hinblick auf die rechtliche Umsetzung stehen bei offenen Innovationsprozessen insbesondere die vorformulierten Bedingungen und damit das Recht der Allgemeinen Geschäftsbedingungen nach §§ 305 ff. BGB im Vordergrund. Neben den Anforderungen an eine wirksame Einbeziehung der Bedingungen als Geltungsvoraussetzung ist vor allem deren Wirksamkeit stets zu hinterfragen. Verschuldensunabhängige Haftungsfreistellungen bzw. der vollständige Rechte Buy-Out zulasten des Teilnehmers müssen sich an den Maßstäben der unangemessenen Benachteiligung im Sinne des § 307 BGB messen lassen. Die rechtssichere Implementierung derartiger Bedingungen ist insofern mit hohen Risiken verbunden.

II. Forschung in Zeiten von 4.0 – Rechteallokation

Die Umsetzung von Open Innovation stellt nicht zu unterschätzende Herausforderungen an die rechtliche Umsetzung, denen nur auf vertraglichem Wege begegnet werden kann. Insbesondere an der Allokation der Ergebnisse des Innovationsprozesses in Form der klassischen Schutzinstrumentarien für Innovationen – namentlich das geistige Eigentum an, dem

[162] *Wündisch* in Meißner/Engelien, Virtuelle Organisation und neue Medien 2005, .S 482; *Teufel*, Mitt. dt. Patentanwälte 2007, 341 (343).

[163] *Teufel*, Mitt. dt. Patentanwälte 2007, 341 (344), *Metzger* in Eifert/Hoffman-Riem (Hrsg.), Geistiges Eigentum und Innovation, S. 198.

Patentrecht zugänglichen, Erfindungen oder dem Urheberrechtsschutz unterliegender Software – wird dies deutlich.[164] Die Vielzahl von Beteiligten, deren individuelle Kreativität und das Entstehen der Innovationen durch interaktive und netzwerkbasierte Innovationsprozesse führen zwangsläufig auf die Frage, wem an diesen Leistungen etwa bestehende gewerbliche Schutz- und Urheberrechte zustehen. Regelmäßig haben sowohl die Beteiligten an semi-offenen Innovationsprozessen wie auch die Initiatoren offener Innovationsprozesse ein hohes Interesse an einem größtmöglichen Erwerb der Rechte an den dort entstehenden Innovationen und damit der Konzentration der Exklusivität auf möglichst nur einen Rechteinhaber. Es ist daher zu beobachten, dass Teilnehmer an semi-offenen bzw. Initiatoren von offenen Innovationsprozessen in der Praxis erhebliche Bemühungen unternehmen, um die geistigen Eigentumsrechte möglichst vollumfänglich zu ihren Gunsten zu allokieren. In Vertragsverhandlungen und der Gestaltung von Bedingungen für Innovationsplattformen stellt die Sicherstellung des Erwerbs der Rechte daher einen wesentlichen und oftmals auch sehr streitigen Punkt dar. Schutzrechtsregelungen über mehrere Seiten sind in Kooperationsverträgen folglich keine Ausnahme.

1. Exklusivität und Blockadevermeidung

Die Ursache hierfür liegt zunächst darin, dass der Innovationsschutz von dem axiomatischen Verständnis geprägt wird, dass die Sicherung der Exklusivität der innovativen Leistung durch Ausschließlichkeitsrechte in Form von geistigen Eigentumsrechten unabdingbare Voraussetzung für den wirtschaftlichen Erfolg ist.[165] Dieser Ansatz steht im Einklang mit der raison d'être geistiger Eigentumsrechte: Durch eine staatlich gewährte Monopolstellung soll dem Kreativen die wirtschaftlichen Verwertung seiner Innovationen vorbehalten und somit ein Anreiz für die Schaffung von Innovationen gesetzt werden.[166]

Vor allem muss der Nutzer aber sicherstellen, dass er seinerseits keine geistigen Eigentumsrechte Dritter bei der Verwertung verletzt. Die fehlende Berechtigung an einer Innovation führt in der Konsequenz dazu, dass der betreffende Inhaber die Verwertung blockieren kann – ein Risiko, dem sich kein Unternehmen sehenden Auges aussetzen kann und darf. Der Erwerb einer Berechtigung an den in der Innovation verkörperten geistigen Eigentumsrechten ist daher zwingende Voraussetzung für deren Verwertung. Ohne das Recht zur Verwertung ist jede Innovation nutzlos.

Selbst bei einer entsprechenden vertraglichen Regelung bleibt die Rechtsübertragung gefährdet, wenn der Kreative über diese Rechte bereits zugunsten eines Dritten verfügt hat oder Verfügungsbeschränkungen unterliegt. Man stelle sich nur den Fall vor, in dem ein Ingenieur eines großen Industrieunternehmens auf der Open Innovation Plattform eines Konkurrenten Lösungen für Konkurrenzprodukte einbringt. Derartige Verfügungen sind seinem

---

[164] *Lutterbeck*, in Eifert/Hoffman-Riem (Hrsg.), Geistiges Eigentum und Innovation, S. 220: „Es gibt keine klare Unterscheidung zwischen Markt und Unternehmen mehr".

[165] In diese Richtung beispielsweise *Kraßer*, Patentrecht, 5. Aufl., S. 34.

[166] *Mes*, PatG, 4. Aufl., § 1 Rz. 2; ausf. *Kraßer*, Patentrecht, 5. Aufl., S. 34; *Metzger* in Eifert/Hoffman -Riem (Hrsg.), Geistiges Eigentum und Innovation, S. 191.

Arbeitgeber gegenüber nach § 7 Abs. 2 ArbnErfG unwirksam. Insoweit besteht eine wesentliche Schnittstelle zum Arbeitsrecht, wonach das Arbeitsergebnis dem Arbeitgeber zusteht und Übertragungen durch den Arbeitnehmer an Dritte regelmäßig im Widerspruch zu arbeitsrechtlichen Regelungen stehen.

2. Strenges Erfinder- und Schöpferprinzip und Erfordernis des abgeleiteten Erwerbs

Für den Erwerb dieser Rechte ist zwingend das dem deutschen Recht immanente Erfinder- bzw. Schöpferprinzip zu beachten.[167] § 6 PatG räumt dem Erfinder als natürlicher Person das *Recht auf das Patent* ein. Diese Bestimmung, die das Recht auf das Patent dem Erfinder als Schöpfer der neuen technischen Lehre zuordnet, ist Ausdruck der Anerkennung der schöpferischen Leistung des Erfinders.[168] Auch nach § 7 UrhG ist Urheber immer die natürliche Person, welche das urheberrechtlich geschützte Werk geschaffen hat. Nur in wenigen Ausnahmenfällen weicht das Gesetz von dieser Grundregel ab und ordnet innovative Leistungen demjenigen zu, welcher die (finanziellen) Investitionen getätigt hat, z. B. bei Datenbanken nach § 87 a ff. UrhG. Ein Dritter – im Übrigen auch der Arbeitgeber – muss mithin immer die Rechte abgeleitet vom Erfinder/Urheber erwerben, was im Wege einer Vollübertragung oder Lizensierung (§ 15 Abs. 1, 2 PatG) bei Erfindungen oder der Einräumung von (exklusiven) Nutzungsrechten an urheberrechtlich geschützten Werken möglich ist.

Der Erwerb der Rechte erweist sich im Regelfall als unproblematisch, wenn – dem gesetzlichen Leitbild des Patent- und Urheberrechts entsprechend – nur ein Erfinder/Urheber bzw. maximal zwei oder drei beteiligt sind. Probleme treten allerdings dann auf, wenn an der Innovation mehrere Erfinder/Schöpfer beteiligt sind. Zwar sehen sowohl das PatG als auch das UrhG Regelungen für Erfinder- und Urhebergemeinschaften (§ 6 PatG, §§ 8, 9 UrhG) i. S. einer Zentralisierung bzw. gemeinsamen Verwertung dieser Rechte vor. Aber auch diese Vorschriften sind nur begrenzt anwendbar, wenn der Teilnehmerkreis unbestimmt und durch sukzessives Zusammenwirken geprägt ist. Die Vereinigung des Gesamtergebnisses auf einen Rechteerwerber stellt dann hohe Anforderungen an die Vertragsgestaltung und das Management dieser Prozesse.

Ein anschauliches Beispiel hierfür findet sich in der Open Source Bewegung. Das der Entwicklung von Open Source Software immanente sukzessive Zusammenwirken einer Vielzahl von Entwicklern führt ebenfalls zu Problemen bei der personellen Zuordnung der Urheberrechte an der Open Source Software und den hieraus fließenden Ausschließlichkeitsrechten. Allerdings ist die Arbeitsteilung dem kreativen Schaffen nicht fremd. Aus diesem Grunde sieht z. B. das Urheberrechtsgesetz detaillierte Regelungen zur Miturheberschaft (§ 8 UrhG) und Urhebern verbundener Werke (§ 9 UrhG) vor (Abbildung 2), deren Innen- und Außenverhältnis detailliert durch Konstituierung einer modifizierten Gesellschaft des bürgerlichen Rechts (GbR) geregelt wird.

---

[167] *Mes*, PatG, 4. Aufl., § 6 Rz. 1.
[168] *Mes*, PatG, 4. Aufl., § 1 Rz. 2.

Ob allerdings diese Vorschriften auch dem Schöpfungsprozess innerhalb einer Open Source-Entwicklungsgemeinschaft gerecht werden, ist aufgrund der für diese Gemeinschaften typischen dezentralen Sukzessivität fraglich:[169] Neben der Frage nach dem Vorhandensein eines Rechtsbindungswillens für den Abschluss eines Gesellschaftsvertrags entzieht sich der Gesellschafterbestand regelmäßig der Bestimmbarkeit und verhindert damit eine Willensbildung bereits im Ansatz, sodass die Verwaltung der Gesellschaft als von Anfang an undurchführbar erscheint. Insbesondere fehlt es an der für die Miturheberschaft bzw. die Urheber verbundener Werke notwendigen gemeinsamen Zweckverfolgung – eine Gesellschaft ad incertas personas ist dem deutschen Recht insoweit fremd.[170] Im Ergebnis wird man von einem Geflecht von individuellen Rechtsbeziehungen ausgehen (Abbildung 1), so dass eine Allokation auf einen Rechtsträger kaum möglich ist.

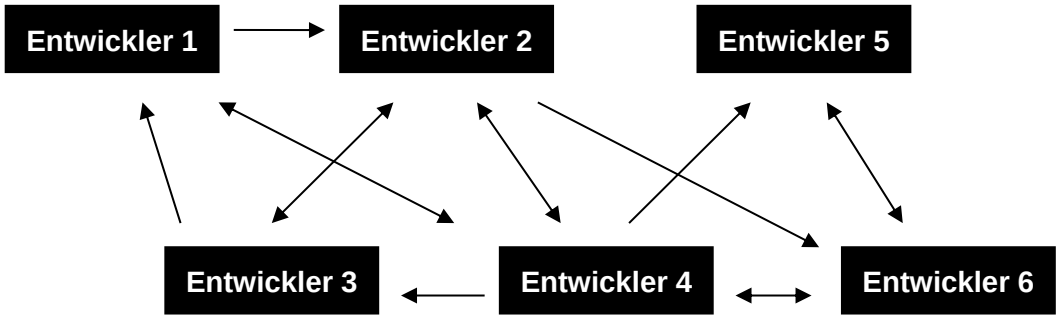
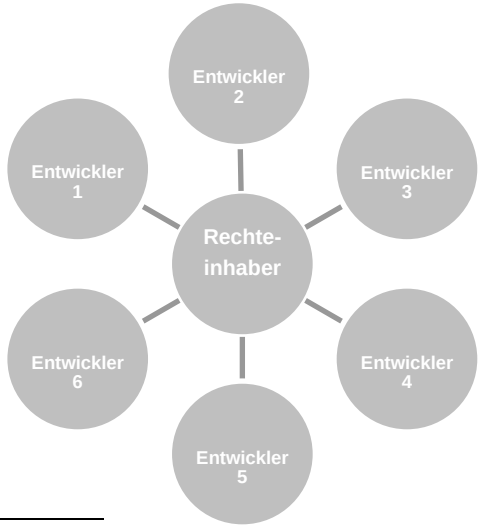


Abbildung 1: Entwicklungsgemeinschaft

Zur Strukturierung dieser komplexen Gemeinschaften und zum Zwecke der effektiven Rechtsverfolgung sind daher die urheberrechtlichen Befugnisse auf einen Rechtsträger zu vereinigen, was letztlich den direkten Erwerb der einzelnen Rechtspositionen vom jeweiligen Entwickler durch eine vertragliche Regelung voraussetzt (Abbildung 2: sog. Zentralisierungsmodell).



[169] Eingehend *Spindler,* in: Spindler (Hrsg.), Rechtsfragen bei Open Source, S. 33 ff.

[170] Zu Gesellschaftsformen und -verträgen für virtuelle Unternehmen *Benz/Kowald*, in Meißner/Engelien (Hrsg.), Virtuelle Organisation und Neue Medien 2005, S 21.

Abbildung 2: Zentralisierungsmodell

III. Erfinderprinzip vs. netzwerkorientierter Eigentumsbegriff

Vor dem skizzierten Spannungsverhältnis zwischen Individualrechtsschutz einerseits und Network Community andererseits verwundert nicht, dass die Rechtswissenschaft bereits einen netzwerkorientierten Eigentumsbegriff diskutiert, der letztlich zu einer Aufweichung oder gar Abschaffung individueller Eigentumspositionen an in Netzwerken geschaffenen geistigen Eigentum führen könnte.[171] Vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts, wonach geistige Eigentumsrechte von Art. 14 GG erfasst werden,[172] erscheint eine Umsetzung dieser vagen Ansätze eher fraglich. Vor allem ist das Recht des geistigen Eigentums aufgrund dessen Ubiquität immer im internationalen Kontext zu sehen und eine neue Definition würde eine umfassende Harmonisierung und Anpassung auf weltweiter Basis voraussetzen – zumal gerade das Netzwerk von seiner internationalen Ausrichtung lebt.

IV. Schutzrechte bei Produktion nach Kundenwunsch und Verantwortung

Die Differenzierungsschwierigkeiten zwischen Kreativen und Nutzern zeigen sich insbesondere bei der durch Industrie 4.0 möglichen individuellen Produktion auf Kundenwunsch. Der Kunde ist heute in der Lage, ein Produkt genau nach seinen Vorstellungen individuell zu entwerfen oder anzupassen und im Anschluss produzieren zu lassen. Das wirft freilich die Frage auf, wem die Rechte an dieser Kundenanfertigung gehören. Auch hier ist nach geltendem Recht (kreative Leistungen des Kunden stehen zunächst dem Kunden zu) eine Allokation der Rechte an das produzierende Unternehmen nur durch vertragliche Vereinbarung – im Regelfall durch AGB – möglich. Neben der Wirksamkeit solcher Vereinbarungen treten die Anforderungen der verbraucherschutzrechtlichen Vorschriften der §§ 312 ff. BGB, die – die Qualifikation des Kunden als Verbraucher vorausgesetzt – bspw. im Hinblick auf Informationspflichten und Widerrufrechte zu der Frage nach der Anwendbarkeit und den jeweiligen Rechtsfolgen führen.

Neben der Allokation der entstehenden Rechte stellt sich bei Produktion nach Kundenwunsch im verstärkten Maße die Frage, wer für die Verletzung der Rechte Dritter einzustehen hat, wen also das Risiko einer Schutzrechtsverletzung trifft. Grundsätzlich verantwortlich für eine Schutzrechtsverletzung sind nach allgemeinen deliktsrechtlichen Grundsätzen die Täter und Störer. Daneben sind zahlreiche Beteiligungsformen möglich, die von einer Mittäterschaft bis hin zu Beihilfe und Anstiftung reichen. Eine Verantwortlichkeit von

[171] *Ladeur/Vesting* in Eifert/Hoffman-Riem (Hrsg.), Geistiges Eigentum und Innovation, S. 139.
[172] BVerfGE 31, 229 (239); 49, 382 ff.; 79, 29 (40 f.); 81, 12 (16); 97, 228 (264).

Kunde und Unternehmen im Außenverhältnis liegt auf der Hand – für das Innenverhältnis kommt es wiederum auf die vertragliche Vereinbarung an.

V. Handlungsbedarf

Forschung und Entwicklung in Zeiten von Open Innovation und Industrie 4.0 sehen sich auch in rechtlicher Hinsicht komplexen Herausforderungen gegenüber. Das etablierte System der geistigen Eigentumsrechte ist in Einklang mit den neuen technischen Möglichkeiten zu bringen. Es ist insbesondere sicherzustellen, dass die geschaffenen Innovationen ohne die Verletzung von Rechten der Kreativen verwertbar sind. Das setzt stets vertragliche Vereinbarungen mit dem Kreativen zum Erwerb der Rechte voraus, die praktisch nur durch AGB implementiert werden können. Während Buy-Out-Klauseln bei formularmäßiger Verwendung unter Beachtung des Transparenzgebotes zumindest im Urheberrecht zulässig sind,[173] gilt dies nicht für verschuldensunabhängige Haftungsfreistellungen.[174] Vor diesem Hintergrund ist weniger an eher metaphysisch anmutende neue netzwerkgerechte Eigentumsmodelle zu denken, sondern vielmehr an eine Anpassung der zwingenden Vorschriften über allgemeine Geschäftsbedingungen gem. §§ 305 ff. BGB zur Sicherstellung des Rechteerwerbs auch in offenen Innovationsprozessen.

[173] BGH, Urteil v. 17.10.2013 – I ZR 41/12.
[174] BGH, Urteil v. 5. 10. 2005 – VIII ZR 16/05, NJW 2006, 47 (49).

Teil 6 IP-Recht in der digitalen Welt *(Sandra Sophia Redeker, Katharina Klett, LL.M., Prof. Dr. Ulrich Michel)*

I. Urheberrecht

1. Rechte an Ergebnissen aus automatisierten Prozessen (computer generated works)

Die Vernetzung und Lernfähigkeit von intelligenten Systemen der Industrie 4.0 wirft die Frage auf, ob Ergebnisse aus automatisierten Prozessen urheberrechtlichen Schutz genießen können und wer als deren Urheber in Betracht zu ziehen ist.

a) Schutzfähigkeit

Werke, die dem Schutz des Urheberrechts unterliegen, sind lediglich persönliche geistige Schöpfungen, § 2 Abs. 2 UrhG. Der Werkbegriff setzt voraus, dass die Schöpfung in ihrer konkreten Gestalt der sinnlichen Wahrnehmung zugänglich ist.[175] Die Idee, auf der die Schöpfung beruht, ist frei.[176] Daher kommt zum Beispiel wissenschaftlichen Lehren und Algorithmen kein urheberrechtlicher Schutz zu.[177] Eine persönliche geistige Schöpfung kann nur eine natürliche Person erbringen. Allein der Mensch besitzt den individuellen Geist, der im Schöpfungsakt Ausdruck findet.[178] Dies gilt auch beim Einsatz neuer Technologien.[179]

Computer generated works genießen folglich von vornherein keinen urheberrechtlichen Schutz, wenn sie ohne menschliche Beteiligung produziert werden.[180] Ihnen fehlt der menschliche Geist, der in der konkreten Formgebung zum Ausdruck kommen muss.[181] Zeichnungen, Musik oder Fotografien, die selbstständig aufgrund eines automatisierten Prozesses ohne menschliches Zutun erzeugt werden, sind dem Schutz des Urheberrechts entzogen.[182] Gleichermaßen mangelt es an einer persönlichen geistigen Schöpfung, wenn Übersetzungen eines Sprachwerks von einem Computerprogramm durchgeführt werden.[183] Irrelevant ist in diesen Fällen, ob das zugrundeliegende Programm urheberrechtlichen Schutz genießt.[184] Erschafft daher ein technisches Erzeugnis selbstständig ein Produkt, das grundsätzlich den Werkkategorien des § 2 Abs. 1 UrhG unterfallen kann, besteht kein urheberrechtlicher Schutz. Löst z.B. ein Roboter im Rahmen eines intelligenten Produktions- o-

---

175 BGH, Urt. v. 09.05.1985 – I ZR 52/83 – CR 1985, 22 (23) – Inkasso-Programm.
176 *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 51 m. w. N.
177 *Bullinger* in Wandtke/Bullinger, UrhR, 4. Aufl., § 2 Rz. 19.
178 LG Berlin, Urt. v. 30.05.1989 – 16 O 33/89 – GRUR 1990, 270 – Satellitenfoto; *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 7 Rz. 2.
179 *Wiebe* in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl., § 7 UrhG Rz. 3.
180 *Dreyer* in Dreyer/Kotthoff/Meckel, UrhG, 2. Aufl., § 2 Rz. 25; *Wiebe* in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl., § 7 UrhG Rz. 3.
181 Vgl. *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 18.
182 Vgl. *Dreyer* in Dreyer/Kotthoff/Meckel, UrhG, 2. Aufl., § 2 Rz. 25; *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 12.
183 *Ahlberg* in Ahlberg/Götting, UrhG, 9. Ed., § 2 Rz. 55; *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 12.
184 Vgl. *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 12.

der Serviceprozesses ein ihm gestelltes Problem selbstständig durch ein Erzeugnis, das dem Urheberrechtsschutz grundsätzlich zugänglich ist, ohne dass die konkrete Gestaltung dieser Lösung von einem Menschen vorgegeben ist, bleibt dem Erzeugnis der Schutz des Urheberrechts verwehrt. Ein Computerprogramm, das durch ein Software-Generatorprogramm erstellt wird, unterfällt folglich nicht dem Urheberrecht.[185] Gleiches gilt für Smart Products, wenn diese aufgrund ihrer Lernfähigkeit ihre Funktionalität oder ihr Verhalten über das vom Programmierer vorbestimmte Maß hinausentwickeln oder mit anderen Smart Products zusammenwirken[186] und neue Ergebnisse kreieren. Das Urheberrecht würdigt ausschließlich die schöpferische Leistung einer Person, indem ihr ein Ausschließlichkeitsrecht gewährt wird.[187] Kann das Erzeugnis lediglich auf die ergebnisoffene Programmierung zurückgeführt werden, fehlt es an dem unabdingbaren unmittelbarem Zusammenhang zwischen Ergebnis und schöpferischem Schaffen.[188]

Der Urheber darf sich allerdings bei der Schaffung seiner persönlichen geistigen Schöpfung technischer Hilfsmittel bedienen.[189] Allein deren Einsatz führt nicht dazu, dass das geschaffene Werk nicht mehr Ausdruck seines individuellen Geistes ist.[190] Voraussetzung ist, dass der Mensch den Schaffungsprozess gestalterisch und planend beeinflusst, so dass eine eigene gestalterische Tätigkeit angenommen werden kann.[191] Wird die Auswahl der Form und des Inhalts dem Werkzeug überlassen, fehlt der maßgebliche menschliche Einfluss, auch wenn der Schaffungsprozess von Menschenhand initiiert wurde.[192] Fehlt es bei computer generated works an jeglicher geistigen Schöpfung, kann computer-aided works Urheberschutz zukommen. Dies gilt insbesondere, wenn das Ergebnis anhand menschlicher Anweisung eindeutig geplant und festgelegt wird.[193] Dem steht nicht entgegen, dass der Urheber gewisse Zufallselemente in seine schöpferische Tätigkeit einbezieht.[194] Wichtig ist dabei, dass der Mensch die Maschine nicht bloß beherrscht, sondern mit ihrer Hilfe aus eigener geistiger Quelle eine schöpferische Gestaltung hervorbringt.[195] Wirken Mensch und technisches Werkzeug so zusammen, dass sich das Ergebnis in selbstständige Teile zerlegen lässt, sind die aufgezeigten Kriterien auf jeden Teil gesondert anzuwenden.[196]

---

185 *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 69a Rz. 15.
186 Vgl. hierzu *Kirn/Müller-Hengstenberg*, MMR 2015, 225 (226).
187 Vgl. *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 12.
188 Vgl. *Ahlberg* in Ahlberg/Götting, UrhG, 9. Ed., § 2 Rz. 55.
189 Vgl. LG Berlin, Urt. v. 30.05.1989 – 16 O 33/89 – GRUR 1990, 270 – Satellitenfoto.
190 *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 13.
191 *Dreyer* in Dreyer/Kotthoff/Meckel, UrhG, 2. Aufl., § 2 Rz. 26.
192 *Dreyer* in Dreyer/Kotthoff/Meckel, UrhG, 2. Aufl., § 2 Rz. 26.
193 *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 13; weitergehend *Hecker* in Limper/Musiol, Handbuch des Fachanwalts für Urheber- und Medienrecht, 3. Kap Rz. 4.
194 *Ahlberg* in Ahlberg/Götting, UrhG, 9. Ed., § 2 Rz. 55; *Bullinger* in Wandtke/Bullinger, UrhR, 4. Aufl., § 2 Rz. 17; S*chulze* in Dreier/Schulze, UrhG, 5. Aufl., § 2 Rz. 8.
195 *Ahlberg* in Ahlberg/Götting, UrhG, 9. Ed., § 7 Rz. 8.
196 *Dreyer* in Dreyer/Kotthoff/Meckel, UrhG, 2. Aufl., § 2 Rz. 30.

b) Urhebereigenschaft

Das deutsche Urheberrecht ist durch das Schöpferprinzip geprägt.[197] Urheber ist der Schöpfer des Werks, § 7 UrhG. Als Schöpfer wird diejenige Person angesehen, die eine zur Schaffung des Werks erforderliche persönliche geistige Schöpfung i. S. d. § 2 Abs. 2 UrhG erbringt.[198] Da allein der Mensch die notwendige geistige Leistung erbringen kann, sind Maschinen, Computer und Apparate mangels individueller geistiger Tätigkeit nie die Urheber ihrer geschaffenen Ergebnisse.[199] Ob die natürliche Person, die sich technischer Hilfsmittel zur Schaffung eines Werks bedient, als Urheber der Erzeugnisse anzusehen ist, bestimmt sich nach der zur Schutzfähigkeit aufgezeigten Abgrenzung zwischen computer generated und computer-aided works. Schutzfähigkeit und Urhebereigenschaft korrespondieren unmittelbar, da nur an schutzfähigen Werken Urheberschaft bestehen kann.

2. Digital Rights Management Systeme (DRM)

Digital Rights Management Systeme (DRM) sind technische Mittel, mit deren Hilfe digitale Inhalte gegen den unbefugten Zugriff geschützt, deren Gebrauch überwacht und die Verwertung abgewickelt werden können.[200] Besondere Bedeutung hat dabei der Kopierschutz erlangt, der lediglich autorisierten Nutzern den Zugriff in einem vertraglich vereinbarten Rahmen gewährt und unbefugte Vervielfältigungen zu verhindern versucht.[201]

Wird der Zugang und die Nutzung urheberrechtlich geschützter Werke oder anderer nach dem UrhG geschützter Schutzgegenstände durch DRM kontrolliert, gewähren die §§ 95a ff. UrhG rechtlichen Schutz gegen die unbefugte Umgehung dieser Systeme.[202] Nach § 95a Abs. 1 UrhG dürfen wirksame technische Maßnahmen zum Schutz eines urheberrechtlich geschützten Werks oder anderer nach dem UrhG geschützter Schutzgegenstände ohne Zustimmung des Rechtsinhabers nicht umgangen werden. Subjektiv hätte dem Handelnden zumindest bekannt sein müssen, dass die Umgehung der Systeme erfolgt, um den Zugang zu einem geschützten Werk oder dessen Nutzung zu ermöglichen. Zudem sind gemäß § 95 Abs. 3 UrhG bestimmte Vorbereitungshandlungen im Vorfeld der Umgehung verboten. Flankiert werden diese Vorschriften zum Schutz der DRM durch entsprechende Straf- und Bußgeldvorschriften in den §§ 108b und 111a UrhG.

Im Rahmen der Entwicklung der Industrie 4.0 und der einhergehenden Vernetzung einzelner Geräte besteht die Gefahr, dass urheberrechtlich geschützte digitale Inhalte unter Umgehung der DRM unbefugt genutzt werden. Werden diese Mechanismen vom Verletzer so

---

[197] *Schulze* in Dreier/Schulze, UrhG, 5. Aufl., § 7 Rz. 1; *Thum* in Wandtke/Bullinger, UrhR, 4. Aufl., § 7 Rz. 1.
[198] OLG Hamburg, Urt. v. 10.07.2002 – 5 U 41/01 – GRUR-RR 2003, 33 (34) – Maschinenmensch.
[199] *Dreyer* in Dreyer/Kotthoff/Meckel, UrhG, 2. Aufl., § 2 Rz. 25; *Loewenheim* in Schricker/Loewenheim, UrhG, 4. Aufl., § 2 Rz. 12; *Schulze* in Dreier/Schulze, UrhG, 5. Aufl., § 7 Rz. 2; *Thum* in Wandtke/Bullinger, UrhR, 4. Aufl., § 7 Rz. 1.
[200] *Arlt*, Digital Rights Management Systeme, 2006, S. 12 m. w. N.
[201] *Schippan*, ZUM 2004, 188 (189).
[202] *Schippan*, ZUM 2004, 188 (196).

eingesetzt, dass er zumindest fahrlässig[203] verkennt, dass DRM umgangen werden, greift § 95a Abs. 1 UrhG unproblematisch. Selbst die Herstellung oder der gewerbliche Besitz von Vorrichtungen und Erzeugnissen, die neben der Umgehung von DRM nur einen begrenzten wirtschaftlichen Nutzen haben oder hauptsächlich zur Ermöglichung oder Erleichterung der Umgehung entworfen, hergestellt oder angepasst wurden, sind nach § 95a Abs. 3 Nr. 2 und 3 UrhG verboten. Von § 95a UrhG nicht erfasst werden hingegen Sachverhalte, in denen Smart Products oder Fertigungsanlagen aufgrund ihrer Vernetzung und ihrer Lernfähigkeit DRM aus „eigenem Antrieb" umgehen, ohne dass dies von Programmierern, Entwicklern oder dem Verwender vorherzusehen war.

Aus diesem Befund ergeben sich jedoch unseres Erachtens keine Anhaltspunkte für ungewollte Schutzlücken, die dem weiteren Fortschritt und der Entwicklung der Industrie 4.0 entgegenstehen. Schon jetzt erfasst § 95a UrhG nicht diejenigen Umgehungshandlungen, die ohne schuldhaftes Verhalten vorgenommen werden. Fehlt es am menschlichen Fehlverhalten, bietet § 95a Abs. 1 UrhG keinen Schutz der technischen Maßnahmen. Ein absoluter Schutz der DRM besteht daher nicht. Zudem besteht ungeachtet der §§ 95a ff. UrhG der urheberrechtliche Schutz des Werks mit den sich aus den §§ 97 ff. UrhG ergebenden Ansprüchen, so dass ausreichende Abwehrmechanismen zur Verfügung stehen.

3. Lizenzmodelle

Die Disposition über Intellectual Property (IP) in Industrie 4.0-Projekten erfolgt regelmäßig im Wege bilateraler und multilateraler Verträge zwischen den am Projekt Beteiligten. Neben einzelnen Nutzungsverträgen können Foreground-IP (IP-Rechte an Projektergebnissen) und/oder Background-IP (für die Forschungs- und Entwicklungsarbeit erworbene IP) gepoolt und auf diesem Wege gemeinschaftlich genutzt werden.

a) Einzelverträge

In jeder möglichen Gestaltung werden die einzelnen am 4.0-Projekt Beteiligten Rechte an Background-IP anderen Beteiligten und/oder einem Pool einräumen. Bei der Lizenzierung von Background-IP wird es sich regelmäßig um nicht exklusive Rechte handeln. Je nach Gestaltung der Verwertung neu geschaffener Technologien wird die Lizenzierung der Background-IP auf die Forschung und Entwicklung neuer Technologien begrenzt sein oder von Anfang an eine Verwertung der mit Hilfe der Background-IP neu entwickelten Technologien gestatten.

Ähnliches gilt für die Lizenzierung von Foreground-IP: Die Rechte an im Wege eines 4.0-Projektes neu entwickelten Technologien wird in der Regel für die Herstellung entsprechender Produkte und die Erbringung von Dienstleistungen durch einzelne oder mehrere Projektbeteiligte und/oder Drittunternehmen genutzt werden. Die Einräumung dieser Nutzungsrechte wird erneut im Wege von einzelnen Lizenzverträgen erfolgen.

[203] Siehe zum Verschuldensgrad *Götting* in Schricker/Loewenheim, UrhG, 4. Aufl., § 95a Rz. 12 einerseits und *Dreyer* in Dreyer/Kotthoff/Meckel, UrhG, 2. Aufl., § 95a Rz. 30 andererseits.

b) Poolverträge

Das Pooling von IP-Rechten kann sinnvoll sein, wenn

- in der Forschungs- und Entwicklungsarbeit im Rahmen eines 4.0-Projektes das Handling von Background-IP aus einem Pool heraus besser gestaltbar ist; oder
- dem Management des Rechtepools eine Überwachung der Nutzung der Background-IP übertragen werden soll; oder
- eine Verwertung neu geschaffener Foreground-IP durch Bündelung von Rechten besser erfolgen kann.

Ob einer oder mehrere dieser Gründe zur Vereinbarung eines Rechtepools vorliegen werden, hängt von den konkreten Umständen bei der Entwicklung und Verwertung neuer Technologien im Rahmen eines 4.0-Projektes ab.

Hinsichtlich der künftigen Lizenzierungspraxis wird das laufende Gesetzgebungsverfahren betreffend das Urhebervertragsrecht möglicherweise sehr bedeutend sein: Der Referentenentwurf des BMVJ zum Urhebervertragsrecht vom 05.10.2015 sieht mit einem neuen § 40a UrhG-E das Recht jeden Urhebers vor, exklusiv eingeräumte Rechte nach 5 Jahren zurückzurufen, wenn sich ein Dritter zur Nutzung dieses Rechtes nach Rückruf verpflichtet hat. Sublizenzen sollen im Falle eines solchen Rückrufs automatisch enden. Der erste Nutzer soll (allein) im Wege eines Rechtes zum Vertragseintritt den Rückruf abwenden können. Im Falle eines In-Kraft-Tretens dieser Vorschrift werden exklusive Rechte betreffend IT und andere urheberrechtlich geschützte Assets nur noch für fünf Jahre gesichert werden können. Lizenznehmer müssen in diesem Szenario mit einer Übernahme dieser exklusiven Rechte durch Dritte, namentlich Wettbewerber, rechnen und - so weit möglich - entsprechende Vorkehrungen treffen.

4. Ausblick: mögliche Folgen aus der digitalen Agenda der EU-Kommission

a) EU-Copyright

In ihrer Strategie für einen digitalen Binnenmarkt für Europa kündigte die EU-Kommission an, das Urheberrecht harmonisierende Rechtssetzungsvorschläge zu unterbreiten. Der EU-Kommission ist die Fragmentierung der digitalen Märkte ein Dorn im Auge, da die Bürger der Mitgliedstaaten der EU oftmals nicht über Grenzen hinweg auf kommerzielle und kulturelle Inhalte und Dienste zugreifen können. Ein fragmentierter Markt verhindert nach Ansicht der EU-Kommission die Entfaltung des Internets der Dinge.[204] Die bestehende uneinheitliche Umsetzung von Urheberrechtsvorschriften erschwert zudem die Entwicklung und Nutzung von Daten und neuer Technologieanwendungen.[205] Diesen Beschränkungen will

[204] EU-Kommission, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 v. 6.5.2015, S. 16.
[205] EU-Kommission, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 v. 6.5.2015, S. 16.

die EU-Kommission durch die Beseitigung rechtlicher Schranken begegnen und die Unterschiede zwischen den nationalen Urheberrechtssystemen verringern.[206] So sah bereits im Jahr 2010 die Agenda der EU-Kommission vor, dass einheitlichere und technologieneutrale Lösungen für eine grenzübergreifende und europaweite Lizenzierung im audiovisuellen Sektor gefunden werden müssen.[207] Noch im Jahr 2015 will die EU-Kommission aufzeigen, wie die Portabilität rechtmäßig erworbener Inhalte und der grenzüberschreitende Zugang zu rechtmäßig erworbenen Online-Diensten im audiovisuellen Sektor gewährleistet werden können. Für die Entwicklung von Produkten und Erzeugnissen der Industrie 4.0, die auf die Nutzung urheberrechtlich geschützter Inhalte angewiesen sind, bietet die Strategie der EU-Kommission erhebliches Entwicklungspotential, indem der Lizenzerwerb und die Nutzung erworbener Rechte auf dem europäischen Markt vereinfacht wird. So wird z.B. die Entwicklung und der Vertrieb von Smart Products, die auf urheberrechtlich geschützte digitale Inhalte zugreifen, gefördert, wenn die Nutzung im privaten Bereich über den nationalen Markt hinaus ermöglicht wird.

Ferner bleibt abzuwarten, ob die EU-Kommission die pauschale Ankündigung einer Regelung der Haftungszuweisung im Rahmen des Internets der Dinge auf urheberrechtliche Aspekte ausweitet.[208]

b) Begrenzung des Geo-Blockings

In engem Zusammenhang mit der Modernisierung des Urheberrechts steht das Ziel der EU-Kommission Geo-Blocking, d.h. die Aufspaltung des europäischen Marktes in einzelne Märkte durch virtuelle Grenzen, zu vermeiden.[209] Bisher erfolgt im Mediensektor ein länderspezifischer selektiver Vertrieb – einschließlich der urheberrechtlichen Verwertung – entlang nationaler Grenzen. Die EU-Kommission hat dieses Geschäftsmodell im Fact Sheet zum Strategiepapier als gerechtfertigtes Geo-Blocking bewertet. Zudem wurde darauf hingewiesen, dass die geplante Urheberrechtsreform keinen Einfluss auf den bisherigen Vertriebsablauf von Filmen haben wird. Inwiefern die Umsetzung der Strategie für einen digitalen Binnenmarkt für Europa das Territorialitätsprinzip des Urheberrechts und die Überwindung der virtuellen Grenzen durch Geo-Blocking in Einklang bringt und den europaweiten Zugriff auf digitale Inhalte dadurch vereinfacht, bleibt fraglich. Denkbar wäre, dass eine an der Interessenlage ausgerichtete Abgrenzung zwischen gerechtfertigtem und ungerechtfertigtem Geo-Blocking vorgenommen wird, deren Ergebnis mit den jeweils einhergehenden Verwertungsbeschränkungen im Rahmen der Entwicklung von Produkten der Industrie 4.0 berücksichtigt werden muss.

---

[206] EU-Kommission, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 v. 6.5.2015, S. 8.
[207] EU-Kommission, Eine Digitale Agenda für Europa, KOM(2010) 245 v. 19.5.2010, S. 9.
[208] Vgl. EU-Kommission, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 v. 6.5.2015, S. 17.
[209] Siehe hierzu EU-Kommission, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 v. 6.5.2015, S. 6.

II. Gewerblicher Rechtsschutz (Patentrecht, Designrecht, Wettbewerbsrecht etc.)

1. Erfinderrechte an Arbeitsergebnissen aus automatisierten Prozessen (computer generated works)

Die mit der Industrie 4.0 verbundene Entwicklung so genannter hybrider Produkte wirft neben der Frage nach einem urheberrechtlichen Schutz von Ergebnissen aus automatisierten Prozessen auch die Frage auf, inwiefern an derartigen Ergebnissen Erfinderrechte begründet werden können.

a) Schutzfähigkeit

Das Erfinderrecht an Arbeitsergebnissen[210] und ebenso das Recht auf das Design entsteht in der Person des Erfinders bzw. Designers.[211] Im Mittelpunkt steht somit der Schöpfungsakt einer natürlichen Person und die darin verkörperte geistige Leistung. Bei Vorliegen der weiteren gesetzlich normierten Voraussetzungen wird diese geistige Leistung mit einem Monopolrecht flankiert.

Handelt es sich bei Arbeitsergebnissen allein um computer generated works fehlt diesen Arbeitsergebnissen die Beziehung zum Erfinder bzw. Designer. Selbst wenn ein Computer aufgrund der jeweiligen Programmierung, etwa auf dem Gebiet von Konstruktion, Kombination, Anwendungen bekannter Erzeugnisse und Verfahren der Auswahl aus bekannten Bereichen, neue Ergebnisse generiert, kann dies allein die Schutzfähigkeit nicht begründen. Erst die Erkenntnis des Erfinders, dass das im Wege der computer generated works erarbeitete Ergebnis die Lösung eines technischen Problems (eine Aufgabe) darstellt und damit eine Erfindung begründet, führt zur Schutzfähigkeit.[212] Ebenso kann der Schutz nach dem DesignG nur dann begründet werden, wenn das Design im Zusammenspiel von computer generated works und menschlicher Beteiligung entstanden ist.

Arbeitsergebnisse die allein durch automatisierte Prozesse geschaffen werden, sind dem Gewerblichen Rechtschutz somit nicht zugänglich.

b) Rechteinhaberschaft

Der deutsche gewerbliche Rechtsschutz ist wie das Urheberrecht durch das Schöpferprinzip geprägt.[213] Rechtsinhaber ist folglich zunächst der jeweilige Schöpfer bzw. Erfinder des Arbeitsergebnisses.

Ist das durch automatisierte Prozesse generierte Arbeitsergebnis durch die Erkenntnis einer natürlichen Person zur Erarbeitung der Lösung eines technischen Problems herangezogen worden, ist derjenige, der durch die Programmgestaltung und die Auswertung der Ergeb-

---

[210] *Melullis* in Benkard, PatG, 10. Aufl. 2006, § 6 Patentgesetz Rz. 3a.
[211] *Eichmann* in Eichmann/von Falckenstein/Kühne, DesignG, 5. Aufl. 2015, § 7 DesignG Rz. 4.
[212] *Melullis* in Benkard, Patentgesetz, 10. Aufl. 2006, § 6 Patentgesetz Rz. 3a.
[213] *Mes* Patentgesetz, 4. Aufl. 2015, § 6 Rz. 9.

nisse der computer generated works die Lösung der technischen Problemstellung erreicht und erkennt, als Erfinder anzusehen. Dem Konstrukteur des Computers, dessen Eigentümer oder Besitzer oder sonstigem Bedienungspersonal, denen zwar die Verbindung zwischen dem Ergebnis der Arbeit des Computers zum schöpferischen Menschen zu verdanken ist, stehen hingegen keine Erfinderrechte an der computer generated works zu.[214]

Ausgehend von dem im Designrecht ebenfalls verwurzelten Schöpferprinzip, kann auch hier die originäre Rechtsinhaberschaft nur unmittelbar aus der geistigen Leistung des Designers resultieren.

2. Standardessentielle Patente als Problem im Digitalisierungsprozess?

Eine Herausforderung für die Industrie 4.0 bilden die sich zunehmend etablierenden standardisierte Technologien. Diese Standards unterstützen die Verbreitung bestimmter Technologien und schaffen die im Technologiezeitalter notwendige Interoperabilität unterschiedlicher Anwendungen, Vorrichtungen und Geräte sowie einzelner Komponenten.[215] Durch die etablierten Standards entfällt die Notwendigkeit Angebote vor- und nachgelagerter Dienstleistungen und Produkte interoperabel auszugestalten. Kosten werden dadurch reduziert. Zugleich wird jedoch ein Wettbewerb unterschiedlicher Technologien auf dem fraglichen Markt ausgeschaltet. Verstärkt wird dieser wettbewerbsbeschränkende Effekt wenn die Standards durch Patente geschützt sind.

Bei solchen standardessentiellen Patenten („SEP“) ist zwischen Standards zu unterscheiden, die von Standardisierungs- und Normungsgesellschaften (Standard Setting Organisations, SSO)[216] gesetzt werden, und Standards die sich *de facto* herausbilden. Während die von SSOs festgelegten Standards auf einer Einigung der beteiligten Kreise beruhen, entstehen *de facto* Standards durch eine tatsächliche Durchsetzung einer Technologie am Markt, weil ein Produkt von den Marktteilnehmern als am besten oder alternativlos angesehen wird.[217]

Standardisierte Technologien sind regelmäßig durch eine Vielzahl von Patenten geschützt, wobei ein einzelnes Patent nur einen kleinen Beitrag zu der technischen Lösung beiträgt. Der einzelne Patentinhaber hat damit faktisch die Möglichkeit, im Wege der Durchsetzung seines Patents die Nutzung des Standards zu untersagen. Zur Lösung dieses Konflikts wird auf das Kartellrecht zurückgegriffen.[218]

Daneben wird diskutiert, ob in diesem Zusammenhang nicht auch eine Lösung innerhalb des Patentsystems selbst gefunden werden kann oder gar muss.[219]

---

[214] *Melullis* in Benkard, Patentgesetz, 10. Aufl. 2006, § 6 Patentgesetz Rz. 3b.
[215] *Hilty/Slowinsky*, GRUR Int. 2015, 78, 782.
[216] Eine SSO ist zum Beispiel das Deutsche Institut für Normierung e.V.
[217] *Hilty/Slowinsky*, GRUR Int. 2015, 78, 782.
[218] *Mes,* Patentgesetz, 4. Aufl. 2015, § 9 Rz. 111 f.
[219] *Osterrieth*, Patentrecht, 5. Aufl. 2015, Rz. 36.

a) Kartellrechtlicher Lizenzierungszwang

Ein kartellrechtlicher Lizenzierungszwang und die damit verbundene Einschränkung des SEP-Inhabers seine Ausschließlichkeitsrechte durchzusetzen ergibt sich zum einen aus der eigenen FRAND-Erklärung (vgl.Teil 1I.2.) auch gegenüber der SSO. Mit Abschluss eines Lizenzvertrages erfüllt der SEP-Inhaber seine privatautonom eingegangene Verpflichtung. Macht der SEP-Inhaber seinen Unterlassungsanspruch trotz FRAND-Erklärung geltend, handelt er missbräuchlich. Der Begriff FRAND ist nach wie vor unzureichend konkretisiert. Offen ist insbesondere die Höhe der angemessenen Lizenzgebühr und der Angemessenheit anderer Konditionen.[220] Die EuGH Entscheidung *Huawei* hat zwar das Vorgehen hinsichtlich der Lizenzerteilung im Zug einer FRAND-Erklärung konkretisiert, die inhaltliche Ausgestaltung jedoch offengelassen (vgl. Teil 1I.2.).[221]

Dagegen wird beim kartellrechtlichen Kontrahierungszwang die Weigerung des SEP-Inhabers eine Lizenz zu erteilen, als kartellrechtswidrig eingestuft und damit die Vertragsfreiheit eingegrenzt.[222]

b) Patentrechtliche Einschränkung des Unterlassungsanspruchs

Im Anwendungsbereich von FRAND-Zusagen und dem kartellrechtlichen Zwangslizenzeinwand wird der negatorische Rechtsschutz zwar ebenfalls ausgeschlossen, Voraussetzung ist jedoch jeweils, dass es sich bei dem SEP-Inhaber um ein marktbeherrschendes Unternehmen handelt. Allein aus dem Vorliegen eines SEP kann jedoch nicht zwingend auf eine marktbeherrschende Stellung geschlossen werden.[223]

Aus diesem Grund wird diskutiert, ob in Rahmen von SEPs der Unterlassungsanspruch grundsätzlich noch angemessen und verhältnismäßig ist, oder nicht bereits ohne den Rückgriff auf das Kartellrecht einzugrenzen sei. Angeführt werden dabei zwei Argument: Bei standardisierten Technologien ist ein Innovationsprozess innerhalb des Standards jedoch ausgeschlossen, so dass der der Sinn und Zweck des Patentschutzes (Entlohnung des Erfinders und der Anreiz für Innovation) leer läuft. Außerdem resultiere der Wert der standardisierten Technologie nicht auf der einzelnen erfinderischen Leistung, sondern aus der Gesamtheit der zu der standardisierten Technologie beitragenden Patente.[224]

3. Computerimplementierte Erfindungen

Die Frage nach der Erforderlichkeit und/oder Notwendigkeit eines Patentschutzes für computerimplementierte Erfindungen ist nicht neu, sondern hat bereits im vorangegangenen Jahrhundert sowohl Rechtslehre als auch Rechtsprechung umfassend beschäftigt.[225] Vom

---

[220] *Heinemann,* GRUR 2015, 855.
[221] EuGH, Urt. v. 16.07.2015, Rs C-170/13 – *Huawei Technologies*.
[222] *Pitch,* GRUR Int 2014, 1 (11f.); BGH Urt. v. 06.05.2009, KZR 39/06 – *Orange-Book-Standard*.
[223] GA *Wathelet*, ECLI: EU: C 2014391 Rn. 57f. – *Huawei Technologies/LTE.*
[224] *Osterrieth*, Patentrecht, 5. Aufl. 2015, Rz. 37.
[225] *Nack*, GRUR Int. 2004, 771.

gesetzlich normierten Ausschluss der Patentfähigkeit sind nur Computerprogramme als solche betroffen (§ 1 Abs. 4 PatG).

Erstmalig definiert wurde der Begriff der computerimplementierten Erfindung in Artikel 2 lit. a) des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über die Patentierbarkeit computerimplementierter Erfindungen.[226] Eine computerimplementierte Erfindung ist *„jede Erfindung, zu deren Ausführung ein Computer, ein Computernetz oder eine sonstige programmierbare Vorrichtung eingesetzt wird und sie auf den ersten Blick mindestens ein neuartiges Merkmal aufweist, das ganz oder teilweise mit einem oder mehreren Computerprogrammen realisiert wird"*. Der die Schutzfähigkeit begründende technische Beitrag ist gemäß lit. b) gegeben, wenn der Beitrag zum Stand der Technik auf einem Gebiet der Technik für eine fachkundige Person nicht naheliegend ist. Aufgrund des nicht aufzulösenden Dissenses betreffend die Schutzfähigkeit und den Schutzumfang von computerimplementierten Erfindungen konnte der Richtlinienentwurf jedoch nicht verabschiedet werden.

Gleichwohl kommt dem Begriff der Technizität bei der Frage der Patentfähigkeit einer computerimplementierten Erfindung eine zentrale Bedeutung zu. Die Patentfähigkeit einer computerimplementieren Erfindung ist anzuerkennen, wenn die Lösung eines technischen Problems mit konkreten technischen Mitteln bewirkt wird.[227] Nach der vom BGH vorzunehmenden Gesamtbetrachtung ist dabei maßgeblich, ob die Lehre bei der gebotenen Gesamtbetrachtung der Lösung eines über die Datenverarbeitung hinausgehenden konkreten technischen Problems dient.[228]

Die vom BGH hierbei herangezogenen Kriterien „technische Belegungen", „weitere technische Effekte" und „über den Computereinsatz hinausgehende Eigenart" führen auf der einen Seite zwar zu gewissen Unsicherheiten, auf der anderen Seite bieten sie jedoch einen weiten Spielraum und eine gewisse Flexibilität für unterschiedliche Interpretationen, um auf neue Entwicklungen einzugehen.

Werden durch industrielle Prozesse Produkte unter den Bedingungen einer hoch flexibilisierten (Großserien-)Produktion angepasst, werden Computerprogramme regelmäßig zur Erreichung bestimmter technischer Effekte eingesetzt. Erfüllen die dabei gestellten Lösungen die übrigen Patentierungsvoraussetzungen, bietet die nunmehr gefestigte Rechtslage zu computerimplementierten Erfindungen hinreichend Schutz unter dem staatlich verliehenen Monopol eines Patents. Erfüllt der Einsatz neuer Technologien im Zeitalter der Industrie 4.0 diese Voraussetzungen nicht, wird der Patentschutz zu Recht versagt.

4. Reformbedarf?

[226] ABl. 2002 151/129.
[227] *Hössle* in Fitzner/Lutz/Bodewig, PatG, 4. Aufl., § 1 Rz. 207.
[228] BGH, Urt. v. 20.01.2009 – X ZB 22/07 – GRUR 2009, 479 – *Steuerungseinrichtung für Untersuchungsmodalitäten*; grundlegend BGH, Urt. v. 04.02.1992 – X ZR 43/91 – GRUR 1990, 430, 431 f. – *Tauchcomputer*.

SEP werden die Industrie 4.0 nachhaltig prägen. Die Herausbildung von Standards und die damit verbundene Schaffung einer Interoperabilität ist für den Bereich der Hochtechnologie unerlässlich. Es muss daher sichergestellt werden, das allen Markteilnehmer Zugang – vorbehaltlich angemessener Konditionen – zu Standards gewährt wird. Die Anforderungen an die angemessenen Konditionen des Zugangs, beispielsweise in Form der Lizenzerteilung sollten dabei konkretisiert werden. Eine entsprechende Klarstellung im Gewerblichen Rechtsschutz sollte sich dabei jedoch nicht nur auf durch SSO festgelegte Standards beziehen, sondern auch auf de facto Standards.

III. Rechtsprobleme des 3D-Drucks

Dem Begriff „3D-Druck" unterfallen Verfahren, in denen Materialien schichtweise auf einen Träger aufgebracht und miteinander zu dreidimensionalen Objekten verfestigt werden. Hierfür sind Computer-aided Design-Dateien („CAD-Dateien") erforderlich, die alle für den Druckvorgang notwendigen technischen Informationen enthalten. Diese Dateien lassen sich entweder mithilfe von CAD-Zeichenprogrammen oder durch Scannen eines bereits existierenden Ausgangsobjekts erstellen. Ist das gescannte oder per CAD als Datei (nach)gezeichnete Ausgangsobjekt immaterialgüterrechtlich geschützt, stellt sich die Frage, ob *de lege lata* hinreichender Schutz gegen eine unautorisierte Erstellung von CAD-Dateien und gegen den unautorisierten 3D-Ausdruck besteht. Diese Frage verschärft sich aufgrund der zunehmenden Verbreitung und Professionalisierung der 3D-Druck-Technologie auch im Privatbereich.[229] CAD-Dateien sind über 3D-Vorlagenportale im Internet verfügbar und werden auch über Filesharing-Plattformen getauscht. Einige Unternehmen erwägen bereits, ihren Kunden selbst solche Dateien zum Zwecke des 3D-Drucks zur Verfügung zu stellen.[230] Ermöglicht der 3D-Druck in der industriellen Herstellung einerseits die flexible, schnelle sowie individuelle Fertigung (sog. „Additive Manufacturing") und beschleunigt hierbei auch die Innovationszyklen, birgt die Technologie zugleich die Gefahr, dass Dritte die (immaterialgüterrechtlich geschützten) Produkte ohne große Schwierigkeiten kopieren können. Bereits seit einiger Zeit wird deshalb eine lebhafte Diskussion geführt, inwieweit die fortschreitende Entwicklung im Bereich des 3D-Drucks verstärkt Probleme mit Produktpiraterie verursachen wird.

1. Urheberrechtlicher Schutz

Schutz vor Produktpiraterie bietet das Urheberrecht nur, wenn das Ausgangsobjekt die urheberrechtliche Schöpfungshöhe als Werk der angewandten Kunst nach § 2 Abs. 1 Nr. 4 UrhG erreicht.[231] Auch die CAD-Datei selbst kann urheberrechtlich geschützt sein. Denn die

---

[229] Die Zahl der 3D-Druck-Copy-Shops und 3D-Druck-Vorlagenportale steigt ständig; einige Beispiele sind „Trinckle.de" (http://www.trinckle.com/index.php), „Thingiverse" (http://www.thingiverse.com) oder „Google 3D-Warehouse" (http://www.3dwarehouse.sketchup.com).

[230] So hat „Lego" bereits in Betracht gezogen, entsprechende CAD-Dateien anzubieten, dass die Steine selbst vom Kunden gedruckt werden können, vgl. http://t3n.de/news/lego-3d-druck-konzern-zukuenftig-532319/.

[231] *Solmecke/Kocatepe,* K&R 2014, 778, 780; vgl. auch *Grosskopf,* CR 2012, 618, 62; seit der Änderung der BGH Rechtsprechung im Bereich des Produktdesigns ist urheberrechtlicher Schutz nicht mehr nur aus-

Datei stellt sowohl das materielle Objekt in digitaler Form dar, enthält zugleich aber auch selbst Anweisungen an den 3D-Drucker zur Erzeugung des Objekts und fungiert damit als eine Art Bauplan. Noch ungeklärt ist, ob der CAD-Datei ein originärer Schutz nach § 2 Abs. 1 Nr. 7 UrhG als Darstellung wissenschaftlich-technischer Art zukommt. Ungeklärt ist umgekehrt, ob die Erstellung der CAD-Datei, die ein urheberrechtlich geschütztes Objekt darstellt, eine urheberrechtlich relevante Handlung begründet – entweder als digitale Vervielfältigung des materiellen Objekts gemäß § 16 Abs. 1 UrhG oder als abhängige Bearbeitung gemäß § 23 UrhG[232] – wobei gleichfalls vertreten wird, dass erst das Drucken des materiellen Objekts die Vervielfältigungshandlung darstelle.[233] Gleichfalls offen ist, ob die Erstellung einer 3D-CAD-Datei aus einer zweidimensionalen Vorlage die Werkqualität der CAD-Datei und damit ihren urheberrechtlichen Schutz begründen kann[234] oder ob hierin wiederum eine Vervielfältigung[235] oder gar eine abhängige Bearbeitung der zweidimensionalen Vorlage gem. § 23 UrhG zu sehen ist.[236]

Besonderes Gewicht gewinnen diese Fragen im Hinblick auf die urheberrechtlichen Schrankenbestimmungen, im Privatbereich insbesondere § 53 UrhG, der einzelne Vervielfältigungen von Werken zum Privatgebrauch gestattet, das Bearbeitungsrecht nach § 23 UrhG jedoch nicht beschränkt. Von jener Schrankenbestimmung nicht gedeckt ist jedenfalls das Verbreiten von CAD-Dateien im Internet, da § 53 Abs. 6 UrhG die öffentliche Wiedergabe und damit auch die öffentliche Zugänglichmachung der Vervielfältigungsstücke gem. § 19a UrhG untersagt. Das Herunterladen der Datei selbst stellt gleichfalls eine Vervielfältigung gem. § 16 Abs. 1 UrhG dar,[237] entweder eine Vervielfältigung der Datei selbst oder schon des in ihr vervielfältigten Objekts. Laden Nutzer CAD-Dateien bspw. in Filesharing-Plattformen herunter, greift § 53 UrhG nicht. Denn aufgrund der Typizität von Filesharingsystemen dürfen deren Nutzer regelmäßig nicht davon ausgehen, dass die anderen Nutzer oder der Plattformbetreiber die dort verbreiteten Kopien rechtmäßig hergestellt haben oder verbreiten.[238]

Auch das Drucken des 3D-Objekts stellt eine Vervielfältigungshandlung nach § 16 Abs. 1 UrhG dar, bei der die Schrankenbestimmung nach § 53 Abs. 1 UrhG greift, wenn dies zu privaten Zwecken geschieht und auf Grundlage einer CAD-Datei erfolgt, die nicht offensicht-

---

nahmsweise gegeben (vgl. BGH, Urteil v. 13.11.2013 – I ZR 143/12, NJW 2014, 469, 472 – *Geburtstagszug*).

232 *Buchalik,* ITRB 2014, 158, 159; *Nordemann/Rüberg/Schaefer,* NJW 2015, 1265, 1266; *Mengden,* MMR 2014, 79, 83; ausführlich zur digitalen Vervielfältigung *Kroitzsch/Götting,* in: Ahlberg/Götting, BeckOK Urheberrecht (Stand 01.07.2015), UrhG § 16, Rn. 3.

233 *Solmecke/Kocatepe,* K&R 2014, 778, 779.

234 So *Buchalik,* ITRB 2014, 158, 160; die betont, dass der Dimensionenwechsel eine eigenständige geistige Leistung erfordert.

235 *Grosskopf,* CR 2012, 618, 622; *Schulze,* in: Dreier/Schulze, UrhG, 4. Aufl. 2013, § 16, Rn. 11; *Kroitzsch/Götting,* in: Ahlberg/Götting, BeckOK Urheberrecht (Stand 01.07.2015), UrhG § 16, Rn.10.

236 *Nordemann/Rüberg/Schaefer,* NJW 2015, 1265, 1266.

237 U.a. *Nordemann/Rüberg/Schaefer,* NJW 2015, 1265, 1266; *Buchalik,* ITRB 2014, 158, 161.

238 *Solmecke/Kocatepe,* K&R 2014, 778, 779; *Mengden,* MMR 2014, 79, 83; *Nordemann/Rüberg/Schaefer,* NJW 2015, 1265, 1266.

lich rechtswidrig hergestellt oder öffentlich zugänglich gemacht wurde. Wird über kommerzielle Online-Druckereien oder in Copy-Shops gedruckt, scheidet eine Privilegierung aus, da diese Marktteilnehmer regelmäßig nur gegen Entgelt, mithin nicht unentgeltlich gem. § 53 Abs. 1 S. 2 1. Fall UrhG handeln. Einer analogen Anwendung der für photomechanische oder Verfahren mit ähnlicher Wirkung geltenden Öffnungsklausel des § 53 Abs. 1 S. 2 2. Fall UrhG, die aufgrund der Vergleichbarkeit der Fallgestaltungen denkbar erscheint, steht der Grundsatz der regelmäßig engen Auslegung urheberrechtlicher Schranken entgegen.[239] Dies wirft die Frage nach der Gleichstellung des 3D-Drucks mit dem klassischen Auftragsdruck auf und ob dies einer klarstellenden Regelung durch den Gesetzgeber bedürfte. Das Verbreiten des gedruckten Objekts ist in jedem Fall nach § 17 Abs. 1 UrhG untersagt. Eine Schrankenbestimmung existiert hier nicht.

1. Gewerbliche Schutzrechte (Marken-, Design-, Patentrecht)

Die Verletzung gewerblicher Schutzrechte erfordert stets und zwingend ein geschäftliches Handeln, d.h. die Teilnahme am Erwerbsleben zur Wahrnehmung bzw. Förderungen eigener oder fremder Geschäftsinteressen.[240] Werden CAD-Dateien durch eine Internetplattformen gegen Entgelt angeboten oder bieten Designer die von ihnen erzeugten CAD-Dateien dort gegen Entgelt an, liegt ein Handeln im geschäftlichen Verkehr vor; nicht so jedoch bei zum privaten Gebrauch auf Filesharing Plattformen unentgeltlich herunterzuladenden Dateien, was aus Sicht der Rechteinhaber zu Friktionen führen kann, da die gewerblichen Schutzrechte gegen jegliche Handlungen zum ausschließlichen Privatgebrauch nicht greifen.

a) Rechtsverletzung durch den 3D-Druck

Werden 3D-Drucke von Gestaltungen erstellt und im geschäftlichen Verkehr vertrieben, kommt ein markenrechtlicher Schutz für das reproduzierte Ausgangsobjekt in Betracht, wenn darauf Wort- oder Bildmarken (z.B. Markennamen oder Logos) angebracht sind oder wenn die äußere Form des Objekts selbst als 3D- oder Bildmarke geschützt ist.

Designrechtlich ist das Ausgangsobjekt geschützt, wenn es gemäß § 2 Abs. 1 DesignG Eigenart besitzt und neu ist. Es liegt nahe, mit der 3D-Druck-Technologie Ersatzteile herzustellen, anstatt Originalersatzteile der Hersteller zu verwenden. Designrechtliche Ansprüche (insbesondere auf Unterlassung) gegen solche Handlungen bestehen nur dann, wenn das Ersatzteil selbst als Design geschützt ist und – wenn es Teil eines aus mehreren Bauteilen bestehenden System ist – bei bestimmungsgemäßer Verwendung noch sichtbar ist, § 4 DesignG.

Auch Patent- bzw. Gebrauchsmusterrechte können durch den Vertrieb von 3D-Reproduktionen verletzt werden. Hierbei ist – jedenfalls solange die 3D-Technologie noch keine komplexen, technisch funktionsfähigen Erzeugnisse als Gesamtobjekte hervorbringen

[239] BGH Urteil vom 24. Januar 2002– I ZR 102/99; ZUM-2002, 636 – *Verhüllter Reichstag;* so auch *Mengden,* MMR 2014, 79, 83.

[240] EuGH Urteil vom 12.06.2008 - C-533/06, GRUR 2008, 698 Rn. 60.

kann – allenfalls mit mittelbaren Rechtsverletzungen und den damit verbundenen Schutzbeschränkungen zu rechnen;[241] dies mag sich aber in Zukunft ändern.

b) Rechtsverletzung durch die CAD-Datei

Ungeklärt ist, ob bereits die Herstellung und Verbreitung der für den 3D-Druck dienenden CAD-Datei gewerbliche Schutzrechte verletzt.

Das Designrecht schützt jede Verkörperung des Designs, weswegen argumentiert wird, dass auch die Erstellung der CAD-Datei als die dem Vertrieb der späteren Reproduktion vorgeschaltete produktbezogene Handlung umfasst sein muss.[242]

Ob die Erstellung der CAD-Datei – oder gar schon das Einscannen eines markenrechtlich geschützten Objekts – eine markenmäßige Benutzung darstellt, ist ebenfalls unklar. Ein sog. Identitätsverstoß gem. § 14 Abs. 2 Nr. 1 MarkenG wird abgelehnt, da die CAD-Datei nicht mit dem Ausgangsobjekt übereinstimmt. Vertreten wird daher, die CAD-Datei als Aufmachung oder Verpackung gem. § 14 Abs. 4 MarkenG einzustufen oder sie als eine dem gedruckten Objekt „ähnliche" Ware i.S.d. § 14 Abs. 2 Nr. 2 MarkenG anzusehen.[243] In diesem Zusammenhang wird empfohlen, die Marke auch in Klasse 9 als „herunterladbare elektronische Publikation zu registrieren,[244] was jedoch neben der möglichen Erhöhung von Markenanmeldekosten auch Konsequenzen für die Benutzung der Marke zeitigt. Denn nach Ablauf der fünfjährigen Benutzungsschonfrist würde eine entsprechend registrierte Marke löschungsreif, wenn tatsächlich keine Verbreitung des Produkt in herunterladbarer elektronischer Form erfolgt ist. Es besteht mithin Klärungs- und ggf. Handlungsbedarf hinsichtlich der offenen Frage, ob die CAD-Datei bereits eine markenmäßige Benutzung darstellt. Im Hinblick auf den Scanvorgang eines markenrechtlich geschützten (oder mit einer Marke versehenen) Ausgangsobjekts liegt es nahe, diesen als bloße Vorbereitungshandlung und nicht als markenmäßige Benutzungshandlung zu qualifizieren.

Die Erstellung der CAD-Datei liegt als reine Vorbereitungshandlung außerhalb des Schutzbereichs des Patent- bzw. Gebrauchsmusterrechts. Allenfalls die Verbreitung der Dateien kann gemäß § 10 PatG bzw. § 11 GebrMG eine mittelbare Rechtsverletzung begründen. Danach ist es Dritten untersagt, ohne Zustimmung des Rechteinhabers unberechtigten Personen solche Mittel anzubieten oder zu liefern, die sich auf ein wesentliches Element der Erfindung beziehen, wenn der Dritte weiß oder dies aufgrund der Umstände offensichtlich ist, dass jene Mittel dazu geeignet und bestimmt sind, für die Benutzung der Erfindung verwendet zu werden. Da die CAD-Datei aber nicht Bestandteil des später gedruckten Produkts

[241] *Nordemann/Rüberg/Schaefer,* NJW 2015, 1265, 1269; vgl. auch *Solmecke/Kocatepe,* K&R 2014, 778, 780.
[242] *Solmecke*, Deutsche Stiftung für Recht und Informatik – Tagungsband Herbstakademie (DSRITB) 2014, 283 (288).
[243] *Nordemann/Rüberg/Schaefer,* NJW 2015, 1265, 1268; *Mengden,* MMR 2014, 79, 82 geht davon aus, dass auch die virtuelle Abbildung einer Marke eine rechtswidrige Nutzung i.S.d. § 14 MarkenG darstellt, ohne dies jedoch genauer zu begründen.
[244] *Nordemann/Rüberg/Schaefer,* NJW 2015, 1265, 1268.

wird, ist fraglich, ob sie tatsächlich „erfindungswesentlich“ ist. Überdies hat die bisherige Rechtsprechung unter einem „Mittel“ stets nur körperliche Gegenstände, nicht jedoch in Dateien verkörperte Modelle verstanden.[245] Die in der CAD-Datei enthaltene „digitale Blaupause“ stellt jedoch wiederum einen exakten und einfachen Weg dar, die geschützte Erfindung bzw. deren Teile zu kopieren. Es besteht deshalb Klärungs- und ggf. Handlungsbedarf.

2. Haftung der 3D-Vorlagenportale und 3D-Druckereien

Hinsichtlich der Haftung für Rechtsverletzungen durch 3D-Druck ist zu unterscheiden: Für die Haftung der 3D-Vorlagenportale im Internet können, soweit es sich bei den CAD-Dateien um nutzergenerierte Inhalte handelt, die bereits zu anderen Internetplattformen von der Rechtsprechung entwickelten Grundsätze der Störerhaftung herangezogen werden. Die Internetportale haften dann nur auf Notice / Takedown und Staydown, d.h. auf Verhinderung des erneuten Uploads dieser Datei sowie weiterer gleichartiger genauso klarer Rechtsverletzungen. Hierbei sind von der Plattform geeignete Filtermaßnahmen in angemessenem Umfang einzusetzen.[246]

Problematischer ist die Haftung kommerzieller, mithin im geschäftlichen Verkehr handelnder 3D-Druckereien. Führt der Nutzer den 3D-Druck in einem Copy-Shop selbst aus, so kommt für den Betreiber des Copy-Shops nur eine Haftung nach den Grundsätzen der Störerhaftung in Betracht.[247] Druckt hingegen eine Online-Druckerei selbst das Objekt aus, stellt dies grundsätzlich eine täterschaftliche markenmäßige Benutzungshandlung nach § 14 Abs. 3 Nr. 1 MarkenG dar, was zumindest den verschuldensunabhängigen Unterlassungsanspruch nach § 14 Abs. 5 MarkenG auslöst. Schadensersatz- oder sonstige Ansprüche, die eine schuldhafte Rechtsverletzung voraussetzen, dürften regelmäßig leerlaufen, weil die Betreiber der Druckereien zumeist nicht vorsätzlich und – mangels gesetzlich im Vorhinein bestehender Prüfpflicht – auch nicht fahrlässig handeln, wenn sie auf Kundenwunsch die 3D-Replik eines markenrechtlich geschützten Objekts ausdrucken. Wir sehen hier Klärungsbedarf, ob und inwieweit hier die Rechtsschutzmöglichkeiten der Rechteinhaber verbessert werden können.

3. Reichweite des Erschöpfungsgrundsatzes bei digitalen Inhalten und Produkten

Insbesondere im Bereich des 3D-Drucks stellt sich auch die Frage, wann in den verschiedenen Fallkonstellationen des (un)autorisierten Nachdrucks von Originalen die Markenrechte an einem Produkt gemäß § 24 MarkenG erschöpft sind.[248] Wie bereits unter Ziff. Teil 6III.2.

---

[245] BGH, Urteil vom 10. 10. 2000 - X ZR 176/9; GRUR 2001, 228, 231 – Luftheizgerät.

[246] BGH, *Urt.* v. 12. 7. 2012 – I ZR 18/11; NJW 2013, 784 - Alone in the dark.

[247] So *Nordemann/Rüberg/Schaefer,* NJW 2015, 1265, 1270; *Solmecke/Kocatepe,* K&R 2014, 778, 782.

[248] Es sind insbesondere drei Fallkonstellationen denkbar: 1. Ein mit einer Marke versehenes und zuvor käuflich frei erworbenes Ausgangsobjekt wird eingescannt, in eine Digitaldatei umgewandelt und dann 3D gedruckt; 2. Ein Dritter erstellt ohne Autorisierung des Markeninhabers eigene 3D-Vorlagen mit Hilfe eines CAD-Programms, die eine Marke beinhalten, und druckt selbst ein Produkt aus oder lässt dies durch einen 3D-Druckanbieter drucken. 3. Ein Hersteller erteilt den Nutzern eine Lizenz, seine Markenprodukte 3D drucken zu lassen.

ausgeführt, kommt Markenschutz im Zusammenhang mit CAD-Dateien u.a. dann in Betracht, wenn das Ausgangsobjekt mit einer Marke versehen ist oder insgesamt als 3D-/Bildmarke geschützt ist und die Marke in der CAD-Datei (sowie später auf dem gedruckten 3D-Objekt) abgebildet wird.

Nach § 24 Abs. 1 MarkenG hat der Inhaber einer Marke oder einer geschäftlichen Bezeichnung nicht das Recht, einem Dritten zu untersagen, die Marke oder die geschäftliche Bezeichnung für Waren zu benutzen, die unter dieser Marke oder dieser geschäftlichen Bezeichnung von ihm oder mit seiner Zustimmung in den Verkehr gebracht worden sind. Sinn und Zweck des markenrechtlichen Erschöpfungsgrundsatzes ist es, einen angemessenen Ausgleich zwischen der Exklusivität des Markenrechts einerseits und der Warenverkehrsfreiheit andererseits zu schaffen.[249] Zwar werden nach der Definition des EuGH grundsätzlich nur körperliche Gegenstände von der Warenverkehrsfreiheit erfasst, jedoch hat der Gerichtshof im Interesse eines lückenlosen Schutzes wirtschaftlicher Tätigkeit das Merkmal stark ausgeweitet.[250]

Die für den 3D-Druck notwendige CAD-Vorlage ist eine digitale Datei gemäß § 312 f Abs. 3 BGB.[251] Kernproblem bei der Anwendung des Erschöpfungsgrundsatzes ist die Frage, ob digitale Inhalte als „Waren“ einzustufen sind. Die auf einem körperlichen Datenträger gespeicherten digitalen Inhalte sind zweifelsfrei als Waren einzuordnen und unterliegen daher der Erschöpfung.[252] Bei nicht auf Datenträgern fixierten Digitalinhalten ist die rechtliche Bewertung hingegen unklar.

a) Urheberrechtliche Erwägungen

Die Erschöpfung von Rechten wurde bislang vor allem für Computerprogramme aus urheberrechtlicher Sicht diskutiert, § 69c Nr. 3 S. 2 UrhG. Erschöpfung des Schutzes an einem Computerprogramm tritt ein, wenn das Programm gegen Entgelt zum Download angeboten und den Nutzern damit die Herstellung von Vervielfältigungsstücken des Computerprogramms erlaubt wird. Dies gilt auch bezüglich eines erneuten Vervielfältigungsstücks, das

---

[249] *Kaiser,* in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 201. Ergänzungslieferung Januar 2015, MarkenG § 24, Rn. 1 m.w.N.

[250] Vgl. *Leible/Streinz,* in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 55. Ergänzungslieferung 2015, AEUV Art. 34, Rn. 28.

[251] Die Begriffsbestimmung geht zurück auf Art. 2 Ziff. 11 der neuen Verbraucherrechterichtlinie, Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates, ABl. L Nr. 304 vom 22.11.2011, S. 64.

[252] Vgl. für eine Anwendbarkeit des § 24 Abs. 1 MarkenG bei einer auf CD-Rom angebotenen Software BGH, 1. Zivilsenat, Urteil vom 06.10.2011, Az. I ZR 6/10, in der konkreten Entscheidung ging der BGH jedoch von einer Ausnahme nach § 24 Abs. 2 MarkenG aus. Dagegen soll keine Erschöpfung möglich sein, wenn lediglich sog. COAs (Certificates of Authenticity, d.h. Echtheitszertifikate zu Computerprogrammpaketen) isoliert angeboten und ausgeliefert werden, da diese keine Ware seien, vgl. LG Frankfurt, 3. Zivilkammer, Urteil vom 27.09.2012, Az. 2-3 O 27/12, 2/3 O 27/12, 2-03 O 27/12, 2/03 O 27/12; ebenso OLG Frankfurt, 11. Zivilsenat, Beschluss vom 30.01.2014, Az. 11 W 34/12.

einem Erwerber der „gebrauchten“ Software zugänglich gemacht wird, wenn der Ersterwerber seine eigene Kopie unbrauchbar gemacht hat.[253]

Gleichwohl die CAD-Datei eine Steuerungsanweisung an den 3D-Drucker beinhaltet, ist sie selbst kein Computerprogramm, sondern eine digitale Abbildung des materiellen Objekts; die Rechtsprechung zu den Computerprogrammen kann daher nicht unmittelbar angewendet werden. Ungeklärt ist daher, inwieweit sich die zu Computerprogrammen ergangenen Entscheidungen auf andere digitale Inhalte übertragen lassen. Die Instanzrechtsprechung verneint dies,[254] die Literatur hingegen plädiert aufgrund der wirtschaftlichen Vergleichbarkeit für eine Anwendung des urheberrechtlichen Erschöpfungsgrundsatzes auf alle digitalen Inhalte.[255] Es besteht mithin Klärungsbedarf.

b) Stand der Diskussion im Rahmen des § 24 MarkenG

Die Überlegungen zum Urheberrecht können grundsätzlich als Ausgangspunkt für die Bewertung der markenrechtlichen Erschöpfung herangezogen werden. Nach Auffassung des BGH ist etwa § 24 Abs. 1 MarkenG entsprechend anzuwenden, soweit sich das Verbreitungsrecht des Urhebers auf nichtkörperliche Kopien von Computerprogrammen erstrecken und hinsichtlich solcher Kopien erschöpfen kann.[256] Dann könne eine Weiterverbreitung auch markenrechtlich nicht unterbunden werden.[257]

Falls mithin die CAD-Datei als markenmäßige Benutzungshandlung zu qualifizieren ist (zur unklaren Rechtslage siehe oben Ziff. Teil 6III.2.) und die Verletzungshandlung im geschäftlichen Verkehr stattfindet, dürften die im Bereich des 3D-Drucks am häufigsten vorkommenden Fallkonstellationen wie folgt zu beurteilen sein:

- Ein 3D-gedrucktes Objekt ist eine Ware, so dass sich die Frage der Anwendbarkeit des § 24 MarkenG bei digitalen Inhalten nicht stellt. Etwaige an dem Ausgangsprodukt bestehende Markenrechte sind nicht erschöpft, da diese stets nur in Bezug auf eine konkrete, mit der Marke gekennzeichnete Ware eintreten kann.[258] Das gedruckte Objekt ist eine Vervielfältigung des Ausgangsobjekts und nicht mit diesem identisch; es existieren daher zwei Produkte. Mangels Erschöpfung kann die (Weiter-)Veräußerung des gedruckten Objekts untersagt werden.

- Stellt der Markeninhaber dem Nutzer selbst eine CAD-Datei zur Verfügung, ist *de lege lata* unklar, ob und inwieweit an dieser Datei Erschöpfung eintreten und der Nutzer die Datei daher weiterveräußern kann.

---

[253] BGH Urteil vom 11.12.2014, I ZR 8/13; GRUR 2015, 772 - UsedSoft III.
[254] OLG Hamm, Urteil vom 15.5.2014 – I-22 U 60/13; MMR 2014, 689; OLG Stuttgart, Urteil vom 3.11.2011 – 2 U 49/11;. MMR 2012, 834.
[255] *Hoeren/Foersterling,* MMR 2012, 642, 647*; Hoeren/Jakopp,* MMR 2014, 646, 648*; Druschel,* GRUR Int 2015, 125, 131.
[256] BGH, Urteil vom 17.07.2013, I ZR 129/08, GRUR 2014, 264 - UsedSoft II.
[257] Dem BGH insoweit folgend *Hacker,* in: Ströbele/Hacker, Markengesetz, 11. Aufl. 2015, § 24 Rn. 135.
[258] Vgl. *Ingerl/Rohnke,* in: Ingerl/Rohnke, Markengesetz, 3. Auflage 2010, § 24, Rn. 15.

- Anders dürfte es zu werten sein, wenn der Markeninhaber eine Lizenz erteilt, die es dem Nutzer erlaubt, selbst unter Verwendung der Marke das Produkt zu kreieren und dieses über eine 3D-Druckerei auszudrucken.[259] Das so erzeugte Produkt ist dann mit Zustimmung des Markeninhabers in den Verkehr gebracht worden und darf - aufgrund erschöpfter Markenrechte – weiterverbreitet werden.

4. Bewertung des Klärungs- und Handlungsbedarfs

Das geltende Immaterialgüterrecht bietet erwartungsgemäß bereits einen grundsätzlichen Schutz vor Produktpiraterie auch durch unautorisierten 3D-Druck. Hierbei gewährt das Urheberrecht – soweit anwendbar – den wohl weitesten Schutz, nämlich auch im Privatbereich. Allerdings ist hierbei zunächst die Schutzschranke der Werkqualität nach § 2 Abs. 2 zu überwinden und im Verletzungsfall die nicht immer einfach nachzuweisende Rechtekette zu belegen. Insbesondere im Markenrecht besteht jedoch Klärungsbedarf, so etwa im Hinblick auf die Einordnung des Einscannens von markenrechtlich geschützten Objekten sowie der Erstellung / Verbreitung der CAD-Dateien als bereits potentiell rechtsverletzende Benutzungshandlungen und im Hinblick auf die Reichweite des Erschöpfungsgrundsatzes. Offene Fragen ergeben sich gleichermaßen im Patentrecht. Auch bei der Störerhaftung und möglicher Weiterungen der Prüfpflichten von Plattformbetreibern und gewerblichen 3D-Druckereien dürfte die Diskussion noch nicht abgeschlossen sein.

[259] So etwa der Spielzeughersteller *Hasbro*, vgl. http://futurezone.at/produkte/hasbro-verkauft-von-fans-erstellte-3d-druck-figuren/76.001.634.

Teil 7 (Produkt-) Haftung/Haftung für Softwaremängel und versicherungsrechtliche Aspekte *(Prof. Dr. Thomas Klindt, Dr. Susanne Wende, LL.M., Dr. Steffen Burrer, Dr. Henning Schaloske, Konrad Żdanowiecki)*

I. Vertragliche[260] Haftung für Software/Softwarefehler

1. Gewährleistung und Haftung bei der Lieferung/Zurverfügungstellung von Software, Maschinen und Smart Products (insbesondere im Zusammenhang mit IT-Sicherheitsmängeln)

a) Grundsätze

Bei dauerhafter Überlassung von Software oder softwareunterstützten Maschinen bzw. Produkten richtet sich die vertragliche Haftung für Softwarefehler im Grundsatz nach allgemeinem kauf- oder werkvertraglichen Gewährleistungsrecht. Der Käufer bzw. Auftraggeber hat somit einen Anspruch auf Verschaffung des Gegenstands frei von Sach- und Rechtsmängeln nach § 433 Abs. 1 S. 2 BGB bzw. § 633 Abs. 1 BGB.

Ist die Software mangelhaft, hat der Käufer die in § 437 BGB bezeichneten Mängelrechte, d. h. primär gemäß § 439 BGB einen Anspruch auf Nacherfüllung in Form der Nachlieferung oder Nachbesserung. Scheitert diese, können Ansprüche auf Schadensersatz oder Ersatz vergeblicher Aufwendungen sowie daneben die Möglichkeit zur Preisminderung oder eines Rücktritts vom Vertrag bestehen. Rücktritt und Schadensersatz statt der ganzen Leistung sind nur möglich, wenn der Mangel wesentlich ist. Ist die Software nur ein Teil des Produkts, etwa im Falle von in Hardware bzw. Maschinen integrierter Firmware, ist für Rücktritt und Schadensersatz statt der Leistung somit entscheidend, ob sich der Mangel in Bezug auf das Gesamtprodukt als wesentlich auswirkt. Da indes die meisten Geräte mit integrierter Software von dieser gesteuert werden oder aber jedenfalls in erheblichem Umfang auf ihre Funktionsfähigkeit angewiesen sind, stellt ein wesentlicher Mangel der Software in aller Regel auch einen Mangel des Gesamtprodukts dar. Dies gilt insbesondere für Smart Products, wie z. B. moderne Mobiltelefone oder „Wearables“, sowie für untereinander verbundene Produktionsmaschinen in der Fabrik 4.0.

---

[260] Davon abzugrenzen ist die deliktische Haftung für Softwarefehler, etwa nach § 823 Abs. 1 BGB. Für einen Anspruch nach § 823 Abs. 1 BGB muss eines der dort aufgeführten Rechtsgüter (z.B. Eigentum) oder ein diesen vergleichbares „sonstiges Recht“ verletzt worden sein. In der Praxis führen Softwarefehler, wie z.B. Abstürze oder fehlerhafte Funktionen, primär zu einer Schädigung des Vermögens des Kunden, etwa Betriebsstörungen oder entgangenen Einnahmen, ohne dass dies auf eine Verletzung der von § 823 Abs. 1 BGB geschützten Rechte zurückzuführen ist. Führen aber die Auswirkungen des Softwarefehlers zu einem Sach- oder Personenschaden (z.B. Autounfall mit „vernetztem“ Fahrzeug), kommt ein Anspruch aus § 823 Abs. 1 BGB nach den Grundsätzen der Produzentenhaftung in Betracht. Der Softwarehersteller kann zwar ggf. im Innenverhältnis zum Verkäufer vertraglich Einschränkungen für den Regress vorsehen (zum diesbezüglichen Handlungsbedarf beim AGB-Recht siehe unten bei I.6.). Wenn aber der geschädigte Endkunde aufgrund der Auswirkungen der Software direkt den Softwarehersteller in Anspruch nimmt, wirken derartige Haftungsbeschränkungen nicht gegenüber dem Endkunden.

Heutzutage wird Software zunehmend nicht mehr dauerhaft, sondern nur noch auf Zeit überlassen. Dieser Trend wird vor allem durch das Cloud Computing verstärkt, bei dem die Software vom Provider[261] betrieben und gepflegt wird.[262] Nicht zuletzt seitdem der BGH für das Application Service Providing – quasi dem „Vorgänger" des Cloud Computing – das Mietrecht für anwendbar erklärt hat,[263] wird dessen Gewährleistungs- und Haftungsregime auf praktisch alle Formen der Softwareüberlassung auf Zeit angewandt. Dies hat für den Provider insbesondere zur Folge, dass er wegen § 535 Abs. 1 BGB während der Vertragsdauer die Software in vertragsgemäßem Zustand zu erhalten hat, was dazu führt, dass in dieser Zeit keine Verjährungsfrist für Ansprüche auf Fehlerbeseitigung läuft und dass Anpassungen an äußere Umstände, wie z. B. Gesetzesänderungen oder Schnittstellenänderungen, geschuldet sein können. Dies kann für den Softwareanbieter zu enormen Aufwänden und Kosten führen. Anderen Rechtsordnungen, die die Softwareüberlassung eher als Rechteeinräumung bzw. Lizenzvertrag verstehen, sind derart weitreichende Aktualisierungspflichten fremd. Es stellt sich die Frage, ob eine schrankenlose Anwendung des Mietrechts auf Softwareüberlassung sachgerecht ist oder ob nicht zumindest die Gebrauchserhaltungspflicht beschränkt werden sollte.

b) (Weiter) Mangelbegriff des deutschen Rechts

Zwar besteht bei Software aufgrund deren Komplexität die Besonderheit, dass eine vollständig fehlerfreie Programmierung faktisch auch bei bestem Qualitätsmanagement nicht möglich ist. Dennoch rechtfertigt dies nach h. M. keine Abweichung von der allgemeinen Definition des Mangels.[264]

Ein Mangel liegt immer dann vor, wenn die Ist- von der Sollbeschaffenheit abweicht. Dabei kann sich die Sollbeschaffenheit aber nach dem weiten Mangelbegriff des deutschen Rechts[265] gemäß den verschiedenen Varianten der § 434 Abs. 1 bzw. § 633 BGB nicht nur aus einer ausdrücklichen Vereinbarung, sondern auch aus der Eignung zur im Vertrag vorausgesetzten bzw. sogar „gewöhnlichen" Verwendung ergeben, „die bei Sachen der gleichen Art üblich ist".[266] Gerade bei individuell für einen Auftraggeber erstellter oder angepasster Software (Stichwort: Customizing), hängt das Design des Programms, der Schnittstellen oder auch der Benutzeroberflächen jedoch derart stark von den individuellen (fachlichen) Anforderungen des jeweiligen Auftraggebers ab, dass sich insofern eine Bestimmung der „gewöhnlichen" Eignung durch einen Vergleich zu anderen Softwareprodukten als äußerst schwierig erweist.

---

[261] Im Folgenden wird einheitlich der Begriff Provider verwendet, wenn von einem Verkäufer, Vermieter, Auftragnehmer oder sonstigen Unternehmen gesprochen wird, welches Software oder softwareunterstützte Produkte vertreibt.

[262] Siehe dazu im Detail Teil 10I. zu Cloud Computing von *Thalhofer*.

[263] BGH NJW 2007, 2394.

[264] *Von dem Bussche/Schelinski*, Münchener Anwaltshandbuch IT-Recht, Teil 1 Rn. 194.

[265] Vgl. *Redeker*, IT-Recht Rn. 334.

[266] Bzw. bei Werkverträgen einer Eigenschaft die bei „Werken der gleichen Art üblich ist".

Leichter festzustellen ist ein Sachmangel hingegen dort, wo es um bestimmte allgemein an ein Softwareprodukt zu stellende Anforderungen geht, wie etwa eine hinreichende Stabilität (d. h. keine Abstürze) oder, dass die Software keine Sicherheitslücken enthält, die beispielsweise Angriffe durch Viren oder Trojaner ermöglichen.

Rechtsmängel liegen vor allem dann vor, wenn der Provider Softwarecode eines Dritten (z. B. Bibliotheken) ohne entsprechende lizenzvertragliche Befugnis verwendet und dieser Dritte deshalb gegen den Nutzer der Software urheberrechtliche Unterlassungs- und ggf. sogar Schadensersatzansprüche geltend macht. Gerade Rechtsmängel können für den Provider besonders schwerwiegende Konsequenzen haben, weil sich viele Kunden (zumindest im B2B) in der Praxis nicht mit den gesetzlichen Mängelrechten begnügen möchten und deshalb vom Provider vertraglich eine unbefristete und unbeschränkte Freistellung im Falle einer solchen Inanspruchnahme durch Dritte verlangen. Gerade wenn der Kunde ein großer Konzern ist und es sich um geschäftskritische Software oder um solche Software handelt, die in millionenfach vertriebenen Produkten integriert ist, kann der Schaden im Zusammenhang mit einem Rechtsmangel schnell in die Millionen gehen.

c) Möglichkeiten/Grenzen einer Haftungsminimierung in B2B und B2C

Angesichts der umfassenden Gewährleistungs- und Haftungsrisiken unter dem BGB sind die Provider bestrebt, diese Risiken vertraglich auszuschließen bzw. zumindest zu minimieren. Im Bereich Haftung sind in der Praxis bestimmte Haftungshöchstgrenzen üblich, meist ausgedrückt als Prozentsatz des vom Kunden zu entrichtenden Preises (häufig 100 %). Dabei sind individualvertraglichen Regelungen fast keine Grenzen gesetzt, sieht man etwa von Extremen wie § 276 Abs. 3 BGB (Ausschluss von Vorsatz) oder § 138 BGB (Sittenwidrigkeit) ab.

In aller Regel muss der Provider jedoch wegen der Anzahl der Kunden standardisierte Vertragsmuster verwenden. Hier gelten dann aber die Restriktionen des AGB-Rechts, insb. § 309 Nr. 7 und § 307 Abs. 1, 2 BGB – und zwar sowohl im B2B als auch im B2C. Neben einer Unzulässigkeit des Haftungsausschlusses für grobe Fahrlässigkeit ist vor allem die Rechtsprechung des BGH zu den sog. „Kardinalpflichten“, häufig auch als „wesentliche Vertragspflichten“ bezeichnet, zu beachten.[267] Demnach darf für diese wesentlichen Pflichten in AGB die Haftung für einfache Fahrlässigkeit nicht den „typischerweise vorhersehbaren“ Schaden beschränken. Dies führt bei Software und softwareunterstützten Produkten aber faktisch dazu, dass eine Haftung für den praktisch relevanten Fall der einfachen Fahrlässigkeit nicht wirklich beschränkt werden kann. Denn die Freiheit der Software von den oben beschriebenen Mängeln wird in aller Regel als wesentliche Vertragspflicht anzusehen sein und der typischerweise vorhersehbare Schaden lässt sich vorab kaum mit einer festen Summe fassen. Etwaigen Beschränkungen auf absolute Zahlen oder feste Prozentwerte des Auftragsvolumens ist deshalb stets eine AGB-Widrigkeit immanent.

[267] Etwa BGH NJW 2002, 673, BGH NJW-RR 2005, 1496.

Auch eine Beschränkung der sonstigen Gewährleistungsrechte ist in AGB nur sehr begrenzt möglich. So kann z. B. das Rücktrittsrecht wegen § 309 Nr. 8a), 8b), bb) BGB nicht ausgeschlossen werden. Möglich und marktüblich ist eine Verkürzung der Verjährungsfrist auf ein Jahr ab Lieferung (vgl. § 309 Nr. 8b), ff) BGB). Zu beachten ist auch § 309 Nr. 8a), aa) BGB, welcher der in vielen Provider-AGB enthaltenen Regelung entgegensteht, wonach keine Gewährleistung für in dem Produkt verwendete Drittsoftware übernommen wird.

AGB-rechtlich zulässig ist hingegen nach auch hier vertretener Auffassung eine Regelung, die in Abweichung von § 439 Abs. 1 BGB bei Softwarekaufverträgen dem Provider die Wahl der Art der Nacherfüllung gestattet. Dies ermöglicht es dem Provider, die technisch und kommerziell sinnvollste Lösung zu wählen. Häufig besteht diese darin, dem Käufer keine neue Kopie der vollständigen Software, sondern lediglich eine Korrektur des betroffenen Codeteils zu überlassen (sog. Patch oder Bugfix). Dagegen ist wegen § 439 Abs. 2 BGB eher fraglich, ob die häufig in Provider-AGB vorgesehene Verpflichtung/Obliegenheit des Käufers, den Patch selbst einzuspielen, AGB-rechtlich haltbar ist.

Angesichts dieser sehr begrenzten Möglichkeiten zur Beschränkung von Gewährleistungs- oder Haftungsansprüchen in AGB, sollten Provider ein besonderes Augenmerk auf die möglichst genaue Beschreibung der Software im Sinne einer Beschaffenheitsvereinbarung legen, einschließlich einer klaren Beschreibung dessen, was nicht zum geschuldeten Leistungsumfang gehört (sog. negative Beschaffenheitsvereinbarung), etwa Kompatibilität mit Drittprodukten oder Schnittstellen. Denn soweit eine solche – positive wie negative – Beschaffenheitsvereinbarung vorliegt, kommt es nach auch hier vertretener Auffassung nicht mehr auf eine objektive Eignung und/oder die Beschaffenheit vergleichbarer Software gemäß § 434 Abs. 1 S. 2 Nr. 2 bzw. 633 Abs. 2 S. 2 Nr. 2 BGB an. Dadurch kann der Provider bis zu einem gewissen Grad über die Leistungsbeschreibung steuern, wann die Software als mangelfrei oder mangelhaft anzusehen ist. Dies gilt jedenfalls dann, wenn durch eine solche – insb. negative – Leistungsbeschreibung nicht in Wirklichkeit ein „versteckter“ Gewährleistungsausschluss für einen nach dem Vertragszweck eigentlich zu erwartenden Leistungsumfang erfolgt.

2. Gewährleistung und Haftung für software-gestützte Dienste in der digitalisierten Wirtschaft

Auch in Fällen, in denen die Software nicht der eigentliche Leistungsgegenstand ist, können Softwarefehler zu vertraglichen Haftungsansprüchen führen. Erstellt etwa der Provider bei einem HR-Outsourcing aufgrund eines Softwarefehlers eine fehlerhafte Abrechnung, liegt darin eine vertragliche Pflichtverletzung des Outsourcing-Vertrags, weil zwar die Fehlerfreiheit der Software selbst vertraglich nicht geschuldet ist, wohl aber das Erstellen einer korrekten Abrechnung. Gleiches gilt, wenn ein bestelltes Produkt aufgrund eines Fehlers der ERP-Software oder einer Lieferdrohnensoftware nicht oder nur verspätet beim Kunden ankommt.

Die konkreten Ansprüche des Kunden sind letztlich eine Frage des ihm gegenüber vertraglich geschuldeten Leistungsinhalts und dem dadurch zu bestimmenden Vertragstyp. So stehen etwa im erstgenannten Beispiel dem Kunden werkvertragsrechtliche Gewährleistungsansprüche gemäß den §§ 637 ff. BGB zu, etwa auf Nacherfüllung, Minderung oder Schadensersatz, weil der geschuldete Erfolg (= die Erstellung einer Abrechnung) nicht mangelfrei erbracht wurde. Schuldet der Provider nach dem jeweiligen Vertragsinhalt gegenüber seinen Kunden allein die Vornahme bestimmter Tätigkeiten und findet daher gemäß §§ 611 ff. BGB Dienstvertragsrecht Anwendung, bestehen keine Gewährleistungsrechte, insbesondere kein Minderungsrecht. Eine durch Softwarefehler verursachte Schlechtleistung kann aber zu Schadensersatzansprüchen des Kunden führen.

a) Kann sich der Verpflichtete nach § 280 Abs. 1 S. 2 BGB vom Fahrlässigkeitsvorwurf exkulpieren?

Ist vertraglich kein abweichender Haftungsmaßstab zwischen den Parteien vereinbart, haftet der Provider jedoch nur dann auf Schadensersatz, wenn ihn der Vorwurf vorsätzlichen oder fahrlässigen Verhaltens trifft, §§ 280 Abs. 1 S. 2, 276 Abs. 1 BGB. Dieser Grundsatz des deutschen Zivilrechts ist ein beachtlicher Unterschied zu einigen anderen Jurisdiktionen, in denen die vereinbarte Beschaffenheit der Software bzw. der Vertragsleistung in der Regel als „warranty“ gewährt wird und ein „breach of warranty“ unabhängig vom Vertretenmüssen zu Schadensersatzansprüchen führt. Dies scheint im internationalen Vergleich zu einer Schlechterstellung des Kunden aufgrund des deutschen Zivilvertragsrecht zu führen.

In der Praxis hat dies aber in vielen Fällen keine Auswirkungen. Zum einen gestatten diese ausländischen Rechtsordnungen dem Provider nämlich häufig sehr weitgehende Haftungsausschlüsse. Zum anderen wird das Vertretenmüssen gemäß § 280 Abs. 1 S. 2 BGB vermutet. Den Provider trifft somit die Beweislast dafür, dass er nicht schuldhaft, d. h. nicht einmal mit leichter Fahrlässigkeit, gehandelt hat.

Dieser Entlastungsbeweis ist jedenfalls für den Hersteller der Software sowie den mit Customizing auf Quellcodeebene beauftragten Auftragnehmer schwer zu führen. Hingegen wird ein auf den Ein- und Verkauf beschränkter Distributor in der Regel keine Kenntnis von dem Mangel haben können, solange dieser nicht bereits von einzelnen Kunden gerügt wurde.

Ist die Software bzw. ein mit dieser ausgestattetes Produkt nicht die „eigentliche“ Vertragsleistung, kommt es auf die Umstände des Einzelfalls an, ob der Softwarefehler für den Anbieter dieser „eigentlichen“ Vertragsleistung erkennbar und vermeidbar war oder ob er sich seinem Kunden gegenüber nach § 280 Abs. 1 S. 2 BGB exkulpieren kann. Problematisch wird es für den Anbieter dann, wenn die Schlechtleistung gegenüber dem Kunden auf einem Softwarefehler beruht, den der Provider des Anbieters in einer neuen Version, etwa einem Update oder Upgrade, eigentlich behoben hatte, der Anbieter aber aus betrieblichen Gründen noch nicht auf diese neue Version aufgerüstet hat. Für den Nutzer einer Software kann es nämlich durchaus berechtigte Interessen geben, nicht bzw. nicht sofort auf die

neue Version „mitzuziehen“, etwa weil die Installation der neuen Version eine zusätzliche Vergütung an den Provider oder interne Aufwände erfordert (z. B. durch die Bindung personeller Ressourcen oder die Notwendigkeit auch die Systemumgebung aufzurüsten). Gleichzeitig dürfte eine Exkulpation nach § 280 Abs. 1 S. 2 BGB im Verhältnis zum eigenen Kunden sehr schwer fallen, wenn vom Provider etwa Sicherheitslücken oder Funktionsstörungen der Software durch die neue Version eigentlich beseitigt wurden. Hier wird es häufig nur noch mehr darauf ankommen, ob der Anbieter/Softwarenutzer wenigstens seinen Provider wegen des zunächst ja bestehenden Fehlers der Software in Regress nehmen kann oder ob der Provider aufgrund einer entsprechenden vertraglichen Regelung nicht für Schäden haftet, die durch das Einspielen der neuen Version hätten vermieden werden können.

b) Gewährleistung/Haftung für fehlerhafte Daten und Datenanalysen

Wenn die gelieferte Software fehlerhafte Daten beim Kunden erzeugt, stellt dies in aller Regel ein Mangel der Software dar, so dass dem Kunden – je nach Vertragsart – die Gewährleistungsansprüche der §§ 437 ff. BGB bei Kaufrecht, §§ 535 ff. BGB bei Mietrecht oder §§ 634 ff. BGB bei Werkvertragsrecht – zustehen. Dabei ist aber zu beachten, dass der Nacherfüllungsanspruch des Kunden auf Beseitigung des Softwarefehlers durch Lieferung eines Patches oder einer fehlerfreien neuen Version gerichtet ist. Der Provider schuldet im Rahmen der Nacherfüllung weder die Neuvornahme der fehlerhaften Datenverarbeitung bzw. Datenanalyse, noch eine Lieferung fehlerfreier Daten bzw. Datenanalyseergebnisse.

Es kommt deshalb entscheidend darauf an, ob dem Kunden ein Anspruch auf Schadensersatz zusteht. Grundvoraussetzung ist in jedem Fall, dass der Provider den Softwarefehler zu vertreten hat. Im Weiteren ist zu differenzieren:

– Sorgt der Softwarefehler dafür, dass beim Kunden zuvor gespeicherte „richtige“ Daten nach dem Verarbeitungsprozess falsch oder verlorengegangen sind, könnte grundsätzlich ein Anspruch auf Kostenersatz für die Widerherstellung der richtigen Daten in Betracht kommen. Die entsprechende gesetzliche Grundlage in § 249 Abs. 2 BGB knüpft allerdings an die Beschädigung einer Sache i. S. d. § 90 BGB an. Daher ist zwar unstrittig, dass bei Beschädigung oder Zerstörung eines Datenträgers (z.B. Festplatte) etwa die Aufwände für eine Rückübertragung gesicherter Daten von einem Backup-Medium oder für das Reproduzieren der Daten durch manuelle oder technische Erfassung von noch vorhandenen Vorlagen nach § 249 Abs. 2 BGB zu erstatten sind.[268] Dies gilt aber nur in dem Fall, dass der Datenträger im Eigentum des Softwarenutzers steht, was in Zeiten von Cloud Computing immer seltener der Fall ist. Da aber verfälschte oder gelöschte Daten in der Regel das eigentliche „wirtschaftliche Eigentum“ des Softwarenutzers ausmachen, stellt sich die Frage einer analoge An-

[268] Ist hingegen eine Neuschaffung der Daten durch eine „geistige oder schöpferische Leistung“ erforderlich, wird nur Wertersatz nach § 251 Abs. 1 BGB gewährt, vgl. BGH NJW 2009, 1066.

wendung der §§ 90, 249 Abs. 2 BGB.[269] Ansonsten kommt ein Wertersatzanspruch nach § 251 Abs. 1 BGB in Betracht. Der Kunde sollte jedenfalls nicht auf eine Naturalrestitution gemäß § 249 Abs. 1 BGB in Form einer Wiederherstellung der „richtigen“ Daten durch den (unzuverlässigen) Provider verwiesen werden.

– Liegt hingegen der Fall vor, dass bestehende Daten unverändert bleiben und dass lediglich durch die fehlerhafte Verarbeitung neu geschaffene Daten „falsch“ sind, besteht kein erstattungsfähiger Wiederherstellungsaufwand. Allerdings können dem Kunden (ebenso im Übrigen auch in Variante (1)) Schadensersatzansprüche etwa wegen entgangenem Gewinn nach § 252 BGB (z. B. wenn der Kunde die Ergebnisse der Datenanalyse an Dritte hätte verkaufen können) oder Freistellungsansprüche wegen einer Inanspruchnahme durch einen Dritten (z. B. wenn der Kunde von Erwerbern der Datenanalyseergebnisse wegen deren Fehlerhaftigkeit in Anspruch genommen wird) zustehen.

c) Probleme sog. mittelbarer Schäden/Vermögensfolgeschäden

Der Provider einer mangelhaften Software bzw. eines softwareunterstützten Produkts haftet regelmäßig nicht nur für die unmittelbaren, das Äquivalenzinteresse betreffenden Schäden an der Software bzw. dem Produkt. Er hat vielmehr auch darüber hinausgehende, mittelbare Schäden (auch Vermögensfolgeschäden genannt), wie etwa entgangenen Gewinn, Nutzungsausfall, Verlust oder Vernichtung von Daten zu ersetzen.[270] Hier drohen dem Provider erhebliche Haftungsrisiken. So kann fehlerhafte Software etwa dazu führen, dass die Produktion in Betrieben komplett stillsteht. Der Provider hat also ein großes Interesse daran, Ansprüche wegen solcher mittelbarer Schäden vertraglich auszuschließen oder zu beschränken.

Während solche Ausschlüsse in Verträgen nach US-Recht und zahlreichen anderen Rechtsordnungen (insb. des Common Law) regelmäßig fester Vertragsbestandteil sind,[271] ist dies in Standardverträgen unter deutschem Recht nicht mit § 307 BGB vereinbar.[272] Dies ist für viele ausländische Provider ein wahrer Kulturschock und stellt aus ihrer Sicht ein nur schwer zu kalkulierbares kommerzielles Risiko dar. Wenn sie in den deutschen Markt eintreten wollen, werden die Provider durch das strenge Korsett des AGB-Rechts dazu gezwungen, Haftungsrisiken einzugehen, die sie oftmals nicht in ihren Business Case einkalkuliert haben und die nicht mit ihren (konzern-)internen Vorgaben und Richtlinien vereinbar sind.

---

[269] Vgl. dazu oben in Teil 2 (Recht an Daten) unter Teil 2II.1.

[270] Vgl. *Grüneberg*, in: Palandt, BGB, Vorb v § 249 Rn. 15; *Schneider*, in: Schneider: Handbuch des EDV-Rechts, 4. A., Kap. J Rn. 313; BGH, NJW 2003, 826 (828).

[271] Vgl. etwa *Funk/Wenn*, CR 2004, 481.

[272] BGH NJW 2001, 292; *Schneider*, in: Schneider: Handbuch des EDV-Rechts, 4. A., Kap. J Rn. 313.

d) Gesetzgeberischer Handlungsbedarf?

Auch deutsche Provider haben jedenfalls im B2B häufig wenig Verständnis dafür, dass ein Ausschluss oder eine Beschränkung der Haftung in einem Standardvertrag keine Gültigkeit haben soll, auch wenn der Kunde die Regelung akzeptiert. Insbesondere die strenge Rechtsauslegung des BGH, wonach ein Verhandeln eines Vertrags noch kein „Aushandeln" darstellen soll,[273] sind in der Praxis nur sehr schwer vermittelbar. Anders als im B2C-Bereich, besteht im B2B-Bereich häufig kein derartiges Ungleichgewicht in der Verhandlungsmacht, sodass es die Beschränkungen des AGB-Rechts gegenüber dem Verwender erfordert. Es stellt sich die Frage, ob man den Parteien im B2B-Bereich bei zentralen kommerziellen Aspekten, wie der Haftung, nicht mehr Vertragsautonomie zutrauen und die Restriktionen des AGB-Rechts nur dort zur Geltung bringen sollte, wo das Gegenüber tatsächlich keinen Einfluss auf den Vertragsinhalt nehmen konnte.

II. Produkthaftung

Vor dem Hintergrund des aktuellen deutschen und europäischen Rechtsrahmens der Produkthaftung werden die Lösungsmöglichkeiten der einzelnen Herausforderungen der digitalen Wirtschaft geprüft. Etwaige Lücken oder Rechtsunsicherheiten, welche den Vertrieb oder die Nutzung der innovativen Technologien behindern oder erschweren könnten, werden mit Lösungsansätzen aufgezeigt.

1. Maßstäbe des Produkthaftungsrechts

a) Wer ist „Hersteller" von Produkten beim Einsatz innovativer Produktionstechnologien?

Der klassische Begriff des „Herstellers" hat eine tatsächliche Verarbeitung von Werkstoffen durch menschliche Beeinflussung vor Augen. Eine begriffliche Weiterung findet sich im Terminus des „Quasi-Herstellers". Schließlich hat das europäische Recht den Herstellerbegriff in Art. 3 der Produkthaftungsrichtlinie (85/374/EWG)/§ 4 ProdHaftG vom Produktionsprozess selbst abstrahiert. Diese weite Auslegung des Herstellerbegriffs lässt sich indessen nur mit der in der Produkthaftungsrichtlinie statuierten Gefährdungshaftung in Einklang bringen – terminologisch genauer wäre es insoweit, allein vom „Inverkehrbringer" zu sprechen.

Im klassischen verschuldensabhängigen deutschen Deliktsrecht lässt sich dieser Ansatz jedoch nicht fruchtbar machen. Ohnehin ist der Begriff des „Herstellers" nicht allein geeignet, das Haftungssubjekt zutreffend zu bezeichnen. Die Schadensersatzpflicht nach dem geltenden Deliktsrecht ist nicht an eine „Hersteller"-Eigenschaft geknüpft.[274] Auch rückt ein Unternehmer dadurch, dass er seinen Namen auf den Verpackungen eines Produkts oder an

[273] Erst dann handelt es sich nach Ansicht des BGH um eine Individualabrede und nicht (mehr) um AGB, vgl. zuletzt BGH NJW 2014, 1725.

[274] BGH, Urt. v. 11.12.1979 – VI ZR 141/78, NJW 1980, 1219 – Klapprad; BGH, Urt. v. 17.3.1981 – VI ZR 286/78, NJW 1981, 1606 (1609) – Benomyl.

dem Produkt selbst anbringt, nicht in die deliktsrechtliche Pflichtenstellung eines Warenerzeugers ein. Entscheidend ist allein, ob der wegen eines Produkt- oder Instruktionsfehlers in Anspruch genommene Unternehmer Verkehrssicherungspflichten verletzt hat.

Die Fragestellung beim Einsatz innovativer Produktionstechnologien wird sich daher vom gedanklichen Grundansatz noch weiter vom klassischen Herstellerbegriff lösen müssen, ohne dass damit die von der Rechtsprechung zur Produzentenhaftung entwickelten Grundsätze in Frage gestellt würden, nach denen es nur darauf ankommt, welche Gefahrabwendungspflichten bei Aufteilung der Herstellungstätigkeiten auf mehrere Unternehmen dem einzelnen Beteiligten obliegen.[275]

Gerade bei innovativen Produktionstechnologien, bei denen sich der menschliche Einfluss auf den Produktionsprozess selbst mehr und mehr reduziert, wird für Haftungsfragen die Frage zentral werden, ob sich ein Unternehmer, der als „Hersteller“ auftritt und ein Erzeugnis als „sein Produkt” auf den Markt bringt, derart mit der Ware identifiziert, dass auch ihm die für den Warenhersteller geltenden Gefahrabwendungspflichten auferlegt werden können und ob er deshalb zum Schutz der Produktgeschädigten haftungsrechtlich nicht mehr wie ein bloßer Vertriebshändler behandelt werden kann.[276]

Die deutsche Deliktsrechtsdogmatik wird daher in der Lage sein, auch im Falle von innovativen Produktionstechnologien die Haftung zutreffend zuzuweisen. Auch wenn damit eine Verlagerung von unmittelbaren Konstruktions- und Fabrikationspflichten auf Überwachungspflichten einhergehen wird, besteht vom Grundsatz her kein Anlass, das deutsche Verschuldensprinzip an dieser Stelle einer Ausdehnung der Gefährdungshaftung des Inverkehrbringers über das derzeitige ProdHaftG hinaus zu opfern – die vom BGH eingeführte Beweislastumkehr führt ohnehin schon in den meisten Fällen zu einer quasi verschuldensunabhängigen Haftung oder zu einer Art „heimlicher Ersatz-Kausalhaftung“.[277]

b) „Produktfehler“ als sachgerechtes Konzept für die digitalisierte Wirtschaft?

Computerprogramme als moderne und inzwischen ubiquitäre Wirtschaftsgüter können ein nicht unerhebliches Gefahrenpotential in sich bergen.[278] Die allgemeinen Grundsätze der Produkthaftung sind uneingeschränkt auf den Computerbereich übertragbar.[279] Zudem ist Software als Produkt i. S.d. § 2 S. 1 ProdHaftG anzusehen.[280]

---

[275] BGH, Urt. v. 14.6.1977 – VI ZR 247/75, VersR 1977, 839 – Autokran; Urt. v. 11.12.1979 – VI ZR 141/78, NJW 1980, 1219 – Klapprad.

[276] Dies hob bereits BGH, Urt. v. 11.12.1979 – VI ZR 141/78, NJW 1980, 1219 – Klapprad hervor; vgl. auch bereits *Schmidt-Salzer*, Produkthaftung, Band III/1, 2. Aufl. 1990, Rdnr. 4.388 und *ders.*, BB 1979, 1 (7).

[277] *Gruber* in Hilgendorf/Günther, Robotik und Gesetzgebung, S. 123 (146).

[278] So bereits *Lehmann*, NJW 1992, 1721; siehe auch die Beispiele bei *Littbarski* in Kilian/Heussen, Computerrechts-Handbuch, Teil 18 Rn. 2.

[279] So bereits *Littbarski* in Kilian/Heussen, Computerrechts-Handbuch, Teil 18 Rn. 24, 116.

[280] Vgl. nur *Wagner* in Münchener Kommentar zum BGB, 6. Aufl. 2013, ProdHaftG, § 2 Rn. 15.

Daher können auch die Fehlerkategorien übertragen werden. Konstruktionsfehler einer Software sind Fehler, die bei der Programmerstellung, Programmierung, Kompilierung usw. eines Computerprogrammes entstanden sind (sei es im Quellcode, sei es im Maschinencode).[281] Auch Fabrikationsfehler kommen bereits in Bezug auf die Software selbst in Betracht, wenn Kopierfehler, Übertragungsfehler etc. geschehen, was insbesondere im Hinblick auf die datenträgerungebundene Übermittlung relevant werden kann, während Instruktionsfehler bei eigenständig agierender Software an Bedeutung verlieren, soweit sie nicht jederzeit vom Nutzer deaktiviert, übersteuert oder aktiviert werden können, so dass dieser über die Auswirkungen seines Verhaltens – insbesondere hinsichtlich der Auswirkungen auf die Verkehrssicherheit bei Fahrassistenzsystemen – besonders aufgeklärt sein muss.[282]

Zum einen folgt damit der zunehmenden Automatisierung und immer weitergehender Aufspaltung des Produktionsprozesses zugleich eine Vorverlagerung der Konstruktionspflicht, die weniger für das rein physische Produkt selbst, als vielmehr für die hinter dem Produkt stehenden steuernden digitalen Vorgänge zentral ist. Hier wird den Programmierern abverlangt, bereits im technischen Design inhärente Sicherheit für alle Folgeprozesse abzubilden, die am Stand von Wissenschaft und Technik orientiert bestmögliche Sicherheit bietet.[283] Dass komplexere Software bekanntermaßen nicht völlig fehlerfrei hergestellt und ausgetestet werden kann, ändert prinzipiell nichts; allenfalls kann dies zu einer gewissen Herabsetzung der allgemeinen Sicherheitserwartungen führen.[284]

Zum anderen wird, wie oben bereits angedeutet wurde, mit zunehmender Komplexität und Digitalisierung von Produkten eine Schwerpunktverschiebung von Sorgfaltspflichten in der physischen Konstruktion und Fabrikation hin zu umfassender Produktbeobachtung als nachgelagerter Verkehrssicherungspflicht einhergehen.[285]

Hinsichtlich der Produktbeobachtung gilt es insbesondere, die softwaregesteuerten Geräte und Anwendungen – gerade auch in der Kombination mit anderen Geräten, mit denen eine digitale Interaktion erfolgt – in der Praxis zu verfolgen. Allein ein „passives“ Beschwerdemanagement wird im Hinblick auf in vieler Weise automatisiert ablaufende Vorgänge den Anforderungen kaum mehr gerecht werden können.[286] Im Hinblick auf die Analyse von Fehlfunktionen muss ein „Produktgedächtnis“ gefordert werden,[287] aus welchem sich nicht nur die wesentlichen Gerätevorgänge im Bedarfsfall entnehmen lassen,[288] sondern neben welchem auch aktiv Fehlermeldungen automatisch an den „Hersteller“ übermittelt und im

[281] Siehe schon *Lehmann*, NJW 1992, 1721 (1723).
[282] Vgl. *Jänich/Schrader/Reck,* NZV 2015, 313 (317).
[283] Vgl. *Bräutigam/Klindt*, NJW 2015, 1137 (1141).
[284] So bereits *Lehmann*, NJW 1992, 1721 (1725).
[285] Vgl. auch *Spindler* in Hilgendorf: Robotik im Kontext von Recht und Moral, S. 63 (73).
[286] Ebenso *Jänich/Schrader/Reck,* NZV 2015, 313 (318).
[287] Vgl. hierzu *Kröner* in Vieweg/Gerhäuser: Digitale Daten in Geräten und Systemen, S. 183.
[288] Vgl. auch *Hanisch* in Hilgendorf: Robotik im Kontext von Recht und Moral, S. 27 (38).

Rahmen eines kontinuierlichen Verbesserungsprozesses ausgewertet werden.[289] Damit ist auch das Product-Lifecycle-Management angesprochen, auf welches unten unter 5. noch eingegangen wird.

Gänzlich unentbehrlich wird eine solche Überwachung in der „intelligenten Fabrik“ sein, um Fabrikationsfehler einerseits zu verhindern und andererseits produktgenau eingrenzen zu können.

All dies ist offen für eine dynamische Entwicklung unter dem Aspekt der Verkehrssicherungspflicht, wobei allerdings Standardisierungen (hierzu Teil 8), vermutlich noch mehr als heute, erhebliche Indizwirkung auch für die Einhaltung der erforderlichen Sorgfaltspflichten zukommen wird, so dass die größte Einflussmöglichkeit weniger im Bereich der Gesetzgebung zu suchen ist, als auf der Ebene der Standardisierungsorganisationen, in die die Industrie selbst seit jeher eingebunden ist.

c) Auswirkungen der digitalisierten Wirtschaft auf den Maßstab „aktueller Stand von Wissenschaft und Technik“

Der rasante Fortschritt im digitalen Bereich stellt hohe Anforderungen daran, mit dem „aktuellen Stand von Wissenschaft und Technik“ Schritt zu halten. Denn auch wenn der BGH nicht verlangt, jederzeit die technische denkbar beste Sicherheit zu bieten, sondern die Umsetzung von überlegenen Alternativen erst dann verlangt, wenn nach dem Fachwissen der einschlägigen Fachkreise praktisch einsatzfähige Lösungen zur Verfügung stehen, so betont er doch ausdrücklich, dass Branchenüblichkeit dabei keine Rolle spielt, da der in der Branche praktizierte Stand der Sicherheit hinter dem technisch Möglichen und damit hinter dem rechtlich Gebotenen zurückbleiben kann.

Dieser Standard ist in einer von kontinuierlicher Fortentwicklung geprägten Softwarelandschaft, bei der oft ein Update das nächste „jagt“, aber nur noch schwer zu fassen. Zugleich ist darauf hinzuweisen, dass dies nicht zu einer stetigen Nachbesserungs- und Nachlieferungspflicht der Softwarehersteller führen darf,[290] während aber den Betreiber durchaus die Pflicht trifft, die Sicherheitsvorkehrungen stets an neue Erkenntnisse anzupassen[291] – worin er wiederum von den Herstellern abhängig ist.

Die Rechtsprechung verlangt dabei nicht, dass Sicherheitskonzepte umzusetzen sind, die nur „auf dem Reißbrett existieren“ oder noch in der Erprobung befindlich sind. Für diesen Maßstab prägend können im Übrigen auch – soweit bereits vorhanden – öffentlich-rechtlich statuierte Sicherheitsanforderungen für das Inverkehrbringen von Produkten einerseits sowie technische Normen und Standardisierungen als (in die Betrachtung einzubeziehende) Mindestanforderungen andererseits relevant werden.[292] Es ist daher aus prakti-

[289] Vgl. auch *Hartmann*, DAR 2015, 122 (124).
[290] Vgl. *Spindler,* MMR 2008, 7 (12).
[291] Vgl. *Spindler* in Hilgendorf: Robotik im Kontext von Recht und Moral, S. 63 (71).
[292] Vgl. auch *Spindler* in Hilgendorf: Robotik im Kontext von Recht und Moral, S. 63 (70).

scher Sicht, wie vorstehend schon erwähnt, damit zu rechnen, dass versucht wird, durch Standardisierungen eine besser zu fassende Ordnung herzustellen, so dass der Stand von Wissenschaft und Technik vor allem in den dafür zuständigen Gremien zu diskutieren sein wird.

d) Auswirkungen der digitalisierten Wirtschaft auf das Konzept der vorhersehbaren Fehlanwendung

Im Rahmen der wie vorstehend erläutert zu verstehenden konstruktiven Sicherheit nach Stand von Wissenschaft und Technik ist für die Industrie im Übrigen nicht nur die bestimmungsgemäße Verwendung, sondern auch eine umfassendere Form des Verwendungseinsatzes in Erwägung zu ziehen: Das ProdHaftG rekurriert hierzu in § 3 Abs. 1 Buchst. b auf den „Gebrauch, mit dem billigerweise gerechnet werden kann". Zu § 823 Abs. 1 BGB spricht die Rechtsprechung von vernünftigerweise vorhersehbarer Fehlanwendung.

Dass der Hersteller jedenfalls bei standardisierter Software und fehlendem unmittelbarem Kontakt mit dem Nutzer nicht in der Lage ist, die Risiken zu kalkulieren und sein Verhalten darauf einzustellen, mag über das Kriterium der Vorhersehbarkeit korrigiert werden können, kann aber nicht dazu führen, jegliche Haftung von vornherein abzulehnen.[293]

In der digitalisierten Wirtschaft wird eine solche mögliche Fehlanwendung zudem aber nicht mehr nur durch den menschlichen Geist beeinflusst, sondern auch durch eigenständig situationsangepasst (inter)agierende Maschinen – ein diesen unterlaufender Fehler muss nicht zugleich einen Konstruktionsfehler der Software bedeuten. Da hier die „Vernunft" als verantwortungsbegrenzendes Kriterium versagt, verbleibt nur, die Abgrenzung nach Risikosphären vorzunehmen, will man nicht den Schritt zur reinen Gefährdungshaftung gehen (siehe näher hierzu unter 3.d)).

2. Produktsicherheit und IT-Sicherheit – Produktfehler durch Cyber-Angriffe im Produktionsprozess und durch unzureichende IT-Sicherheit am Produkt selbst

Ein sensibler Punkt bei der Produkthaftung im Rahmen von Softwareprodukten ist die Haftung für das Einwirken von Dritten. Grundsätzlich endet die Verantwortlichkeit des Herstellers dort, wo ein Dritter vorsätzlich und rechtswidrig missbräuchlich eingreift und es dadurch zum Schaden kommt. Eine Ausnahme besteht nur dann, wenn es ein Merkmal des Produktes ist, gegen derartige Eingriffe gesichert zu sein. Nur in diesen Fällen, in denen der Schutz gegen Sicherheitslücken der berechtigten Sicherheitserwartung der Produktnutzer entspricht, und in denen der Hersteller zudem die Sicherheitslücke nach dem Stand von Wissenschaft und Technik hätte voraussehen müssen, kann er selbst in die Verantwortung genommen werden.[294] Hinsichtlich der Allgegenwärtigkeit von nicht zielgerichtet gesteuer-

[293] Vgl. *Spindler*, MMR 2008, 7 (12).

[294] Insofern zu pauschal *Droste*, CCZ 2015, 105 (107); vgl. *Spindler*, NJW 2004, 3145 (3146); grundlegend zur Haftung für die Wirkungslosigkeit von Sicherungsmitteln siehe BGH Urt. v. 17.03.1981 – VI ZR 191/79, BGHZ 80, 186 – Derosal und Urt. v. 17.03.1981 – VI ZR 286/78, BGHZ 80, 199 – Benomyl sowie aus der

ten Computerviren, -würmern und Trojanern ist daher eine intensive Beobachtung der Software unerlässlich.[295]

Eine Legaldefinition des Begriffs IT-Sicherheit findet sich in § 2 Abs. 2 BSIG. Demnach bedeutet Sicherheit in der Informationstechnik die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen. Für die erforderliche Sabotagefestigkeit – also Resilienz – von Produkten sind vor allem die Verfügbarkeit und Unversehrtheit der Systeme von Bedeutung.[296] Die Anforderungen daran wachsen mit der Bedeutung des Systems für Wirtschaft und Versorgung.

Da in einer Industrie 4.0 nach wie vor Produkte hergestellt werden, muss ein Angriff im Produktionsprozess nicht nur diesen beeinträchtigen, sondern er kann sich zum Beispiel auch erst im gefertigten Produkt als Produktmangel offenbaren. Die sichere Bedienbarkeit und Funktionsweise von Big-Data-Anwendungen gehört zudem zu den berechtigten Verbrauchererwartungen. Derartige Anwendungen müssen daher eine genügende Absicherung vor Cyber-Schädigungen durch Dritte enthalten, wenn und soweit durch derartige Eingriffe produkthaftungsrechtlich relevante Schädigungen (z. B. anderer Verkehrsteilnehmer) hervorgerufen werden können.[297] Die Risiken reichen hier von der Ausspähung der Nutzerdaten bis hin zur Produkterpressung.[298] Die IT-Sicherheit und die Produktsicherheit sind daher zu einem gemeinsamen Schutzkonzept zu entwickeln.[299]

3. Risikoverteilung/Zurechnung

Kernpunkt der Haftungsproblematik ist die haftungsrechtliche Risikoverteilung und Zurechnung, d. h. die Frage, wem welche Gefahrabwendungspflichten abverlangt werden und wem verbleibende Restrisiken zugewiesen werden.

a) Abgrenzung von Verantwortungsbereichen in der Produktions- und Lieferkette (z.B. in der Produktionskette Zulieferer, Hersteller, Dienstleister, Endnutzer) im Zusammenhang mit neuen Technologien

In der Produktions- und Lieferkette werden sich bei digitaler Vernetzung einzelne Bearbeitungsschritte oftmals nicht mehr eindeutig voneinander abgrenzen lassen. Durch die Technik des 3D-Drucks lassen sich sogar schon jetzt Produktionsschritte bis zum Endnutzer hin

---

„analogen“ Welt Urt. v. 19.12.1989 – VI ZR 182/89, NJW 1990, 1236 (1237) zur Pflicht des Eigentümers und Vermieters eines Mehrfamilienhauses, Abdeckroste eines Lichtschachtes gegen unbefugtes Abheben zu sichern, wenn der Schacht sich über die volle Breite des Hauseingangs erstreckt.

295 Ebenso *Droste*, CCZ 2015, 105 (108); *Spindler*, NJW 2004, 3145 (3147).

296 *Bräutigam/Klindt*, NJW 2015, 1137 (1241).

297 *Hartmann*, DAR 2015, 122 (123).

298 Siehe den Verweis auf die Dissertation von *Moseschus* bei *Bräutigam/Klindt*, NJW 2015, 1137 (1142).

299 Vgl. auch *Bräutigam/Klindt*, NJW 2015, 1137 (1240).

verlagern. Die softwaregesteuerte Koordinierung bildet hier dann das verbindende Element, aus dem ersichtlich wird, dass neben der reinen Produktverantwortlichkeit auch eine übergeordnete Steuerungsverantwortlichkeit desjenigen, der die Verantwortung für die Implementierung der Steuerungslogik trägt, bei neuen Technologien mehr und mehr zum Tragen kommt.

Daneben lässt sich auch der Grundgedanke des § 278 BGB fruchtbar machen: Wenn man Vorteile der menschlichen Arbeitsteilung zum Anlass nehmen kann, einer Person das Risiko dieser Arbeitsteilung zuzuordnen, so lassen sich die Vorteile der technischen Arbeitsteilung ebenfalls zuweisen.[300] Eine solche Haftungszuweisung ohne Exkulpationsmöglichkeit liefe allerdings auf eine Gefährdungshaftung hinaus, die zum einen gesetzlicher Verankerung bedürfte und für die zum anderen in solcher Allgemeinheit kein Bedürfnis besteht, da sich auch auf der Grundlage verschuldensbasierter Haftung mit Beweiserleichterungen bzw. Beweislastumkehr für den Geschädigten eine adäquate Risikoverteilung erreichen lässt,[301] was nicht bedeutet, dass in einzelnen Bereichen eine gesetzliche Zuordnung erforderlich scheinen kann.[302] Insoweit ist noch vieles im Fluss.

b) Abgrenzung von Verursachungs- und Verantwortungsbereichen zwischen Hersteller und Benutzer der innovativen Technologie, z. B. bei autonomem Fahren, Big Data Analysen, Smart Watch

Einerseits erwartet der Mensch von der Maschine Perfektion – andererseits muss er aus dem täglichen Umgang wissen, dass diese Erwartungshaltung kaum begründet ist.[303] Es bleibt daher vom Grundsatz her dabei, dass die eigene Vorsicht ein wesentlicher Teil von Schadensprävention ist. Dieser Ansatz kann aber dann nicht verfangen, wenn es gerade darum geht, dass Maschinen autonom handeln, eigenständig Ergebnisse liefern, die der Mensch nachzuvollziehen überhaupt nicht in der Lage ist, oder wenn sie den Menschen selbst auf Gefahren hinweisen sollen, die er selbst nicht erkennen kann.

Es geht um eine immer tiefere Integration der Automaten und Roboter in unsere Gesellschaft. „Big Data“ steht sinnbildlich für die Vernetzung scheinbar ungeordneter, heterogener Datenmengen über alle Ebenen hinweg. Eine sinnvolle Abgrenzung von Verantwortungsbereichen kann daher nicht mehr allein darüber erfolgen, wem eine Schadensprävention und -abwehr möglich war, sondern muss auf einer Risiko-Nutzen-Abwägung basieren, die dem Produkthaftungsrecht bereits jetzt nicht fremd ist: ein Produkt darf auch mit Restrisiken in Verkehr gebracht werden, wenn der zu erwartende Nutzen diese Risiken überwiegt. In diesem Moment wird die Risikotragung dem Benutzer und auch ggf. dem „inno-

[300] Vgl. *Hanisch* in Hilgendorf, Robotik im Kontext von Recht und Moral, S. 27 (39).

[301] Vgl. dazu auch *Hanisch* a. a. O., S. 40 in kritischer Betrachtung des Vorschlags der Tilburg Group für eine Unternehmenshaftung im Hinblick auf Automation in Art. 4:202 ihrer „Grundsätze eines Europäischen Deliktsrechts“ (siehe www.egtl.org).

[302] Kritisch zur von *Medicus*, Schuldrecht I, 20. Aufl. 2004 Rn. 339 vorgeschlagenen Beweislastlösung *Hanisch* a. a. O., S. 46.

[303] *Hanisch* a. a. O., S. 58.

cent bystander“ überbürdet. Geklärt werden muss dabei letztlich die Verteilung der sicherheitsnotwendigen Anforderungen auf bestimmte Risikosphären, nämlich auf diejenigen, die die Risiken am effizientesten beherrschen können („cheapest cost avoider“).[304]

c) Haftungsrechtliche Verantwortung bei Weiterentwicklung des Produktes nach Inverkehrbringen, insbesondere bei maschinellem Lernen

Das Verschuldensprinzip basiert auf dem Konzept der Willensfreiheit. Für durch Software eigenständig nach einem bestimmen Algorithmus ermittelte und ausgeführte Handlungen, scheidet dieses von vornherein aus.[305]

Es kann bei maschinellem Lernen bzw. bei maschinell induzierten Handlungen daher zu überlegen sein, ob man das Zurechnungsmodell übertragen kann und dabei gleichwohl den Bezug zum Menschen behält.

Bedeutsam ist dabei, dass selbst beim sog. „maschinellen Lernen“ der Roboter eine „deterministische Maschine“ bleibt – es besteht eine Vorfestlegung des Verhaltens, auch wenn diese nicht bedeuten muss, dass das maschinelle Verhalten im Sinne einer sicheren Vorhersage prognostizierbar ist.[306] Eine Zurechenbarkeit liegt dann streng genommen nur beim früheren Programmierer vor, der aber die Entscheidungsalternativen überhaupt nicht in jeder Einzelheit durchdenken konnte.[307] Jedoch müssen auch konstruktionsseitig Vorbereitungen getroffen werden, um systemimmanente Sicherheitsrisiken im Rahmen des objektiv Gebotenen und Zumutbaren zu vermeiden.[308] Im dennoch erfolgenden Schadensfall liegt dann zwar durchaus ein „Fehlverhalten“ nicht aber per se ein „Konstruktionsfehler“ vor.

Letztlich lässt sich dies nur über die Definition von Risikosphären lösen. Hinter der Maschine steht eine menschliche Einheit von Entwickler, Hersteller, Betreiber etc.. Es erscheint angemessen, dieser Einheit als „Geflecht von Mitverursachern“ das Risiko des Fehlverhaltens in Form der Garantenhaftung zuzurechnen.[309] Ob hierfür das Konzept der Gesamtschuld ausreicht oder eine etwas abgeänderte Konstruktion sinnvoll ist,[310] bedarf einer eingehenderen Betrachtung. Die Entwicklung spezieller Haftungsregelungen durch den Gesetzgeber erscheint insoweit aus Gründen der Rechtssicherheit wünschenswert. Dabei wird in den Blick zu nehmen sein, wie groß das Interesse der Allgemeinheit an der Entwicklung und dem Einsatz der digitalen Technik ist und wie weit dieser Nutzen auch wirtschaftlich streut oder zu besonderem unternehmerischem Gewinn der hinter der Maschine stehenden Personen führt.[311]

---

[304] *Spindler,* MMR 2008, 7 (8).
[305] S. dazu auch *Hanisch* a. a. O., S. 29.
[306] *Schuhr* in Hilgendorf: Robotik im Kontext von Recht und Moral, S. 13 (17).
[307] Kritisch daher auch *Hanisch* a. a. O., S. 34.
[308] *Hartmann,* DAR 2015, 122 (123); *Geissl*, BB-Sonderausgabe/RWW 2013, 20 (25).
[309] *Schuhr* a. a. O., S. 21; für einen Haftungsverbund auch *Hanisch* a. a. O., S. 57.
[310] Dafür *Schuhr* a. a. O., S. 22.
[311] *Schuhr* a. a. O., S. 24.

d) Verschuldenshaftung oder Gefährdungshaftung – Eignung des Verschuldensprinzips in der deutschen deliktsrechtlichen Produzentenhaftung für neue Risiken der digitalisierten Wirtschaft, auch im internationalen Vergleich

Als weitgehendes ausländisches Beispiel kann Frankreich herangezogen werden, wo die deklaratorische Zurechnungsnorm des Art. 1384 Abs. 1 Code Civil[312] durch die Rechtsprechung in eine Gefährdungshaftung für Sachen umgewandelt worden ist, wonach allein entscheidend die Verantwortung für eine Sache und eine aktive Rolle des Systems ist anstatt dessen Gefährlichkeit („Gardien-Haftung").[313]

Dies stellt eine sehr weitgehende Gefährdungshaftung dar, die im deutschen Recht nicht durch bloße richterliche Rechtsfortbildung erreicht werden könnte und zudem einen Fremdkörper darstellen würde.[314] Bei einer Zurechnung wie im vorstehenden Abschnitt dargelegt bleibt es jedem Einzelnen unbenommen, in der Haftungseinheit darzulegen, dass ihm die Erfüllung der Anforderungen tatsächlich unmöglich war. Ansonsten werden ein zurechenbares Verhalten und entsprechend auch zumindest die Fahrlässigkeit des Verstoßes vermutet und dem Geschädigten wird erspart, sich mit den technischen Zusammenhängen und den Verhältnissen der hinter der Maschine stehenden Personen untereinander auseinanderzusetzen.[315] Allein in dem Falle, dass diese Exkulpation umfassend gelingt, wird es nach dem Konzept des deutschen Haftungsrechts als angemessen erachtet, das Risiko dem Geschädigten zu überbürden. Für eine grundsätzliche Einführung einer strikten Gefährdungshaftung besteht demnach weder Anlass noch Bedürfnis.[316]

Einen Ausnahmefall mag man annehmen, wenn durch den Betrieb einer intelligenten Fabrik ein Personenschaden ohne jedweden aufklärbaren Verursachungspfad entsteht. Für diesen (technologisch zukünftigen) Ausnahmefall ist an eine Erweiterung des § 3 HaftPflG zu einer Betreiberhaftung für automatisierte Betriebsmittel zu denken.

4. Spezielle Herausforderungen durch „Smart Products" (Wearable computing/intelligent fashion) – neue Produktrisiken durch neue Funktionen, insbesondere bei Erfassung und Auswertung von Körperfunktionen

Zunehmend bietet die Kombination mobiler Endgeräte mit entsprechenden Software-Entwicklungen, hauptsächlich Apps, dem einzelnen Nutzer verschiedenste Möglichkeiten, bestimmte Körperparameter zu erfassen und auszuwerten. Dazu zählt z. B. die Erfassung von am Tag getätigten Schritten, Pulsmessung oder auch die Erfassung von Ernährungsgewohnheiten. Neben Fragen der Produktregulierung stellen sich hierdurch auch neue pro-

---

[312] „Man ist nicht allein für den durch seine eigene Handlung, sondern auch für den durch andere, für welche man einstehen muss, oder durch Sachen, die man in seiner Verwahrung hat, verursachten Schaden verantwortlich."

[313] Siehe näher dazu bei *Hanisch* a. a. O., S. 36.

[314] Ähnlich *Gruber* in Hilgendorf/Günther: Robotik und Gesetzgebung, S. 123 (147).

[315] *Schuhr* a. a. O., S. 21.

[316] Kritisch zu einer umfassenden Gefährdungshaftung auch *Hanisch* a. a. O., S. 36, 55; tendenziell anders *Spindler* ebd., S. 63 (80).

dukthaftungsrechtliche Herausforderungen, die auf ihre Lösbarkeit mit der existierenden Rechtsprechung zum Produkthaftungsrecht überprüft werden müssen. Neue Produktrisiken können sich vor allem ergeben, wenn der Benutzer aufgrund der Erfassung und Auswertung der Daten Entscheidungen trifft oder sich auf von dem Produkt vorgegebene Handlungsempfehlungen verlässt, die dann zu Schadensfällen führen. Da hierbei im Moment vor allem Produkte und Funktionen im Bereich Lifestyle und Gesundheit im Vormarsch sind, werden diese Fragen in Teil 17 ausführlicher behandelt.

a) Automatisierte Haushaltsgeräte und Fernauslösung von automatisierten Vorgängen im Haushalt

Technische Fehler sind heute in der Softwareentwicklung ein gängiges Problem, welches sich in der regelmäßigen Veröffentlichung von Beta-Programmversionen widerspiegelt. Sollen Menschen jedoch mit intelligenten Objekten und sogar Umgebungen interagieren und sich auf diese verlassen, darf sich eine solche „Beta-Mentalität“ nicht fortpflanzen.[317] Extensiven Testphasen und Qualitätsstandards kommt in diesem Bereich daher besondere Bedeutung zu.

Ferner ist zu berücksichtigen, dass Technik ihre Grenzen hat; Algorithmen eben doch nicht immer die richtige Entscheidungsgrundlage liefern oder die Entscheidungsvorlagen von Menschen falsch interpretiert werden.

Auch die Funktionslosigkeit eines „Smart-Home“-Produktes kann kritisch werden, wenn es der Überwachung des Hauses oder von alleinlebenden Senioren dient. Zusätzliche Gefahren können insoweit auch daraus resultieren, dass die erforderliche Netzverfügbarkeit nicht gewährleistet ist und entweder Gefahrenmeldungen den Nutzer nicht erreichen oder aber relevante Steuerimpulse nicht versendet werden können.

b) Die App als Produkt

Sog. „mobileHealth“-Dienste bergen besondere Fehlerquellen, die auf fehlerhaften Algorithmen, unzulänglichen Parametern oder defekten Endgeräten beruhen können. Beispielhaft ist eine App, die versprach, das Hautkrebsrisiko privater Nutzer durch eine Bilderkennungssoftware zu ermitteln und fälschlicherweise 30 % der gefährlichen Melanome als harmlos qualifizierte.[318] Bekannt ist auch der Rückruf einer App, die hinsichtlich der Aktivität verschiedener Entzündungskrankheiten unrichtige Werte errechnete.[319] Eingehender zu gesundheitsbezogenen Fragestellungen siehe in Teil 17.

---

[317] Vgl. *TAUCIS* – Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung Studie im Auftrag des Bundesministeriums für Bildung und Forschung, 2006, S. 166.

[318] Beispiel bei *Rübsamen*, MedR 2015, 485 (489).

[319] Sicherheitshinweis des BfArM für die iPhone/Android-Applikation „Pfizer Rheumatology Calculator“ vom 2.11.2011, Referenznummer 4757/11.

Eine weitere besondere Herausforderung ergibt sich aus der Nutzung von Apps und anderen Softwareergänzungen bei Autos. Dies können Funktionen zur Navigation des Autos aber auch bloße Unterhaltungsprogramme wie Mediatheken von Fernsehsendern oder Apps von sozialen Netzwerken sein. Die Apps werden in aller Regel von Drittanbietern bereitgestellt. Probleme und Sicherheitslücken bei Software können hier weitreichende Folgen haben, wenn das Fahrsicherheitssystem von den Zusatzfunktionalitäten nicht unabhängig ist und einzelne Apps oder die Kombination aus Apps zu einem Absturz des Systems führt.[320]

5. Auswirkung von Product-Lifecycle-Management-Lösungen auf die Produkthaftung

Das Produktlebenszyklusmanagement (PLM) ist ein Konzept zur nahtlosen Integration sämtlicher Informationen, die im Verlauf des Lebenszyklus eines Produktes anfallen. Das Konzept beruht auf abgestimmten Methoden, Prozessen und Organisationsstrukturen und bedient sich üblicherweise IT-Systemen für die Aufzeichnung und Verwaltung der Daten.

Der Einsatz von RFID-gestütztem PLM kann helfen, Millionenschäden abzuwenden.[321] Dabei halten die beteiligten IT-Systeme die relevanten Produktdaten wie Einzelteile oder Chargen fest. Anhand der auf dem Tag gespeicherten Informationen ist jedes einzelne Produkt oder jede Charge eindeutig nachvollziehbar.

PLM-Lösungen ermöglichen daher erst, die zunehmenden Anforderungen an die Produktbeobachtungspflichten sinnvoll zu erfüllen und stellen ein wesentliches Instrument der Haftungssteuerung und -begrenzung dar.

6. Die Nichtspeicherung von Funktionsdaten als Produkthaftungsfall

Bei digitalen Funktionsdaten ist zu unterscheiden zwischen Diagnosedaten – sie dienen ausschließlich der Wartung und Weiterentwicklung –, punktuellen Daten – diese werden ereignisbedingt in den Steuergeräten gespeichert und ihnen wird im Rahmen der Produktbeobachtung, wie dargelegt, eine besondere Bedeutung zukommen.

Daneben kommt die Speicherung von Unfalldaten in Betracht, die der umfassenden Rekonstruktion eines Unfallgeschehens dienen. Werden hierfür trotz entsprechender „Black Box“ nicht genügend Daten gespeichert, kann sich durchaus die Frage stellen, wie ein Hersteller haften soll, wenn sein Automat die entsprechenden Funktionsdaten nicht gespeichert hat und damit ein Entlastungsbeweis nicht nur für den Hersteller selbst, sondern auch für den Betreiber/Nutzer – z. B. beim autonomen Fahren – selbst nicht möglich ist und er deshalb einen Haftungsschaden hat.[322] Da es insoweit an einer Verletzung eines absolut ge-

[320] *Droste*, CCZ 2015, 105 (109).
[321] Vgl. *Erkayhan*, RFID-to-PLM, 2008, S. 8.
[322] Vgl. *Salje* in Vieweg/Gerhäuser: Digitale Daten in Geräten und Systemen, S. 221 (232).

schützten Rechts mangelt, steht dafür aber *de lege lata* keine Haftungsgrundlage zur Verfügung.[323]

Nichts desto weniger ist aber nicht nur für Automobilhersteller der cher“ ein wichtiges Thema, welches allen datenschutzrechtlichen Bedenken zum Trotz auf längere Sicht nur an Relevanz gewinnen kann.[324]

III. Versicherungen

Ein wichtiger Bestandteil eines wirksamen Risikomanagements ist die angemessene Absicherung aus der Unternehmenstätigkeit resultierender Risiken durch Versicherungsschutz. Die zunehmende Digitalisierung und die Vernetzung aller an der Wertschöpfung beteiligten Instanzen führen für die versicherungsnehmende Industrie zu einer Veränderung bestehender und zum Entstehen neuer Risiken, denen neben präventiven Maßnahmen, beispielsweise auf dem Gebiet der IT-Sicherheit, auch durch die Anpassung des durch die Unternehmen unterhaltenen Versicherungsschutzes zu begegnen ist. Insoweit stellen sich in erster Linie Herausforderungen bei der (Fort-)Entwicklung bestehender und neuer Versicherungslösungen, die auf privatautonomer Ebene durch die Unternehmen und die Versicherungswirtschaft erfolgen kann. Hingegen ist kein grundlegender Reformbedarf auf legislativer Ebene zu erkennen.

1. Versicherungsbedarf infolge veränderter Risikosituation

Der Versicherungsbedarf der Unternehmen erfordert aufgrund einer veränderten Risikosituation der Industrie 4.0 neue Lösungen. Dies betrifft vor allem zwei Felder: Wie vorstehend aufgezeigt, ergeben sich aus der Digitalisierung und Vernetzung der Wirtschaft zunächst neue und geänderte Produkthaftungsrisiken. Darüber hinaus entstehen aus der Vernetzung der Produktionsanlagen neue sog. Cyber-Risiken, die ein immenses Bedrohungspotential für die Unternehmen darstellen können. Diese Cyber-Risiken reichen von Datenverlusten und Datenschutzverletzungen über Industriespionage und Erpressung bis hin zu Betriebsunterbrechungen. Sie resultieren aus unterschiedlichen sog. Cyber-Angriffen, wie beispielsweise Schadprogrammen, Botnetzen, Denial-of-Service-Angriffen, Advanced Persistent Threats, durch unterschiedliche Angreifer, wie Cyber-Kriminelle, Nachrichtendienste, sog. Hacktivisten, aber auch Innentäter.[325] Zahlreiche Schadensfälle weltweit haben das erhebliche Schadenpotential für die Industrie aufgezeigt. Als bekannte Cyber-Angriffe sind etwa der gezielte Angriff auf Produktionsanlagen- und -netze deutscher Unternehmen durch die sog. Dragonfly-Gruppe im Jahr 2014[326] oder der Hackerangriff gegen Sony, der zu

---

[323] Vgl. *Salje* a. a. O., S. 233.

[324] Vgl. zum Unfalldatenspeicher bereits *Schmidt-Cotta*, ZRP 2000, 518 und *Brenner/Schmidt-Cotta*, SVR 2008, 41 sowie *Weber* in Vieweg/Gerhäuser: Digitale Daten in Geräten und Systemen, S. 83.

[325] Vgl. zur Gefährdungslage ausführlich: Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2014, S. 10 ff. (https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html).

[326] Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2014, S. 32 (https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html).

einem Schaden von bis zu 500 Mio. US-Dollar geführt haben soll,[327] zu nennen. Zudem belegen zahlreiche Studien die Aktualität und Dimension von Cyber-Risiken. So zeigt beispielsweise eine Studie des Bitkom e.V., dass im Durchschnitt jedes zweite Unternehmen in den vergangen zwei Jahren durch Datendiebstahl, Spionage oder Sabotage betroffen war, dies nahezu alle Branchen, insbesondere Automobilbau, Chemie und Pharma sowie Finanzdienstleister, betrifft und sich die verursachten Schäden auf rund 51 Mrd. Euro im Jahr belaufen sollen.[328] Laut Allianz Risk Barometer 2015 zählen Unternehmen in Deutschland und weltweit Risiken aufgrund von Betriebs- und Lieferkettenunterbrechung, insbesondere infolge von Cyber-Angriffen, sowie Risiken aufgrund von Cyberkriminalität, IT-Ausfällen, Spionage und Datenmissbrauch mittlerweile zu den größten Geschäftsrisiken.[329]

2. Innovationsbedarf durch angepasste und neue Versicherungsprodukte

Der veränderten Risikosituation der Unternehmen ist in erster Linie durch die Anpassung bestehender und die Entwicklung neuer Versicherungslösungen Rechnung zu tragen. Im Vordergrund dürften insoweit die Produkthaftpflichtversicherung sowie die zunehmend auch in Deutschland angebotenen sog. Cyber-Versicherungen stehen.

Produktübergreifend ist zu prognostizieren, dass die passgenaue Absicherung durch Versicherungsschutz vermehrt individualisierte Lösungen erfordern wird. Dies betrifft nicht nur die Bedingungs-, sondern auch die Prämienseite. Aktuell diskutiert werden beispielsweise individuelle Tarifmodelle in der Kfz-Haftpflichtversicherung auf der Grundlage sog. Telematik-Tarife, bei denen der Versicherer von der Fahrzeugelektronik erhobene Daten, beispielsweise zur Fahrweise, auswertet und abhängig von der Risikobewertung des Verhaltens des Versicherungsnehmers die Versicherungsprämien festsetzt. Denkbar ist, dass solche Modelle auch auf andere Versicherungssparten ausgeweitet und/oder Daten nicht nur zur Tarifierung, sondern auch für andere Zwecke, etwa der Prüfung von Schadensfällen, genutzt werden. In rechtlicher Hinsicht stellen sich dabei zahlreiche Fragen zur versicherungsrechtlichen wie auch datenschutzrechtlichen Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung, die bislang weitgehend ungeklärt sind.[330]

a) Produkthaftpflichtversicherung

Im Zuge der Digitalisierung und Vernetzung der Wertschöpfungsketten dürfte ein risikoadäquater Versicherungsschutz durch Produkthaftpflichtversicherungen für die Unternehmen noch wichtiger werden. Zwei Themenfelder sind hervorzuheben: einerseits die Überprüfung und gegebenenfalls Anpassung der bislang unterhaltenen Produkthaftpflichtversi-

---

[327] Handelsblatt vom 20.12.2014 (http://www.handelsblatt.com/politik/international/nordkorea-hacker angriff-kostet-sony-bis-zu-500-millionen-dollar/11147738.html).

[328] Pressemitteilung des Bitkom e.V. vom 16.04.2015 (https://www.bitkom.org/Presse/Presseinformation/Pressemitteilung_5253.html).

[329] Appendix zum Allianz Risk Barometer 2015, S. 5 (http://www.agcs.allianz.com/insights/white-papers-and-case-studies/risk-barometer-2015/).

[330] Vgl. *Kienast/Kühnl*, NJW 2014, 3057; *Klimke*, r+s 2015, 217.

cherungen an die veränderte Risikosituation und andererseits die Absicherung neuer Produkthaftpflichtrisiken.

Durch die Vernetzung bislang vertikal getrennter Wertschöpfungsprozesse in der Produktions- und Lieferkette können sich neue und veränderte haftungsrechtliche Verantwortlichkeiten ergeben. Dies kann zur Folge haben, dass beispielsweise bislang reine Zulieferer zukünftig stärker in die Konstruktions- oder Fabrikationsverantwortung eingebunden werden und sie neue Produktbeobachtungspflichten treffen, so dass sie in deutlich höherem Maße als bislang Haftpflichtrisiken für das mit weiteren Herstellern gemeinsam geschaffene Produkt ausgesetzt sind. Vor diesem Hintergrund ist zu prüfen, inwieweit bislang vereinbarte Versicherungssummen ausreichend oder anzupassen sind, was in der Konsequenz zu einer höheren Prämienbelastung der versicherungsnehmenden Wirtschaft führen kann. Zugleich ist im Hinblick auf die typischerweise für die Produkthaftpflichtversicherung vereinbarten Versicherungsbedingungen zu hinterfragen, ob durch neue Produktionsabläufe Deckungslücken entstehen. Beispielhaft sei der vielfach vereinbarte Deckungsschluss der sog. Erprobungsklausel (vgl. Ziffer A3-8.26 der Musterbedingungen des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) (Stand: 25.08.2014) für die Allgemeinen Versicherungsbedingungen für die Betriebs- und Berufshaftpflichtversicherung (AVB BHV)) genannt. Danach sind Ansprüche aus Sachschäden und sich daraus ergebender Vermögensschäden durch Erzeugnisse, deren Verwendung oder Wirkung im Hinblick auf den konkreten Verwendungszweck nicht nach dem Stand der Technik oder in sonstiger Weise ausreichend erprobt sind, vom Versicherungsschutz ausgeschlossen. Dieser bereits in der gegenwärtigen Schadenpraxis für die versicherungsnehmende Industrie häufig kritische Ausschlusstatbestand kann im Zuge von durch Innovations- und Wettbewerbsdruck zukünftig noch verkürzter Produktlebenszyklen weitere Relevanz gewinnen.

Daneben können neue Produkthaftpflichtrisiken etwa durch „Smart Products“ entstehen, für die Versicherungslösungen gegebenenfalls noch zu entwickeln sind. Hervorzuheben sind in diesem Zusammenhang insbesondere die Anforderungen an neue Versicherungslösungen, die sich aus der Einführung autonomer Kraftfahrzeuge ergeben werden.[331] Denkbar erscheint, dass die Haftung der Kfz-Hersteller neben der etablierten Halter- und Fahrerhaftung gemäß §§ 7, 18 StVG zukünftig eine größere Rolle spielen wird. Abhängig von der Ausgestaltung des Haftungsrechts sind zugleich neue Versicherungslösungen zu entwickeln. Diskutiert werden etwa eine Beteiligung der Kfz-Hersteller an den Versicherungsprämien der Kfz-Haftpflichtversicherung im Gegenzug für eine partielle Haftungsbefreiung bis zu einer Produkthaftung der Kfz-Hersteller unabhängig vom Vorliegen eines Produktfehlers,[332] die auf Versicherungsseite die Entwicklung neuer Produkthaftpflicht-Versicherungskonzepte und einen erheblich gesteigerten Versicherungsbedarf nach sich ziehen dürfte.

[331] Vgl. *Schubert*, PHi 2015, 46.
[332] *Schubert*, PHi 2015, 46, 49 ff.

b) Cyber-Versicherungen

Seit etwa vier Jahren haben sich ursprünglich in den angloamerikanischen Versicherungsmärkten entwickelte Cyber-Versicherungen auch in Deutschland etabliert. Mittlerweile bieten nach unserer Marktkenntnis geschätzt rund 20 Versicherer solche Deckungen mit Kapazitäten zwischen 5 und 50 Mio. Euro an, wobei die Gesamtmarktkapazität aktuell bei etwa 200 Mio. Euro liegen dürfte. Obwohl die Zahl der abgeschlossenen Versicherungen sich bislang nach unseren Marktinformationen im niedrigen dreistelligen Bereich befindet, soll seit dem Jahr 2014 nach Auskunft durch Versicherungsmakler ein erheblicher Anstieg des Interesses seitens der Industrie festzustellen sein.

Teilweise können Cyber-Risiken bereits durch bislang angebotene Versicherungen, wie Betriebshaftpflicht-, Sach- oder Vertrauensschadenversicherung abgedeckt werden. Die neuen Cyber-Versicherungen zeichnen sich demgegenüber durch eine weitgehende und spartenunabhängige Risikoabsicherung aus. Cyber-Versicherungen sind durch drei Deckungselemente gekennzeichnet: Haftpflichtversicherungsschutz, die Versicherung von Eigenschäden und von Assistance-Leistungen, etwa durch Kooperation mit IT-Dienstleistern, deren Beratungsleistung die Versicherungsnehmer in Anspruch nehmen können. Von besonderer Bedeutung dürfte die Möglichkeit der Versicherung von Eigenschäden der Versicherungsnehmer sein. Hervorzuheben ist insoweit vor allem die durch Cyber-Versicherung erstmals angebotene Deckung für Betriebsunterbrechungsschäden, die nicht durch einen vorausgehenden Sachschaden verursacht sind. Die bislang angebotenen Cyber-Versicherungen unterscheiden sich allerdings vielfach durch unterschiedliche Bedingungen und Terminologie, was einen Produktvergleich für die Versicherungsnehmer erschwert. Eine Orientierungshilfe sollen zukünftig Musterbedingungen, welche derzeit durch den Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) entwickelt werden, bieten.[333]

Wichtig wird bei der weiteren Produktentwicklung ein intensiver Dialog mit der versicherungsnehmenden Wirtschaft sein, um einen hinreichenden Versicherungsschutz zu gewährleisten. Besondere Herausforderungen werden sich bei der internationalen Risikoabdeckung durch internationale Versicherungsprogramme stellen, die außerhalb der Europäischen Union und dem Europäischen Wirtschaftsraum den jeweils nationalstaatlichen versicherungsaufsichtsrechtlichen Vorgaben entsprechen müssen.

Ein für die Unternehmen an Bedeutung zunehmendes, nach gegenwärtiger deutscher Rechtslage aber wohl nicht versicherbares Risiko betrifft Geldbußen, die gegen Unternehmen, beispielsweise bei Datenschutzverstößen, verhängt werden. So sieht etwa der Entwurf einer Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) in Art. 79a Geldbußen gegen Unternehmen von bis zu zwischen 0,5 und 2 Prozent des gesamten weltweit erzielten Jahresumsatzes vor.[334] Die Versi-

[333] GDV vom 17.06.2015 (http://www.gdv.de/2015/06/mehr-schutz-gegen-hacker/).
[334] Vermerk des Rats der Europäischen Union vom 15.06.2015, 9565/15.

cherung von Geldbußen soll nach im Schrifttum ganz überwiegend vertretener Auffassung jedoch generell sittenwidrig und folglich gemäß § 138 Abs. 1 BGB nichtig sein.[335] Diese Auffassung lässt sich hinterfragen. Denkbar erscheint beispielsweise, nach Schuldform – Vorsatz oder Fahrlässigkeit – oder angelehnt an versicherungsrechtliche Grundsätze der Repräsentantenhaftung[336] danach zu differenzieren, welche Personen im Unternehmen für das ordnungswidrige Handeln verantwortlich sind. Insoweit wäre aus Unternehmenssicht eine Fortentwicklung der Rechtslage durch die Rechtsprechung oder *de lege ferenda* eine gesetzliche Regelung zur partiellen Versicherbarkeit von Geldbußen wünschenswert.

3. Kein gesetzlicher Reformbedarf

Die Entwicklung passender Versicherungslösungen durch versicherungsnehmende Wirtschaft und Versicherer erscheint grundsätzlich geeignet, den Unternehmen den benötigten Versicherungsschutz zur Verfügung zu stellen. Vor diesem Hintergrund ist ein grundlegender gesetzlicher Reformbedarf derzeit nicht zu erkennen. Den rechtlichen Rahmen für den vertraglichen Versicherungsschutz bietet in erster Linie das Versicherungsvertragsgesetz. Dieses sieht zwar insbesondere für Cyber-Versicherungen keine speziellen Vorgaben vor, enthält aber mit den für alle Versicherungsverträge geltenden Vorschriften in Teil 1 Kapitel 1 sowie den besonderen Vorgaben für die Schadenversicherungen in Teil 1 Kapitel 2 Abschnitt 1 einerseits eine hinreichende gesetzliche Grundlage und lässt andererseits Raum für privatautonome, der neuen und sich weiter entwickelnden Risikosituation angepasste Lösungen.

Angesichts des enormen Schadenpotentials von Cyber-Risiken könnte allerdings daran gedacht werden, dass der Gesetzgeber Cyber-Risiken nicht nur, wie mit dem IT-Sicherheitsgesetz[337] zunächst für Betreiber sog. Kritischer Infrastrukturen zur Verbesserung der IT-Sicherheit erfolgt, mit gesetzlich vorgeschriebenen präventiven Maßnahmen begegnet, sondern darüber hinaus eine Versicherungspflicht zum Abschluss von Versicherungsverträgen festlegt, die bestimmte Cyber-Risiken absichern. Zu berücksichtigen ist jedoch, dass die Einführung einer Pflichtversicherung als Berufsausübungsregelung einen rechtfertigungsbedürftigen Eingriff in Art. 12 Abs. 1 GG bedeutete. Da Cyber-Risiken überwiegend wohl zu Eigenschäden der Unternehmen und, anders als etwa in der Kfz-Haftpflichtversicherung, nicht zu Schäden Dritter führen dürften, Cyber-Risiken zudem zunächst durch präventive Maßnahmen der IT-Sicherheit reduziert werden können und schließlich derzeit auch nicht zu erkennen ist, dass Industrie und Versicherer nicht zu hinreichenden vertraglichen Lösungen kommen, ist weder ein Bedürfnis für eine Pflichtversicherung zu erkennen noch erscheint ein damit verbundener Grundrechtseingriff als erforderlich und verhältnismäßig.

---

[335] *Dreher*, VersR 2015, 781 (792 f.); *Fleischer*, WM 2005, 909 (916); *Gädtke* in Bruck/Möller, VVG, 9. Aufl., Ziff. 5 AVB-AVG Rn. 115 f.; *Hauger/Palzer*, ZGR 2015, 33 (63); *Hölters*, AktG, 2. Aufl., § 93 Rn. 392.

[336] *Armbrüster* in Prölss/Martin, VVG, 29. Aufl., § 28 Rn. 98 ff.

[337] BGBl. I 2015, S. 1324.

IV. Richterliche Rechtsfortbildung als alleinige Lösung?

Das deutsche Recht hat sich unter der Geltung des BGB nun schon seit über 100 Jahren als flexibel genug erwiesen, Generalklauseln an aktuelle Entwicklungen des Wirtschaftslebens anzupassen. Aufbauend auf den deliktrechtlichen Grundprinzipien kann daher eine Abgrenzung von Risikosphären durchaus der Rechtsprechung überlassen werden. Problematisch stellt sich der immer stärkere Eingriff in deutsches Rechtsverständnis durch europäische Rechtssetzung dar, der es an einem durchgängigen Konzept mangelt und die im Hinblick auf die – wenig berechenbare und vor allem für das deutsche Recht wenig Verständnis aufbringende – Deutungshoheit des EuGH sich für richterliche Rechtsfortbildung in großen Zügen nicht als flexibel und konsistent genug erweist.

Die bislang bekannten Fälle lassen sich durch Rechtsfortbildung lösen. Mit weiterem Fortschreiten der Entwicklung automatisierter Vorgänge, wird allerdings kaum ein Weg an neuen gesetzlichen Regelungen bis hin zu einer speziellen „Roboterhaftung“ vorbeiführen.[338]

[338] In diesem Sinne auch *Hanisch* in Hilgendorf: Robotik im Kontext von Recht und Moral, S. 27 (54).

Teil 8 Standardisierung und Produktkonformität *(Prof. Dr. Thomas Klindt, Dr. Susanne Wende, LL.M., Dr. Steffen Burrer)*

I. Standardisierung

1. Status Quo der Standardisierung und technischen Normung für die digitale Wirtschaft in Deutschland, Europa und international

Die – im Folgenden als inhaltlich gleich verstandenen – Vorgänge von Standardisierung und technischer Normung bezeichnen die durch interessierte Kreise außerhalb der Legislative erfolgende Erarbeitung und Verabschiedung von Dokumenten über technisches Design, Prüfmethodiken und Dokumentationsanforderungen in einem vorher generell festgelegten Verfahren. Die so entstandenen technischen Normen/Standards unterliegen dem Urheberrecht der jeweiligen Standardisierungsgruppe als deren geistiges Eigentum. Sie werden (üblicherweise gegen Lizenz-Entgelt) öffentlich zugänglich gemacht, weil jeder Standardisierungserfolg naturgemäß von einer größtmöglichen Nutzung und Verbreitung innerhalb aller involvierten Wirtschaftskreise abhängt. De jure ist die Einhaltung technischer Normen/ Standards nicht zwingend, sondern ausschließlich freiwillig, soweit nicht ausnahmsweise ein Gesetzgeber durch (statische oder dynamische) Verweisungen auf Normenwerke privater Regelsetzer Bezug nimmt. Zudem können die Inhalte technischer Normen/Standards ganz oder teilweise in Verträgen bilateral in Bezug genommen werden; sie entfalten dann zwischen den Vertragsparteien rechtsgestaltende Wirkung.

Im Bereich der Produkt- und Produzentenhaftung nach § 823 BGB/§ 1 ProdHaftG entbindet die Einhaltung technischer Standards nicht vom rechtlich gebotenen Maß an Sicherheit (Maßstab ist der Stand von Wissenschaft und Technik),[339] wobei umgekehrt die Nichteinhaltung technischer Normen ein klärungsbedürftiger Indikator für ein Unterschreiten sicherheitstechnisch möglicher Lösungen sein kann.

Standardisierungen finden aufgrund der damit verbundenen wirtschaftsfördernden Wirkung heute üblicherweise kaum noch in rein nationalem Rahmen statt; nationale Normungsorganisationen wie der DIN oder VDE/DKE, DVGW etc. sind deshalb in ihrer Normungstätigkeit zunehmend auf die Mitarbeit in internationalen Normungsorganisationen fokussiert. Auf europäischer Ebene sind hier insbesondere CEN, CENELEC und ETSI zu nennen, auf übereuropäischer Ebene gibt es namentlich die Regelsetzer ISO und IEC. Industriepolitisch wird indes vorrangig zu beachten sein, ob sich außerhalb regulierter Normungsverfahren und durch schiere Anwendungsübermacht faktische „Quasi-Standards“ etwa in den USA oder in China durchsetzen, die dann nur noch nachgeahmt werden können.[340]

Technische Normen und Standards für die in dieser Begutachtung angesprochene Digitale Wirtschaft lassen sich strukturell in zwei Gruppen unterteilen:

---

[339] Dazu *Stöhr*, InTeR 2015, 35.

[340] Dazu etwa http://www.ingenieur.de/Panorama/Hannover-Messe/T-Systems-Chef-Clemens-USA-China-schaffen-Fakten-Industrie-40.

- Es gibt zum einen technische Normen für „klassische“ Industrielösungen, die – unverändert – auch in der Digitalen Wirtschaft eine Rolle spielen und insofern weiter benutzt werden, dann als Bestandteil einer digitalen Wirtschaftslösung. Hierzu gehört analog zu den Rechtsvorschriften über die Produktkonformität (dazu sogleich unter II.) namentlich das gesamte vorhandene europäische Normungswerk im Zusammenhang mit CE-Kennzeichnung, New Approach und der europarechtlichen Vermutungswirkung harmonisierter EN-Normen.

- Zum anderen mag es bereits erste Normungen geben, die dezidiert und ausschließlich solche Fragen standardisiert beantworten, die industriehistorisch erstmals im Zusammenhang mit Fertigungslösungen im Umfeld von Industrie 4.0, Internet of Things und der Digitalisierung der Wirtschaft auftauchen. Ihr Inhalt war vorher in „klassischer“ Industrietechnologie nicht notwendig; die Anzahl solcher spezifischen Digitalisierungs-Normen wird in den nächsten Jahren naturgemäß sprunghaft ansteigen.

Im Umgang mit beiden Produktnormengruppen gilt aus rechtlicher wie industriepolitischer Sicht folgendes: Für die schon vorhandenen (alten wie neuen) Normen gilt der etablierte Rechtsrahmen der Wirkung von Normen, namentlich im New Approach (dazu sogleich unter 2.). Hier werden also allenfalls neue Normungsinhalte einem unverändert vorhandenen, alten Regelungsprogramm unterlegt. Zudem wird sich die Aufgabe für die Normungsorganisationen wie auch für die Industriepolitik stellen, den vorhandenen Normungsbestand in toto zu sichten, auf detaillierten Novellierungsbedarf im Hinblick auf Digitalisierungsaspekte zu identifizieren und sodann in den entsprechenden Normungsorganisationen (ggf. sogar noch internationaler ausgerichtet) entsprechende Normungs- oder Normänderungsverfahren in Gang zu bringen. Erste Schritte einer solchen Sichtung erfolgen nach unserer Kenntnis auch über die vom BMV und BMFK gesteuerte Plattform Industrie 4.0, und zwar dort in der Arbeitsgruppe 3 (Technische Standardisierung).

Die nicht-juristische Standardisierungs-Diskussion ist im Übrigen in vollem Gang, vgl. z.B. die vom DKE vorgelegte die Standardisierungs-Roadmap.[341]

2. New Approach: Rechtliche Anreizmöglichkeiten für die Entwicklung und Einhaltung technischer Standards

Das in den 1980er Jahren entwickelte Konzept des New Approach[342] war und ist ein industriepolitisches Meisterwerk deregulierender Wirtschaftsliberalisierung. Grundlage des Konzepts ist eine Art Arbeitsteilung zwischen Recht und technischer Normung; über die Rechtsvorschriften werden dabei rahmenartig die von der Industrie einzuhaltenden Ziele vorgegeben, ohne dass indes die Mittel und Wege dahin gesetzlich geregelt würden. Diese verblei-

[341] https://www.dke.de/de/std/Industrie40/Seiten/RoadmapIndustrie40.aspx.

[342] Dazu umfangreich *Klindt/Schucht* in *Ehlers/Fehling/Pünder*, Besonderes Verwaltungsrecht, Bd. 1, 3. Aufl. 2012, § 36 Rn. 33ff.

ben vielmehr im technologischen Wettbewerb der Ideen und sind allesamt juristisch zulässig, solange keine Zielverfehlung festgestellt würde.

Um andererseits gerade für kleine und mittelständische Unternehmen etablierte Lösungswege anzubieten, wird – das ist die andere Seite der Arbeitsteilung – über die dafür gegründeten europäischen Normungsorganisationen ein Konvolut von Einzelnormen verfasst, deren Fundstellen im Amtsblatt der Europäischen Gemeinschaft veröffentlicht werden. Die einzelnen europäischen Richtlinien/Verordnungen enthalten dann Artikel, die jeweils mit der Einhaltung solcher publizierter harmonisierter EN-Normung zugleich die Vermutung rechtskonformer Lösungen aussprechen.[343] Aus der Normkonformität wird also beweisrechtlich die (vermutete) Rechtskonformität abgeleitet. Diese Vermutung ist zwar widerleglich, aber ohne eine solche Widerlegung für die Marktüberwachungsbehörden bindend.

Betriebswirtschaftlich erlaubt dies für einzelne Unternehmen, etablierte technische Lösungen nachzuahmen, ohne im EU-Export in der Sorge agieren zu müssen, mit den Zielen des EU-Rechts in Konflikt zu geraten. Volkswirtschaftlich werden über die so erreichte EU-weite Synchronisierung genormter Anforderungen eine echte Warenverkehrsfreiheit im EU-Binnenmarkt und damit zugleich andere Skalengrößen möglich, die margenattraktive Fertigungen erlauben. Der Erfolg[344] dieser Arbeitsteilung wird auch durch das *New Legislative Framework*[345] aufgezeigt, das zwar einzelne gesetzliche Nachjustierungen vorgenommen hat, das Gesamtkonzept aber dezidiert bestätigt hat.

Für zukünftig anstehende Normung im Bereich der Digitalisierung der Wirtschaft besteht nach über 30 Jahren Erfahrung mit diesem Normungskonzept keinerlei Anlass, den bewährten New Approach konzeptionell zu verändern: Soweit im Zusammenhang mit IEC- und/oder ISO-Normung übereuropäische Regelwerke geschaffen werden, gilt es, diese danach auch parallel zur harmonisierten EN-Normung umzugestalten. Das ist ein ebenfalls bekannter und bewährter operativer Vorgang.

3. Rechtsrahmen für CEN-/CENELEC- und ETSI-Normung

Die drei europäischen Normungsorganisationen CEN, CENELEC und ETSI fokussieren sich jeweils auf unterschiedliche Industriesektoren. Sie sind allesamt als Vereine nach belgischem Recht gegründet und von der EU mit entsprechenden Mandaten zur Erstellung harmonisierter Normung ausgestattet. Als private Regelsetzer unterliegen sie autonomem Satzungsrecht, wobei die entsprechenden internen Standardisierungsabläufe mit den online-Darstellungen von CEN (www.CEN.eu), CENELEC (www.CENELEC.eu) und ETSI (www.ETSI.org) publik sind.

---

[343] Dazu auch *Schucht*, NVwZ 2015, 852 (853).
[344] Zur industriepolitischen Bewertung als Erfolg jüngst *Klindt*, VDMA-Nachrichten 6/2015, 36.
[345] Weiterführend *Kapoor/Klindt* EuZW 2008, 649; dies. EuZW 2009, 134.

II. Produktkonformitätsrecht

1. Deutscher und Europäischer Rechtsrahmen des Produktkonformitätsrechts in Zusammenschau mit der Strategie für einen digitalen Binnenmarkt in Europa

Produktkonformität bezeichnet die Gesamtheit aller rechtlichen Anforderungen des EU-Rechts für ein zulässiges Inverkehrbringen von Waren aller Art innerhalb des EU-Binnenmarkts. Dieser Rechtsrahmen stützt sich zum einen primärrechtlich auf die Vorgaben des AEUV, dort namentlich Art. 34 AEUV ff. Zudem hat der europäische Gesetzgeber in den vergangenen Jahrzehnten über Sekundärrechtsakte sukzessive Branchen- und/oder Sektorenanforderungen EU-weit einheitlich geregelt. Die Einhaltung (Compliance) dieser EU-rechtlichen Vorschriften ermöglicht ein von nationalen Behörden nicht behinderbares Bereitstellen der Produkte auf dem europäischen Markt; umgekehrt ist die Nicht-Konformität (Non-Compliance) mit den produktrechtlichen Vorschriften für nationale Marktüberwachungsbehörden Grund und Berechtigung, mit warenvertriebsbeschränkenden Maßnahmen zu intervenieren.

Innerhalb des EU-Rechts hat sich dabei die Rechtssetzungstechnik in den letzten Jahren von der EU-Richtlinie hin zur EU-Verordnung verschoben, so dass sich derzeit „handwerklich“ ein gemischtes Bild zeigt. Maßgebliche EU-Rechtsvorschriften, die aufgrund ihres tatbestandlichen Regelungsgegenstands unverändert auch in einer zukünftigen immer mehr digitalisierten Wirtschaft zwingend zu beachten sein werden, sind vor allem:

- Maschinenrichtlinie 2006/42/EG
- Niederspannungsrichtlinie 2014/35/EU
- EMV-Richtlinie 2014/30/EU
- R&TT-Richtlinie 1999/5/EG[346]
- Bauprodukteverordnung (EU) 305/2011
- Druckgeräterichtlinien 2010/35/EU (bewegliche) und 2014/68/EU
- ATEX-Richtlinie 2014/34/EU
- Medizinprodukterichtlinien 93/42/EWG, 90/385/EWG und 98/79/EG
- sowie generell Marktüberwachungsverordnung Nr. 765/2008/EG

2. Werden die aktuellen Begriffe des „Herstellers“ und des „Inverkehrbringens“ den Herausforderungen der digitalisierten Wirtschaft gerecht?

Beide Begriffe sind maßgeblich unter Betrachtung der zentralen Vorschriften und den darin enthaltenen Legaldefinitionen zu verstehen. Hierzu zählen insbesondere die Marktüberwa-

[346] Jede nationale Umsetzung steht zur Ablösung an durch die neue RED-Richtlinie 2014/53/EG; dazu *Menz*, InTeR 2015, 82.

chungsverordnung Nr. 765/2008/EG sowie der selbstverpflichtende Beschluss Nr. 768/2008/EG.

Nach Anhang I des Beschlusses 768/2008/EG, dort Kapitel R1, Artikel R1 Nr. 2 ist unter „Inverkehrbringen“ die erstmalige Bereitstellung eines Produktes auf dem Gemeinschaftsmarkt gemeint; nach der dortigen Nr. 3 gilt als „Hersteller“ jede natürliche oder juristische Person, die ein Produkt herstellt bzw. entwickeln oder herstellen lässt und dieses Produkt unter ihrem eigenen Namen oder ihrer eigenen Marke vermarktet.

Beiden Begriffen[347] liegt ein historisch gewachsenes Verständnis gewissermaßen haptischer Warenwirtschaft, also der Übergabe körperlich vorhandener Gegenstände, zu Grunde. Das zeigt sich schon daran, dass der so zentrale Begriff des „Produkts“ trotz einer langen Liste von Legaldefinitionen keine eigene europarechtliche Beschreibung erfährt. Er wird offenbar als selbsterklärend wahrgenommen und vorausgesetzt; vgl. auch Art. 2 lit. a) der Richtlinie 2091/95/EG. Im nationalen deutschen Recht sind Produkte dagegen in § 2 Nr. 22 ProdSG als „Waren, Stoffe und Zubereitungen, die durch einen Fertigungsprozess hergestellt worden sind“ definiert.

Soweit Digitalisierung der Wirtschaft im hier verstandenen Sinne die für die Produktfertigung notwendigen Interaktionen, Fertigungsschritte und Dokumentation/Kommunikation in der OEM-Fabrikation wie der Zulieferkette meint, hat dies zwar gravierende Konsequenzen für Geschäftsmodelle und Geschäftsfelder. Solange indes „am Ende“ Produkte klassischen Zuschnitts entstehen, werden die Begriffe des Herstellers und des Inverkehrbringens unverändert notwendige Deskriptionen des zu überwachenden Binnenmarktesvorgangs darstellen. Soweit die Digitalisierung der Wirtschaft (im B2B- wie B2C-Business) dem Kunden dagegen reine Dienstleistungen jedweder Art anbieten wird, unterfallen diese weder jetzt noch zukünftig den klassischen Herstellervorschriften des EU-Rechts: Eine im EU-politischen Raum diskutierte Regelung von Dienstleistungssicherheit und Dienstleistungshaftung – analog zu Produktsicherheit und Produkthaftung – ist bisher nicht Wirklichkeit geworden.

Konzeptionell fraglich kann das bestehende Recht also nur dort werden, wo nichtkörperliche „Produkte“ Gegenstand des digitalisierten Business werden. Dies wirft die bisher allenfalls theoretisch diskutierte Frage auf, ob der Produktbegriff des europäischen Produktrechts auch Download-Software, Online-Dienste, Cloud-Speicherplatz oder ähnliches umfasst. Entgegen mancher, rudimentärer Äußerungen im rechtswissenschaftlichen Schrifttum wird man dies in Anbetracht der konzeptionellen abweichenden „Produkt“-Logik und -DNA wohl verneinen müssen, zumal auch die parallele, ebenfalls historisch entstandene Behördenlandschaft der Marktüberwachung durch Gewerbeaufsichtsämter für eine derartige sicherheitstechnische IT-Überwachung weder ausgestattet noch ausreichend vorbereitet wirkt. Sie nimmt diese Überwachung in der Realität ohnehin nicht wahr.

[347] Vgl. auch *Schucht*, EuZW 2014, 848 (850).

Die Forderung nach einem digitalen Produktsicherheitsrecht[348] hat diese Lücke bereits mit einem prägnanten Namen benannt, zumal Vorschriften wie etwa das BSI-Gesetz und die IT-Sicherheitsgesetzgebung nur erste, rudimentäre infrastrukturelle Maßnahmen umfassen.

Andererseits erscheint es rechtspolitisch deutlich verfrüht, die Forderung nach einem Regulator bereits aufzuwerfen: Es ist derzeit seriös nicht prognostizierbar, in welchen Bereichen aus Gründen etwa des Verbraucher- oder Arbeitnehmerschutzes notwendige legislative Handlungsfelder entstehen werden. Entsprechende Defizite und die gesetzgeberische Reaktion auf solche Defizite müssen einer zukünftigen Identifikation und gesellschaftspolitischen Diskussion vorbehalten bleiben. Auf EU-Ebene wird diese dann auch eine ggf. notwendige Anpassung der VO Nr. 765/2008 und des Beschlusses Nr. 768/2008 beinhalten.

3. Eignung des Konzepts der Vermutungswirkung des New Approach im Umfeld der digitalen Wirtschaft – Probleme der Normierbarkeit und der Auswahl der maßgeblichen (auch internationalen) Normen

Das Konzept des New Approach wird möglicherweise – das gilt dann für die gesetzliche wie für die standardisierte Seite gleichermaßen – an seine konzeptionellen Grenzen stoßen, wenn in fernerer Zukunft Digitalisierung der Wirtschaft auch autonome Entscheidungsprozesse innerhalb der Industriefertigung umfasst. Die unter den Stichworten selbstlernende Algorithmen, Supply-Chain-übergreifende Interaktion oder auch autarke Robotik diskutierte Entwicklungsstufe, dass die zugrundeliegenden Programmierungen darauf angelegt sind, das Handeln erfahrungsbasiert zu verändern/nachzujustieren, wird Konsequenzen zeigen; diese betreffen allerdings weniger den Output der Produktion, also das Gesamtprodukt oder den ihm zuzuordnenden Hersteller. Sehr wohl aber mag es sein, dass Fertigungsschritte mangels exakter Kenntnis des Herstellers wie in „black boxes“ wirken werden, was wiederum Schwierigkeiten bei einer seriösen und wahrheitsgetreuen EU-Konformitätserklärung zur Normeinhaltung bedeuten kann. Dies ist allerdings nach derzeitigem Kenntnisstand noch so ferne Zukunftsmusik, dass eine rechtliche Diskussion oder gar Anpassung zum derzeitigen Zeitpunkt nicht notwendig erscheint.

4. Erhöhte Anforderungen an den Hersteller durch neuen Funktionsumfang von Produkten als Hindernis für die neuen Techniken, z.B. Smart Watch, Smart Textiles, Intelligent Fashion als Medizinprodukte

Produktinnovationen und technische Produktweiterentwicklungen führen oftmals dazu, dass die bisher einschlägigen europäischen Produktvorschriften tatbestandlich verlassen werden, weil andere Regelungswerke und ihr Scope berührt werden. Parallel dazu finden dann auch andere, zu diesen CE-Vorschriften gelistete harmonisierte Normen erstmals Anwendung, die entsprechend in der Konformitätserklärung zu spiegeln sind. Diese mit technischen Veränderungen einhergehenden rechtlichen Veränderungen sind in der Industrie insbesondere aus der Elektrisierung ehemals mechanischer Bewegungen bekannt, wodurch

[348] *Schmidt-Kessel*, VuR 2015, 121.

z. B. Vorschriften des Niederspannungsrechts, der Maschinenrichtlinie und des EMV-Rechts (erstmals) aufgerufen wurden. So kann vor allem ein Aufrüsten bisher „toter“ Produkte um Funkelemente in die Einschlägigkeit der R&TTE-Richtlinie (demnächst RED-Richtlinie) führen. Die R&TTE-Befassung wird dabei sicherlich eine der ganz zentralen Veränderungen sein, auf die viele Herstellerbranchen – von Medizinprodukten über Bekleidungsartikel bis zu Persönlichen Schutzausrüstungen (PSA) – zulaufen. Aus industriepolitischer wie wirtschaftsrechtlicher Sicht ist dieser Vorgang allerdings nicht zu beanstanden; es wäre eine Wettbewerbsverzerrung, wenn diejenigen Unternehmen, die neu in ein Produktsegment eintreten, die dafür bereits geltenden Vorschriften nicht einhalten müssten, existente Konkurrenten aber schon. Wenn der mit den neuen Funktionalitäten verbundene erhöhte Aufwand (z.B. für Herstellung und/oder Prüfung) sich in einem entsprechenden Produktmehrwert widerspiegelt, wird er im Übrigen über einen erhöhten Nutzungspreis refinanzierbar sein.

Teil 9 IT-Sicherheit (*Stefan Wilmer*)

In der IT-Sicherheit liegt eines der Kernthemen der digitalisierten Wirtschaft. Denn die immer stärkere Vernetzung von Systemen und Produktionsanlagen, ebenso wie die voranschreitende Autonomisierung von Produktionsprozessen führen – ob gewollt oder nicht – zu einer signifikanten Erhöhung der Bedrohungslage im Cyberraum. Gleichzeitig erfolgen Cyberangriffe zunehmend zielgerichteter und mit technologisch ausgereifteren Mitteln, was die Bedrohungslage weiter erhöht. Durch die zunehmende Digitalisierung der Wirtschaft und damit einhergehend eine erhöhte Flut an sensiblen und aussagekräftigen Daten besteht in erhöhtem Maße die Gefahr, dass Daten für Cyber-Kriminelle noch attraktiver werden.[349] Wie groß diese Gefahren tatsächlich sind, zeigte erst jüngst der – erfolgreiche – Hackerangriff auf die IT-Systeme des Bundestags.[350]

I. IT-Sicherheit als determinierender Faktor der digitalisierten Wirtschaft

1. Begriff der IT-Sicherheit

Eine gesetzliche Definition des Begriffs „*IT-Sicherheit*“ findet sich in § 2 Abs. 2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Sicherheit in der Informationstechnik im Sinne des Gesetzes bedeutet danach

> *„die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen*
> *1. in informationstechnischen Systemen oder Komponenten oder*
> *2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.“*

Die IT-Sicherheit hat dabei letztlich zwei Aspekte, die nebeneinander stehen und gleichermaßen zu berücksichtigen sind: (1) den Schutz von Menschen und der Umgebung vor den Systemen[351] und (2) den Schutz von Anlagen und Produkten selbst vor unbefugtem Zugriff und Missbrauch von Know-how und sonstigen.[352]

Bei der Verwirklichung der IT-Sicherheit geht es dabei im Wesentlichen um die Umsetzung der vier international anerkannten Grundwerte der IT-Sicherheit: den Schutz der Verfügbarkeit, der Integrität, der Vertraulichkeit und Authentizität.[353] Daneben spielt vor allem auch die Qualitätsprüfung bzw. -bestätigung eine wichtige Rolle.[354] Während der Schutz der Verfügbarkeit zum Inhalt hat, dass die Funktionalität des IT-Systems gewährleistet und da-

---

[349] *Stanczyk*, VW 2014, 22; *Mühlich*, ZD 2014, 381 (382).

[350] http://www.spiegel.de/politik/deutschland/cyberangriff-auf-bundestag-abgeordneten-e-mails-erbeutet-a-1039388.html; abgerufen am 31.08.2015.

[351] Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 50; zur Produkthaftung und zum Produktmangel wegen mangelnder IT-Sicherheit im Produktionsprozess siehe unter Teil 7II.2, Produkthaftung.
Sind Schäden bereits entstanden, ist dies eine Frage der Versicherbarkeit, siehe unter Teil 7III., Produkthaftung „Versicherungen“.

[353] *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 4.

[354] *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 4.

mit der Zugang zu Daten sowie IT-Systemen sichergestellt ist, hat der Schutz der Integrität die Verhinderung inhaltlicher Manipulation von Informationen zum Gegenstand.[355] Vertraulichkeit ist gewährleistet, wenn der Zugang zu Daten nur den zum Zugriff Befugten offensteht[356] und Authentizität erfordert, dass Daten und Informationen aus der angegebenen Quelle stammen und die Identität von Nutzern und angeschlossenen Systemen korrekt ist.[357] Schließlich wird von der Qualitätsprüfung und -bestätigung verlangt, dass die sachgerechte Umsetzung von Sicherheitsmaßnahmen kontinuierlich überprüft wird.[358]

Darüber hinaus spielt auch die Betriebssicherheit eine wichtige Rolle.[359] Darunter wird die Abwesenheit der durch den Betrieb eines Systems hervortretenden unvertretbaren Risiken und Gefahren für Menschen und Umgebung verstanden.[360]

2. Bedeutung in der digitalisierten Wirtschaft

Der Aspekt der Betriebssicherheit spielt bereits seit geraumer Zeit bei der Errichtung und dem Betrieb produktionstechnischer Anlagen eine Rolle und ist bereits in einer Fülle von Normen und Standards adressiert.[361] Akuter und für den fortwährenden Ausbau der digitalen Wirtschaft wichtiger ist jedoch der Schutz von Systemen und Produktionsanlagen vor Eingriffen von außen. Dies umfasst den Schutz vor Schädigungen und Manipulationen ebenso wie Fragen des Schutzes von Daten und Informationen vor unbefugtem Zugriff und Missbrauch, also insbesondere die Gewähr von Integrität, Vertraulichkeit und Authentizität durch sicherheitstechnische Einrichtungen.[362] Studien zufolge entstehen der deutschen Wirtschaft derzeit allein durch Industriespionage jährlich Schäden in Höhe von 11,8 bis 51,0 Milliarden Euro[363], wobei über die Hälfte der befragten Unternehmen bereits von Industriespionage betroffen waren oder jedenfalls einen entsprechenden Verdacht hatten.[364] Neben materiellen, entstanden vor allem auch erhebliche immaterielle Schäden, wie zum Beispiel Ausfall oder Schädigung von IT- oder Telekommunikationsgeräten, Umsatzeinbußen wegen Verlusts von Wettbewerbsvorteilen, Imageschäden und Patentrechtsverletzungen.

Insgesamt ist zu konstatieren, dass die IT-Sicherheit eine der entscheidenden Faktoren für den Erfolg der digitalisierten Wirtschaft ist. So groß auch die Vorteile und Möglichkeiten

---

355 *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 4, 6 f.
356 *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 8.
357 *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 9.
358 *Holznagel*, Recht der IT-Sicherheit, § 2 Rn. 4.
359 Zur Produkthaftung wegen IT-Sicherheitsmängeln siehe unter Teil 7II.2, Produkthaftung.
360 Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 51.
361 Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 50.
362 Vgl. Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 50.
363 Vgl. Corporate Trust, Studie: Industriespionage 2014, S. 8 und https://www.bitkom.org/Presse/Presseinformation/Pressemitteilung_5253.html.
364 Zu den folgenden Ergebnissen siehe Corporate Trust, Studie: Industriespionage 2014, S. 8 f.; Zur Frage einer Versicherungspflicht für Cyber-Risiken siehe unter Teil 7III.3., Produkthaftung.

sind, die sich aus der digitalisierten Wirtschaft ergeben – so wichtig ist es doch auch die Gefahren und Risiken, die mit der fortschreitenden Vernetzung und Autonomisierung von Systemen und Produktionsanlagen einhergehen, zu kennen und entsprechende Vorkehrungen zu treffen. Neben fachlichen und tatsächlichen Aspekten hat das Thema auch eine bedeutende juristische Dimension, die Gegenstand dieses Gutachtens ist.

Gleichzeitig muss aber stets im Blick behalten werden, dass eine falsche Umsetzung IT-sicherheitstechnischer Maßnahmen den Ausbau der digitalisierten Industrie wesentlich behindern kann. Erforderlich sind hochgradig vernetzte Systemstrukturen bei Beteiligung einer Vielzahl von Menschen, Automatisierungskomponenten, Maschinen und IT-Systemen.[365] Gesetzgeberische Maßnahmen haben folgendes zu berücksichtigen: Es muss gewährleistet werden, dass Informationen zur richtigen Zeit verfügbar sind.[366] Bei der Planung von Produktionssystemen müssen daher Maßnahmen der IT-Sicherheit von vornherein Berücksichtigung finden und es sind Konzepte zu unterstützen, die ein hohes Maß an Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen.[367]

II. Rechtliche Rahmenbedingungen

Zunächst gilt es, den bestehenden und zukünftig absehbaren Rechtsrahmen zur IT-Sicherheit zu analysieren und zu bewerten. Vorschriften, welche die IT-Sicherheit betreffen, sind nach derzeitige Rechtslage nicht zusammenhängend geregelt, sie finden sich vielmehr verstreut in diversen Gesetzen.

Bestimmte Industriesektoren werden von dem Gesetzgeber als besonders systemrelevant betrachtet und sind daher auch insbesondere hinsichtlich des Risikomanagements besonderen regulatorischen Anforderungen unterworfen, was de lege lata auch die Pflicht beinhaltet ein bestimmtes Maß an IT-Sicherheit sicherzustellen. Derartige Regelungen bestehen vor allem für Kreditinstitute, Wertpapierdienstleistungsunternehmen, Finanzdienstleistungsinstitute, als Investmentvermögen einzuordnende Kapitalsammlungen sowie Versicherungsunternehmen.[368]

Daneben treffen die Geschäftsführung von Aktiengesellschaften und Gesellschaften mit beschränkter Haftung. Pflichten, eine ordnungsgemäße Geschäftsorganisation sicherzustellen. Teil einer ordnungsgemäßen Geschäftsorganisation sind nach allgemeiner Auffassung auch angemessene Vorkehrungen zur IT-Sicherheit.

Weiter finden sich auch im Bundesdatenschutzgesetz (BDSG) mit §§ 9 und 42a Regelungen, welche die IT-Sicherheit, insbesondere Vorkehrungen gegen unbefugten Zugriff sowie In-

[365] Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 50.
[366] Vgl. Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 50.
[367] Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 50 f.
[368] Vgl. §§ 25a, 25b KWG, § 33 WpHG, §§ 28, 29 KAGB, §§ 64a, 32 VAG.

formationspflichten bei unrechtmäßiger Kenntniserlangung von Daten betreffen. Diese greifen jedoch nur, soweit personenbezogene Daten betroffen sind, da andernfalls der Anwendungsbereich des Datenschutzrechts nicht eröffnet ist.

Neben diesen allgemeinen, wenig IT-Sicherheits-spezifischen, Regelungen rückt neuerdings eine spezifische Regulierung der IT-Sicherheit in den Fokus der öffentlichen Diskussion und der gesetzgeberischen Tätigkeiten. Einer besonderen Betrachtung bedürfen an dieser Stelle das so genannte „IT-Sicherheitsgesetz“[369] und die sich am Horizont abzeichnende EU-Richtlinie zur Netz- und Informationssicherheit („NIS-Richtlinie“), weil sie vor allem auch den Ausbau der digitalen Industrie betreffen.

1. IT-Sicherheitsgesetz

Neuerungen auf dem Gebiet der IT-Sicherheit bringt das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, das am 25.07.2015 in Kraft getreten ist. Dabei handelt es sich nicht um ein eigenständiges Gesetz. Es werden vielmehr verschiedene Einzelgesetze an die neuen Herausforderungen der IT-Sicherheit angepasst.

Inhaltlich wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale Aufsichtsbehörde für IT-Sicherheit etabliert. Adressat der Regelungen sind vor allem Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, vgl. § 2 Abs. 10 BSIG. Eine nähere Konkretisierung des Begriffs des „Betreibers einer kritischen Infrastruktur“ soll in einer Rechtsverordnung des Bundesministerium des Innern erfolgen (vgl. § 2 Abs. 10 BSIG). Die Betreiber kritischer Infrastrukturen werden gem. § 8a Abs. 1 BSIG verpflichtet, ein Mindestniveau an IT-Sicherheit einzuhalten, weil sie eine besondere Verantwortung für das Gemeinwohl haben.[370] Das BSIG spricht insoweit von *„angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“,* die unter Berücksichtigung des aktuellen Stands der Technik zu bestimmen sind. Sicherheitsvorfälle sind darüber dem BSI zu melden, wobei eine namentliche Meldung erforderlich ist, wenn der Sicherheitsvorfall zum Ausfall oder der Beeinträchtigung einer kritischen Infrastruktur im Sinne des Gesetzes führt.[371] Zum Schutz des Fernmeldegeheimnisses, zum Schutz personenbezogener Daten und im Hinblick auf die Verfügbarkeit von Telekommunikations- und Datenverarbeitungssystemen werden darüber hinaus auch Telekommunikationsanbieter verpflichtet, IT-Sicherheit zu gewährleisten; die entsprechenden Pflichten haben in § 109 TKG Einzug ge-

[369] Bei dem IT-Sicherheitsgesetz handelt es sich nicht um ein eigenständiges Gesetz zur IT-Sicherheit, sondern um ein Änderungsgesetz, welches insbesondere die Einfügung bestimmter Vorschriften in das BSIG zum Gegenstand hat.
[370] BT-Drs. 18/4096, S. 2.
[371] BT-Drs. 18/4096, S. 2.

funden und entsprechen inhaltlich im Wesentlichen den Pflichten, die auch die Betreiber kritischer Infrastrukturen treffen.[372]

2. NIS-Richtlinie der EU

Auch auf europäischer Ebene ist das Thema IT-Sicherheit Gegenstand steter Diskussionen. Seit 2013 liegt dabei ein Richtlinienentwurf des Europäischen Parlaments und des Rates für eine EU-Richtlinie zu Netz- und Informationssicherheit vor.[373] Nach derzeitigem Planungsstand könnte die NIS-Richtlinie noch im Jahr 2015 in Kraft treten.[374] Ziel der Richtlinie ist die Erhöhung sowohl der Sicherheit des Internets als auch der Sicherheit der privaten Netze und Informationssysteme, die für das Funktionieren der Gesellschaft und Volkswirtschaft unabdingbar sind.[375] Hierfür werden den Mitgliedstaaten Verpflichtungen hinsichtlich Prävention, Umgang und Reaktion in Bezug auf Sicherheitsrisiken und -vorfälle auferlegt.[376] Art. 7 des Entwurfs[377] legt den Mitgliedstaaten etwa auf, dass sie ein IT-Notfallteam einzurichten haben, das für die Bewältigung von Sicherheitsvorfällen und -risiken zuständig ist. Nach Art. 10 des Entwurfs[378] sollen die zuständigen Behörden oder die Kommission Frühwarnungen herausgeben, wenn sich Sicherheitsrisiken und -vorfälle rasch ausweiten oder ausweiten können, wenn die nationale Reaktionskapazität überschritten wird oder überschritten werden kann oder wenn sie mehr als einen Mitgliedstaat betreffen bzw. betreffen können. Anschließend wird eine koordinierte Reaktion auf diese Risiken und Vorfälle eingeführt, Art. 11 des Entwurfs. Außerdem werden Regelungen zur Schaffung kooperativer Mechanismen getroffen und Sicherheitsvorschriften für Marktteilnehmer und die öffentliche Verwaltung eingeführt.[379] So sollen die Mitgliedstaaten etwa sicherstellen, dass geeignete technische und organisatorische Maßnahmen ergriffen werden, um die Risiken für die IT-sicherheit der Netze und Informationssysteme zu managen, Art. 14 Abs. 1 des Entwurfs[380] und Sicherheitsvorfälle sollen den nach nationalem Recht zuständigen Behörden gemeldet werden, Art. 14 Abs. 2 des Entwurfs.[381]

3. Ausblick: Nationales Referenzprojekt zum Schutz der Produktion vor Cyberangriffen und Spionage

Nicht Teil der rechtlichen Rahmenbedingungen im allgemeinen Sinne, aber von hoher Relevanz für die IT-Sicherheit in der digitalisierten Industrie in Deutschland ist das so genannte

---

372 BT-Drs. 18/4096, S. 2.
373 Entwurf 2013/0027 (COD), S. 2.
374 Vgl. zum Durchbruch bei den Verhandlungen im Juni https://eu2015.lv/news/media-releases/2489-latvian-presidency-reaches-a-breakthrough-in-talks-with-european-parliament-on-network-and-information-security (zuletzt abgerufen am 19.08.2015).
375 Entwurf 2013/0027 (COD), S. 2.
376 Art. 1 Nr. 2 lit. a) Entwurf 2013/0027 (COD).
377 Entwurf 2013/0027 (COD), S. 2.
378 Entwurf 2013/0027 (COD), S. 2.
379 Art. 1 Nr. 2 lit. b) und c) Entwurf 2013/0027 (COD).
380 Entwurf 2013/0027 (COD), S. 2.
381 Entwurf 2013/0027 (COD), S. 2.

„nationale Referenzprojekt für IT-Sicherheit in der Industrie 4.0“. Mit der Gründung der Plattform Industrie 4.0 wurde ein weiterer Schritt auf dem Weg zu einer vernetzten Industrie 4.0 getan. Unterhalb dem Dach dieser Plattform wurde auch das nationale Referenzprojekt gegründet, mit dem gezeigt werden soll, wie in konkreten Anwendungsfällen die Gefahr von Hackerangriffen minimiert werden kann.[382] Im Projekt werden auch IT-Sicherheitslösungen entwickelt, welche standardisiert werden, um auch kleinen und mittleren Unternehmen kostengünstige Lösungen anbieten zu können.[383] Gerade die Erarbeitung kostengünstiger, aber zugleich effizienter Lösungen zur Absicherung der IT-Sicherheit dürfte einer der wesentlichsten Schritte zum Erfolg der digitalisierten Wirtschaft in Deutschland sein. Denn bei aller Bedeutung, die eine regulatorische Erfassung der IT-Sicherheit hat, so stößt diese bei einer der zentralen, tatsächlichen Herausforderungen der digitalisierten Wirtschaft an ihre natürlichen Grenzen. Viele kleinere und mittelständische Unternehmen verfügen schlicht nicht über die Ressourcen und das Know-how, um ein hinreichendes Maß an IT-Sicherheit zu gewährleisten. Zwar kann der Gesetzgeber Ihnen – theoretisch – die Pflicht auferlegen, dennoch entsprechende Vorkehrungen zu treffen, doch ob dies allein zu volkswirtschaftlich und im Sinne der Unternehmen gewünschten Lösungen führt, ist mit einem großen Fragezeichen zu versehen. Entscheidend dürfte sein, dass die Bundesregierung eben dieses Problem angeht und Lösungen findet, kleineren und mittelständischen Unternehmen auch in tatsächlicher Hinsicht die Möglichkeit zu bieten, IT-Sicherheit zu gewährleisten. Denn bei allen Ausführungen darf nicht vergessen werden, dass IT-Sicherheit – sofern keine Unternehmen von Bedeutung für das Gemeinwohl betroffen sind – zuvorderst immer noch im ureigenen Interesse der Unternehmen selbst liegt. Die Ergebnisse des Referenzprojekts werden im November 2015 auf dem nationalen IT-Gipfel vorgestellt.[384]

III. Bewertung der Rechtslage

Insgesamt lässt sich festhalten, dass es de lege lata noch kein umfassendes, aufeinander abgestimmtes IT-Sicherheitsrecht gibt.[385] Auch nach Verabschiedung des IT-Sicherheitsgesetzes handelt es sich bei dem Recht der IT-Sicherheit nach wie vor um eine Regelungsmaterie, die sich auf verschiedene Gesetze und Regelungsbereiche verteilt. Allen bestehenden Regelungen gemein ist, dass sie nur einzelne, meist besonders schützenswerte Teilbereiche der deutschen Wirtschaft oder besonders schützenswerte Daten treffen.

Sämtliche Regelungen zur IT-Sicherheit sind weitgehend generisch, wodurch für die betroffenen Unternehmen stets Unsicherheiten folgen, welche Vorkehrungen im konkreten Fall zu treffen sind. Zwar hat der Bundestag mit dem IT-Sicherheitsgesetz einen Anfang gemacht, der „weite Wurf“ ist damit aber nicht gelungen. Erforderlich ist ein einheitliches

[382] http://www.bmbf.de/press/3807.php.
[383] http://www.bmbf.de/press/3807.php.
[384] http://www.bmwi.de/DE/Presse/pressemitteilungen,did=701050.html (zuletzt abgerufen am 19.08.2015).
[385] Vgl. auch *Spindler*, MMR 2008, 7 (13).

Konzept, mit Mindestanforderungen an die IT-Sicherheit,[386] um einen Diebstahl von Know-how, sonstigen Daten und Informationen einzugrenzen oder zu verhindern.

Für eine Verbesserung der Sicherheit von Datensystemen beim fortschreitenden Ausbau der Digitalisierung der Wirtschaft ist das IT-Sicherheitsgesetz als erster Ansatz jedoch positiv zu bewerten.[387] Vor Herausforderungen stellen wird die digitalisierte Wirtschaft jedoch insbesondere die nach § 8b Abs. 4 BSIG bestehende Meldepflicht im Fall von Sicherheitsvorfällen. Danach haben Betreiber kritischer Infrastrukturen

> *„erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen*
> *1. führen können oder*
> *2. geführt haben,*
> *über die Kontaktstelle unverzüglich an das Bundesamt zu melden."*

Problematisch ist insoweit, dass die Voraussetzungen der Meldepflicht sehr weit und wenig konkret gefasst sind.[388] Insbesondere soweit bereits die Möglichkeit der Beeinträchtigung genügt, um die Meldepflicht auszulösen (*„führen können"*), wird dies zu erheblichen Rechtsunsicherheiten führen. Denn führt man sich die Komplexität der IT-Struktur eines modernen Unternehmens vor Augen, so wird schnell klar, dass sich praktisch häufig kaum abgrenzen lassen wird, welche Störungen zu einer solchen Beeinträchtigung *führen können* und welche nicht. Auch das Erfordernis einer Beeinträchtigung der Funktion ist nicht geeignet, eine Einschränkung der Meldepflicht zu bewirken. IT-Systeme werden immer komplexer, sodass theoretisch jede – nicht alltägliche – Störung in allgemeinen Systemen zu Beeinträchtigungen in den kritischen Infrastrukturen führen können.[389] Unternehmen werden damit praktisch vor der Wahl stehen, einen Verstoß gegen die Meldepflicht und damit ein Bußgeld nach § 14 Abs. 1 Nr. 4 BSIG zu riskieren oder zur Sicherheit eine Vielzahl von Meldungen vornehmen zu müssen – was mit einem erheblichen administrativen Mehraufwand und unter Umständen auch der Preisgabe vertraulicher Informationen in hohem Maße verbunden wäre.[390] Problematisch ist auch die in § 13 BSIG vorgesehene Berichtspflicht, die gegenüber dem Bundesministerium des Inneren besteht. Sie dient nach § 13 Abs. 2 BSIG dazu, die Öffentlichkeit aufzuklären. Im Falle der Veröffentlichung besteht insbesondere die Gefahr, dass sensible Informationen preisgegeben werden und den betroffenen Unternehmen Imageschäden und wirtschaftliche Nachteile drohen.[391] Schließlich weicht das IT-

---

[386] Vgl. auch *Bräutigam/Klindt*, NJW 2015, 1137 (1142), die einen interdisziplinären Meinungsaustausch anregen.
[387] *Bräutigam/Wilmer*, ZRP 2015, 38 (42); *Roth*, ZD 2015, 17 (22); *Roos*, MMR 2014, 729 f.; *Eckhardt*, ZD 2014, 599 (605).
[388] *Bräutigam/Wilmer*, ZRP 2015, 38 (40).
[389] *Bräutigam/Wilmer*, ZRP 2015, 38 (40).
[390] *Bräutigam/Wilmer*, ZRP 2015, 38 (40).
[391] *Bräutigam/Wilmer*, ZRP 2015, 38 (40).

Sicherheitsgesetz teilweise von der geplanten NIS-Richtlinie der EU ab.[392] Tritt diese in Kraft, wären auch die Vorschriften des IT-Sicherheitsgesetzes zu überarbeiten.

Am IT-Sicherheitsgesetz wird allgemein darüber hinaus kritisiert,[393] dass Fokus nur der Schutz kritischer Infrastrukturen ist, nicht aber die Stärkung des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme. Hierbei ist jedoch zu berücksichtigen, dass regulatorische Anforderungen immer auch einen Eingriff in die Geschäftsautonomie eines Unternehmens darstellen. Soweit Unternehmen in besonderem Maße für das Gemeinwohl relevant sind – wie die „kritischen Infrastrukturen" im Sinne des BSIG –scheint dies sinnvoll und vor dem Hintergrund der Interessen der Allgemeinheit gerechtfertigt. Soweit dies jedoch nicht der Fall ist, verbleibt es bei der Grundregel, dass die Schaffung von Regelungen zur IT-Sicherheit zuvorderst im eigenen Interesse der betroffenen Unternehmen steht.

Kritisch zu betrachten ist, dass im Rahmen der durch das IT-Sicherheitsgesetz veranlassten Änderung des § 100 Abs. 1 des Telekommunikationsgesetzes, in dem Telekommunikationsanbieter weitgehende Befugnisse erhalten, Verkehrsdaten der Nutzer zu verarbeiten (insbesondere diese zu speichern und zu erheben), soweit dies dazu dient, Störungen oder Fehler der Telekommunikationsanlagen zu erkennen oder zu beseitigen. Viele Kritiker sehen hier eine „Vorratsdatenspeicherung durch die Hintertür", bei der auf eine Massenspeicherung personenbezogener Daten gesetzt wird, was zwar positive Auswirkungen auf die IT-Sicherheit haben kann, dafür aber massiv in die Grundrechte der Betroffenen eingreift.[394]

Statt oder zumindest zusätzlich zu den oben angesprochenen, strafbewehrten Meldepflichten sollten positive Anreize für ein leistungsstarkes IT-Sicherheitskonzept gesetzt werden. Gleichzeitig müssen Sanktionen auf eine Art und Weise wirkungsvoll sein, die weder aus Angst vor Fehltritten zu einem Überfluss an Meldungen an das BSI führt, noch einen Verstoß gegen das IT-Sicherheitsgesetz zu einer bloßen Lappalie werden lässt. Auch Haftungstatbestände bei unzureichenden IT-Sicherheitsmaßnahmen könnten eine sinnvolle Motivation für Hersteller von vernetzten Systemen sein. Für eine zukunftsweisende Weiterentwicklung und Stärkung der IT-Sicherheit müssten zudem – rein tatsächlich und weniger rechtlich – Konzepte und Techniken wie die Ende-zu-Ende-Verschlüsselung,[395] „Privacy by Design" und „Privacy by Default" oder „Security by Design" gefördert werden.

---

[392] *Roth*, ZD 2015, 17 (22); näher hierzu *Bräutigam/Wilmer*, ZRP 2015, 38 (41 f.).

[393] Vgl. auch zu weiteren Punkten BT-Drs. 18/4096, S. 12 f.

[394] Vgl. auch zu weiteren Punkten BT-Drs. 18/4096, S. 12 f.

[395] Diese ist momentan noch kein gesetzlicher Standard, so hat der Gesetzgeber z. B. im De-Mail-Gesetz eine Transportverschlüsselung ausreichen lassen (§ 5 Abs. 3 Nr. 1 De-Mail-G) – dabei soll hier gerade die Sicherheit der elektronischen Kommunikation erhöht werden.

IV. Technische Entwicklung und Gesetzgebungsprozess

1. Herausforderung

Eine der großen Herausforderungen des Themas IT-Sicherheit ist dessen Komplexität. Es liegt in der Natur der Sache, dass die Festlegung konkreter Regelungen, die zugleich allgemeingültig Geltung beanspruchen können, nicht möglich ist. Die konkreten technischen und organisatorischen Maßnahmen zur IT-Sicherheit hängen immer entscheidend von dem konkreten Unternehmen, dessen Branche und dem generellen Risikoprofil ab. Es liegt darüber hinaus auf der Hand, dass bspw. für Produktionsanlagen gänzlich andere Maßnahmen zur IT-Sicherheit erforderlich sind als für Desktoprechner.[396] Zunächst besteht die Herausforderung bei der Verabschiedung IT-sicherheitsrechtlicher Vorschriften vor allem darin, dort, wo Unternehmen in besonderem Maße Cyber-Attacken ausgesetzt sind, die richtigen Anreize zu setzen, sicherheitstechnische Vorkehrungen einzuführen. Zwar sollte jedes Unternehmen ein originär eigenes Interesse daran haben, ausreichend Sicherheitsmaßnahmen einzuführen, um eigenes Know-how zu schützen und Gefahren für die eigenen Systeme und Produktionsanlagen zu vermeiden. Bei einem Blick in die Praxis lässt sich jedoch beobachten, dass dem Thema IT-Sicherheit oft nur eine untergeordnete Bedeutung beigemessen wird.[397] Es lässt sich nur mutmaßen, dass dies in den Kosten für IT-Sicherheitstechnik und der Komplexität des Themas begründet liegt. Daher ist es insbesondere notwendig, auch für kleine und mittlere Unternehmen Wege vorzusehen, wie sie sich vor Cyber-Attacken schützen können. Mit dem nationalen Referenzprojekt zum Schutz der Produktion vor Cyberangriffen und Spionage ist hierbei bereits ein erster wichtiger Schritt getan, indem standardisierte Lösungen entwickelt werden, damit sich auch diese Unternehmen adäquat vor Cyber-Attacken schützen können. Zu beachten ist jedoch immer auch, dass es auf dem Gebiet der IT-Sicherheit 100%igen Schutz nicht geben kann.

Eine der großen Herausforderungen für den Gesetzgeber liegt auch darin, ein geeignetes Regelungskonzept zur Erfassung der IT-Sicherheit zu entwickeln. IT-Sicherheitsrisiken sind erfahrungsgemäß einem stetigen Wandel unterworfen. In diesem schnelllebigen Bereich ändern sich sowohl die Risiken, als auch die notwendigen technischen und organisatorischen Schutzmaßnahmen laufend. Mag bspw. eine Verschlüsselungstechnik heutzutage noch „state of the art“ sein, so kann Sie schon morgen hoffnungslos veraltet sein, weil eine entscheidende Umgehungsmöglichkeit gefunden wurde. Daher ist es notwendig, ein Regelungskonzept zu entwickeln, das auf sich verändernde Umstände schnell reagieren kann.

Zu detaillierte Regelungen sind daher zwar zu vermeiden, zu generische Regelungen können aber dazu führen, dass beim Adressaten der Vorschrift ein hohes Maß an Rechtsunsicherheit entsteht. Während formelle Gesetze einen langen Gesetzgebungsprozess durchlaufen müssen, können Verordnungen und technische Regelwerke schneller auf sich verän-

[396] Vgl. auch *Schulzki-Haddouti* unter: http://blog.zdf.de/hyperland/2014/02/industrie-4-0-als-herausforderung-fuer-die-it-sicherheit.

[397] Vgl. Studie „Datenklau 2015“, abrufbar unter http://www.ey.com/Publication/vwLUAssets/EY-Datenklau-2015-Praesentation-final/$FILE/EY-Datenklau-2015-Praesentation-final.pdf.

dernde Umstände reagieren. Vorzugswürdig scheint daher ein abgestuftes Regelungskonzept aus formellen Gesetzen, Verwaltungsvorschriften und technischen Regelwerken, um ein austariertes Ergebnis zu erzielen.

Die Entwicklung solcher aufeinander abgestimmter Regelwerke erfordert ein hohes Maß an interdisziplinärer Zusammenarbeit zwischen Rechts- und den betroffenen Ingenieurwissenschaften.[398]

Unabhängig von rechtlichen Aspekten wird es notwendig sein, Entscheidungsträger in Wirtschaft und Politik für das Thema IT-Sicherheit noch mehr zu sensibilisieren. Im Gegensatz zu Angriffen in der „realen Welt" sind „Cyber-Angriffe" oft nicht sichtbar. Dies macht es manchmal schwer, auf sie aufmerksam zu machen und ihnen angemessen entgegen zu wirken.

2. Denkbare Lösungswege

Im Folgenden sollen kurz einige denkbare Wege skizziert werden, wie die Herausforderungen um die IT-Sicherheit beim Ausbau der digitalen Wirtschaft gelöst und ein geeignetes Regelungskonzept erstellt werden kann.

a) Formelle Gesetze

Zunächst besteht die Möglichkeit, IT-sicherheitsrechtliche Vorschriften durch formelle, also parlamentarische Gesetze zu erlassen. Dies hat den Vorteil, dass die Anforderungen im Zweifel durch Behördenzwang durchsetzbar sind. Nachteilig ist der lange Gesetzgebungsprozess, dem der Erlass solcher Vorschriften unterworfen ist. Auf Ebene der gesetzlichen Regelung scheinen nur generische Regelungen, mit einem hohen Abstraktionsgrad möglich. Jede konkrete Regelung wäre der Gefahr ausgesetzt, bereits kurz nach, im schlimmsten Fall schon vor, In-Kraft-treten wieder veraltet zu sein.

b) Rechtsverordnungen

Rechtsverordnungen sind materielle Gesetze, die von Regierungen oder Ministern erlassen werden können. Erforderlich ist eine Ermächtigung für den Erlass von Rechtsverordnungen in einem formellen Gesetz. Der Prozess des Erlasses einer Rechtsverordnung ist weniger langwierig, als beim Erlass formeller Gesetze. Auch hier können Zuwiderhandlungen mit Behördenzwang durchgesetzt werden. Im Grundsatz scheinen Rechtsverordnungen damit als geeignetere Instrumente zur Festlegung konkreterer Anforderungen an die IT-Sicherheit.

c) Branchenübliche Standards (vgl. BSIG)

Eine weitere sinnvolle Möglichkeit, zeitnah auf sich ergebende Veränderungen reagieren zu können, kann ein Vorgehen wie in § 8a Abs. 2 BSIG vorgesehen sein. Danach können Be-

[398] *Bräutigam/Klindt*, NJW 2015, 1137 (1142).

treiber kritischer Infrastrukturen und ihre Branchenverbände branchenspezifische Sicherheitsstandards vorschlagen. Das BSI kann diesbezüglich feststellen, ob sie geeignet sind, die sicherheitstechnischen Anforderungen nach § 8a Abs. 1 BSIG zu erfüllen. Der Vorteil dieser Regelungen liegt darin, dass Branchenverbände ein großes Know-how haben, geeignete Sicherheitsstandards einzuführen. Dabei sollte jedoch beachtet werden, dass Klauseln eingefügt werden, die verpflichtend eine Überprüfung in Bezug auf die Aktualität der Vorschriften vorsehen.

d) Unabhängige Maßstäbe (ISO)

Ähnlich der Einführung branchenüblicher Standards wäre auch denkbar, auf die Einhaltung unabhängiger Maßstäbe wie ISO oder DIN-Normen abzustellen, wobei hier jedoch zu beachten ist, dass der Gesetzgeber ein Stück seiner Regelungshoheit in die Hände von Dritten legt. Diese sind insbesondere zu berücksichtigen, wenn in einer Vorschrift auf den Stand der Technik abgestellt wird.

e) Richterliche Rechtsfortbildung

Grundsätzlich denkbar wäre noch die Konkretisierung unbestimmter, gesetzlicher Rechtsbegriffe durch richterliche Rechtsfortbildung. Dies scheint für Anforderungen an die IT-Sicherheit jedoch nicht praktikabel. Zum Einen vergehen häufig Jahre, bis sich eine einheitliche (höchstrichterliche) Linie herausgebildet hat, die dann in wenigen Monaten wieder veraltet wäre. Darüber hinaus darf praktisch auch in Frage gezogen werden, ob die technische Kompetenz der Richter hoch genug ist, dieses technisch komplexe und schwierige Thema, das eine hohe Kenntnis der jeweiligen Branche voraussetzt, korrekt zu beurteilen.

f) Behördenpraxis (analog MaRisk)

Schließlich wäre es auch denkbar, dass das BSI als zentrale Behörde für Informationssicherheit eine einheitliche Aufsichtspraxis herausbildet und diese deutlich und offen kommuniziert. Als positives Beispiel können insoweit die Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) dienen. Hier werden durch ein Rundschreiben der BaFin die gesetzlich nur generisch umschriebenen Mindestanforderungen an das Risikomanagement konkretisiert. Dadurch kann zeitnah auf veränderte Umstände reagiert werden. Gleichzeitig bietet sich für die betroffenen Unternehmen ein gewisses Maß an Rechtssicherheit durch einen höheren Konkretisierungsgrad der Anforderungen. Außerdem gewährleistet die Einbeziehung einer Fachbehörde ein hohes Maß an Fachkompetenz.

Teil 10 IT-Infrastruktur/Cloud (*Dr. Thomas Thalhofer*)

Ein weiterer Aspekt im Rahmen von Industrie 4.0 ist das Cloud Computing.[399] Es ermöglicht Unternehmen, flexibel und bedarfsorientiert über Netze auf eine virtuelle IT-Infrastruktur („Infrastructure as a Service"), auf IT-Plattformen („Platform as a Service") oder Softwareprodukte („Software as a Service") zuzugreifen und bietet insbesondere aufgrund der exzellenten Skalierbarkeit mit Blick auf die Bedürfnisse der Unternehmen enorme technische und wirtschaftliche Vorteile.[400]

I. Datenschutz und Cloud

Hinsichtlich der mit dem Cloud Computing verbundenen datenschutzrechtlichen Problemstellungen gibt es seit 2011 wesentliche Rechtsentwicklungen, welche die Rechtssicherheit der Anwendung von Cloud Computing für die Unternehmen in Deutschland erheblich erhöht haben. Die bundesweite Zusammenarbeit der Datenschutzbehörden, namentlich im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und im so genannten „Düsseldorfer Kreis" hat hier die „Orientierungshilfe – Cloud Computing"[401] hervorgebracht. Diese bietet innerhalb Deutschlands eine große Hilfe zur datenschutzrechtskonformen Nutzung der Dienste,[402] da sie die Richtlinien für die behördliche Praxis in der rechtlichen Einstufung von Cloud-Nutzung vorgibt. Durch ihren hohen Detaillierungsgrad, zum Beispiel mit Blick auf IT-Sicherheitsanforderungen, bietet die Orientierungshilfe sehr gute Anhaltspunkte für Unternehmen, was für eine rechtskonforme Cloud-Nutzung zu beachten ist. Ausdrücklich zu begrüßen ist dabei auch die einheitliche Anwendung der Orientierungshilfe im gesamten Bundesgebiet. Man wird durchaus sagen können, dass diese einheitliche Behördenpraxis für die Förderung des Cloud Computing wertvoller ist, als dies cloud-spezifische Gesetzesänderungen sein könnten. Letztere würden mit hoher Wahrscheinlichkeit wieder Auslegungsmöglichkeiten (und evtl. Auslegungsschwierigkeiten) mit sich bringen.

---

399 Zum Begriff und zu Ausprägungen näher *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 1ff. Nachfolgend wird der Begriff des Cloud Computing unter dem Gesichtspunkt der „public cloud", also das Angebot eines standardisierten Cloud-Dienstes für eine Vielzahl von Kunden, genutzt.

400 Zu den Vor- und Nachteilen des Cloud Computings vgl. *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 11.

401 Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Version 2.0, Stand 09.10.2014, abrufbar unter: http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/orientierungshilfen-node.html.

402 So auch *Eckhardt,* DuD 2015, 176 (182).

Auf europäischer Ebene hat die Art. 29-Datenschutzgruppe ebenfalls Vorgaben für eine datenschutzgerechte Cloud-Nutzung aufgestellt.[403] Darüber hinaus ist zu erwarten, dass die geplante Datenschutz-Grundverordnung[404] mit der darin angestrebten Vollharmonisierung einen weiteren Schritt in Richtung Rechtssicherheit und -klarheit mit sich bringt.[405]

1. Das Institut der ADV – Reformbedarf für die Cloud?

Datenschutzrechtlich wird das Cloud Computing, soweit sich die Daten im Bereich der EU/des EWR befinden, überwiegend als Auftragsdatenverarbeitung gem. § 3 Abs. 8 Satz 3 BDSG eingeordnet.[406] Der Cloud-Anbieter gilt dabei nicht als Dritter, sodass keine erlaubnispflichtige Datenübertragung gem. § 3 Abs. 4 Nr. 3 BDSG vorliegt. Diese Privilegierung bringt jedoch zugleich besondere Anforderungen mit sich. Grundsätzlich bleibt der Cloud-Anwender weiterhin gem. § 11 Abs. 1 BDSG für die Einhaltung der datenschutzrechtlichen Anforderungen verantwortlich.

a) Weisungsrechte und Kontrollpflichten des Auftraggebers

Entsprechend dieser Letztverantwortung legt § 11 Abs. 2 Satz 4 BDSG dem Cloud-Anwender umfassende Kontrollpflichten über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen vor Beginn der Datenverarbeitung durch den Cloud-Provider sowie *„regelmäßig“* während der gesamten Dauer der Cloud-Nutzung auf. Hinsichtlich der Ausgestaltung der Datenverarbeitung ist, damit eine Auftragsdatenverarbeitung im Rechtssinne vorliegt, ein Weisungsrecht gemäß § 11 Abs. 3 BDSG erforderlich. Im Rahmen der in § 9 BDSG i.V.m. Anlage 1 Satz 2 Nr. 6 vorgesehenen Auftragskontrolle, die sowohl Auftragnehmer als auch Auftragsgeber bindet,[407] muss die Einhaltung der Weisungen überprüft und sichergestellt werden.

Diese umfassenden Kontrollpflichten stehen im Gegensatz zu der tatsächlichen Ausgestaltung der Cloud-Nutzung.[408] De facto beherrschen die Cloud-Anbieter den Datenverarbei-

---

[403] Article 29 Data Protection Working Party, „Opinion on Cloud Computing“, July 1, 2012 (03/12/EN WP 196), abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[404] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzgrundverordnung) vom 25.01.2012, KOM (2012) 11. Zum aktuellen Stand vgl. die Webseite von *Jan Albrecht*, MdEP: https://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html (Stand: 19.08.2015).

[405] *Kühling/Biendl,* CR 2014, 150 (153).

[406] U.a. *Schild* in Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, 12. Edition, Stand 01.02.2015, BDSG § 3, Rn. 111; *Schröder/Haag,* ZD 2012, 495 (497); *Rath/Rothe,* K&R 2013, 623 (625); *Kühling/Biendl,* CR 2014, 150 (151) m. w. N.; so auch die Einschätzung der Aufsichtsbehörden, vgl. die Orientierungshilfe Cloud Computing Version 2.0, S. 9,Fn. 401.

[407] *Karg* in Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, 12. Edition, Stand 01.02.2015, BDSG Anlage, Rn. 33.

[408] *Borges,* DUD 2014, 165 spricht daher von einem echten Dilemma, in dem sich die Cloud-Nutzer durch die Kontrollpflichten einerseits und dem Bestreben nach technischer und wirtschaftlicher Entlastung andererseits befinden.

tungsvorgang in der Cloud und geben somit die Bedingungen für die Nutzung vor.[409] Zudem sind Einzelweisungsrechte nicht mit der hinter der Cloud-Nutzung stehenden Intention der Standardisierung und Skalierbarkeit vereinbar. Schließlich erfordern effiziente Kontrollen auf Seiten des Cloud-Anwenders erhebliche fachliche Kenntnisse,[410] welche dieser mit Blick auf die komplexen Cloud-Anwendungen oft nicht haben wird. Darüber hinaus wird die Durchführung von Vor-Ort-Kontrollen bei Massenprodukten, was Cloud Computing Anwendungen häufig sind, sogar als Gefahr für die Datensicherheit eingestuft.[411]

Als Alternative zu einer eigenen Kontrolle wird daher für den Bereich des Cloud Computings der Weg über Zertifizierungen befürwortet.[412] Gesetzlich ist eine tatsächliche Vor-Ort-Kontrolle nicht vorgeschrieben.[413] Auch die Aufsichtsbehörden erkennen einen solchen Ersatz der eigenen Kontrolle durch unabhängige Stellen mit entsprechender Zertifizierungsbefugnis an, sofern sich der Cloud-Anwender darüber Klarheit verschafft, dass sich die Zertifizierung auch auf die cloudspezifischen Datenschutzrisiken bezieht,[414] dies gilt insbesondere bei der bereits bestehenden Zertifizierungsmöglichkeit nach ISO 27001 (Datensicherheit),[415] die nach Ansicht der Aufsichtsbehörden alleine nicht genügt.[416] Speziell für Cloud-Dienste existiert seit August 2014 nun die ISO 27018, die Standards für den Datenschutz in der Cloud festlegt.[417] Gegenwärtig gibt es jedoch noch kein einheitliches, durch eine gesetzliche Grundlage gestütztes Zertifizierungsverfahren.[418] Die Folge ist nach wie vor erhebliche Rechtsunsicherheit. Mit der geplanten Datenschutz-Grundverordnung besteht jedoch die Chance, eine europäische Lösung zu erreichen.[419] Uneinigkeit besteht hierbei aber insbe-

---

409 *Karg* in Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 12. Edition, Stand 01.02.2015, BDSG Anlage, Rn. 32.

410 *Kühling/Biendl,* CR 2014, 150 (152); *Borges,* DUD 2014, 165, 166.

411 *Rath/Rothe,* K&R 2013, 623 (627).

412 U.a. *Kühling/Biendl,* CR 2014, 150 (152); *Rath/Rothe,* K&R 2013, 623 (627); *Karg* in Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 12. Edition, Stand 01.02.2015, BDSG Anlage, Rn. 32; ausführlich zu den bereits existierenden Möglichkeiten der Zertifizierung der momentanen Bestrebungen in diese Richtung: *Borges,* DUD 2014, 165 (166).

413 So die überwiegende Meinung, u.a. *Eckhardt,* DuD 2015, 176 (178); *Rath/Rothe,* K&R 2013, 623 (627); *Bergt* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 37 (46), mit Verweis auf die Gesetzesbegründung, vgl. BT-Drs. 16/13657, S. 18.

414 Vgl. Orientierungshilfe – Cloud Computing, S. 10, Fn. 401, dem zustimmend *Bergt* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 37 (48).

415 ISO/IEC 27001:2013(en), Information technology – Security techniques – Information security management systems – Requirements, abrufbar unter: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

416 Vgl. Orientierungshilfe – Cloud Computing, S. 10, Fn. 401.

417 ISO/IEC 27018: 2014(en), Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, abrufbar unter: https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en.

418 Es gibt mehrere Forschungsansätze und Pilotprojekte, siehe dazu *Borges,* DuD 165 (166).

419 Der ursprüngliche Kommissions-Entwurf enthielt noch keine detaillierte Regelung zu einem möglichen Zertifizierungsverfahren, jedoch sind im Laufe des Gesetzgebungsprozesses Stimmen laut geworden, die sich hierfür aussprechen, vgl. dazu *Borges,* DuD 2014, 165 (168). Am detailliertesten ist der am 15. Juni 2015 vom Rat der Innen- und Justizminister angenommene Änderungsvorschlag, der in Art. 39 die Möglichkeit einer Zertifizierung auf eine gesetzliche Grundlage stellt und in Art. 39 a Regelungen zu den Zertifizierungsstellen und zum Verfahren enthält, die Dokumente des Rats sind abrufbar auf der Website

sondere noch darüber, ob die Zertifizierung von besonderen privaten Stellen oder von den Aufsichtsbehörden durchgeführt werden soll.[420]

Hinsichtlich der Weisungsrechte lassen sich teils geäußerte Bedenken[421] durch eine Vorverlagerung der Weisungen und durch Transparenz zerstreuen.[422] So kann der Cloud-Anwender seine Weisungsrechte beispielsweise durch die Wahl zwischen verschiedenen Standard-Modellen ausüben. Hinsichtlich der Sicherheitsanforderungen sind vertragliche Vereinbarungen mit dem Cloud-Provider über die anwendbaren Standards erforderlich. Schließlich sind dort, wo aufgrund eines hohen Standardisierungsgrades kundenindividuellen Bedürfnissen nur in geringem Maße Rechnung getragen werden kann, erleichterte Lösungsmöglichkeiten vom Vertrag für den Cloud-Anwender vorzusehen.

b) Der Einsatz von Subunternehmern

Ebenfalls problematisch ist die beim Cloud-Computing übliche Einschaltung von Unter-Anbietern, um dadurch insbesondere Kapazitätsengpässe abzufangen. § 11 Abs. 2 Satz 2 Nr. 6 BDSG bestimmt, dass die Beauftragung von Subunternehmern vertraglich geregelt werden muss. Die Aufsichtsbehörden konkretisieren dies ausgehend von der Letztverantwortung des Cloud-Anwenders dahingehend, dass vertraglich feststehen muss, welche Subunternehmer an welchen Standorten eingeschaltet werden.[423] Werden nachträglich neue Subunternehmer beauftragt, muss dies vor der Übertragung der personenbezogenen Daten anzuzeigen sein, und dem Cloud-Anwender muss ein Widerspruchs- und ggf. Sonderkündigungsrecht vertraglich zustehen.[424]

Darüber hinaus gilt im Verhältnis zwischen Cloud-Anwender und Subunternehmer der gleiche Kontrollmaßstab wie zum Cloud-Anbieter.[425] Hier bietet sich ebenfalls der Weg der Zertifizierung an, da sich eine eigene Kontrolle der Subunternehmer durch den Cloud-Anwender in der Praxis regelmäßig noch schwieriger gestalten wird. Zudem muss gewährleistet sein, dass dem Cloud-Anbieter entsprechende Kontrollrechte auch gegenüber dem Subunternehmer zustehen. Hierauf kann der Cloud-Anwender nicht verzichten.[426] Problematisch ist hierbei, dass der Cloud-Anwender nicht zwingend in einem vertraglichen Ver-

---

von Jan Albrecht, MdEP und Berichterstatter für das Europäische Parlament, abrufbar unter: https://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/alles-wichtige-zur-datenschutzreform.html.

[420] Dazu *Borges,* DuD 2014, 165 (169).

[421] So etwa Deutscher Anwaltverein, Stellungnahme zur Mitteilung der Europäischen Kommission „Freisetzung des Cloud-Computing-Potenzials in Europa“, 02/2013, S. 9f.

[422] Ausführlich zu diesem Komplex *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 40ff.

[423] Vgl. Orientierungshilfe – Cloud Computing, S. 9, oben Fn. 401; a.A. *Spoerr* in Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, 12. Edition Stand 01.05.2015, BDSG § 11, Rn. 118, der sich gegen eine Offenlegung der Identität der einzelnen Unterauftragnehmer ausspricht.

[424] Vgl. Orientierungshilfe – Cloud Computing, S. 9, Fn. 401.

[425] *Spoerr* in Wolff/Brink, Beck’scher Online-Kommentar Datenschutzrecht, 12. Edition Stand 01.05.2015, BDSG § 11, Rn. 118.

[426] *Eckhart,* DuD 2015, 176 (179).

hältnis zu dem Subunternehmer steht. Daher müssen bereits im Vertrag zum Cloud-Anbieter die entsprechenden Regelungen enthalten sein und der Cloud-Anbieter verpflichtet werden, einen Vertrag mit dem Subunternehmer zu schließen, der die zwischen Cloud-Anwender und Cloud-Anbieter geltenden Vertragsbedingungen widerspiegelt.[427]

c) Zwischenergebnis

Werden die Vorgaben der Aufsichtsbehörden beachtet, stellen die Anforderungen des § 11 BDSG keine unüberwindbare Hürde für das Cloud Computing dar.[428] Dazu bedarf es jedoch zwingend vor der Nutzung eines Cloud-Dienstes einer anfänglichen Risikobewertung durch die Unternehmen.[429] Für kleinere oder mittlere Unternehmen besteht die Problematik, dass sie regelmäßig über weniger Marktmacht als die Cloud-Anbieter verfügen. Hier muss dann die Initiative für rechtskonforme Verträge vom Cloud-Anbieter ausgehen.[430] Abgesehen von den positiven Werbeeffekten gegenüber anderen Anbietern kann der Cloud-Anbieter damit die bestehenden Bedenken bei potentiellen Kunden ausräumen und so die Inanspruchnahme seiner Dienste fördern.

2. Sonderregelungen für bestimmte Bereiche (z.B. § 203 StGB) – faktischer Ausschluss der Cloud-Nutzung?

Besonders problematisch stellt sich die Nutzung von Cloud-Diensten für solche Berufsgruppen dar, die dem Geheimnisschutz des § 203 StGB unterliegen. Doch auch für diese Berufsgruppen brächte die Cloud-Nutzung erhebliche Vorteile mit sich. Zum Beispiel ist dabei an die Speicherung von Patientendaten in Cloud Anwendungen zu denken, welche dann von verschiedenen Ärzten und Krankenhäusern genutzt und fortgeschrieben werden könnten. Diesen Bedürfnissen wird § 203 StGB in seiner momentanen Fassung nicht gerecht. Er bildet die modernen Formen der IT-Nutzung nicht mehr praxisgerecht ab.

a) Geheimnisschutzrelevante Daten in der Cloud?

§ 203 Abs. 1 StGB untersagt es bestimmten Berufsgruppen, unbefugt fremde Geheimnisse zu offenbaren. Bei der Auslagerung von Kundendaten o. ä. in einen Cloud-Service ohne Einwilligung oder Entbindung von der Schweigepflicht wird der Tatbestand des § 203 StGB von der herrschenden Meinung als erfüllt angesehen.[431] § 11 BDSG kann nach überwiegen-

---

[427] Orientierungshilfe – Cloud Computing, S. 11, oben Fn. 401.
[428] *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 37.
[429] *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 34.
[430] *Bergt* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 37 (45).
[431] U.a. *Spoerr* in Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 12. Edition Stand: 01.05.2015, BDSG § 11, Rn. 18; *Vander* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 105 (117). Ausführlich zum Gesamtkomplex *Bräutigam/Brandt,* in: Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 11, Rn. 67ff.

der Auffassung nicht als ausreichende gesetzliche Ermächtigung zur Weitergabe der Daten herangezogen werden.[432]

Eine Strafbarkeit kann nur abgewendet werden, wenn die Informationen anonymisiert oder mit einer hochwertigen Sicherung verschlüsselt in die Cloud verlagert werden, ohne dort wieder reanonymisiert oder entschlüsselt zu werden.[433]

Eine Strafbarkeit scheidet auch dann aus, wenn man den Cloud-Anbieter als Gehilfen i.S.d. § 203 Abs. 3 Satz 2 StGB einordnen würde. Nach traditionellem Verständnis kann Gehilfe jedoch nur sein, wer organisatorisch in den Arbeitsablauf des Geheimnisträgers eingebunden und weisungsabhängig ist und eine Tätigkeit ausübt, die in einem funktionalen Zusammenhang mit der Berufsausübung steht. Ein außenstehender Dritter kann nicht Gehilfe sein.[434] Dagegen wird nach einem weiteren Verständnis der Norm eine Gehilfenstellung auch dann angenommen, wenn der Dritte, hier der Cloud-Anbieter, lediglich einer hinreichenden, effektiven Steuerungsmacht unterliegt.[435] Dem wird aber mit dem Argument entgegengetreten, dass eine solche Steuerungsmacht aufgrund der tatsächlichen Ausgestaltung der Cloud-Dienste unrealistisch sei und daher der Cloud-Anbieter generell nicht als Gehilfe eingestuft werden könne.[436] Hinzu kommt, dass eine Erweiterung des Gehilfen-Begriffs auf Auftragsdatenverarbeiter diese einer Strafbarkeit nach § 203 Abs. 2 Satz 1 i.V.m. Abs. 1 StGB unterwirft. Analogien bzw. eine Auslegung über den Wortlaut hinaus, die zu einer Strafbarkeitsausweitung führen, sind aber mit Art. 103 Abs. 2 GG bzw. § 1 StGB nicht vereinbar.[437]

Teilweise wird angedacht, eine Entscheidung des EuGH, in der dieser die Weitergabe von Telekommunikationsdaten durch einen Diensteanbieter zum Forderungseinzug als mit dem Fernmeldegeheimnis vereinbar erlaubt, sofern eine Weisungsbefugnis besteht und die Datenübertragung sich im Rahmen des Erforderlichen hält,[438] auf die Datenverarbeitung durch Dritte im Rahmen des § 203 StGB zu übertragen.[439] Hier hat sich jedoch noch keine einheitliche Linie herausgebildet.

---

[432] *Spoerr* in Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 12. Edition Stand: 01.05.2015, BDSG § 11, Rn. 18; *Becker* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 343 (348); *Vander* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 105 (119).

[433] *Kroschwald/Wicker,* CR 2012, 758 (760); *Vander* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 105 (117). So auch für den vergleichbaren Sachverhalt des Outsourcings *Bräutigam* CR 2011, 411 (413).

[434] *Lenckner/Eisele* in Schönke/Schröder, Strafgesetzbuch, 29. Aufl. 2014, § 203, Rn. 64; *Vander* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 105 (118); *Heger* in Lackner/Kühl, StGB, 28. Aufl. 2014, § 203 StGB, Rn. 11b.

[435] *Spoerr* in Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 12. Edition Stand: 01.05.2015, BDSG § 11, Rn. 23.

[436] *Kroschwald/Wicker,* CR 2012, 758 (762); *Becker* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 343 (351).

[437] Vgl. u.a. *Eser/Hecker* in Schönke/Schröder, Strafgesetzbuch, 29. Aufl. 2014, § 1, Rn. 25.

[438] Vgl. EuGH, Urteil vom 22.11.2012 – C-119/12, K&R 2013, 31.

[439] Dazu *Becker* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 343 (351); kritisch *Vander* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 105 (121).

Im Outsourcing-Bereich greift die Vertragspraxis daher auf Modelle zur organisatorischen Eingliederung von Mitarbeitern, die mit Geheimnissen im Sinne des § 203 StGB in Berührung kommen, zurück.[440] Diese Modelle sind indes – aufgrund der Standardisierung und dem Angebot für eine Vielzahl von Kunden – im Bereich des Cloud Computing nicht tragfähig.

b) Reformbedarf

Jedenfalls besteht für die berufsmäßigen Geheimnisträger in diesem Bereich keine Rechtssicherheit. Da eine Entbindung von der Schweigepflicht durch jeden einzelnen Patienten regelmäßig nicht als praktikabler Weg angesehen wird,[441] besteht hier ein erheblicher Reformbedarf. Als Lösung wird vorgeschlagen, in § 11 BDSG ausdrücklich eine eng begrenzte Offenbarungsbefugnis zu schaffen und die Auftragsdatenverarbeiter strafrechtlich den Gehilfen i.S.d. § 203 Abs. 3 Satz 2 StGB gleichzustellen.[442] Ein Tätigwerden des Gesetzgebers erscheint hier dringend erforderlich.

3. Sonstige datenschutzrechtliche Hindernisse

a) Schriftlichkeitserfordernis

Ein weiteres Hindernis für eine praxisgerechte Nutzung von Cloud-Diensten stellt das in § 11 Abs. 2 Satz 2 BDSG normierte Schriftformerfordernis dar.[443] Teilweise wird zwar eine Ersetzung der Schriftform durch die elektronische Form nach § 126 a BGB in Betracht gezogen,[444] was aber nicht zwingend eine Erleichterung bedeutet. Mit der geplanten Datenschutz-Grundverordnung steht hier eine positive Veränderung in Aussicht; danach wird lediglich eine Dokumentation der Vereinbarung gefordert.[445]

b) Verschlüsselung der Daten

Problematisch ist weiter, dass den Unternehmen auch eine Verschlüsselung der Daten regelmäßig keine Erleichterung aus datenschutzrechtlicher Sicht bringt. Nach der Einschätzung der Aufsichtsbehörden liegen personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG regelmäßig auch dann vor, wenn diese verschlüsselt sind.[446]

---

[440] Ausführlich hierzu *Bräutigam/Brandt* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 11, Rn. 76ff.

[441] *Kroschwald/Wicker,* CR 2012, 758 (763); *Becker* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 343 (347).

[442] *Petri,* DuD 2014, 862 (861).

[443] *Bergt* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 37 (49) spricht insoweit von einem „Medienbruch".

[444] U.a. *Funke/Wittmann,* ZD 2013, 221 (225); *Spindler/Nink* in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, BDSG § 11, Rn. 18.

[445] Vgl. Art. 26 Abs. 2 und 3 des Vorschlags der Kommission für eine Datenschutz-Grundverordnung, KOM (2012) 11.

[446] Vgl. Orientierungshilfe – Cloud Computing, S. 12.

Dies stößt in der Literatur zwar erheblich auf Kritik. Hier wird vertreten, dass bei einer Verschlüsselung nach dem Stand der Technik der Anwendungsbereich des Datenschutzrechts ausgeschlossen sei.[447] Werden Daten jedoch in der Cloud nicht nur gespeichert, sondern auch verarbeitet, ist nach den derzeitigen technischen Möglichkeiten regelmäßig eine Entschlüsselung erforderlich.[448] Aber auch sonst ist die Gefahr, dass anonymisierte Daten mittels vorhandenen Zusatzwissens wieder mit natürlichen Personen verknüpft werden, in der Cloud sehr hoch,[449] weshalb sich die Einhaltung der datenschutzrechtlichen Bestimmungen empfiehlt. Die Verschlüsselung ist aber wirksames Instrument zur Datensicherung i.S.d. § 9 BDSG.

c) Regelungen für Internationale Datentransfers

Ein Problem stellt es auch dar, dass die Privilegierung der Auftragsdatenverarbeitung i.S.d. § 3 Abs. 8 Satz 3 BDSG nur greift, wenn der Cloud-Anbieter die Datenverarbeitung im Inland oder in einem Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR) vornimmt.[450] Die Nutzung von Cloud-Diensten im außereuropäischen Raum ist damit eine Übermittlung i.S.d. § 3 Abs. 4 Nr. 3 BDSG und bedarf auf der ersten Stufe einer Rechtsgrundlage, § 4 Abs. 1 BDSG. Darüber hinaus gilt es auf der zweiten Stufe die Anforderungen der §§ 4b, 4c BDSG zu erfüllen.[451]

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG wird von den Aufsichtsbehörden als Rechtsgrundlage dann anerkannt, wenn zwischen Cloud-Anwender und Cloud-Anbieter im außereuropäischen Raum ein Vertrag entsprechend den Anforderungen des § 11 Abs. 2 BDSG geschlossen wird; dann könne die Abwägung zugunsten der Datenübermittlung ausfallen.[452] Im Schrifttum wird eine Legitimation über § 28 Abs. 1 Satz 1 Nr. 2 BDSG jedoch teilweise kritisch gesehen.[453] Da andererseits eine Einwilligung entsprechend der Anforderungen des § 4a BDSG aufgrund der Masse der Betroffenen regelmäßig als nicht praktikabel erscheint, schiede dann eine Auslagerung personenbezogener Daten in außereuropäische Clouds gänzlich aus. Für die Übermittlung besonderer Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG, wie beispielsweise Gesundheitsdaten, kann § 28 Abs. 1 Satz 1 Nr. 2 BDSG nicht als Legitimationsgrundlage dienen.[454] Da die strengen Voraussetzungen der §§ 28 Abs. 6-9, welche die Übermittlung besonderer Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG regeln, bei

---

447 *Becker* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 343 (358); für eine Privilegierung verschlüsselter Daten *de lege ferenda* sprechen sich *Kühling/Biendl,* CR 2014, 150, 155 aus.

448 *Kroschwald/Wicker,* CR 2012, 758 (760).

449 *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 91.

450 U.a. *Selzer,* DuD 2014, 470 (471); *Schantz* in Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 12. Edition Stand: 01.11.2014, BDSG § 4b, Rn. 13; so auch die Einschätzung der Aufsichtsbehörden, vgl. Orientierungshilfe – Cloud Computing, S. 16, Fn. 401.

451 Zu dieser zweistufigen Prüfung vgl. *Gola/Klug/Körffer* in Gola/Schomerus, Bundesdatenschutzgesetz, 12. Aufl. 2015, § 4b, Rn. 6.

452 Vgl. Orientierungshilfe – Cloud Computing, S. 16; *Selzer,* DuD 2014, 470 (472).

453 *Becker* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 343 (355).

454 Vgl. Orientierungshilfe – Cloud Computing, S. 16; *Becker* in Taeger, Law as a Service, Tagungsband DSRI-Herbstakademie 2013, S. 343 (355).

Cloud Diensten in den allermeisten Fällen nicht erfüllt sein dürften, besteht in diesem Bereich eine erhebliche Einschränkung der Nutzbarkeit von Cloud-Diensten.

Eine Lösung könnte dadurch erreicht werden, dass diejenigen Cloud-Anbieter mit Sitz in einem Drittstaat mit angemessenem Datenschutzniveau ebenfalls als Auftragsdatenverarbeiter i.S.d. § 3 Abs. 8. S 3 BDSG anerkannt werden. Dies wird teilweise bereits vertreten, indem § 3 Abs. 8 S. 3 BDSG richtlinienkonform ausgelegt wird, da die Datenschutz-Richtlinie eine Beschränkung auf Auftragnehmer innerhalb des EWR nicht vorsieht.[455] Eine Chance bietet auch hier die geplante Datenschutz-Grundverordnung, nach der eine Privilegierung der Auftragsdatenverarbeitung auch beim Einsatz außereuropäischer Cloud-Anbieter in Betracht kommen kann.[456] Andererseits kann eine praktische Lösung dadurch erreicht werden, dass innereuropäische Clouds gefördert und gestärkt werden, sodass europäische Unternehmen nicht mehr auf außereuropäische Cloud-Anbieter zurückgreifen müssten.

Auf einer zweiten Stufe kommt es im Rahmen der Anforderungen der §§ 4b, 4c BDSG zunächst darauf an, ob in dem Drittland ein dem europäischen Datenschutz entsprechendes Datenschutzniveau besteht, § 4b Abs. 2 BDSG. Ist ein solches nicht vorhanden, besteht die Möglichkeit einer Legitimation über § 4c BDSG. Da ein Ausnahmetatbestand des § 4c Abs. 1 BDSG selten erfüllt sein wird,[457] verbleibt regelmäßig nur die Möglichkeit ‚ein angemessenes Datenschutzniveau über vertragliche Regelungen herzustellen, § 4c Abs. 2 BDSG. Dies kann zum einen durch die Verwendung der EU-Standardvertragsklauseln der Europäischen Kommission geschehen[458]. In diesem Zusammenhang ist jedoch umstritten, ob zusätzlich die Anforderungen des § 11 Abs. 2 BDSG in der vertraglichen Vereinbarung abzubilden sind.[459] Dies ist empfehlenswert, da die Aufsichtsbehörden auf eine Einhaltung bestehen.[460]. Erfolgt die Auslagerung innerhalb eines Unternehmenskonzerns, kann die Herstellung eines angemessenen Datenschutzniveaus zum anderen durch die Verwendung sog. Binding Corporate Rules erreicht werden.[461]

Für U.S.-amerikanische Cloud-Anbieter bestand darüber hinaus die Möglichkeit einer Safe-Harbor-Zertifizierung bei der US-amerikanischen Federal Trade Commission (FTC). Aufgrund der Entscheidung der Kommission 2000/520/EG galt ein angemessenes Datenschutzniveau bei US-Unternehmen, welche diese Zertifizierung innehatten. Durch die Entscheidung des EuGH vom 06.10.2015 ist diese Möglichkeit entfallen. In seinem Urteil hat der EuGH diese Kommissionsentscheidung 2000/520/EG für unwirksam erklärt. Hauptargument des EuGH war dabei, dass die Safe-Harbor-Zertifizierung von US-Unternehmen für US-Behörden keine

---

455 *Funke/Wittmann,* ZD 2013, 221 (228); a.A. u.a. *Dammann* in Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 3, Rn. 246.

456 *Koós/Englisch*, ZD 2014, 276 (278).

457 *Selzer,* DuD, 2012, 470 (472).

458 Vgl. Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, 2010/87/EU, ABl. EU L 39 vom 12.2.2010, S. 5.

459 *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 75.

460 Orientierungshilfe – Cloud Computing, S. 16, 17, 19, Fn. 401.

461 *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 78.

Bindungswirkung habe und vielmehr Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen der Vereinigten Staaten Vorrang vor der Safe-Harbor-Regelung hätten. Die generelle Zugriffsmöglichkeit von US-Behörden auf elektronische Kommunikation sei mit der EU-Grundrechtscharta nicht vereinbar. Eine ausreichende Information der Betroffenen über etwaige Zugriffe von US-Behörden sei ebenso wenig sichergestellt wie ein wirksamer gerichtlicher Rechtsschutz, was ebenfalls der EU-Grundrechtscharta widerspräche. Schließlich habe die Kommission durch ihre Entscheidung die Befugnisse der nationalen Datenschutzbehörden in unzulässiger Weise eingeschränkt. Damit ist die Herstellung eines angemessenen Schutzniveaus für den Datenexport aufgrund einer Safe Harbor Zertifizierung nicht mehr möglich, und es muss auch für die USA auf die oben geschilderten Möglichkeiten der EU-Standardvertragsklauseln, Binding Corporate Rules oder Einwilligungen der Betroffenen zurückgegriffen werden.[462]

Die Einschaltung von Subunternehmern erhöht die Komplexität beim Datenverkehr mit Drittländern weiter. Hat der Cloud-Anbieter seinen Sitz im EWR oder in einem Drittstaat mit angemessenem Schutzniveau, der Subunternehmer jedoch in einem Drittland ohne entsprechendes Schutzniveau, so fordern die Aufsichtsbehörden den Abschluss von EU-Standardvertragsklauseln direkt zwischen dem Cloud-Anwender und Subunternehmer.[463] Je nach Anzahl der Subunternehmer, kann dies wieder zu einem erheblichen – teils prohibitiven – Verwaltungsaufwand führen, der durch die Nutzung der Cloud-Dienste aber gerade vermieden werden soll.

d) Zugriff ausländischer Behörden auf Daten in der Cloud

Ein weiteres Problem sind die insbesondere in den USA bestehenden gesetzlichen Ermächtigungen nationaler Sicherheitsbehörden datenverarbeitende Unternehmen auf die Herausgabe von Daten in Anspruch zu nehmen.[464] Das deutsche bzw. das europäische Datenschutzrecht untersagt jedoch diese Datenweitergabe.[465] Eine Lösung dieses Dilemmas muss – gerade mit Blick auf die Safe-Harbor-Entscheidung des EuGH – über internationale Vereinbarungen gefunden werden.

II. Das deutsche AGB-Recht

Ein weiteres Problemfeld im Rahmen des Cloud Computing stellt das deutsche AGB-Recht dar. Da es sich bei der Cloud-Nutzung mittlerweile um ein Massengeschäft handelt, sind

---

[462] Entscheidung des EuGH vom 06.10.2015, EuGH C-362/14 – Safe Harbor; vereinzelt wird nun in diesem Zusammenhang darüber hinaus die Ansicht vertreten, dass eine Datenübermittlung in die USA aufgrund einer Einwilligung oder aufgrund von EU-Standardvertragsklauseln nicht mehr in Betracht kommen soll, vgl. Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2016, C-362/14 vom 14.10.2015.

[463] Orientierungshilfe – Cloud Computing, S. 15, Fn. 401.

[464] Vgl. hierzu *Bräutigam/Thalhofer* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 14, Rn. 97.

[465] Orientierungshilfe – Cloud Computing, S. 20, Fn. 401.

standardisierte Vertragsklauseln an der Tagesordnung. Verwender i.S.d. § 305 Abs. 1 BGB ist dabei regelmäßig der Cloud-Anbieter.

1. Vertragliche Flexibilität als Voraussetzung für Cloud Computing – Grenzen des AGB-Recht bei Änderungen der angebotenen Leistungen

Zentraler Vorteil, den die Nutzung von Cloud-Diensten mit sich bringt, ist die damit einhergehende Flexibilität für die Unternehmen. Gerade diese Flexibilität wird jedoch durch das deutsche AGB-Recht erheblich eingeschränkt. § 308 Nr. 4 BGB kann es den Cloud-Anbietern erschweren, die vertraglichen Leistungen bedarfsgerecht und entsprechend der technischen Entwicklungen zu verändern. Danach ist eine Vereinbarung eines Rechts des Verwenders, die versprochene Leistung zu ändern oder von ihr abzuweichen, unwirksam, wenn nicht die Vereinbarung der Änderung oder Abweichung unter Berücksichtigung der Interessen des Verwenders für den anderen Vertragsteil zumutbar ist. Erfasst werden nicht nur Änderungen der Hauptleistung, sondern auch vertraglicher Nebenleistungen,[466] so dass beispielsweise auch der Einsatz eines den neusten technischen Anforderungen entsprechenden Sicherungsprogramms durch den Cloud-Anbieter unter die Vorschrift fallen würde. Im B2B Bereich gilt die Norm gem. § 310 Abs. 1 Satz 1 BGB zwar nicht unmittelbar, jedoch wendet die Rechtsprechung die Regelung sinngemäß an.[467] Eine einseitige Änderung kommt damit nur in Betracht, wenn die Klausel transparent ist, auf Seiten des Cloud-Anbieters kein schutzwürdiges Interesse gerade an der Erbringung der vereinbarten Leistung besteht, der Cloud-Anbieter einen erheblichen Grund für die Änderung hat und der Änderungsvorbehalt das Verhältnis zwischen Leistung und Gegenleistung berücksichtigt.[468] Diese Formel ist gefüllt mit unbestimmten Rechtsbegriffen und hat damit zur Folge, dass etwa bei Änderungsklauseln keine Rechtssicherheit besteht.

2. Strenge Anforderungen an Haftungsklauseln

Auch die Möglichkeit einer Haftungsbeschränkung ist erheblich eingeschränkt. Zwar gilt § 309 Nr. 7 BGB nicht unmittelbar für den B2B Bereich, dennoch stellt die Rechtsprechung hier über § 307 Abs. 1, 2 BGB vergleichbare Anforderungen.[469]

Ein Haftungsausschluss kommt danach nur für leichte Fahrlässigkeit in Betracht, § 307 Abs. 2 Nr. 1 i.V.m. § 276 Abs. 3 BGB sowie § 309 Nr. 7b BGB. Dies gilt jedoch nicht für den Fall der Verletzung von Körper, Leben und Gesundheit, § 309 Nr. 7a BGB. Nach der Rechtsprechung kann die Haftung für leichte Fahrlässigkeit auch nicht für die Verletzung von sog. Kardinalpflichten ausgeschlossen werden; das sind solche Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Ein-

---

[466] *Becker* in Bamberger/Roth, Beck'scher Online-Kommentar BGB, Edition 35, Stand: 01.05.2015, § 308 Nr. 4, Rn. 6.

[467] U.a. BGH, Urteil vom 21.12.1983 – VIII ZR 195/82, NJW 1984, 1182.

[468] *Becker* in Bamberger/Roth, Beck'scher Online-Kommentar BGB, Edition 35, Stand: 01.05.2015, § 308 Nr. 4, Rn. 40.

[469] *Bräutigam* in Bräutigam, IT-Outsourcing und Cloud-Computing, 3. Aufl. 2013, Teil 13, Rn. 201.

haltung der Vertragspartner regelmäßig vertrauen darf.[470] Möglich ist in diesem Bereich der vertragswesentlichen Pflichten lediglich eine Begrenzung der Haftung auf typischerweise vorhersehbare Schäden,[471] wobei die Rechtsprechung den Begriff der Vorhersehbarkeit aber weit interpretiert.

Ordnet man die Nutzung von Cloud-Diensten vertragstypologisch als Mietvertrag ein, so kann der Cloud-Anbieter immerhin die nach § 536a Abs. 1 BGB gesetzlich vorgeschriebene Garantiehaftung ausschließen.[472] Ein Ausschluss der Haftung wegen leichter Fahrlässigkeit kommt aber auch hier nicht in Betracht, wenn dies zu einer Aushöhlung wesentlicher Vertragspflichten führt.[473]

Mit den unbestimmten Rechtsbegriffen der Kardinalpflichten bzw. der vorhersehbaren Schäden besteht eine erhebliche Rechtsunsicherheit. Beim Cloud Computing werden in jedem Fall die Verfügbarkeit des Services sowie die Sicherung vor Datenverlust zu den Kardinalpflichten gezählt und von den typischerweise vorhersehbaren Schäden ein Gewinnausfall sowie die Kosten für die Datenrekonstruktion erfasst.[474] Dies führt im Massengeschäft des Cloud Computing zu einem kaum überschaubaren und kalkulierbaren Haftungsrisiko für die Cloud-Anbieter, das schnell existenzbedrohend sein kann.[475]

Auch die grundsätzlich zu empfehlenden detaillierten Leistungsbeschreibungen können hier keine sichere Lösung bieten. Zwar sind reine Leistungsbeschreibungen gem. § 307 Abs. 3 Satz 1 BGB kontrollfrei. Jedoch gilt auch hier das Transparenz-Gebot, § 307 Abs. 3 Satz 2 BGB. Die von Internetdienstleistern oft verwendeten pauschalen „as is"-Klauseln, wonach der Dienst nur in der jeweils aktuell verfügbaren Form zur Verfügung gestellt wird, sind daher in jedem Fall unzulässig. Darüber hinaus besteht die Gefahr, dass solche Leistungsbeschreibungen als Einschränkung der vertraglich versprochenen Leistung und damit wieder als unzulässige Haftungsbeschränkungen eingeordnet werden.[476]

Aufgrund des erheblichen Risikos besteht zumindest im B2B Bereich zu befürchten, dass hier eine Rechtswahl weg vom deutschen Recht erfolgt.

---

[470] So die ständige Rechtsprechung, vgl. u.a. BGH, Urteil vom 20.07.2005 – VIII ZR 121/04, NJW-RR 2005, 1496, (1505).

[471] *Wurmnest* in Münchener Kommentar zum BGB, 6. Aufl. 2012, § 309 Nr. 7, Rn 30.

[472] Zur grundsätzlichen Abdingbarkeit auch in AGB vgl. *Ehlert* in Bamberger/Roth, Beck'scher Online-Kommentar BGB, § 536a, Rn. 36a.

[473] BGH, Beschluss vom 24.10.2001 – VIII ARZ 1/01, NJW 2002, 673.

[474] *Wicker,* MMR 2014, 787 (788).

[475] *Wicker,* MMR 2014, 787 (788).

[476] Vgl. zu dieser insbesondere im Rahmen von Verfügbarkeitsregelungen schwierigen Abgrenzung *Redeker* in Hoeren/Sieber/Holznagel, Multimedia-Recht, 41. Ergänzungslieferung März 2015, Teil 12, Rn. 23.

III. Chancen vertraglicher Lösungen gegenüber gesetzlichen Ansätzen und konzertierter Abstimmung der Datenschutzaufsichtsbehörden

Eine ausgewogene vertragliche Lösung erscheint im Bereich des Cloud Computing oft problematisch, da häufig eine unterschiedliche Verhandlungsmacht besteht. Insbesondere kleine und mittelständische Unternehmen werden sich schwer gegenüber den großen Cloud-Anbietern durchsetzen können.

Dagegen besteht auf Behördenebene eine hohe Kompetenz im Bereich der Cloud-Dienste. Mit der Orientierungshilfe Cloud-Computing steht den Cloud-Anwendern eine praxistaugliche Leitlinie zur Hand. Gleiches gilt für die Stellungnahme der Art. 29-Datenschutzgruppe. Durch die geplante Datenschutzgrundverordnung ist weitere Besserung in dem Bereich in Sicht, da – zwar noch nicht in ausreichendem Maße – den Bedürfnissen der modernen IT-Nutzung Rechnung getragen wird. Mit Spannung abzuwarten bleiben auch die Ergebnisse der Initiativen „freier Datenfluss (insbesondere zwischen Cloud-Anbietern“ und „europäische Cloud“, die die europäische Kommission im Jahr 2016 vorschlagen wird.[477]

Handlungsbedarf von gesetzgeberischer Seite besteht indes im Hinblick auf die Möglichkeit, besondere Arten personenbezogener Daten in der Cloud zu verarbeiten. Auch die Friktionen, die durch die Zugriffsbefugnisse ausländischer Behörden, z. B. der USA, verursacht werden, bedürfen einer Lösung im internationalen Diskurs. Schließlich bietet das deutsche AGB-Recht Hemmnisse für Cloud-Anbieter, wobei dieses Thema natürlich auch in anderen Wirtschaftszweigen Auswirkungen hat und daher in einem größeren Kontext zu betrachten ist.

[477] Europäische Kommission, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_de.pdf S. 17

Teil 11 Vertragsrecht *(Tilmann Walz)*

Autonom kommunizierende Maschinen und Bauteile, Fertigungsstraßen die sich dynamisch je nach Bedarf umbauen und bis hin zur Losgröße „1“ produzieren, werfen die Frage auf, ob die heutigen Regelungen im Bürgerlichen Gesetzbuch („BGB“) ausreichen, um die Herausforderungen der Industrie 4.0 zu bewältigen. Im Folgenden werden der Vertragsschluss und seine Voraussetzungen im Lichte autonomer Systeme (I.) und die Eignung bestimmter Vertragstypen im Rahmen der Massenproduktion von Unikaten beleuchtet (II.). Sodann erfolgt im Hinblick auf die Notwendigkeit eines digitalen Binnenmarktes in Europa eine Auseinandersetzung mit der Digitalen Strategie der EU Kommission sowie dem Erfordernis einer europäischen Rechtsvereinheitlichung (III.).

I. Vertragsschluss

Die „Automatisierung“ basiert aktuell auf vordefinierten Prozessen, die die Grenzen für technische Systeme festlegen. Aufgrund der Digitalisierung ist eine „Autonomisierung“ der Systeme zu erwarten, d. h. künstlich intelligente Systeme, die ihre Funktionalität über die ursprüngliche Intention des Nutzers hinaus verändern und so eine gewisse Eigenständigkeit besitzen.[478] Fraglich ist, wie Erklärungsakte autonomer Systeme behandelt werden müssen.

1. „Willenserklärungen“ von autonomen Systemen

Gegenwärtig sind natürliche und juristische Personen Rechtsubjekte, d. h nur sie sind rechtsfähig, können also Träger von Rechten und Pflichten sein.[479] Autonome Systeme sind de lege lata nicht rechtsfähig.[480] Sie können daher auch keine rechtserheblichen Erklärungen abgeben, vielmehr müssen etwaige Erklärungsakte von der Willenserklärung einer natürlichen Person umfasst sein.

2. Zurechnung elektronischer Erklärungsakte zur Willenserklärung

Automatisch erzeugte Erklärungsakte, denen eine Dateneingabe durch eine natürliche Person vorangeht (automatisierte Willenserklärungen), werden heute als Willenserklärungen anerkannt.[481]

Die Computererklärung hingegen wird von einer Software ohne aktuellen menschlichen Beitrag selbsttätig erzeugt, wobei die maßgeblichen Parameter durch den Menschen gesetzt werden.[482] Die Zurechnung solcher Computererklärungen kann nicht über Ansätze wie

---

478 *Kirn/Müller-Hengstenberg*, MMR 2014, 225 (226).

479 So h. M.: vgl. *Saenger* in Erman, BGB, 14. Aufl. 2014, Vor § 1 Rz. 1; *Kannowski* in Staudinger, BGB, Neubearbeitung 2013, Vor § 1 Rz. 1, § 1 Rz. 1.

480 Vgl. *Bräutigam/Klindt*, NJW 2015, 1137; *Spindler* in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Vor §§ 116 BGB Rz. 9; ausführlich *Sorge*, Softwareagenten, 2006, S. 33 ff.

481 *Spindler* in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Vor §§ 116 BGB Rz. 5; *Busche* in Münchener Kommentar, BGB, 6. Aufl. 2012, Vor § 145 Rz. 38.

482 *Mehrings*, MMR 1998, 30 (31); *Cornelius*, MMR *2002*, 353 (354); *Spindler* in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015 Vor §§ 116 BGB Rz. 6.

das Angebot „ad incertas personas“ oder eine Vertreterstellung erfolgen,[483] sondern muss über die Reichweite der initialen Willenserklärung des Nutzers der Computererklärungen gelöst werden. Die Willenserklärung kann zunächst im gestreckten arbeitsteiligen Prozess erstellt werden.[484] Durch den bewussten Einsatz der Software besteht der für die Willenserklärung erforderliche Handlungswille. Die rechtliche Bindung beruht dann auf dem Erklärungswillen, die Software zur Ausfüllung der initialen Willenserklärung zu nutzen, dabei aber auf eine konkrete Kontrolle zu verzichten.[485]

3. Zurechnung autonomer Erklärungsakte zur Willenserklärung

Erklärungen autonomer Systeme unterscheiden sich von der Computererklärungen dadurch, dass sie aufgrund der Autonomie des Systems die menschlich gesetzten Parameter verlassen können.[486] Die Frage bleibt indes gleich: erfasst die initiale Willenserklärung auch dann alle weiteren (autonomen) Erklärungen?

Bei Softwareagenten, die ohne Vorgabe der Lösung durch korrekte mathematische Gesetzmäßigkeiten geleitet werden, soll dies verneint werden, weil „Lösungsfehler“ keine Funktionsmängel und für den Nutzer nicht vorhersehbar seien.[487] Dies ändert aber nichts am Handlungs- und Erklärungswillen des Nutzers. Dass Lösungsfehler trotz Befolgung mathematisch korrekter Gesetzmäßigkeiten zu erwarten sind, zeigt zudem gerade, dass diese nicht außerhalb jeder Wahrscheinlichkeit liegen. Wie bei Computererklärungen dürften derartige Erklärungsakte daher von der initialen Willenserklärung des Nutzers umfasst sein.[488]

Ein Vertragsschluss über Erklärungsakte von autonomen Systemen kann daher weiterhin mit den bestehenden Mitteln des BGB, also durch übereinstimmende initiale Willenserklärungen der Nutzer, begründet werden. In diesem Zusammenhang diskutierte Probleme, wie die Rückverfolgbarkeit autonomer Erklärungsakte oder die Unvermeidbarkeit von Lösungsfehlern,[489] sind indes nicht im Rahmen der Reichweite der Willenserklärung zu verorten, sondern müssen durch regulatorische Vorgaben und Haftungskonzepte bewältigt werden.

4. Rechtsfähigkeit autonomer Systeme: „ePerson“

Ausgehend von vorstehenden Erwägungen, ist die eigene Rechtssubjektivität autonomer Systeme[490] („ePerson“) eher vor dem Hintergrund eines adäquaten Umgangs mit Risiken als

---

[483] *Müller-Hengstenberg/Kirn*, MMR 2014, 307 (308 f.) – zum Meinungsstand; *Cornelius*, MMR 2002 353, (354 f.); *Bräutigam/Klindt*, NJW 2015, 1137 – zur Ablehnung der Stellvertretung.

[484] *Cornelius*, MMR 2002, 353 (355); *Spindler* in Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, Vor §§ 116 BGB Rz. 6.

[485] Vgl. *Cornelius*, MMR 2002, 353 (355); *Mehrings*, MMR 1998, 30 (31).

[486] Vgl. *Kirn/Müller-Hengstenberg*, MMR 2014, 225 (226).

[487] So wohl *Müller-Hengstenberg/Kirn*, MMR 2014, 307 (311).

[488] Nur *Cornelius*, MMR 2002, 353 (356).

[489] *Müller-Hengstenberg/Kirn*, MMR 2014, 307 (311).

[490] Vgl. *Gruber* in Beck, Jenseits von Mensch und Maschine, 2012, S. 133 ff.; *Sorge*, Softwareagenten, 2006, S. 33 ff.; *Wettig/Zehendner*, 2003, The electronic Agent: A Legal Personality under German Law.

im Zusammenhang mit Willenserklärungen zu diskutieren, wenngleich nicht stets punktgenau abgegrenzt werden kann.

a) Status quo

Autonome Systeme sind nicht rechtsfähig.[491] Auch eine Gesetzesanalogie zur juristischen Person wird bereits an der Vergleichbarkeit der Sachverhalte[492] scheitern. Während für die juristische Person unmittelbar natürliche Personen handeln, liegt diese Unmittelbarkeit bei autonomen Systemen gerade nicht vor. Angesichts der Vielzahl juristischer Personen wäre auch eine völlige Rechtsunsicherheit bezüglich der tatsächlich analog anzuwenden Vorschriften zu erwarten. Auch für die ePerson dürfte daher gelten, dass der Inhalt der (juristischen) *Persönlichkeit* im Gesetz festgestellt bzw. verliehen werden muss.[493]

b) „ePerson“ de lege ferenda

Die gesetzliche Kodifizierung einer „ePerson“ wäre zu empfehlen, wenn die rechtliche Handhabung vereinfacht würde. Einige der Probleme, an welchen Lösungsansätze „de lege lata“ scheitern, könnten so sicherlich über ähnliche Mechanismen wie bei der juristischen Person[494] in den Griff bekommen werden. Über die Mindestkapitalisierung einer „ePerson“ könnte zumindest grundsätzlich eine originäre Haftungsmasse gesichert werden,[495] die angesichts der globalen Vernetzung und der exponentiellen Risikosteigerung sicherlich entsprechend hoch sein müsste. Für andere Aspekte, wie die faktischen Probleme bei der Rückverfolgbarkeit oder die ggf. objektiv unmögliche Schadensprävention im Rahmen der Haftung, bedürfte es ggf. weiterer Rechtssetzungsakte, z. B. in Bezug auf eine Gefährdungshaftung oder der Entwicklung von Risikosphären.[496]

c) Ausblick

Aus ökonomischer Sicht ist zu bezweifeln, ob die „ePerson“ geeignet ist Transaktionskosten – wie die juristische Person[497] – zu senken. Jedenfalls mittelfristig dürften die Kosten im Zusammenhang mit den Rechtsunsicherheiten bei Einführung einer neuen Rechtspersönlichkeit steigen. Vor allem aber ist die „ePerson“ kein „Allheilmittel“, weshalb vor einer so weitreichenden Änderung hinreichend sicher sein muss, dass Lösungen nicht auch durch punktuelle gesetzliche Maßnahmen erzielt werden können.

---

[491] Vgl. oben unter I. 1., Fußnote 480.

[492] Siehe hierzu näher *Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991, S. 381 ff.

[493] Motive zu dem Entwurfe eines bürgerlichen Gesetzbuches für das Deutsche Reich, Bd. I, Allgemeiner Theil, 2. Aufl. 1896, S. 78; h. M.: vgl. *Westermann* in Erman, BGB, 14. Aufl. 2014, Vor § 21 Rz. 2; *Reuter* in Münchener Kommentar, BGB, 6. Aufl. 2012, Vor § 21 Rz. 2.

[494] Vgl. *Wettig/Zehendner*, 2003, The electronic Agent: A Legal Personality under German Law, IV. 4.

[495] Vgl. *Gruber* in Beck, Jenseits von Mensch und Maschine, 2012, S. 156.

[496] Vgl. BGH, Urt. v 11.03.2009 – I ZR 114/06 – juris Rz. 18 = MDR 2009, 879 (880) – Halzband; vgl. *Bräutigam/Klindt*, NJW 2015, 1137 (1139); vgl. näher oben unter Teil 7II.1.a), d), 3., IV. (zur Produkthaftung).

[497] Vgl. *Sorge*, Softwareagenten, 2006, S. 35.

II. Vertragstypen

Das BGB regelt explizit verschiedene Vertragstypen und berücksichtigt dabei die jeweiligen wirtschaftlichen Bedürfnisse.[498] Das Zivilrecht kennt darüber hinaus weitere, atypische Verträge, die Elemente verschiedener Vertragstypen umfassen (z. B. sog. typengemischte Verträge).[499] Bereits heute kann daher weitgehend flexibel auf Änderungen der ökonomischen Umwelt reagiert werden.

1. Das Unikat als standardisiertes Produkt

Die digitalisierte Produktion wird die Fertigung von Unikaten nach Kundenwunsch als standardisiertes (Massen-)Produkt ermöglichen. Können diese ökonomischen Veränderungen mit den Vertragstypen des Kauf-, Werk- oder Werklieferungsvertrag oder nur über atypische Verträge abgebildet werden?

a) Werksvertragliche Qualifikation aufgrund der Individualisierung

Werk- und Kaufvertragsrecht sollen für die von ihnen umfassten Sachverhaltskonstellationen die Grundlage für einen angemessene Interessensausgleich der Parteien bilden. Die Differenzierung erfolgt danach, ob die Pflicht zur Eigentumsübertragung oder die Herstellungspflicht überwiegt.[500] Die Herstellungspflicht muss dabei über den rein technischen Herstellungsvorgang hinausgehen und jedenfalls weitere Leistungen (z. B. Planungs-, Konstruktions- oder Integrationsleistungen) von erheblichem Gewicht enthalten.[501] Angesichts der Individualität und damit zumeist verbundenen Komplexität von Werken wird – im Unterschied zum Kaufrecht – dem Besteller z. B. über die Abnahme eine Testphase[502] und dem Hersteller z. B. das Nacherfüllungswahlrecht[503] eingeräumt.

Im Rahmen der Industrie 4.0 wird die konzeptionelle Einflussnahme des Kunden und die damit verbundene Individualisierung steigen. Aufgrund der Möglichkeiten der digitalen (Massen-)Produktion wird dies jedoch keine über die technische Herstellung maßgeblich hinausgehende Leistungen erfordern, weshalb die Maßstäbe des Werkvertragsrechts nicht passend wären. Soweit hier – insb. im B2B-Bereich – Zweifelsfälle bestehen, können die bestehenden Abgrenzungskriterien weiterhin herangezogen werden.

---

498 Vgl. nur §§ 434 ff. BGB im Kaufrecht im Gegensatz zu §§ 633 ff. BGB im Werkvertragsrecht.

499 *Martinek*, Moderne Vertragstypen, Bd. 1, 1991, S. 17 ff.

500 BGH, Urt. v. 22.12.2005 – VII ZR 183/04 – juris Rz. 12, 15 = MDR 2006, 683 (684); Urt. v. 15.04.2004 – VII ZR 291/03 – juris Rz. 11 = MDR 2004, 987 (988).

501 OLG Hamm, Urt. v. 29.10.2012 – I 17 U 130/11 – juris Rz. 36. = NJW-RR 2013, 213 (214); OLG Naumburg, Urt. v. 26.06.2014 – 2 U 131/13 – juris Rz. 56; so wohl auch BGH, Urt. v. 23.07.2009 – VII ZR 151/08 – juris Rz. 21, 25 = MDR 2009, 1155 (1156); Urt. v. 09.02.2010 – X ZR 82/07 – juris Rz. 9.

502 *Leistner*, JA 2007, 81 (84); siehe auch § 640 Abs. 1 Satz 3 BGB.

503 Siehe § 635 Abs. 1 BGB.

b) Interessengerechte Lösung durch das Kaufrecht

Die Interessenslagen der Parteien bei Produktion von Unikaten im Wege eines standardisierten (Massen-)Produktionsverfahrens kann im Wesentlichen über das Kaufrecht abgebildet werden. Die Lieferung herzustellender beweglicher Sachen (sog. „Werklieferungsvertrag“) wird bereits heute dem Kaufrecht zugeordnet und nur bei beweglichen, nicht vertretbaren Sachen um werkvertragliche Normen ergänzt.[504]

Das „massenhaft“ hergestellte Unikat wird regelmäßig werkvertragliche Qualifikationskriterien trotz Individualität nicht aufweisen. Die generelle Anknüpfung an den Gefahrübergang anstelle der Abnahme ist daher wertungstechnisch ebenso passend wie die Anwendung von Untersuchungs- und Rügeobliegenheiten (§ 377 HGB), letztere insbesondere vor dem Hintergrund der zu erwartenden Transaktionsgeschwindigkeit. Kann ein Produkt künftig in Losgröße „1“ ebenso wirtschaftlich wie heute in der Massenproduktion hergestellt werden, ist auch eine vom Kunden im Rahmen seines Nacherfüllungswahlrechts geforderte „Ersatzlieferung“ nicht mehr unangemessen.

Die ergänzende Anwendung werkvertraglicher Vorschriften wird davon abhängen, ob standardisiert produzierte Unikate weiterhin als „nicht vertretbare“ Sache i. S. d. §§ 651 Satz 3, 91 BGB zu werten sind. Da Unikate eine individuelle Prägung haben,[505] scheint diese Annahme offensichtlich. Der Grund für die Einbeziehung werkvertraglicher Vorschriften war aber, dass den möglichen Änderungen während des Herstellungsprozesses[506] und wohl auch der fehlenden anderweitigen Absetzbarkeit von vertretbaren Sachen Rechnung getragen werden sollte. Können Unikate aber ebenso schnell und kostengünstig wie Massenprodukte herstellt werden, passen diese Überlegungen und damit die Anwendung werkvertraglicher Vorschriften ggf. nicht mehr. Ob bzw. inwieweit darüber hinaus im B2C-Bereich die Verantwortlichkeit i. S. d. § 645 Abs. 1 Satz 1 BGB für erteilte Anweisungen – oder eher Wünsche – des Kunden im Lichte des „überlegenen“ Sachwissen Herstellers bestehen kann, bleibt abzuwarten.

Eines gesetzgeberischen Eingriffs bedarf es indes (noch) nicht. Vielmehr können adäquate Lösungen zunächst durch die richterliche Fortentwicklung des Begriffs „nicht vertretbare Sache“ anhand der sich mit dem Grad der Industrialisierung 4.0 voraussichtlich ändernden Verkehrsanschauung gefunden werden.

---

[504] BGH, Urt. v. 23.07.2009 – VII ZR 151/08 – juris Rz. 8 = MDR 2009, 1155; *Busche* in Münchener Kommentar, BGB, 6. Aufl. 2012, § 651 Rz. 16.

[505] Vgl. BGH, Urteil vom 30.06.1971 – VIII ZR 39/70 = MDR 1971, 837; *Peters/Jacoby* in Staudinger, BGB, Neubearbeitung 2014, § 651 Rz. 17; *Busche* in Münchener Kommentar, BGB, 6. Aufl. 2012, § 651 Rz. 17.

[506] BR-Drucks. 338/01 (Beschluss) v. 13.07.2001, Ziff. 137 – Stellungnahme des Bundesrates zum Entwurf eines Gesetzes zur Modernisierung des Schuldrechts.

2. Smart Products

Smart Products werden hier als Produkte verstanden, deren Funktion durch serverbasierte Zusatzdienste erweitert wird.[507] Fraglich ist, wie die steigende Prägung der Produkte durch Dienste rechtlich erfasst werden kann.

a) Personenidentität von Verkäufer und Dienstanbieter

Im B2B-Bereich dürften Hardware- und Serverdienstkomponente häufig aus einer Hand angeboten werden. Der Gesamtvertrag könnte nach dem Schwerpunkt, z. B. als Kaufvertrag qualifiziert werden.[508] Ist dies nicht möglich, bliebe eine Differenzierung nach kauf- und dienstvertraglichen Elementen.

Beide Komponenten werden bei Smart Products jedoch so verwoben sein, dass eine Abgrenzung kauf- und dienstvertraglicher Elemente zunehmend erschwert wird. Es ist zu erwarten, dass die Leistungspflicht gleichzeitig Elemente verschiedener Vertragstypen enthält und der Vertrag demnach als Typenkombinationsvertrag behandelt werden muss.[509] Können Leistungsstörungen nicht einem der kombinierten Typen zugeordnet werden, wird die maßgebliche Regelung zumeist teleologisch anhand des Vertragszwecks zu bestimmen sein.[510]

b) Personenverschiedenheit von Verkäufer und Dienstanbieter

Komplexer werden die Vertragsbeziehungen, wenn Händler am Absatz des Produktes beteiligt sind. Sowohl die Hardware als auch die Dienste ließen sich ggf. über einen Kaufvertrag zwischen Kunde und Händler abbilden.[511] Die Beschaffenheit als Maßstab für die Mängelrechte umfasst auch Bezüge der Sache zu ihrer Umwelt, soweit eine Anknüpfung zu physischen Merkmalen besteht.[512] Dies wird i. d. R. der Fall sein, wenn eine Funktion des (physischen) Produkts z. B. durch Abschalten des Dienstes beeinträchtigt ist. Erfolgt das Abschalten nach Gefahrübergang, läge nach gegenwärtiger Rechtslage jedoch kein Mangel vor.[513] Problematisch ist ferner die Nacherfüllung bzw. der Regress des Händlers entlang der Lieferkette (§§ 478, 479 BGB). Da der Dienst direkt angeboten wird und anders als die Hardware die Lieferkette gerade nicht durchläuft, würde die Rückabwicklung entlang der Lieferkette die wirtschaftliche Realität ignorieren.

---

[507] Vgl. *Solmecke/Vondrlik*, MMR 2013, 755.
[508] Zur Problematik der Qualifizierung als Kaufvertrag siehe unten unter II. 2 lit. b).
[509] *Larenz/Canaris*, Lehrbuch des Schuldrechts, Bd. II/2, 13. Aufl. 1994, S. 41 ff. (46 ff.); *Martinek*, Moderne Vertragstypen, Bd. 1, 1991, S. 19 ff.
[510] Wohl h. M.: vgl. *Larenz/Canaris*, Lehrbuch des Schuldrechts, Bd. II/2, 13. Aufl. 1994, S. 44, 51; *Kindl* in Erman, BGB, 14. Aufl. 2014, Vor § 311 Rz. 17; kritisch *Martinek*, Moderne Vertragstypen, Bd. 1, 1991, S. 22 ff. (25).
[511] Vgl. *Bräutigam/Klindt*, NJW 2015, 1137 (1138).
[512] BGH, Urt. v. 30.11.2012 – V ZR 25/12 – juris Rz. 10; *Herresthal/Grigoleit*, JZ 2003, 233.
[513] Vgl. *Solmecke/Vondrlik*, MMR 2013, 755 (757); *Bräutigam/Klindt*, NJW 2015, 1137 (1138).

Erfolgt hingegen eine Aufspaltung in einen Kauf- und einen Dienstvertrag erscheint der Händler als Partei des Dienstvertrag ungeeignet,[514] da er die Störung gerade nicht so einfach wie einen Mangel beseitigen könnte. Umgekehrt würde die Entwicklung der Dienste durch den Hersteller beeinträchtigt, soweit die Änderung in das Vertragsverhältnis zwischen Kunden und Händler eingreift.

Zu erwägen ist daher eine Aufspaltung in einen Kaufvertrag mit dem Händler sowie ein Dienstvertrag mit dem Dienstanbieter/Hersteller,[515] der z. B. online bei Erstnutzung des Produkts oder durch den Händler als Vertreter des Herstellers geschlossen wird.[516] Nachteile des Kunden durch die Separierung der Verträge könnten durch Behandlung als einheitliches Rechtsgeschäft analog § 139 BGB entgegnet werden.[517] Ebenso denkbar wäre ein inzidenter Kündigungsverzicht des Dienstanbieters, ggf. ausgerichtet an der Verjährung der Mängelrechte.[518]

c) Gesetzgeberischer Handlungsbedarf

Schon heute bietet das Recht Möglichkeiten, vertragliche Beziehungen bei Smart Products zu regeln, wobei die Ansätze grundsätzlich Lösungen für die Vertragsbeendigung, nicht aber z. B. für die Vertragserfüllung bereithalten. Ob aber eine effiziente Durchsetzung dieser Rechte angesichts der diffizilen Leistungsabgrenzung mit existenten Mitteln gelöst werden kann, oder nicht doch eine gesetzliche Regelung verlangt, wird zu untersuchen sein.

III. Europäische Dimension

Um die Wettbewerbsfähigkeit insb. mit den USA und Asien sicherzustellen, muss der digitale Binnenmarkt einen Rechtsrahmen bereitstellen, der der Transaktionsgeschwindigkeit von autonomen Systemen gewachsen ist und entwicklungshemmende Transaktionskosten und Rechtsunsicherheit beseitigt.

1. Digitale Agenda: Ausreichende Thematisierung der digitalen Produktion?

Die Digitale Agenda[519] und die Arbeitsmaterialien[520] der Kommission befassen sich zumeist mit Online-Handel und Endkundengeschäft, folglich mit Verbraucherrecht und diesbezüglichen Handelshemmnissen.[521] Marktbegebenheiten werden daher i. E. nicht hinsichtlich industrieller Anwendungsszenarien analysiert. Die Auseinandersetzung mit Online-Platt-

---

[514] A. A. wohl *Solmecke/Vondrlik*, MMR 2013, 755.
[515] Für Mobilfunkverträge vgl. *Schöpflin*, BB 1997, 105 und BGH, Urt. v. 08.10.1998 – I ZR 187/97 – juris Rz. 13 = MDR 1999, 49.
[516] Vgl. BGH, Urt. v. 23.03.1988 – VIII ZR 58/87 – juris Rz. 17 = MDR 1988, 669 – Herstellergarantie.
[517] AG Karlsruhe, Urt. v. 12.10.2007 – 12 C 169/07; *Schöpflin*, BB 1997, 105 (111 f.).
[518] *Solmecke/Vondrlik*, MMR 2013, 755 (757).
[519] COM(2015) 192 final v. 06.05.2015 – Strategie für einen digitalen Binnenmarkt für Europa.
[520] SWD(2015) 100 final v. 06.05.2015 – A Digital Single Market Strategy for Europe – Analysis and Evidence.
[521] COM(2015) 192 final v. 06.05.2015, Ziff. 2.1.

formen ist begrüßenswert, orientiert sich jedoch ebenfalls – abgesehen von wenigen industrierelevanten Aspekten wie Preisintransparenz[522] – stark am Endkundengeschäft.

Mit Ausnahme der Interoperabilität befasst sich die Kommission nur peripher mit dem Thema Industrie 4.0 und folglich nicht mit einem rechtlichen Rahmen für grenzüberschreitende digitale Produktionsprozesse,[523] was das Risiko fehlender diesbezüglicher Strukturmaßnahmen birgt. Auch der angekündigte geänderte Rechtsetzungsvorschlag[524] zum Gemeinsamen Europäischen Kaufrecht („GEK") zur Förderung des elektronischen Handels,[525] wird keinen strukturellen Rahmen für die digitale Produktion liefern.

2. Notwendigkeit eines einheitlichen vertragsrechtlichen Rahmens?

Die Geschwindigkeit autonomer Steuerungssysteme bzw. die Echtzeitbeschaffung lassen Transaktionen ohne vorherige Verhandlungen von Verträgen erwarten. Allgemeine Geschäftsbedingungen („AGB") werden sich i. d. R. nivellieren, was – ohne einheitlichen Rechtsrahmen – den Rückgriff nationales Recht erfordert und den Anstieg grenzüberschreitender Transkationen bremsen könnte.

a) Gemeinsames Europäisches Kaufrecht

Das GEK böte diesen Rechtsrahmen, wenn es angesichts der durch die Industrie 4.0 gestellten Herausforderungen geeignet ist, Transaktionskosten zu senken und eine umfassende eine flexible Grundlage zu bilden.

Der Widerstand einiger Mitgliedsstaaten,[526] Erfahrung mit supranationalem Kaufrecht und Opt-out Modellen,[527] die zu erwartenden „Zersplitterung" aufgrund des elektiven Anwendungsbereichs bzgl. Inlandssachverhalten und Großunternehmen,[528] lässt keine umfassende Akzeptanz erwarten.[529] Eine Senkung von Transaktionskosten – soweit sie überhaupt auf Rechtsdifferenzen beruhen – ist daher zweifelhaft.[530] Zudem sind wichtige Aspekte wie z. B. einige Vertragstypen gegenwärtig im GEK nicht bzw. nicht ausreichend berücksichtigt.[531] Trotz des weniger strengen Maßstabes für eine Inhaltskontrolle von AGB lässt die Ausge-

---

522 SWD(2015) 100 final v. 06.05.2015, Ziff. 4.5.
523 http://www.vdma.org/article/-/articleview/7958206.
524 COM(2015) 192 final v. 06.05.2015, Ziff. 2.1.
525 COM(2014) 910 final v. 16.12.2014 – Arbeitsprogramm der Kommission für 2015, Annex 2.
526 Siehe nur Ministry of Justice/BIS – A Common European Sales Law for the European Union – A proposal for a Regulation from the European Commission; BT-Drucks. 17/8000 v. 30.11.2011.
527 *Mankowski*, IHR 2012, 45 (47 ff).
528 Vgl. *Ayad/*Schnell, BB 2012, 1487 (1488); vgl. *Hellwege*, IHR 2012, 221 (222 f.).
529 So auch *Rüfner*, ZJS 2012, 476 (483 f.).
530 Vgl. *O'Cllaghan/Hutt*, IHR 2011,137 (138); *Tamm*, VuR 2012, 3 (10); *Hellwege*, IHR 2012, 221 (222 f., 231); BT-Drucks. 17/8000 v. 30.11.2011, S. 222 ff.
531 Vgl. *Grigoleit*, ZSE 2011, 560 (568); vgl. *Hellwege*, IHR 2012, 221 (223 f.).

staltung befürchten, dass die erforderliche Privatautonomie – z. B. durch Übertragung nationaler Rechtsansichten – nicht ausreichend gewahrt wird.[532]

b) Alternative Vorgehensweise

Das GEK bildet derzeit auch aufgrund seines umfassenden Regelungsanspruchs, der mit einer pragmatischer Ausgestaltung in Konflikt steht,[533] keine geeignete Basis. Rechtsunsicherheiten ließen sich – ihrer Bedeutung als Handelshemmnisse entsprechend – ggf. schon durch „Leitlinien" reduzieren, die rechtsvergleichend nationale und auch europäische Rechtsakte berücksichtigen. Mangels Verbindlichkeit und umfassenden Regelungsanspruchs, könnten sie sich auf Problemfelder der digitalen Wirtschaft konzentrieren,[534] schneller „beschlossen", und so zu Auslegungshilfen für nationale Gerichte werden.

---

[532] Vgl. *Ayad*/*Schnell*, BB 2012, 1487 (1491 f. 1495); vgl. *Hellwege*, IHR 2012, 221 (227, 231); vgl. *Herresthal*, EuZW 2011, 7 (10, 12); vgl. *von Westphalen*, NJOZ 2012, 441 (447).

[533] *Staudenmayer*, NJW 2011, 3491 (3496).

[534] Zu einem fokussierten Ansatz des GEK vgl. *DiMatteo,* JITLP 2012, 222 (235 f.).

Teil 12 Handelsbeschränkungen für Dual-Use-Güter (Dr. Bärbel Sachs)

Industrie 4.0 macht nicht an Ländergrenzen halt. Der Begriff „Industrie 4.0“ steht für eine neue Stufe der Steuerung der gesamten Wertschöpfungskette von Produkten über den gesamten Lebenszyklus hinweg. Es kann mit einer starken Zunahme der Digitalisierung und der Prozessintegration sowohl in horizontaler als auch vertikaler Hinsicht gerechnet werden. Der damit zusammenhängende und von Ländergrenzen weitgehend unabhängige Datenfluss trifft auf ein Exportkontrollrecht, das noch physisch auf nationale oder EU-Außengrenzen abstellt.

Bei Produkten, die der Exportkontrolle unterliegen, setzt das Exportkontrollrecht bei der Ausgestaltung der IT-Architektur der Wertschöpfungskette enge Grenzen (I.). Ähnliche Herausforderungen bestehen für das Produktionsmittel Kryptographie: Aufgrund des mit der Digitalisierung verbundenen zunehmenden Sicherungsbedarfs dürfte in Zukunft der Einsatz von Kryptotechnik stark steigen. Kryptographische Hard- und Software unterliegt allerdings empfindlichen Exportbeschränkungen (II.).

I. Beschränkungen für den Transfer von Software und Technologie nach der EG-Dual Use VO

Das Exportkontrollrecht und insbesondere das Dual-Use-Recht der EU setzen der Digitalisierung der Wertschöpfungskette insbesondere von gelisteten Gütern sprichwörtlich Grenzen (1.). Daneben ist zu berücksichtigen, dass die Grenze zwischen gelisteten und damit der Exportkontrolle unterliegenden und nicht gelisteten Gütern durch den als Mass Customization bezeichneten Prozess zunehmend fließender und damit schwieriger handhabbar werden wird (2.).

1. Digitalisierung der Wertschöpfungskette von der Exportkontrolle unterliegenden Gütern

Bei Produkten, die der Exportkontrolle unterliegen, setzt das Exportkontrollrecht bei der Ausgestaltung der IT-Architektur der Wertschöpfungskette enge Grenzen. Das betrifft sowohl den Wertschöpfungsprozess bei gelisteten Rüstungsgütern als auch bei Gütern, die sowohl für zivile als auch militärische Zwecke verwendet werden können und nach Anhang I der EG Dual-Use-Verordnung[535] gelistet sind. Aufgrund der Bedeutung der Dual-Use-Güter für nahezu alle Industriezweige werden die sich aus dem Exportkontrollrecht folgenden Herausforderungen hier exemplarisch anhand des Dual-Use-Rechts erläutert.

a) Genehmigungsbedürftige Technologietransfers

Hintergrund für die genannten Einschränkungen ist, dass nicht nur die Ausfuhr von gelisteten Gütern genehmigungsbedürftig ist, sondern auch die Übertragung von Software und

[535] Verordnung (EG)Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchführung von Gütern mit doppeltem Verwendungszweck (ABl. L134 vom 29.05.2009, S. 1) zuletzt geändert durch delegierte Verordnung (EU)-Nr. 1382/2014 der Kommission zum 22.10.2014 (ABl. L371 vom 30.12.2014, S. 1).

Technologie. Nach der EG Dual-Use-Verordnung ist Ausfuhr auch „die Übertragung von Software oder Technologie mittels elektronischer Medien […]; dies beinhaltet auch das Bereitstellen solcher Software oder Technologie in elektronischer Form für juristische oder natürliche Personen […] außerhalb der Gemeinschaft."[536] Das bedeutet, dass alleine die Einräumung eines Zugriffs auf gelistete Daten durch Personen außerhalb der EU einen genehmigungsbedürftigen Vorgang darstellen kann.[537]

Voraussetzung für all dies ist, dass die entsprechende Technologie oder Software auch in Anhang I zur EG Dual-Use-Verordnung aufgeführt ist. Hier wird Technologie definiert als „spezifisches technisches Wissen, dass für die Entwicklung, Herstellung oder Verwendung eines Produkts nötig ist".[538] Es gibt eine umfassende allgemeine Technologieanmerkung, die Anhang I der EG Dual-Use-Verordnung vorangestellt ist und die generelle Voraussetzungen enthält, wann Technologie von der Liste umfasst ist. Wichtig ist in diesem Zusammenhang, dass nur solche Technologie umfasst ist, die für die Entwicklung, Herstellung oder Verwendung von erfassten Gütern unverzichtbar ist.

Unverzichtbar wird definiert als „bezieht sich ausschließlich auf den Teil der Technologie, der besonders dafür verantwortlich ist, dass die [in der Liste] erfassten Leistungsmerkmale, Charakteristiken oder Funktionen erreicht oder überschritten werden."[539] Bei einer gelisteten Werkzeugmaschine ist zum Beispiel diejenige Technologie mit umfasst, die dafür verantwortlich ist, dass die Maschine die spezifischen in der Dual-Use-Liste genannten Genauigkeitswerte erreicht.

b) Herausforderungen für die Industrie

Dieses Wissen bzw. diese Technologie unterliegt damit den genannten Transferbeschränkungen und stellt bereits jetzt Herausforderungen an die IT-Sicherheitsarchitektur der Unternehmen, da der Forschungs- und Entwicklungsverband aber auch die Produktion häufig arbeitsteilig international erfolgt. Beispielsweise sollen außerhalb der EU ansässige Konzerngesellschaften auf entsprechende Daten zugreifen können, Projektpartner sollen Zugriffsmöglichkeiten erhalten oder Server oder IT Administrationen sollen ins Ausland verlagert werden. Diese Herausforderungen werden mit der zunehmenden Digitalisierung und Vernetzung noch sehr stark zunehmen.

c) Lösungsansätze

In den genannten Konstellationen gibt es *de lege lata* sowohl technische als auch rechtliche Möglichkeiten, um eine Compliance mit außenwirtschaftsrechtlichen Vorschriften sicher zu stellen. Eine technische Möglichkeit liegt etwa darin, eine effektive IT-Sicherheitsstruktur aufzubauen, die einen Zugriff auf sensible Daten von außerhalb der EU effektiv unterbindet.

---

[536] Art. 2 Nr. 2 (iii) EG Dual-Use-VO.
[537] Vgl. *Friedrich*, in Hocke/Friedrich, Außenwirtschaftsrecht, Art. 2 Dual-Use-VO, Rn. 26.
[538] Begriffsbestimmungen Anhang I EG Dual-Use-Verordnung.
[539] Begriffsbestimmungen Anhang I EG Dual-Use-Verordnung.

Hierfür verlangen die deutschen Behörden, dass diese Architektur „*auch im Nachhinein belastbar*“ ist.[540]

Eine rechtliche Lösungsmöglichkeit besteht z. B. darin, im Falle von Forschungskooperationen über gemeinsame Entwicklungsplattformen oder gemeinschaftlichen Entwicklungen und Produktionsprozessen mit einzelnen Kunden eine Sammelausfuhrgenehmigung zu beantragen, die z.T. als „*Technologieausfuhrgenehmigung*“ bezeichnet wird.[541] Hierbei ist zu beachten, dass derzeit sehr strenge Vorschriften bestehen, die für die Inanspruchnahme einer solchen Verfahrenserleichterung gelten. Bei Inanspruchnahme ist es unverzichtbar, ein funktionierendes und belastbares internes Compliance Programm implementiert zu haben.[542]

Hierbei ist auch zu berücksichtigen, dass die deutschen Behörden im Vergleich zu anderen EU Mitgliedstaaten eine deutlich strengere Genehmigungspraxis verfolgen, was deutschen Unternehmen Wettbewerbsnachteile gegenüber Unternehmen im EU-Ausland bereitet. Diese Nachteile könnten bereits durch eine Trendwende in der Behördenpraxis deutlich abgemildert werden. In diesem Zusammenhang soll nicht unerwähnt bleiben, dass der deutsche Verordnungsgeber im Juli 2015 mit der 4. Verordnung zur Änderung der Außenwirtschaftsverordnung[543] für Dual Use Güter weitere strenge nationale Sonderregelungen eingeführt hat.[544] Diese neuen Regelungen betreffen u.a. technische Unterstützung für Güter der Sicherheits- und Überwachungsindustrie.

Daneben wird das reibungslose Funktionieren von Industrie 4.0 *de lege ferenda* weitere Verfahrenserleichterungen erfordern, wie z.B. den Verzicht auf bestimmte Notifizierungspflichten z.B. für Projekte im Konzernverbund.

2. Mass Customization

Eine der starken Veränderungen wird in der Wandlung von einer Massenproduktion zu einer starken Anpassung der Produkte im Rahmen einer hoch flexibilisierten Produktion liegen, die sogar Anpassungen bei einzelnen Chargen ermöglichen wird. Dieses als „mass customization“ bezeichnete Phänomen wird zu weiteren Herausforderungen im Zusammenhang mit der exportkontrollrechtlichen Klassifizierung führen, da viele Listungstatbestände auf eine spezifische Konstruktion oder Änderung für bestimmte Zwecke abstellen.

Unter derzeitigen Bedingungen ist daher zumindest für Massenprodukte häufig auszuschließen, dass es sich um speziell für militärische oder andere spezifische Einsatzzwecke geänderte Produkte handelt. Dies ist nicht mehr ohne weiteres möglich, wenn Mass

---

[540] Vgl. dazu *BAFA*, Technologietransfer und Non-Proliferation, Leitfaden für Industrie und Wissenschaft, 2011, S. 15.
[541] *BAFA*, a.a.O. S. 19.
[542] Vgl. *Sachs/Krebs*, Quid pro quo im Außenhandel: Compliance gegen Verfahrensprivilegien, CCZ 2013, S. 12.
[543] BAnz AT 17.07.2015 V1.
[544] Vgl. hierzu ausführlich Höft/Kreuzer, RiW 2015, 587.

Customization Standard wird. Hier ist der EU-Gesetzgeber gefordert, eine handhabbare Einschränkung der Begriffe *„speziell konstruiert“* bzw. *„speziell geändert für“* zu ermöglichen. Gleichzeitig werden auch hier unweigerlich die Compliance Anforderungen an die Unternehmen steigen: Es wird zunehmend wichtiger, Kunden nach dem Prinzip *„know your customer“* zu überprüfen[545] und verbindliche Auskünfte zu ihren Verwendungszwecken zu erhalten.

II. Insbesondere: Beschränkungen für Software mit kryptographischen Eigenschaften

Existenzvoraussetzung für die zunehmende Digitalisierung und Vernetzung im Zusammenhang mit Industrie 4.0 wird sein, dass unter allen Beteiligten sensible Produktions- und Prozessdaten sicher miteinander ausgetauscht werden können. Es ist absehbar, dass dabei vor allem auch Kryptotechnik zum Zwecke des Vertraulichkeits- und Integritätsschutzes eingesetzt werden wird. Kryptotechnik wird damit zu einem der maßgeblichen Produktionsmittel. Dieses Produktionsmittel unterliegt allerdings selbst empfindlichen Exporteinschränkungen.[546]

1. Gelistete Kryptotechnik

De lege lata dürfte die von der Industrie einzusetzende Kryptotechnik in Anhang I zur EG Dual-Use-Verordnung aufgeführt sein. Dieser umfasst unter Position 5A002 lit. a *„Systeme, Geräte, anwenderspezifische elektronische Baugruppen, Module und integrierte Schaltungen für Informationssicherheit, wie folgt, und besonders für Informationssicherheit entwickelte Bestandteile hierfür: […] 1. Entwickelt oder geändert zum Einsatz von Kryptotechnik unter Verwendung digitaler Verfahren, soweit es sich nicht um Authentisierung, digitale Signatur oder die Ausfuhr kopiergeschützter Software handelt, mit einer der folgenden Eigenschaften.“*

Erfasst werden sodann sowohl symmetrische Algorithmen mit einer Schlüssellänge von über 56 Bit und asymmetrische Algorithmen mit einem spezifisch genannten Sicherheitsverfahren. Diese technischen Anforderungen entsprechen der im Wassenaar Arrangement vereinbarten Kontrollliste.[547] Des Weiteren erfasst Position 5D002 des Anhangs I zur EG Dual-Use-Verordnung sowohl Software, die für die Verwendung dieser o. g. Einrichtungen entwickelt wurde, als auch solche Software *„die die Eigenschaften der von Nr. 5A002 erfassten Geräte besitzt oder deren Funktionen ausführt oder simuliert“*. Verschlüsselungshardware und Software, die nicht diese Eigenschaften besitzt, ist nach unserem Dafürhalten schon jetzt veraltet und sollte bereits aus Sicherheitsgründen nicht eingesetzt werden.

---

[545] Verbindliche Regeln gelten hier freilich im Bereich der Geldwäscheprävention, vgl. Richtlinie 2005/60/EG.
[546] Vgl. hierzu auch *Beucher/Schmoll*, Kryptotechnologie und Exportbeschränkungen, CR 1999, S. 529.
[547] http://www.wassenaar.org/controllists.

Anhang I zur EG Dual-Use-Verordnung enthält eine ausführliche „Kryptotechnik-Anmerkung“,[548] die zahlreiche eigentlich qua ihrer Leistungsmerkmale erfasste Hard- und Softwareprodukte insbesondere für den Massenmarkt wieder von dem Anwendungsbereich der Liste ausnimmt. Die für industrielle Zwecke eingesetzte Kryptotechnik dürfte aber einige der hierfür aufgestellten Voraussetzungen nicht erfüllen, wie z.B. die mangelnde Unterstützung durch den Anbieter bei der Installation oder die mangelnde Änderungsmöglichkeit durch den Benutzer.

2. Derzeitige Genehmigungserfordernisse

Das bedeutet, dass grundsätzlich jeder der die EU-Außengrenzen überschreitende Transfer dieser Kryptotechnik genehmigungsbedürftig ist. Jedes Mal, wenn im Rahmen eines internationalen Projektes Sicherheitssoftware oder Hardware an einen Kunden, Kooperationspartner, etc. zur Verfügung gestellt wird, um eine gemeinsame Sicherheitsarchitektur zu ermöglichen, ist eine Ausfuhrgenehmigung erforderlich. Ähnliches dürfte bei jedem Update der Kryptotechnik gelten.

Bisher wurde versucht, die damit einhergehenden Probleme mit Hilfe von Allgemeingenehmigungen abzuschwächen: Hierbei handelt es sich um die allgemeine Genehmigung der EU Nr. EU001 sowie die nationale allgemeine Genehmigung Nr. 16 (Telekommunikation und Informationssicherheit).[549] Auf dieser Basis kann entsprechende Technologie in bestimmte Länder transferiert werden, ohne dass eine Einzelgenehmigung erforderlich ist. Die allgemeine Genehmigung Nr. EU001 ist beschränkt auf acht Länder, nämlich Australien, Japan, Kanada, Neuseeland, Norwegen, Schweiz und Liechtenstein. Der geografische Kreis der Allgemeingenehmigung Nr. 16 ist sehr viel weiter, es sind lediglich Embargoländer und eine Handvoll weiterer Staaten ausgeschlossen.

Die Verwendung dieser allgemeinen Genehmigungen ist jedoch nicht trivial und stellt die Unternehmen vor große Herausforderungen: Für die Nutzung beider Ausfuhrgenehmigungen ist allerdings eine Registrierung über das Portal ELAN-K2 erforderlich und eine halbjährliche Meldungen aller Transfers. Ein Verstoß gegen die Voraussetzungen stellt eine ungenehmigte Ausfuhr dar.[550] Schon aus diesen Gründen werden damit zukünftig auch in Unternehmen, die sonst keine gelisteten Güter herstellen oder vertreiben, interne Compliance Programme zur Einhaltung der exportkontrollrechtlichen Vorschriften unabdingbar.[551]

---

[548] Anmerkung 3 zu Teil 2 „Informationssicherheit“ der Kategorie 5 Anhang I EG Dual-Use-Verordnung, Kryptotechnik-Anmerkung und Anmerkung zur Kryptotechnik-Anmerkung.

[549] *BAFA*, Bekanntmachung über die allgemeine Genehmigung Nr. 16 (Telekommunikation und Informationssicherheit) vom 24.03.2015.

[550] Vgl. *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, Stand 1/2015, § 33 AWG a.F. Rn. 11.

[551] Vgl. hierzu *Sachs*, EU moving towards DIY export control, WorldECR No. 13, 2012, S. 12.

3. Lösungsansätze

De lege ferenda gibt es einige Ansätze, um den zu erwartenden erheblichen Mehraufwand für exportkontrollrechtliche Prozesse einigermaßen zu senken. Es ist möglich, die im Rahmen des Wassenaar Arrangement getroffenen und in der EG Dual-Use-Verordnung umgesetzten Anforderungen der Erfassung an Hard- und Software zur Verschlüsselung deutlich zu entschärfen, da es sich bei den derzeit gelisteten Systemen nicht mehr um schwer erhältliche Spitzentechnologie handeln dürfte.

Ein anderer Ansatz wäre, die Anforderungen administrativer Art der allgemeinen Genehmigungen zu senken, etwa in dem nur noch eine Registrierung, aber keine halbjährliche Meldung mehr erforderlich ist. Diese zweite Variante würde allerdings den Aufwand der Unternehmen, angemessene interne Compliance Programme zu implementieren, nicht zwingend schmälern. Schließlich ist auch an allgemeine Genehmigungen und Ausnahmen bei konzerninterner Verwendung von Verschlüsselungshard- und -software zu denken. Auch sind ist der EU-Gesetzgeber und die deutsche Verwaltung gefragt, die bestehenden Beschränkungen für den Übergang zu Industrie 4.0 abzubauen.

Teil 13 Prozessrecht *(Dr. Steffen Burrer)*

In Deutschland beschreitet die Gerichtsbarkeit gerade mühsam den Übergang zur elektronischen Kommunikation mit dem Gericht und zur elektronischen Akte. Man kann sagen, dass das Prozesswesen nach der Einführung von Schreibmaschinen und dem Übergang zur Textverarbeitung mit Computern überhaupt erst in der „Dritten Revolution“ steckt. Von einem „Gericht 4.0“ ist die Realität noch weit entfernt – jedoch wird die wirtschaftliche Realität von Industrie 4.0-Sachverhalten Streitparteien und Gerichte bald einholen und Fragen aufwerfen, die in erster Linie Beweislast und Beweisbarkeit betreffen.

I. Beweislast und beweisrechtliche Probleme

Digitale Vorgänge sind der Wahrnehmung der beweisbelasteten Partei zumeist entzogen, so dass sie sich primär nur auf Indizien und Vermutungen stützen kann, sich im Übrigen aber in Beweisnot befindet. Im Rahmen der Produkthaftung wird diesem Problem nach ausreichender Darlegung eines Mangels über eine Umkehrung der Beweislast begegnet. Auch im vertraglichen Bereich kommt dem Anspruchsteller die Verschuldensvermutung zugute. Dies allein kann aber die Problematik nicht lösen; beweisrelevante Daten müssen verwertbar gemacht werden können, wobei hierbei dann auch oftmals die Hürde zu nehmen ist, dass sich die Daten in der Sphäre des Anspruchsgegners befinden oder aber zumindest vom Anspruchsteller ohne entsprechende Auswertungssoftware nicht sinnvoll verwertet werden können. Das deutsche Zivilprozessrecht ist indes vom Beibringungsgrundsatz geprägt.

Erleichterungen für die beweisbelastete Partei können sich aber vor allem durch den Anscheinsbeweis und die sekundäre Darlegungslast bei Vorgängen in der Sphäre des Anspruchsgegners ergeben. Dies kann den Betreiber etwa **bei softwaregesteuerten Vorgängen** dazu anhalten, notwendige Beweismittel (z. B. Anlernprotokolle, Fehlerspeicher) vorzuhalten und zu sichern,[552] da er sonst als Anspruchsgegner im Falle der **unterbliebenen Speicherung** seiner Darlegungslast nicht genügen kann.

Weitergehend kann sich bei einer unterbliebenen Speicherung sogar die Frage stellen, ob eine Beweisvereitelung durch den Hersteller vorliegt. Zwar besteht keine generelle Dokumentationspflicht, um einen späteren Beweis zu ermöglichen, die Herstellung/Sicherung von Nachweisen kann aber dann zur Obliegenheit werden, wenn erkennbar wird, dass es zu einem Rechtsstreit kommen kann.[553] Unter den Grundsätzen der Beweisvereitelung und von Treu und Glauben wäre es nämlich treuwidrig, wenn der Beweisgegner daraus, dass er den Beweis des anderen verunmöglicht, prozessuale Vorteile zieht, indem er sich auf die Beweislast des anderen beruft.[554]

---

[552] *Hanisch* in Hilgendorf: Robotik im Kontext von Recht und Moral, S. 109 (119).
[553] Vgl. *Regenfus* in Vieweg/Gerhäuser: Digitale Daten in Geräten und Systemen, S. 243 (251, 264).
[554] Vgl. *Regenfus* a. a. O., S. 251; s. auch *Zahrnt*, NJW 2002, 1531 (1533) mit Beispielen aus der Rechtsprechung zu Software-Fehlern.

Auch dann, wenn bspw. die „Black Box“ eines Automaten wegen eines Defekts keine telemetrische Speicherung von Daten vorgenommen hat, wird man von einer Beweisvereitelung ausgehen müssen. Eine Vernichtung von beweiserheblichen Daten liegt zwar nicht vor, es wäre aber treuwidrig, wenn sich der Hersteller in diesem Fall auf die Beweisfälligkeit der anderen Prozesspartei berufen könnte, wenn dies auf einem Fehler aus seiner eigenen Sphäre beruht.[555]

Problematischer wird die Beweislage, wenn keine der beiden Parteien Einfluss auf die Daten hat und den zur automatisierten Entscheidung führenden Prozess auch nicht nachträglich auswerten kann, wie dies bei **Big-Data-Analysen** der Fall ist. Diese Frage lässt sich daher nur im Zusammenhang mit der Zuordnung von Verantwortungsbereichen und entsprechender Zuordnung der Beweislast – wie etwa durch die Umkehr der Beweislast bei der Produkthaftung – lösen.

Ähnliche Probleme können sich stellen, wenn die Frage beweiserheblich ist, ob auf das Produktverhalten durch **Datenkommunikation von außen** Einfluss genommen wurde, falls sich keine „Einbruchspuren“ zeigen. Auch hier kann ggf. die Datenspeicherung und Auswertung eine entscheidende Rolle spielen.

II. Zivilprozessuale Fragestellungen

1. Anforderungen an den substantiierten Parteivortrag bei vermuteten Fehlern in Datenverarbeitungsvorgängen

Oftmals wird der Anspruchsteller selbst nicht wissen, welche Erkenntnisse sich letztlich aus den gespeicherten Daten werden gewinnen lassen und kann daher nicht mit Gewissheit vortragen, was durch die Auswertung wird bewiesen werden können. Zivilprozessual genügt jedoch die Vermutung, dass ein Beweismittel bestimmte Erkenntnisse bringen kann. Erhofft die Prozesspartei daher, der Speicherinhalt werde Daten aufweisen, die einen bestimmten, vorgetragenen Schadenshergang bestätigen, liegt darin weder ein Ausforschungsbeweis noch eine Behauptung ins Blaue hinein.[556]

Handelt es sich um Gegenstände, die der Wahrnehmung der darlegungspflichtigen Partei nicht zugänglich sind, wie z. B. Geschäftsgeheimnisse des Softwareherstellers, so verkürzt sich zudem die Vortragspflicht der beweisführenden Partei auf ein Mindestmaß gem. § 138 Abs. 4 ZPO. Es genügt dann, darzulegen, inwieweit und weshalb sie zu erheblichen Tatsachen keine Erklärung abgeben kann. Entsprechend verstärkt sich die Darlegungslast der Gegenpartei. Danach kann es im Einzelfall Sache des Softwarelieferanten sein, die Fehlerfreiheit des gelieferten Programms darzulegen und zu beweisen.[557]

---

[555] *Regenfus* a. a. O., S. 265.
[556] *Regenfus* a. a. O., S. 254.
[557] *Bergmann/Streitz*, NJW 1992, 1726 (1728).

Das Gericht kann daher die Substantiierungspflicht unter Berücksichtigung des Standes der Technik und der Wahrnehmungssphäre beider Parteien flexibel verteilen. Mindestmaß der Darlegung bleibt jedoch die phänomenologische Darstellung der Mangelerscheinungen.[558] Bloß tatsächliche Darlegungsschwierigkeiten begründen keine Umkehr der Beweislast, sondern machen die Hinzuziehung eines Privatgutachters erforderlich, um den Mindestanforderungen zu genügen. [559]

2. Frage der Notwendigkeit prozessualer Auskunfts-/Vorlageansprüche („e-discovery")

Mit guten Gründen lehnt man in Deutschland eine „Discovery" nach amerikanischem und englischem Vorbild ab und kommt auch entsprechenden Amtshilfeersuchen nicht nach (Vorbehalt nach Art. 23 HaagBewÜbk).[560] Ebenso zu begrüßen ist aber die Öffnung, die das zweite ZPO-Reformgesetz mit der Neufassung der §§ 142 und 144 ZPO mit sich gebracht hat. Dies weist in die richtige Richtung, um auch den oben erläuterten Beweisschwierigkeiten hinsichtlich beim Gegner gespeicherter oder nur von diesem auswertbarer Daten zu begegnen: die Ausweitung der Vorlagepflichten für Urkunden (§ 142 Abs. 1 u. 2 ZPO) und Augenscheinsobjekte (§ 371 Abs. 2, § 144 Abs. 1 u. 2 ZPO) auf gespeicherte Daten zum Zwecke ihrer Auswertung oder die Anordnung einer entsprechenden Auswertung erscheint unbedingt erforderlich.

In umgekehrter Richtung, d. h. wenn sich der Hersteller bei Inanspruchnahme wegen eines behaupteten Fehlers entlasten möchte und dazu vom Kläger den Datenspeicher benötigt, kann die Problematik über die analoge Anwendung des Besichtigungsanspruchs aus § 809 BGB gelöst werden.[561]

Unabhängig von zivilprozessualen Auskunftspflichten in Deutschland ist ein Unternehmen aber gut beraten, sich über die elektronische Archivierung von Dokumenten – aber auch deren Löschung – sinnvoll Gedanken zu machen, um einerseits der Konfrontation mit einem Common-Law-Verfahren, speziell mit US-amerikanischen Klagen und einer damit einhergehenden „e-discovery", gewachsen[562] und andererseits auch für eine eventuell erforderliche eigene Verteidigung anhand von Entwicklungsunterlagen und Ähnlichem gewappnet zu sein. Besondere Anforderungen gerade im digitalen Bereich stellt das Gebot des „litigation hold" nach den Common-Law-Verfahrensordnungen, der schon bei drohender Streitigkeit den sofortigen Stopp jeglicher Dokumentenvernichtung im Unternehmen und ggf. auch verbundenen Unternehmen verlangt, was IT-seitig eine sofortige und nicht immer triviale Änderung einer ggf. vorhandenen automatischen Löschroutine erforderlich macht,[563] und

---

[558] Vgl. auch *Zahrnt,* NJW 2002, 1531.
[559] *Bergmann/Streitz*, NJW 1992, 1726 (1728).
[560] Vgl. auch *Regenfus* a. a. O., S. 252 gegen eine allgemeine prozessuale Aufklärungspflicht.
[561] *Regenfus* a. a. O., S. 263.
[562] Vgl. eingehender hierzu *Imberg/Geissl*, CCZ 2009, 190; *Katko/Knöpfle/Kirschner*, ZD 2014, 238.
[563] Vgl. *Imberg/Geissl*, CCZ 2009, 190 (193).

bei einem Verstoß zu erheblichen verfahrensrechtlichen Nachteilen, von der Umkehr der Beweislast bis zum Prozessverlust, führen kann.[564]

3. Beweiswert von Datenpaketen

Neue, europäisch harmonisierte Beweisvorschriften für elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt bringt die ab dem 1.7.2016 geltende eIDAS-Verordnung VO (EU) Nr. 910/2014 in Form qualifizierter Siegel, qualifizierter Zeitstempel und qualifizierter elektronischer Einschreiben mit sich.[565] Dies trägt der Verlagerung früher verschriftlichter Vorgänge in den digitalen Raum Rechnung, betrifft aber immer noch lediglich aus sich selbst heraus verständliche elektronische Dokumente.

Für reine Datenpakete helfen diese Beweisregelungen nicht weiter, denn ohne Information über die Bedeutung der Zahlenwerte sind die im Speicher festgehaltenen Daten praktisch wertlos. Für die Auswertung von Daten, aus denen Erkenntnisse über zurückliegende Betriebsvorgänge gezogen werden sollen, sind mehrere Einzelvorgänge erforderlich: Das Auslesen des Speicherinhalts; die Umwandlung der abstrakten Daten in konkrete Informationen; schließlich die Herstellung des Sinnzusammenhanges zwischen den Informationen zur Rekonstruktion des Betriebsvorgangs.[566] Hierbei stellen sich die wesentlichen Schwierigkeiten bei den ersten beiden Schritten, während der letzte „klassische“ Sachverständigenaufgabe ist.

Für die Auswertung der Daten ist eine genaue Kenntnis der Software und der Betriebsweise des technischen Systems erforderlich. In vielen Fällen werden allerdings Auswertungsprogramme zur Verfügung stehen, die die gespeicherten Informationen „übersetzen“. Hier erscheint es geboten, über die erfolgte Erstreckung des Urkundsbeweises auf elektronische Dokumente in § 371a ZPO hinaus als neues Strengbeweismittel den „Datenbeweis“ einzuführen, nach dem unter bestimmten Auswertungsvoraussetzungen der volle Beweis des durch die Datenauswertung belegten Vorganges bzw. zumindest der belegten Informationen, soweit diese noch einer weiteren (sachverständigen) Bewertung zugeführt werden müssen, angenommen wird. Dann böte sich auch die Einführung von den §§ 427 und 444 ZPO entsprechenden Regelungen für die Folgen der Nichtvorlage oder der Löschung von Daten über die Grundsätze der Beweisvereitelung hinaus an.

4. Auswertung von Daten durch das Gericht und Mitwirkungspflichten des Herstellers

Die größte Schwierigkeit der Verwertung von Daten kann dann schon darin bestehen, die geeignete Auslesevorrichtung und Auswertungsprogramme zur Verfügung zu bekommen. Gelingt es der Prozesspartei, beim Systemhersteller die Daten in geeigneter ausgewerteter Form zu beschaffen, können sie als urkundlich belegter substantiierter Parteivortrag in den

---

[564] Eingehender hierzu *Pant*, CCZ 2014 , 139.
[565] Eingehend hierzu *Jandt*, NJW 2015, 1205.
[566] *Regenfus* a. a. O., S. 254.

Prozess eingeführt werden.[567] Eine zivilprozessuale Pflicht des Gegners, in seinem Besitz befindliche Lesegeräte zur Verfügung zu stellen, gibt es jedoch nicht – die Daten selbst sind bereits vorhanden und das Gerät selbst soll nicht in Augenschein genommen werden, sondern lediglich das Ergebnis der Auswertung.[568] Nach derzeitiger Rechtslage kann eine Pflicht, aktiv Daten unter Verwendung nicht allgemein zugänglicher Verfahren aufzubereiten, lediglich im Rahmen der Einschaltung eines Sachverständigengutachtens auferlegt werden – wozu der Sachverständige dann aber selbst auch über die technischen Mittel verfügen muss, zu deren Bereitstellung der Gegner auch in diesem Fall nicht verpflichtet wäre. Denn eine aus dem Prozessrechtsverhältnis entspringende Mitwirkungspflicht gibt es nicht, so dass sich ein Anspruch auf Mitwirkung nur aus der materiell-rechtlichen Beziehung zwischen den Parteien ergeben kann.[569] De lege ferenda ist daher die vorstehend unter 2. angesprochene maßvolle Ausweitung der Pflicht des Gegners, an der Aufklärung mitzuwirken, erforderlich.[570]

5. Geheimnisschutz und Zeugnisverweigerungsrechte

Versucht der Prozessgegner die Aussagekraft von Daten zu erschüttern, kann es erforderlich werden, Details über die Funktionsweise der Maschinensysteme offen zu legen. Dies könnte das Zeugnisverweigerungsrecht gem. § 384 Nr. 3 ZPO berühren. Besteht im Einzelfall ein Geschäftsgeheimnis, so stellt ein etwaiger Ausschluss der Öffentlichkeit und das Schweigegebot nach §§ 172 Nr. 2, 174 Abs. 3 GVG indes noch keinen hinreichenden Grund dar, das Zeugnisverweigerungsrecht des Gegners aufzuheben,[571] zumal diese Vorschriften nur die mündliche Verhandlung, nicht aber den Zugang zu Dokumenten betreffen.[572] Ein „In-camera-Verfahren“, wie es sich in Teilbereichen des Wettbewerbs- und Immaterialgüterrechts etabliert hat[573] und wie es § 99 Abs. 2 VwGO und § 138 TKG vorsehen, könnte hier Abhilfe schaffen. Der Entwurf einer EU-Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen[574] weist in seinem Art. 8 in genau diese Richtung.[575]

6. Alternative Online-Streitbeilegung in Verbraucherangelegenheiten

Die EU-Richtlinie 2013/11/EU über alternative Streitbeilegung in Verbraucherangelegenheiten und die Verordnung VO (EU) Nr. 524/2013 über die Online-Streitbeilegung in Verbraucherangelegenheiten betreffen einen anderen Aspekt der Digitalisierung: Bei Kauf- und Dienstleistungsverträgen muss über die staatliche Ziviljustiz hinaus den Verbrauchern die außergerichtliche kostengünstige Streitbeilegung durch Schlichtungsstellen, insbesondere

---

567 *Regenfus* a. a. O., S. 259.
568 *Regenfus* a. a. O., S. 256.
569 Vgl. *Regenfus* a. a. O., S. 261.
570 Vgl. bereits *Schmidt-Cotta*, ZRP 2000, 518 (519).
571 *Regenfus* a. a. O., S. 260.
572 Vgl. *Redeker/Pres/Gittinger,* WRP 2015, 812 (814).
573 Vgl. *Regenfus* a. a. O., S. 261.
574 KOM (2013) 813 endg.
575 Näher dazu *Redeker/Pres/Gittinger,* WRP 2015, 812 (817).

auch über die Online-Streitbeilegungs-Plattform („OS-Plattform“) der Europäischen Kommission, ermöglicht werden, welche ab dem kommenden Jahr zur Verfügung stehen soll. Dies wird sich insbesondere im E-Commerce auswirken, wo die Hemmschwelle zu einer Klage gegen einen unbekannten und weit entfernten Vertragspartner oftmals besonders hoch ist.

Die Bundesregierung hat zur Umsetzung der Richtlinie am 27.5.2015 den Entwurf eines Verbraucherstreitbeilegungsgesetzes veröffentlicht.[576]

Unternehmer, die sich dieser Art der Schlichtung nicht gänzlich verschließen, müssen darüber dann auf ihrer Homepage und in ihren allgemeinen Geschäftsbedingungen informieren und sich bei der Ablehnung einer Verbraucherbeschwerde darüber erklären, ob sie zur Durchführung eines Streitbeilegungsverfahrens bereit sind.

Bedeutsam für den grenzüberschreitenden Verkehr ist dabei, dass jeder Mitgliedstaat eine Kontaktstelle zu benennen hat, die als innerstaatliche Anlaufstelle für Verbraucher, Unternehmer und Streitbeilegungsstellen in grenzübergreifenden Konflikten aus online geschlossenen Verträgen zur Verfügung steht.

7. Probleme mit nationalen Prozessregelungen angesichts internationaler Vernetzung – Internationalisierung des Prozessrechts/Stärkung der internationalen Schiedsgerichtsbarkeit

Aus supranationaler Sicht erscheint es wahrscheinlich, dass der Grundsatz, dass keine Partei gehalten ist, dem Gegner für seinen Prozesserfolg das Material zu verschaffen, über das er nicht schon von sich aus verfügt,[577] über die im nationalen Prozessrecht bereits ten - sinnvollen – Öffnungen hinaus noch weiter aufgeweicht werden wird.[578] Dies gilt insbesondere im Rahmen der internationalen Schiedsgerichtsbarkeit, die weitgehend „discovery“ oder „requests for documents“ zulässt.[579] Angesichts der Einflüsse, die das amerikanische Verfahrensrecht bereits jetzt auf deutsche Unternehmen ausübt,[580] wenn mit ihnen verbundene Gesellschaften in den USA verklagt werden, wird eine Internationalisierung des Prozessrechts sich schon rein faktisch ergeben. Die Anerkennung einer prozessualen Aufklärungspflicht der Parteien liegt zudem im „internationalen Trend“.[581] Die Ungewissheiten verschiedener nationaler Prozessordnungen werden vertraglich verbundene Parteien indes am besten durch eine Schiedsvereinbarung in den Griff bekommen können, durch die sie die Verfahrensregeln selbst bestimmen können. Die Probleme der Industrie

[576] BT-Drucks. 18/5089.
[577] Vgl. BGH, Urt. v. 11.06.1990 – II ZR 159/89, NJW 1990, 3151.
[578] Vgl. *Wagner*, ZEuP 2001, 441 (467).
[579] Insbesondere die IBA-Regeln für die Beweisaufnahme in internationalen Schiedsgerichtsverfahren; weitere Beispiele bei *Burianski/Reindl*, SchiedsVZ 2010, 187.
[580] Eingehend dazu *Spies/Schröder*, MMR 2008, 275.
[581] *Wagner*, ZEuP 2001, 441 (469).

4.0 erscheinen insoweit als guter Nährboden für eine Stärkung der internationalen Schiedsgerichtsbarkeit.

Teil 14 Kartell- und Beihilfenrecht *(Dr. Alexander Birnstiel, LL.M., Helge Heinrich, Dr. Tobias Kruis, LL.M.)*

Die Digitalisierung der Wirtschaft sowie die Vernetzung der Industrie stellen das Kartell- und Beihilfenrecht vor Herausforderungen, die sowohl in Fachkreisen als auch in der breiten Öffentlichkeit kontrovers diskutiert werden. Die folgende Untersuchung greift in diesem Zusammenhang vier Themenkomplexe heraus. Im I. Abschnitt werden allgemein die Herausforderungen der digitalen Wirtschaft für das Kartellrecht behandelt, wobei der Schwerpunkt auf der Rolle von Internetplattformen liegt. Anschließend werden die kartellrechtlichen Rahmenbedingungen für eine vernetzte Industrie analysiert (II.). Der III. Abschnitt befasst sich mit der Bedeutung von „Big Data" für das Kartellrecht. Im Rahmen der Untersuchung sollen dabei zunächst die (möglichen) Herausforderungen des Kartellrechts sowie der derzeitige Rechtsrahmen beschrieben und der Reformbedarf bzw. mögliche Lösungsansätze diskutiert werden. Im IV. Abschnitt wird schließlich die beihilfenrechtliche Dimension untersucht.

I. Digitale Wirtschaft und Kartellrecht

Die digitale Wirtschaft stellt das Kartellrecht vor zahlreiche neue Herausforderungen. Dies gilt vor allem mit Blick auf die Entwicklung neuer und innovativer Geschäfts- und Vertriebsmodelle, z. B. Vertrieb über das Internet und Betrieb von Internetplattformen. In diesem Zusammenhang stellen sich die Fragen, welche besonderen kartellrechtlichen Probleme sich aus den veränderten Bedingungen im Rahmen der digitalen Wirtschaft ergeben und ob die herkömmlichen kartellrechtlichen Instrumente den damit verbundenen Anforderungen gewachsen sind.

Diese Fragen wurden in der jüngsten Vergangenheit durch nationale und supranationale Behörden und Institutionen aufgegriffen. Anfang Mai leitete die Europäische Kommission eine Sektoruntersuchung im Bereich des Online-Handels ein.[582] Ziel der Untersuchung ist es, etwaige Wettbewerbshindernisse beim grenzüberschreitenden Online-Handel mit Waren und Dienstleistungen zu identifizieren. Zudem startete die Kommission am 24.09.2015 im Rahmen der Strategie für einen digitalen Binnenmarkt eine öffentliche Konsultation zur Rolle von Plattformen.[583] Am 01.06.2015 veröffentlichte ferner die Monopolkommission ein Sondergutachten, in der sie den Reformbedarf des rechtlichen und regulatorischen Rahmens für ausgewählte digitale Märkte analysierte.[584] Im Juli 2015 veröffentlichte schließlich das Europäische Parlament eine Studie zu den Herausforderungen der Wettbewerbspolitik

[582] Vgl. *Europäische Kommission*, Pressemitteilung v. 06.05.2015, IP/15/4921.
[583] Vgl. *Europäische Kommission*, Pressemitteilung v. 24.09.2015, IP/15/5704.
[584] *Monopolkommission*, Sondergutachten 68, Wettbewerbspolitik: Herausforderung digitaler Märkte, 2015, im Internet abrufbar unter http://tinyurl.com/qjj3nxn.

in der digitalisierten Wirtschaft.[585] Darüber hinaus werden auch von Seiten der Politik immer wieder Forderungen nach einer Regulierung, vor allem im Zusammenhang mit Internetplattformen, laut.[586]

Im Folgenden werden zunächst allgemein die Herausforderungen des Kartellrechts in der digitalen Wirtschaft beschrieben (1.), um dann auf die besonderen Problemfelder der Regulierung digitaler Märkte und innovativer Geschäftsmodelle (2.) sowie insbesondere der Regulierungsnotwendigkeit marktmächtiger Internetplattformen (3.) einzugehen.

1. Herausforderungen der digitalen Wirtschaft für das Kartellrechts

Die Digitalisierung der Wirtschaft und damit verbunden die Möglichkeiten zur Nutzung des Internets für neue Geschäftsmodelle haben zu einem tiefgreifenden Strukturwandel geführt. Es stellt sich die Frage, ob die derzeitigen kartellrechtlichen Rahmenbedingungen den Anforderungen der digitalen Wirtschaft noch gewachsen sind.

a) Problemaufriss

Zahlreiche Dienstleistungen im Internet werden **kostenlos** erbracht (z. B. Leistungen von Suchmaschinen, Preisvergleichswebseiten oder Hotelbuchungsportalen). Aus kartellrechtlicher Sicht wirft dies die Frage auf, wie mit solchen kostenlosen Dienstleistungen umgegangen werden soll und ob daraus überhaupt Wettbewerbsprobleme entstehen können.[587]

Darüber hinaus bietet das Internet einerseits scheinbar grenzenlose Möglichkeiten für den Vertrieb von Waren, Dienstleistungen und digitalen Inhalten. Andererseits bestehen zahlreiche Tendenzen zur Beschränkung der Vertriebsmöglichkeiten. Ein Beispiel ist der Einsatz von **Geo-blocking**.[588] Dieses kann z. B. genutzt werden, um Preisunterschiede zwischen verschiedenen Mitgliedstaaten aufrecht zu erhalten. Allerdings können diese Maßnahmen ihren Ursprung im Urheberrecht haben, wenn etwa bestimmte digitale Inhalte nur zur Verbreitung in einem Land lizensiert wurden.

Weiterhin spielen Beschränkungen eine Rolle, die den Vertrieb über das Internet ganz oder teilweise ausschließen (hierzu gehören z. B. **Drittplattformverbote**[589] oder generelle Verbo-

---

585 *Europäisches Parlament*, Challenges for Competition Policy in a Digitalised Economy, 2015, im Internet abrufbar unter http://tinyurl.com/n9u7qu4.

586 Vgl. das Schreiben mehrerer Bundesminister an die Kommission v. November 2014, S. 6, im Internet abrufbar unter http://tinyurl.com/o8x88xy. Ebenso das gemeinsame Schreiben von Bundeswirtschaftsminister Gabriel und dem frz. Wirtschaftsminister Macron an Kommissar Ansip vom April 2015, im Internet abrufbar unter http://tinyurl.com/py7t4gv.

587 *Podszun/Franz*, NZKart 2015, 121.

588 Dabei handelt es sich um technische Maßnahmen, mit denen der Zugang für Nutzer zu einer Website aufgrund des Aufenthalts- bzw. Standorts gesperrt oder der Verbraucher auf eine inländische Website umgeleitet wird, vgl. Kommission, KOM(2015) 192 endg., S. 6 f. (Strategie für einen Digitalen Binnenmarkt).

589 Mit sog. Drittplattformverboten untersagen Hersteller ihren Händlern den Vertrieb über Online-Marktplätze, wie z. B. eBay oder Amazon Marketplace. Drittplattformverbote werden von Herstellern

te des Internetvertriebs) oder die Preissetzungsfreiheit im Internet beeinflussen (z. B. **Doppelpreisstrategien**[590] und **Bestpreis**- oder **Preisparitätsklauseln**[591]).

Digitale Märkte neigen aufgrund von **Netzwerkeffekten** (siehe dazu unten, I. 3. a)) zu Konzentrationstendenzen. Hier stellt sich die Frage, ob diese Konzentrationstendenzen zu Marktmacht führen können bzw. wie sich Marktmacht im digitalen Umfeld sinnvoll messen lässt. Daran anknüpfend können sich Wettbewerbsbeschränkungen ergeben, wenn marktmächtige Unternehmen diese Marktmacht einsetzen, um Wettbewerber zu behindern (z. B. durch Preiskampfstrategien, Zugangsbehinderung, Bevorzugung eigener Angebote) oder um ihre Kunden auszunutzen (z. B. durch überhöhte Preise).

Schließlich muss berücksichtigt werden, dass die Marktbedingungen in dem dynamischen Umfeld, in dem neue Vertriebsmodelle etabliert werden, ständig im Fluss sind, so dass Analysen zu den Marktverhältnissen regelmäßig nur von geringer Halbwertszeit sind.[592]

b) Derzeitiger Rechtsrahmen

Den derzeitigen Rechtsrahmen für die oben beschriebenen Probleme bilden die §§ 1, 19 ff. GWB sowie die Art. 101, 102 AEUV. Die Anwendung dieser Vorschriften setzt eine Abgrenzung der relevanten Märkte sowie die Beurteilung von Marktanteilen bzw. Marktmacht voraus.

– Marktabgrenzung und Marktmacht

Der sachlich relevante Markt umfasst grundsätzlich alle Produkte, die aus Sicht des Nachfragers austauschbar sind, wobei sich die Austauschbarkeit nach den Produkteigenschaften sowie nach der Bereitschaft der Nachfrager richtet, im Falle einer geringen, aber doch spürbaren und nicht bloß vorübergehenden Preiserhöhung (sog. SSNIP[593]-Test) auf ein Substitut auszuweichen.[594] In digitalen Märkten führen diese Methoden häufig jedoch nicht weiter. Digitale Geschäftsmodelle können so einzigartig sein, dass sich oftmals kein Substitut findet.[595] Jedenfalls bei kostenlosen Angebo-

---

sowohl im selektiven als auch im nicht-selektiven Vertrieb eingesetzt. Näher dazu *Monopolkommission* (Fn. 582), Rn. 420 ff.

590 Doppelpreissysteme werden von Herstellern verwendet, um einen bestimmten Vertriebsweg, üblicherweise den stationären Vertrieb gegenüber dem Internetvertrieb, zu unterstützen. Dabei werden den Händlern in der Regel je nach Vertriebsweg unterschiedliche Rabatte oder Zuschüsse eingeräumt. Vgl. *Monopolkommission* (Fn. 584), Rn. 419.

591 Bestpreis- bzw. Preisparitätsklauseln (die Begriffe werden in der Regel synonym verwendet) spielen derzeit vor allem im Zusammenhang mit dem Vertrieb über Online-Plattformen eine Rolle. Mit diesen Klauseln verlangen Plattformbetreiber von den auf ihrer Plattform aktiven Verkäufern, Händlern oder Dienstleistern, dass letztere ihre Waren oder Dienstleistungen über andere Vertriebskanäle (einschließlich andere Plattformen) nicht zu günstigeren oder zu besseren Bedingungen anbieten. Vgl. *Monopolkommission* (Fn. 584), Rn. 408 ff.

592 *Körber*, WuW 2015, 120 (124).

593 **S**mall but **S**ignificant **N**on-permanent **I**ncrease in **P**rice.

594 *Eilmansberger* in Streinz, EUV/AEUV, 2. Aufl. 2012, vor Art. 101, Rz. 45 ff.

595 Vgl. *Europäisches Parlament* (Fn. 585), S. 56.

ten versagt darüber hinaus der SSNIP-Test.[596] Ähnliche Punkte lassen sich bei der räumlichen Marktabgrenzung anführen, die üblicherweise auf die Homogenität der Wettbewerbsverhältnisse abstellt.[597] Klassische Faktoren wie z. B. Transportkosten oder das Erfordernis einer inländischen Niederlassung spielen im Internet keine Rolle.

Vergleichbare Schwierigkeiten bestehen bei der Berechnung von **Marktanteilen** sowie bei der Messung von **Marktmacht**. Insbesondere die Unentgeltlichkeit von Angeboten wirft die Frage nach alternativen Berechnungsmethoden auf. Die hohe Dynamik digitaler Märkte und die regelmäßig kurzen Innovationszyklen führen zudem dazu, dass Marktanteile in digitalen Märkten sehr volatil sind und ihnen daher in der Praxis oftmals nur eine geringe Bedeutung zukommt.[598]

– Anwendung von § 1 GWB, Art. 101 AEUV

§ 1 GWB, Art. 101 Abs. 1 AEUV verbieten wettbewerbsbeschränkende Vereinbarungen und abgestimmte Verhaltensweisen. Die Vorschriften werden grundsätzlich weit ausgelegt und erfassen sowohl zwei- bzw. mehrseitige Wettbewerbsbeschränkungen zwischen Wettbewerbern (horizontal) als auch solche zwischen Unternehmen auf verschiedenen Marktstufen (vertikal). Damit lassen sich grundsätzlich vertragliche Vertriebsbeschränkungen (z. B. Drittplattformverbote oder generelle Verbote des Internetvertriebs sowie Doppelpreissysteme) erfassen.[599] Insbesondere bei Drittplattformverboten wird es zukünftig darauf ankommen, dass nationale Kartellbehörden und Kommission eine einheitliche Linie herausarbeiten, wie mit diesen Vertriebsbeschränkungen umgegangen werden soll. Während solche Drittplattformverbote nach Ansicht der Kommission jedenfalls im Rahmen von selektiven Vertriebssystemen möglich sein sollen,[600] haben das Bundeskartellamt sowie deutsche Gerichte in der Vergangenheit eine andere Auffassung vertreten.[601]

---

596 *Dewenter/Rösch/Terschüren*, NZKart 2014, 387.

597 *Eilmansberger* in Streinz, EUV/AEUV, 2. Aufl. 2012, vor Art. 101, Rz. 50 f.

598 Vgl. *Europäische Kommission*, Beschl. v. 07.10.2011 im Fall COMP/M.6281 - *Microsoft/Skype*, Rz. 78.

599 Vgl. z. B. EuGH, Urt. v. 13.10.2011, Rs. C-439/09, *Pierre Fabre*, ECLI:EU:C:2011:649 (Verbot des Internetvertriebs); Bundeskartellamt, Fallbericht v. 23.12.2013, Az. B7-11/13 - *Bosch Siemens Haushaltsgeräte* (Doppelpreissystem); Fallbericht v. 19.08.2014, Az. B3-137/12 - *Adidas* (Drittplattformverbot), Pressemitteilung v. 27.08.2015 - *Asics* (Beschränkung des Online-Vertriebs).

600 *Europäische Kommission*, Leitlinien für vertikale Beschränkungen, ABl. EU 2010 C 130/1, Rz. 54. Inwieweit diese Auffassung der Kommission zu Drittplattformverboten noch zutreffend ist, kann vor allem vor dem Hintergrund der Entscheidung des EuGH EuGH, Urt. v. 13.10.2011, Rs. C-439/09, *Pierre Fabre*, ECLI:EU:C:2011:649, hinterfragt werden. Darin äußerte sich das Gericht insbesondere kritisch zu der Möglichkeit, Beschränkungen des Online-Vertriebs mit dem Prestigecharakter einer Marke zu begründen.

601 Bundeskartellamt, Fallbericht v. 19.08.2014, Az. B3-137/12 - *Adidas* (Drittplattformverbot). Offengelassen im Verfahren gegen Asics, vgl. Pressemitteilung v. 27.08.2015 - *Asics* (Beschränkung des Online-Vertriebs). Vgl. auch OLG Frankfurt, Urt. v. 31.07.2013, 2-03 O 128/13 – *Depotkosmetik*.

Bei neuen Vertriebsmodellen – insbesondere über digitale Plattformen – verschwimmt jedoch die klassische Abgrenzung zwischen horizontalen und vertikalen Beschränkungen. Plattformen agieren in erster Linie als Intermediär/Vermittler zwischen verschiedenen Nutzergruppen. Bei den Beziehungen zwischen einer Plattform und ihren Nutzergruppen handelt es sich dann aber nicht um klassische vertikale Vereinbarungen, sondern vielmehr um Drei- bzw. Mehrecksbeziehungen. Dies zeigen z. B. die Schwierigkeiten des Bundeskartellamtes bei der Beurteilung von so genannten Bestpreis- bzw. Preisparitätsklauseln im Online-Hotelbuchungs-Sektor. Das Bundeskartellamt wertete die zwischen dem Hotelportal HRS und den Hotels vereinbarten Bestpreisklauseln als vertikale Beschränkungen im Sinne der VO (EU) Nr. 330/2010 („Vertikal-GVO"). Die Frage, ob es sich bei diesen Klauseln um Kernbeschränkungen gem. Art. 4 Vertikal-GVO handelte, konnte das Bundeskartellamt jedoch nicht eindeutig beantworten. Letztendlich konnte die Frage offen gelassen werden, da die Vertikal-GVO aus Sicht des Bundeskartellamtes ohnehin nicht anwendbar war. [602] Zusätzlich wurden die Regeln zur Einordnung von Vermittlern bzw. Handelsvertretern[603] für die „Brick&Mortar"-Welt geschaffen und lassen sich nicht 1:1 auf den Online-Vertrieb übertragen.[604] Hinzu kommt, dass Internetplattformen oftmals eigene Dienstleistungen bzw. Inhalte anbieten und damit in Wettbewerb zu ihren Nutzergruppen treten.[605]

Geo-blocking z. B. wird von § 1 GWB, Art. 101 Abs. 1 AEUV nicht erfasst, solange es sich dabei um einseitige Maßnahmen handelt.[606] Anders ist dies jedoch, wenn solche Maßnahmen vertraglich vereinbart wurden. Letzteres kann vor allem bei der Verbreitung digitaler Inhalte eine Rolle spielen.[607] In diesem Zusammenhang stellen sich jedoch schwierige Fragen zum Verhältnis zwischen Kartellrecht und Urheberrecht.[608]

– Anwendung von §§ 19 ff. GWB, Art. 102 AEUV

---

602 Vgl. Bundeskartellamt, Beschl. v. 20.12.2013, Az. B9-66/10 - *HRS*.

603 Vgl. dazu *Europäische Kommission*, Leitlinien für vertikale Beschränkungen, ABl. EU 2010 C 130/1, Rz. 12 ff.

604 Dazu *Kjølbye/Aresu/Stephanou*, The Commission's e-commerce Sector Inquiry – Analysis of Legal Issues and Suggested Practical Approach, Journal of European Competition Law & Practice 2015, 465, im Internet abrufbar unter http://tinyurl.com/oqukb2x.

605 Das Bundeskartellamt behandelte deshalb z. B. die Preisparitätsklauseln von Amazon bei der Ausgestaltung des Amazon Marketplace als horizontale Wettbewerbsbeschränkungen. Bundeskartellamt, Fallbericht v. 09.12.2013, Az. B6-46/12.

606 Vgl. *Kjølbye/Aresu/Stephanou* (Fn. 604).

607 Die Kommission führt aktuell ein Verfahren gegen den britischen Pay-TV Betreiber Sky UK und sechs Hollywood-Filmstudios. Der Vorwurf lautet, dass die bestehenden Lizenzvereinbarungen zwischen den Filmstudios und Sky UK dazu führen, dass Verbraucher außerhalb des Vereinigten Königreichs und Irlands die Pay-TV-Inhalte (z. B. Filme und TV-Serien) von Sky UK weder online („*Streaming*") noch über Satellit abrufen können. Die Kommission sieht darin die vertragliche Vereinbarung eines absoluten Gebietsschutzes, welche ohne Vorliegen einer überzeugenden Rechtfertigung gegen das Kartellverbot nach Art. 101 Abs. 1 AEUV verstößt. *Europäische Kommission*, Pressemeldung v. 23.07.2015, IP/15/5432.

608 Vgl. dazu EuGH, Urt. v. 18.03.1980, Rs. 62/79, *Coditel I*, ECLI:EU:C:1980:84; Urt. v. 06.10.1982, Rs. 262/81, *Coditel II*, ECLI:EU:C:1982:334; Urt. v. 04.10.2011, verb. Rs. C-403/08 u. C-429/08, *Premier League/Murphy*, ECLI:EU:C:2011:631. Vgl. auch Kjølbye/Aresu/Stephanou (Fn. 604).

Der Missbrauch von Marktmacht fällt unter §§ 19 ff. GWB, Art. 102 AEUV. Dabei unterscheidet man typischerweise zwischen Ausbeutungsmissbrauch (z. B. Erzwingung unangemessener Preise und Konditionen) und Behinderungsmissbrauch (z. B. Kampfpreise, Preis-Kosten-Scheren, Lieferverweigerung, sowie Kopplung und Bündelung).[609]

Bei der Anwendung des Missbrauchsverbots auf den Internetvertrieb bereitet die Trennung des auch für marktbeherrschende Unternehmen zulässigen Leistungswettbewerbs („*competition on the merits*"[610]) vom unzulässigen Nichtleistungswettbewerb oftmals Schwierigkeiten. So ist z. B. die Aufdeckung von Preiskampfstrategien oder von Preis-Kosten-Scheren problematisch, wenn bestimmte Dienstleistungen im Internet typischerweise kostenlos angeboten und erbracht werden.[611] Andere Verhaltensweisen, z. B. die Kopplung und Bündelung von Produkten, können auch Ausdruck innovativer Geschäftsmodelle sein, die keinen Missbrauch von Marktmacht darstellen sollten.[612]

Die Ausbeutung und Diskriminierung von Verbrauchern (z. B. durch Geo-blocking oder durch unterschiedliche Preisstrategien) sollte sich grundsätzlich von §§ 19 ff. GWB, Art. 102 AEUV erfassen lassen.[613] Dies ist bisher in der Praxis jedoch noch nicht relevant geworden.

c) Reformbedarf?

Wegen der Vielfalt an unterschiedlichen, innovativen Geschäftsmodellen in der digitalen Wirtschaft erscheint bei der Analyse möglicher Kartellrechtsprobleme eine **Einzelfallbetrachtung** geboten. Die kartellrechtlichen Generalklauseln (§§ 1, 19 ff. GWB, Art. 101, 102 AEUV) sind hinreichend abstrakt formuliert und damit flexibel genug, um diese neuen Entwicklungen in den Griff zu bekommen. Allerdings sollte bei der Anwendung und Auslegung dieser Klauseln den Besonderheiten der digitalen Wirtschaft hinreichend Rechnung getragen werden.

---

609 Bei den bisher geführten Verfahren der Kommission ging es jeweils um Behinderungsmissbrauch; Microsoft: Verweigerung Zugang zu Schnittstelleninformationen und Bündelung mit Media Player (2004), Interoperabilitätsprobleme (2008), Bündelung Internet Explorer (2009). Google: Privilegierung eigener Suchergebnisse, unautorisierte Verwendung fremder Inhalte, Alleinbezug der Werbung per AdSense, keine Verwendung von AdWords mit konkurrierenden Plattformen. Google Android: Bündelung mit weiteren Google-Apps, Beschränkung der Entwicklung von Android Forks, Bündelung mit eigenen Apps. Siehe auch *Jaeger*, WuW 2015, 702.

610 Vgl. EuGH, Urt. v. 27.03.2012, Rs. C-209/10, *Post Danmark*, ECLI:EU:C:2012:172, Rz. 21 ff.

611 *Europäisches Parlament* (Fn. 585), S. 58 f.; *Körber*, WuW 2015, 120 (129 f.); *Jaeger*, WuW 2015, 702 (707).

612 Deshalb kritisch zur *Microsoft*-Entscheidung der Kommission Körber, WuW 2015, 120.

613 Vgl. *Nothdurft* in Langen/Bunte, Kartellrecht, 12. Aufl. 2015, § 19 GWB, Rz. 97, 102; *Eilmansberger* in Streinz, EUV/AEUV, 2. Aufl. 2012, Art. 102 AEUV, Rz. 28. Kritisch dazu *Kjølbye/Aresu/Stephanou* (Fn. 604).

Um dies zu gewährleisten sollte eine Fortentwicklung des „Soft Law“ erfolgen – d. h. vor allem der Mitteilungen der Kommission bzgl. Marktdefinition, Beurteilung von Marktmacht sowie Anwendung der Kartell- und der Missbrauchsverbote.[614] Kartellbehörden sollten außerdem über das ökonomische und technische Know-how sowie über ausreichende finanzielle und personelle Ressourcen verfügen, um Verfahren in diesem Bereich effizient und zügig durchzuführen, eventuell unter verstärktem Einsatz einstweiliger Maßnahmen.[615]

Daneben kommen grundsätzlich flankierende Maßnahmen in anderen Rechtsbereichen in Betracht, z. B. im Verbraucherschutz- und Urheberrecht hinsichtlich Geo-blocking.[616]

Ob darüber hinaus weitere gesetzgeberische Maßnahmen zur Regulierung erforderlich sind, bedarf einer sorgfältigen Prüfung. Regulatorische Eingriffe in dynamische, innovationsgetriebene Märkte sollten stets die Ausnahme bilden und sollten sich außerdem darauf beschränken, Märkte offen zu halten, ohne in spezifische Geschäftsmodelle einzugreifen.

2. Kartellrechtliche Fragen bei der Regulierung digitaler Märkte und innovativer Geschäftsmodelle

a) Problemaufriss

In der digitalen Wirtschaft treten zahlreiche neue Geschäftsmodelle in Konkurrenz zu tradierten Geschäftsbereichen. Dies gilt zum Beispiel für sog. Over-The-Top („OTT“) Kommunikationsanbieter (z. B. Skype, Facebook Messenger, WhatsApp, etc.), die zunehmend eine Alternative zu herkömmlichen Telekommunikationsdienstleistungen darstellen. Geschäftsmodelle der sog. „Sharing Economy“ wie z. B. Uber oder Airbnb treten außerdem in Konkurrenz zu traditionellem Hotel- und Taxi-Gewerbe. Weiterhin gewinnen Online-Streamingdienste (z. B. Netflix) im Vergleich zu herkömmlichen Fernsehsendern zunehmend an Attraktivität.[617]

Wettbewerbsverzerrungen können entstehen, wenn etablierte und neue Geschäftsmodelle nicht den gleichen Regeln unterliegen.

b) Derzeitiger Rechtsrahmen

Ob die neuen Geschäftsmodelle dem gleichen regulatorischen Rahmen unterliegen wie die etablierten Geschäftsmodelle, muss jeweils im Einzelfall geprüft werden. So unterliegen z. B. OTT-Dienstleister nicht derselben sektorspezifischen Regulierung wie Telekommunikations-

---

[614] *Körber*, WuW 2015, 120; *Jaeger*, WuW 2015, 702.
[615] Dafür *Monopolkommission* (Fn. 584), Rz. 510.
[616] Siehe *Europäische Kommission*, KOM(2015) 192 endg., S. 6 ff. (Strategie für einen Digitalen Binnenmarkt).
[617] Vgl. *Monopolkommission* (Fn. 584),Rz. 543 für weitere Bsp.

anbieter. Andererseits erscheint es z. B. für den Share-Economy-Transportdienstleister Uber durchaus möglich, dass dieser der Regulierung für Taxis unterfällt.[618]

c) Reformbedarf?

Ein sog. „*level playing field*“ kann auf zwei verschiedene Arten erreicht werden. Entweder wird die bestehende Regulierung auf die neuen Geschäftsbereiche, *mutatis mutandis*, ausgedehnt. Oder es wird geprüft, inwieweit die bestehende Regulierung für die etablierten Geschäftsmodelle abgebaut werden kann. Jedenfalls gilt auch hier, dass in jedem Einzelfall sorgfältig geprüft werden sollte, ob und in welchem Umfang ein regulatorischer Eingriff in digitale, innovationsgetriebene Märkte tatsächlich erforderlich ist.

3. Regulierungsnotwendigkeit marktmächtiger Internetplattformen

In jüngster Vergangenheit kamen vermehrt Forderungen auf, gegen marktmächtige Internetplattformen (z. B. Suchmaschinen, soziale Netzwerke, e-commerce Marktplätze, App Stores) vorzugehen. Hervorzuheben ist die gegen Google gerichtete Forderung des Europäischen Parlaments v. 27.11.2014 nach der Entflechtung von Internetsuchmaschinen.[619]

a) Problemaufriss

– Digitale Plattformen

Eine Internetplattform dient als Vermittler zwischen verschiedenen Nutzergruppen, die über die Plattform miteinander in Kontakt treten.[620] Die unterschiedlichen Nutzergruppen werden üblicherweise als „Markt-“ oder „Plattformseiten“ bezeichnet.

Trotz der zahlreichen unterschiedlichen Geschäftsmodelle zeichnen sich digitale Plattformen allgemein durch die folgenden Eigenschaften aus:

- Digitale Plattformen profitieren von Netzwerkeffekten. Bei zwei- oder mehrseitigen Plattformen stehen dabei sog. **indirekte Netzwerkeffekte** im Vordergrund. Danach wird eine Plattform für eine Nutzergruppe umso attraktiver, je mehr Nutzer einer anderen Gruppe auf diese zugreifen und umgekehrt.[621]

---

618 Vgl. *Linke*, NVwZ 2015, 476.

619 Entschließung des Europäischen Parlaments v. 27.11.2014 zur Stärkung der Verbraucherrechte im digitalen Binnenmarkt (2014/2973(RSP)), Rz. 15, im Internet abrufbar unter http://tinyurl.com/ntvdpdb. Die Entschließung ist rechtlich unverbindlich.

620 Zum Plattformbegriff *Europäisches Parlament* (Fn. 585), S. 21; *Europäische Kommission*, SWD(2015) 100 final, S. 52.

621 Zum Beispiel ist ein Hotelbuchungsportal für Hotelbetreiber umso attraktiver, je mehr potenzielle Hotelsuchende die Seite frequentieren. Umgekehrt steigt die Attraktivität für Hotelsuchende mit der Anzahl an Hotels, die ihre Dienstleistungen über die Plattform anbieten. Dagegen beziehen sich **direkte Netzwerkeffekte** auf die Anzahl der Nutzer auf einer Plattformseite. Beispiele sind Kommunikationsdienste und soziale Plattformen. Hier profitieren die Nutzer unmittelbar von der Größe der eigenen Nutzergruppe, z. B. ist eine Kommunikations-App wie WhatsApp umso attraktiver, je mehr Nutzer sie hat. Vgl. zu

- Digitale Plattformen machen sich diese indirekten Netzwerkeffekte für ihre Geschäftsmodelle zu eigen, und zwar v. a. bei der Preisgestaltung. Um die Plattform so attraktiv wie möglich zu machen, wird in der Regel die Plattformseite belastet, die weniger preissensibel ist. Dadurch können erhebliche **Preisasymmetrien** entstehen, bei denen etwa eine Plattformseite komplett durch eine andere Plattformseite subventioniert wird.[622]

- Wegen dieser asymmetrischen Preisstrukturen spielen Preise als Wettbewerbsfaktor eine geringere Rolle als in herkömmlichen Märkten. Andere Faktoren, wie z. B. **Innovation** und **Qualität** (bzw. Kundenerlebnis) treten in den Vordergrund.

– Kartellrechtliche Probleme

Aus ökonomischer Sicht ist anerkannt, dass Plattformmärkte aufgrund der indirekten Netzwerkeffekte zur **Konzentration** neigen.[623] Diese Konzentrationstendenz kann die Entstehung von Marktmacht begünstigen, vor allem wenn noch weitere Faktoren hinzukommen. Z. B. könnten Plattformen ihre Marktposition gegenüber (potenziellen) Wettbewerbern absichern, indem sie ihren Nutzern einen Wechsel zu anderen Plattformen (z. B. durch Verwendung von Nutzerdaten oder durch fehlende Interoperabilität) erschweren oder sogar unmöglich machen (sog. Lock-in Effekt).[624]

Marktstarke oder marktbeherrschende Internetplattformen könnten ihre Marktmacht ausnutzen. Diskutiert werden hier vor allem zwei Gefahren: (i) Behinderung von Wettbewerbern durch Beschränkung des Zugangs zu der Plattform; sowie (ii) sog. „*leveraging*“ von Marktmacht auf andere Bereiche, z. B. durch Bündelung von Dienstleistungen und Bevorzugung plattformeigener Dienste.[625]

Netzwerkeffekten *Monopolkommission* (Fn. 584), Rz. 35 ff. Neben dem Internet spielen indirekte Netzwerkeffekte vor allem im Presse- und Medienbereich eine Rolle, vgl. Bundeskartellamt, Entsch. v. 25.04.2014, Az. B6-98/13 – *Funke Medien Gruppe/Axel Springer*; Entsch. v. 21.04.2009, Az. B6-150/08 - *NPG/Detjen*; Entsch. v. 29.08.2008, Az. B6-52/08 – *Intermedia/Health & Beauty*.

622 Dies ist z. B. typisch für Internetsuchmaschinen. Für Internetnutzer ist die Suche kostenlos, weil sich die Suchmaschine in der Regel über Werbeeinnahmen finanziert. Grundlegend dazu *Rochet/Tirole*, Platform competition in two-sided markets, J EUR ECON ASSOC 2003, 90. Vgl. auch *Filistrucchi/Geradin/van Damme/Affeldt*, Market Definition in Two-Sided Markets: Theory and Practice, Journal of Competition Law and Economics 2013, 293; *Dewenter/Rösch/Terschüren*, NZKart 2014, 387.

623 Bundeskartellamt, Fallbericht v. 11.06.2015, Az. B6-39/15 – *Axel Springer/Immowelt*; *Monopolkommission* (Fn. 584), Rz. 42; *Europäisches Parlament* (Fn. 585), S. 22; *Körber*, WuW 2015, 120 (123).

624 Vgl. *Jaeger*, WuW 2015, 702; *Monopolkommission* (Fn. 584), Rz. 49. Weitere Faktoren sind das sog. „Tipping“ des Marktes sowie „first mover advantages“.

625 Dieser Vorwurf steht im Zentrum der laufenden Verfahren der Kommission gegen Google. So wird Google u. a. vorgeworfen, seine marktbeherrschende Stellung im Bereich der Online-Suche durch Privilegierung eigener Inhalte/Dienste bei den Suchergebnissen auszunutzen. Außerdem untersucht die Kommission seit 15.04.2015, ob Google seine marktbeherrschende Stellung in Bezug auf das mobile Betriebssystem Android ausgenutzt hat, u. a. durch Koppelung mit googleeigenen Anwendungen. Vgl. Pressemitteilung v. 15.04.2015, IP/15/4780.

b) Derzeitige Rechtslage

Die Ausnutzung von Marktmacht durch Internetplattformen fällt grundsätzlich in den Anwendungsbereich der §§ 19 ff. GWB, Art. 101, 102 AEUV. Die bereits beschriebenen Probleme bei der Anwendung des Kartellrechts im digitalen Umfeld (s. o., I. 1. b)) gelten grundsätzlich auch in diesem Kontext. Hinzu kommt, dass bei sog. **zwei- bzw. mehrseitigen Plattformen** Wechselwirkungen zwischen verschiedenen Plattformseiten bestehen, die bei der Marktabgrenzung nur schwer zu fassen sind.[626] Eine allgemeingültige Methode zur Marktabgrenzung existiert bisher nicht.[627]

Darüber hinaus können herkömmliche Methoden zur Beurteilung von Marktmacht die Interdependenzen zwischen den verschiedenen Plattformseiten nicht erfassen.[628]

– Zugang zu marktmächtigen Plattformen

  Die Gewährleistung eines (diskriminierungsfreien) Zugangs zu marktmächtigen Internetplattformen wird grundsätzlich von der ***essential-facilities*-Doktrin** erfasst, die im deutschen Recht ausdrücklich in § 19 Abs. 2 Nr. 4 GWB verankert ist.[629] Die *essential-facilities*-Doktrin ist jedoch an strenge Voraussetzungen geknüpft, die für den Zugang zu nicht duplizierbaren Infrastruktureinrichtungen wie Brücken und Häfen entwickelt wurden. Netzwerk- und Lock-in Effekte, welche digitale Plattformen prägen, spielen insofern keine Rolle.[630]

– Bündelung und Bevorzugung plattformeigener Dienste

  Die Bündelung von Dienstleistungen und die Bevorzugung plattformeigener Dienste lassen sich mit den herkömmlichen Fallgruppen des Missbrauchsverbots erfassen, nämlich Kopplung und Bündelung.[631] Allerdings besteht auch hier das bereits beschriebene Problem, dass kartellrechtswidrige Maßnahmen von Leistungs- und Inno-

---

[626] *Dewenter/Rösch/Terschüren*, NZKart 2014, 387; *Körber*, WuW 2015, 120; Monopolkommission, (Fn. 584), Rz. 54 ff.; *Europäisches Parlament* (Fn. 585), S. 52 ff.

[627] *Dewenter/Rösch/Terschüren*, NZKart 2014, 387; *Höppner/Grabenschröer*, NZKart 2015, 162.

[628] *Monopolkommission* (Fn. 584), Rz. 56.

[629] Vgl. *Paal*, GRUR 2013, 873. Im Microsoft-Verfahren wurde das Unternehmen von der Kommission unter Anwendung der *essential facilities*-Doktrin gezwungen, anderen Unternehmen vollständigen Zugang zu den Programmierschnittstellen zu gewähren. Vgl. *EU-Kommission*, WuW/E EU-V-931; EuG, Urt. v. 17.09.2007, Rs. T-201/04, *Microsoft*, Slg. 2007, II-3601.

[630] Vgl. *Monopolkommission*, XX. Hauptgutachten, S. 65; *Jaeger*, WuW 2015, 702 (711). Beispielsweise verlangt die Doktrin, dass eine wesentliche Einrichtung nicht duplizierbar ist. Im Internet lässt sich jedoch jede Plattform grundsätzlich duplizieren (z. B. Errichtung einer neuen Suchmaschine, Schaffung einer neuen sozialen Netzwerk-Plattform). Dass dies trotzdem nicht ausreichen kann, um wirksam in Wettbewerb zu treten, liegt an den oben beschriebenen Netzwerk- und Lock-in Effekten.

[631] Vgl. auch *Paal*, GRUR 2013, 873.

vationswettbewerb unterschieden werden müssen. Bei der Bündelung verschiedener Leistungen kann es sich auch um ein innovatives Geschäftsmodell handeln.[632]

– Verfahren

Ein weiteres Problem bei der Anwendung des Kartellrechts ist die Verfahrensdauer, die häufig nicht mit der technologischen Entwicklung Schritt halten kann. Z. B. zogen sich die Verfahren der Kommission gegen Microsoft über 14 Jahre. Das Verfahren gegen Google läuft bereits seit fünf Jahren.[633] Schließlich ist bei Verfahrensbeendigung durch Auflagen und Bedingungen besondere Vorsicht geboten, damit die Eingriffe in das dynamische Marktgeschehen nicht zu einer Innovationsbeeinträchtigung führen.[634]

c) Reformbedarf?

Wie bereits allgemein ausgeführt (s. o., Teil 14I.c)), sind die kartellrechtlichen Generalklauseln (§§ 1, 19 ff. GWB, Art. 101, 102 AEUV) grundsätzlich hinreichend flexibel, um auch im Einzelfall auf Kartellrechtsverstöße durch digitale Plattformen Anwendung zu finden. Allerdings sollte bei der Anwendung und Auslegung dieser Klauseln den Besonderheiten von digitalen Plattformen hinreichend Rechnung getragen werden. Dazu kann eine Fortentwicklung des „Soft Law“ (z. B. der Mitteilung der Kommission zu Marktdefinition, Beurteilung von Marktmacht und Anwendung der Missbrauchsverbote) förderlich sein.

Flankierende Maßnahmen in anderen Rechtsbereichen – primär im Datenschutz-, Urheber- und Verbraucherschutzrecht[635] – können ebenfalls dazu beitragen, die Entstehung von Marktmacht auf digitalen Plattformmärkten zu verhindern.

Die Frage, ob es darüber hinaus einer gesonderten Regulierung für marktmächtige Internetplattformen bedarf, wird kontrovers diskutiert. Während dies von politischer Seite teilweise vehement gefordert wird,[636] wird andererseits zur Zurückhaltung aufgerufen.[637] Für eine plattformspezifische Regulierung gibt es mehrere Möglichkeiten, z. B.:

- Regelungen zur **Entflechtung** der Plattform von spezialisierten Inhalten oder Dienstleistungen. Anknüpfend an die sektorspezifische Regulierung z. B. im Bereich Gas- und Stromerzeugung könnte man so die Unabhängigkeit von Plattformbetreibern sicherstellen.

---

632 *Körber*, WuW 2015, 120.
633 Vgl. *Jaeger*, WuW 2015, 702 (705). *Monopolkommission* (Fn. 584), Rz. 504.
634 *Körber* WuW 2015, 120.
635 Siehe Kommission, KOM(2015) 192 endg. (Strategie für einen Digitalen Binnenmarkt).
636 Vgl. das Schreiben mehrerer Bundesminister an die Kommission v. November 2014, S. 6, im Internet abrufbar unter http://tinyurl.com/o8x88xy sowie das gemeinsame Schreiben von Bundeswirtschaftsminister Gabriel und dem frz. Wirtschaftsminister Macron an Kommissar Ansip vom April 2015, im Internet abrufbar unter http://tinyurl.com/py7t4gv. In diese Richtung geht auch die Entschließung des *Europäischen Parlaments* v. 27.11.2014 (Fn. 619).
637 Vgl. *Jaeger*, WuW 2015, 702 (703); *Monopolkommission* (Fn. 584), Rz. 258 ff., 587.

- Schaffung einer Vorschrift (in Anlehnung an § 19 Abs. 2 Nr. 4 GWB), welche den Zugang zu „essentiellen“ Internetplattformen regelt, z. B. unter Bezugnahme auf FRAND-Bedingungen (zum Begriff s. u., II.b)).

- Erweiterung des Missbrauchsverbots, so dass weitergehende Verhaltensgebote an marktmächtige Plattformen gestellt werden.

- Die Einführung eines Prinzips der **Plattformneutralität,**[638] mit dem die diskriminierungsfreie Übermittlung und der neutrale Zugang zu Inhalten sichergestellt werden.

- Regelungen zur Interoperabilität und Transparenz von Plattformen, z. B. zur Offenlegung von Schnittstellen und zur Gewährleistung der Datenübertragbarkeit für Nutzer.[639]

Bei regulatorischen Eingriffen in dynamische, innovationsgetriebene Märkte sollte jedoch stets sorgfältig geprüft werden, ob ein Eingriff tatsächlich erforderlich ist.

Hinzu kommt, dass eine Konzentration in Plattformmärkten aus ökonomischer Sicht nicht *per se* schädlich ist, sondern durchaus wettbewerbs- bzw. wohlfahrtsfördernd sein kann, indem z. B. Transaktionskosten für Nutzer gesenkt werden, solange die Märkte offengehalten werden und Nutzer die Möglichkeit haben, zwischen verschiedenen Plattformen zu wechseln (sog. „*multi-homing*“).[640] Eingriffe sollten sich daher im Idealfall auf die Gewährleistung dieser Bedingungen beschränken.

II. Vernetzung der Industrie

1. Horizontale und vertikale Themen

a) Problemaufriss

Die Vernetzung der Industrie setzt voraus, dass Unternehmen miteinander kooperieren, z. B. bei der Forschung und Entwicklung („F&E“) oder bei der Lizensierung von Patenten. Zugleich spielen Interoperabilität und Kompatibilität eine zentrale Rolle. Ebenso wächst die Bedeutung von Standards und technischen Normen, welche in der Regel zwischen den verschiedenen Marktteilnehmer erarbeitet und vereinbart werden müssen. Damit stellt sich die Frage nach den kartellrechtlichen Grenzen einer solchen Kooperation.

---

[638] Siehe dazu bereits den Koalitionsvertrag der Bundesregierung, im Internet abrufbar unter http://tinyurl.com/p7wanoo. Vgl. frz. Digitalrat, Platform Neutrality, 2014, im Internet abrufbar unter http://tinyurl.com/lfkbztx.

[639] Ein „Recht auf Datenportabilität“ findet sich im aktuellen Entwurf der Datenschutzgrundverordnung (Art. 18), auf den sich die Justizminister der 28 EU-Mitgliedstaaten am 15.06.2015 einigen konnten, vgl. http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf. Dieses Recht wurde jedoch im Vergleich zum ursprünglichen Entwurf der Kommission eingeschränkt..

[640] Bundeskartellamt, Fallbericht vom 25.06.2015, Az. B6-39/15 – *Axel Springer/Immowelt*, S. 4.

b) Derzeitiger Rechtsrahmen

– Anwendung von § 1 GWB, Art. 101 Abs. 1 AEUV

§ 1 GWB, Art. 101 Abs. 1 AEUV verbieten wettbewerbsbeschränkende Vereinbarungen und abgestimmte Verhaltensweisen. Die Begriffe „Vereinbarung“ und „abgestimmte Verhaltensweise“ werden grundsätzlich weit ausgelegt und können nicht immer trennscharf voneinander abgegrenzt werden. Während es bei der Vereinbarung wesentlich auf die Willensübereinkunft ankommt,[641] soll es für eine abgestimmte Verhaltensweise bereits genügen, dass es sich um eine Form der Koordinierung handelt, bei der die beteiligten Unternehmen „bewusst eine praktische Zusammenarbeit an die Stelle des mit Risiken verbundenen Wettbewerbs treten lässt.“[642] Das Konzept der abgestimmten Verhaltensweise erfasst damit insbesondere Formen des Informationsaustausches, mit denen Wettbewerber die Ungewissheit über ihr zukünftiges Marktverhalten verringern oder beseitigen.

In diesem Zusammenhang stellt sich die Frage, ob der **automatisierte Datenaustausch** zwischen Unternehmen – z. B. aufgrund der gemeinsamen Teilnahme an einem computergesteuerten System – als „abgestimmte Verhaltensweise“ gegen das Kartellverbot verstoßen kann (§ 1 GWB, Art. 101 Abs. 1 AEUV).

– Kartellrechtliche Rahmenbedingungen der Kooperation

Nicht jede Form der Kooperation zwischen Unternehmen ist schlechthin verboten. Insbesondere ist anerkannt, dass die gemeinsame **F&E** zu positiven Effizienz- und Leistungssteigerungen führen kann – dies kommt auch F&E-Kooperationen im Rahmen der vernetzten Industrie zugute. Die Kommission geht davon aus, dass die meisten F&E-Vereinbarungen nicht unter Art. 101 Abs. 1 AEUV fallen. Dies gilt insbesondere für F&E-Vereinbarungen zwischen Nicht-Wettbewerbern, Outsourcing von zuvor selbst durchgeführter F&E, sowie für reine F&E-Kooperationen, die sich nicht auf die gemeinsame Verwertung möglicher F&E-Ergebnisse erstrecken.[643] Darüber hinaus wird die Zulässigkeit von F&E-Vereinbarungen durch die VO (EU) Nr. 1217/2010 („F&E-GVO“) geregelt.

Im Jahr 2014 verabschiedete die Kommission außerdem einen überarbeiteten Rechtsrahmen zur kartellrechtlichen Beurteilung von Technologie-Transfer-Vereinbarungen, bestehend aus der VO (EU) Nr. 316/2014 („TT-GVO“) sowie überarbeiteten Leitlinien der Kommission („TT-LL“). Solche Vereinbarungen ermöglichen es Unternehmen die Nutzung von Patenten, Know-how oder Software anderer Unternehmen zu lizensieren, die für die Produktion von Waren und Dienstleistungen eingesetzt werden.

---

641 Vgl. *Eilmansberger* in Streinz, EUV/AEUV, 2. Aufl. 2012, Art. 101 AEUV, Rz. 1.
642 EuGH, Urt. v. 08.07.1999, Rs. C-49/92 P, *Anic*, ECLI:EU:C:1999:356, Rz. 115.
643 Kommission, Horizontal-LL, Rz. 129 ff.

Die überarbeiteten TT-LL enthalten insbesondere Richtlinien zur Beurteilung von Technologiepools (d. h., Vereinbarungen, bei denen zwei oder mehr Parteien ein Technologiepaket zusammenstellen, das nicht nur an die Mitglieder des Pools, sondern auch an Dritte in Lizenz vergeben wird). Diese fallen unter bestimmten Voraussetzungen nicht in den Anwendungsbereich von Art. 101 Abs. 1 AEUV und sind damit grundsätzlich zulässig.[644]

– Kartellrechtliche Grenzen von Standardisierung und technischer Normung

Aus kartellrechtlicher Sicht ist ein **Standardsetzungsprozess** grundsätzlich unproblematisch, wenn (i) die Mitwirkung allen von dem Standard betroffenen Wettbewerbern offensteht, (ii) die Standardsetzung transparent erfolgt, (iii) die Einhaltung des Standards für die Beteiligten nicht verpflichtend ist, sowie (iv) der Zugang zu dem Standard zu fairen, zumutbaren und diskriminierungsfreien Bedingungen (sog. **FRAND-Bedingungen**) gewährleistet wird.[645]

Soweit nicht alle oben genannten Voraussetzungen erfüllt sind, muss im Einzelfall im Wege der „Selbsteinschätzung" geprüft werden, ob eine Standardsetzung nach Art. 101 Abs. 3 AEUV gerechtfertigt ist. Dabei geht die Kommission davon aus, dass Normierungsvereinbarungen oftmals zu erheblichen Effizienzgewinnen führen.[646] Wird ein Standard für verbindlich erklärt oder soll einer Einrichtung die exklusive Befugnis übertragen werden, die Einhaltung des Standards zu überprüfen, scheidet eine Freistellung jedoch in der Regel aus.[647]

c) Reformbedarf?

Die Frage, ob ein automatisierter Datenaustausch zwischen Unternehmen durch Teilnahme an einem gemeinsamen computergesteuerten System zu einem Kartellrechtsverstoß führen kann, bildet derzeit den Gegenstand eines Vorabentscheidungsverfahrens vor dem EuGH.[648] Nach Ansicht des zuständigen Generalanwalts kommt ein Verstoß jedenfalls in Betracht, wenn die Unternehmen den Inhalt der ausgetauschten Informationen kannten (oder hätten kennen müssen) und trotzdem weiter an dem gemeinsamen System teilnahmen, ohne sich öffentlich davon zu distanzieren.[649] Auch wenn die Vorlagefrage eine sehr spezifische Fallkonstellation betrifft, die hier nicht detailliert beschrieben werden kann, könnten sich dieser Entscheidung u. U. dennoch allgemein gültige Aussagen für vergleichbare Konstellationen entnehmen lassen.

---

644 TT-LL, Rz. 244 ff.
645 Horizontal-LL; Rz. 280.
646 Horizontal-LL; Rz. 308 ff.
647 Horizontal-LL; Rz. 318 f.
648 Rs. C-74/14, *UAB Eturas u.a*.
649 GA *Szpunar*, Schlussanträge v. 16.07.2015 in der Rs. C-74/14, *UAB Eturas u.a.*, Rz. 44 ff.

Schließlich ist anzumerken, dass die Kommission nach Art. 1 Abs. 1 lit. a VO EWG Nr. 2821/71 eine Gruppenfreistellungsverordnung für Normen- und Typenkartelle erlassen und so mehr Rechtsklarheit für Standardisierungsprozesse schaffen könnte. Von dieser Möglichkeit wurde bisher kein Gebrauch gemacht.

2. Marktmacht und einseitige Wettbewerbsbeschränkungen (Standardisierung und Interoperabilität, Essential Facilities)

a) Problemaufriss

In der vernetzten Industrie befinden sich Inhaber von sog. standardessentiellen Patenten („SEPs“) – das sind Patente, die durch eine Standardisierungsorganisation für die Implementierung eines Standards als wesentlich erklärt wurden und für die es keine Alternativen gibt – in einer Schlüsselposition, da sie gegebenenfalls den Zugang zu einem gesamten Produktmarkt kontrollieren können. SEP-Inhaber verfügen daher regelmäßig über eine marktbeherrschende Stellung im Sinne der §§ 19, 20 GWB, Art. 102 AEUV.[650] Sie können den Wettbewerb behindern, indem sie eine Lizensierung verweigern oder überhöhte Lizenzgebühren verlangen.[651]

Gleichfalls befinden sich Internetdienstanbieter in einer Schlüsselposition, da sie den Internetzugang kontrollieren. Sie können in den paketvermittelten Datenverkehr im Internet eingreifen, indem sie z. B. eigene Dienste priorisieren und Datenströme von anderen Dienstleistern (z. B. von OTT-Diensten) drosseln.

b) Derzeitiger Rechtsrahmen

– Standardessenzielle Patente

Im Rahmen des Standardsetzungsverfahrens werden die Teilnehmer zur Offenlegung standardrelevanter Patente aufgefordert. Setzt sich ein Standard durch, so verpflichten sich die SEP-Inhaber, diese zu FRAND-Bedingungen zu lizenzieren. Besondere Probleme können allerdings auftreten, wenn beteiligte Unternehmen ihre Patente erst nach Annahme des Standards offenbaren.[652]

Darüber hinaus war lange umstritten, unter welchen Bedingungen ein SEP-Inhaber seine marktbeherrschende Stellung missbraucht, wenn er gegen einen mutmaßlichen Patentverletzer im Wege der gerichtlichen Untersagungsverfügung vorgeht. Der EuGH machte im Urteil ***Huawei Technologies*** konkrete Vorgaben an das Verfahren,

---

[650] Das SEP bildet insoweit den relevanten Technologiemarkt, vgl. Kommission, Entsch. v. 29.04.2014 im Fall AT.39985 – *Motorola*, Rz. 190 ff.; Entsch. v. 29.04.2014 im Fall AT.39939 – *Samsung*, Rz. 41 ff.; Entsch. v. 13.02.2012 im Fall COMP/M.6381 – *Google/MMI*, Rz. 54. Vgl. auch *Schröter/Bartl* in von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 102 AEUV, Rz. 316.

[651] Vgl. Kommission Horizontal-LL, Rz. 269.

[652] Zu so genannten Patenthinterhalten („*patent ambush*“) vgl. Kommission, Beschl. v. 09.12.2009 im Fall COMP/38.636 – *Rambus*; *Klees* in Kilian/Heussen, Computerrecht, 32. Erg.-Lfg. 2013, Rz. 90 ff.

mit dem ein SEP-Inhaber seine Schutzrechte ohne Verstoß gegen Kartellrecht geltend machen kann. Danach muss er den potenziellen Verletzer zunächst auf die Patentverletzung hinweisen und ihm anschließend ein konkretes schriftliches Lizenzangebot zu FRAND-Bedingungen unterbreiten. Der potenzielle Patentverletzer ist seinerseits verpflichtet, die Bereitschaft zum Abschluss eines Lizenzvertrags auszudrücken, das Angebot sorgfältig zu prüfen und für den Fall, dass er dieses ablehnt, dem SEP-Inhaber ein Gegenangebot zu unterbreiten. Soweit die Parteien keine Einigung erzielen, können die Lizenzgebühren durch einen unabhängigen Dritten festgesetzt werden.[653]

– Netzneutralität

Die Datenübermittlung im Internet erfolgt herkömmlicherweise nach dem sog. „***Best-Effort***" Prinzip, wonach Daten grundsätzlich im Rahmen der zur Verfügung stehenden Kapazitäten transportiert werden.[654] Diskriminierende Maßnahmen von marktmächtigen Internetdienstanbietern zum Blocken oder zur Drosselung bestimmter Datenströme werden grundsätzlich durch das kartellrechtliche Missbrauchsverbot (§§ 19 ff. GWB, Art. 102 AEUV). Allerdings können Netzwerkmanagementmaßnahmen zur Drosselung von Daten sachlich gerechtfertigt sein, z. B. zur Sicherung der Netzqualität.[655]

c) Reformbedarf?

Trotz der klärenden Rechtsprechung des EuGH zum Missbrauch einer marktbeherrschenden Stellung im Zusammenhang mit SEPs ist weiterhin ungeklärt, unter welchen Voraussetzungen ein Lizenzangebot den FRAND-Bedingungen entspricht. Diesbezüglich könnte eine Klarstellung im IP-Recht Rechtssicherheit schaffen.[656]

Hinsichtlich der Netzneutralität stellt sich die Frage nach der Notwendigkeit einer nationalen oder supranationalen Regulierung. So hat die US Federal Communications Commission (FCC) am 26.02.2015 Regelungen zur Netzneutralität verabschiedet, die am 12.06.2015 in Kraft traten.[657] Auf deutscher und europäischer Ebene konnten sich dagegen Regelungen für eine strikte Netzneutralität nicht durchsetzen.[658]

---

[653] EuGH, Urt. v. 16.07.2015, Rs. C-170/13, *Huawei Technologies*, ECLI:EU:C:2015:477, Rz. 60 ff. Anders noch BGH, Urt. v. 06.05.2009, KZR 39/06 – *Orange-Book-Standard*. Danach sollte der mutmaßliche Patentverletzer verpflichtet sein, dem Patentinhaber zunächst ein Lizenzangebot zu machen. Allerdings bezog sich die Entscheidung des BGH nicht auf SEPs.

[654] *Holznagel* in Hoeren/Sieber/Holznagel, Multimedia-Recht, 41. Erg.-Lfg. 2015, Teil 3, Rz. 135.

[655] *Paal*, GRUR 2013, 873.

[656] *Europäisches Parlament* (Fn. 585), S. 47. Vgl. auch *Klees* in Kilian/Heussen, Computerrecht, 32. Erg.-Lfg. 2013, Rz. 82 ff. Zu Lösungsansätzen *Kommission*, Horizontal-LL, Rz. 289 f.; *Jakobs*, NZKart 2014, 394 (398).

[657] https://www.fcc.gov/openinternet.

[658] Ein Entwurf des BMWi v. 31.07.2013 wurde unter Verweis auf das Gesetzgebungsverfahren auf EU-Ebene nicht weiterverfolgt. Am 01.07.2015 stellte die Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN ei-

Wie bereits oben dargelegt, sollte auch in diesem Zusammenhang sorgfältig geprüft werden, ob über die kartellrechtliche Missbrauchskontrolle hinaus eine (sektorspezifische) Regulierung erforderlich ist. Dabei sollte berücksichtigt werden, dass Internetdienstanbieter in der Regel kein Interesse daran haben werden, bestimmte Dienste (wie z. B. OTT-Dienste) zu drosseln, da sie dadurch die Qualität und den Wert ihrer eigenen Dienstleistung für den Endkunden schmälern.[659] Sollte z. B. eine vertikal integrierter Telekommunikationsanbieter versuchen, eine populäre Messaging-App zu behindern, indem die Datenströme für diese Dienstleistung gedrosselt werden, so läuft der Telekommunikationsanbieter Gefahr, dass die Nutzer zu einem anderen Internetdienstanbieter wechseln.

III. Big Data als neue Herausforderung des Kartellrechts

Die digitale Ökonomie ist geprägt durch „Big Data". Dabei handelt es sich nach klassischer Definition um gewaltige Datenmengen, die nicht mehr mit herkömmlichen Datenverarbeitungsmethoden erfasst werden können.[660] Die zunehmende Bedeutung von Big Data stellt auch das Kartellrecht vor neue Herausforderungen, die im Folgenden kurz erläutert werden sollen.

1. Datenschutz und Kartellrecht

a) Problemaufriss

Vor allem im Internet ersetzen Daten zunehmend monetäre Gegenleistungen. Zahlreiche vermeintlich kostenlose Inhalte werden tatsächlich mit der (bewussten oder unbewussten) Zurverfügungstellung von personenbezogenen Nutzerdaten bezahlt. Die Bedeutung von Daten in der digitalen Wirtschaft und die Tendenz zur Datenkonzentration darf im Kartellrechtskontext nicht ignoriert werden.

Aus kartellrechtlicher Sicht stellt sich zunächst die Frage, ob kostenlose Dienstleistungen überhaupt einen relevanten Markt darstellen können. Wegen der kommerziellen Bedeutung von Daten ist weiterhin fraglich, ob es einen eigenen Markt für die Konzentration und Bereitstellung von Nutzerdaten gibt, der in der kartellrechtlichen Beurteilung berücksichtigt werden sollte.[661]

Darüber hinaus wird diskutiert, ob die Sammlung und Konzentration von Nutzerdaten zur Entstehung oder Verstärkung von Marktmacht oder zu Marktmachtmissbräuchen führen kann. Im Vordergrund stehen dabei die folgenden Bedenken, dass die Sammlung von Daten dazu dienen könnte, einen Nutzer an ein bestimmtes Unternehmen zu binden und so des-

---

nen Antrag zur Netzneutralität, BT-Drs. 18/5382. Der am 27.10.2015 vom EU-Parlament angenommene Gesetzgebungsakt zur Netzneutralität enthält Ausnahmen für das „Traffic Management" sowie für die Erbringung von Spezialdienstleistungen, vgl. Art. 3 des Entwurfs, im Internet abrufbar unter http://data.consilium.europa.eu/doc/document/ST-10788-2015-REV-2/en/pdf.

659 Vgl. auch *Europäisches Parlament* (Fn. 585), S. 25.

660 Vgl. auch die Definition der *Monopolkommission* (Fn. 584), Rz. 67.

661 Vgl. auch *Weber/Volz*, WuW 2015, 356.

sen Marktposition zu stärken (Lock-in Effekt), sowie dass ein marktmächtiges Unternehmen seine Nutzer ausbeuten könnte, indem es in übermäßiger Weise personenbezogene Daten abfragt. Daneben kommt eine Behinderung von Wettbewerbern in Betracht, wenn die angesammelten Datenbestände verwendet werden, um in andere Märkte zu expandieren oder wenn der Zugang zu „wesentlichen" Datenbeständen verweigert wird.

Ein Sonderproblem ist in diesem Zusammenhang, dass die Aufgreifkriterien der deutschen und europäischen Fusionskontrolle nicht an diese veränderten Marktgegebenheiten angepasst sind (dazu sogleich unten, Teil 1I.2.).

b) Derzeitiger Rechtsrahmen

Bei der Beurteilung von kostenlosen Dienstleistungen im Rahmen der Marktdefinition hat sich die kartellrechtliche Praxis mittlerweile weitgehend an die veränderten Bedingungen angepasst. Während Leistungen, die ohne monetäre Gegenleistung erbracht werden, nach klassischer Auffassung keinen Markt im Sinne der kartellrechtlichen Marktdefinition bildeten,[662] geben Behörden, Rechtsprechung und Literatur diese Auffassung im Rahmen der digitalisierten Ökonomie zunehmend auf.[663] So prüft z. B. die Kommission mittlerweile ganz selbstverständlich die Auswirkungen von Zusammenschlüssen auf Märkten, auf denen keine entgeltlichen Leistungen erbracht werden.[664]

Darüber hinaus können Wettbewerbsbeschränkungen im Zusammenhang mit der Konzentration und Verwendung von Daten grundsätzlich von den kartellrechtlichen Generalklauseln - insbesondere dem Missbrauchsverbot gem. §§ 19 ff. GWB, Art. 102 AEUV - erfasst werden. Dies gilt auch für die Ausnutzung von Verbrauchern durch die unverhältnismäßige Abfrage von Nutzerdaten und für die Behinderung von Wettbewerbern durch Zugangsverweigerung zu wesentlichen Daten sowie für den Missbrauch von Datenbeständen zur Expansion in andere Märkte (siehe dazu sogleich unten, Teil 1I.3.). In der bisherigen kartellrechtlichen Praxis haben diese Fragen jedoch keine große Rolle gespielt.[665] Die Konzentration von Nutzerdaten wurde allenfalls im Zusammenhang mit Online-Werbemärkten relevant.[666] Gleichfalls wurde bisher - soweit ersichtlich - kein eigener Markt für Nutzerdaten definiert.

---

[662] Zusammenfassend *Podszun/Franz*, NZKart 2015, 121.

[663] Vgl. *Weber/Volz*, WuW 2015, 356.

[664] Kommission, Beschl. v. 07.10.2011 im Fall COMP/M.6281 – *Microsoft/Skype*; Beschl. v. 04.12.2013 im Fall COMP/M.7047 – *Microsoft/Nokia*; Beschl. v. 03.10.2014 im Fall COMP/M.7217 – *Facebook/WhatsApp*. In diese Richtung auch Bundeskartellamt, Fallbericht v. 20.04.2015, Az. B6-39/15 – *Axel Springer/Immowelt*.

[665] Vgl. dazu EuGH, Urt. v. 23.11.2006, Rs. C-238/05, *Asnef-Equifax*, ECLI:EU:C:2006:734, Rz. 63; Kommission, Beschl. v. 03.10.2014 im Fall COMP/M.7217 – *Facebook/WhatsApp*, Rz. 163. Vgl. nun aber das Verfahren der belgischen Kartellbehörde gegen den staatlichen belgischen Lotterieanbieter, Nationale Loterij, Pressemitteilung v. 23.09.2015, im Internet abrufbar unter http://tinyurl.com/pae5x3w. Nationale Loterij wurde vorgeworfen, ihre Marktmacht missbraucht zu haben, indem sie die im Rahmen des Monopols für Lotterien gesammelten Kundendaten nutzte, um für ein neues Sportwettenangebot zu werben.

[666] Vgl. Kommission, Beschl. v. 03.10.2014 im Fall Nr. COMP/M.7217 – *Facebook/WhatsApp*, Rz. 70, 164.

c) Reformbedarf

Ob ein potentieller Markt für die Konzentration und Bereitstellung von Nutzerdaten kartellrechtliche Probleme aufwerfen könnte, müsste vertieft analysiert werden. Dagegen spricht zumindest auf den ersten Blick, dass zahlreiche Unternehmen (z. B. Apple, Amazon, eBay, Google, Microsoft, AOL, Yahoo!, Twitter, Facebook, etc.) Nutzerdaten sammeln und Nutzer ihre Daten nicht exklusiv zur Verfügung stellen.[667] Die zukünftige Entwicklung sollte jedoch sorgfältig beobachtet werden.

Darüber hinaus können Maßnahmen in den Bereichen Datenschutz- und Verbraucherschutzrecht getroffen werden, um auch die kartellrechtliche Missbrauchsgefahr zu verringern.[668] Auch hier sollte jedoch sorgfältig geprüft werden, inwieweit ein regulatorischer Eingriff tatsächlich erforderlich ist.

2. Notwendigkeit veränderter Aufgreifkriterien in der Fusionskontrolle

a) Problemaufriss

Der Erwerb des Kommunikationsdienstleisters WhatsApp durch Facebook im Jahr 2014 hat eine Debatte darüber ausgelöst, ob die Aufgreifkriterien in der Fusionskontrolle an die veränderten Bedingungen in der digitalen Ökonomie angepasst werden müssen. Insoweit wird die Gefahr gesehen, dass der Erwerb eines Unternehmens, welches zwar derzeit nur geringe Umsätze erwirtschaftet, jedoch über kommerziell wertvolle Datenbestände verfügt, „*unter dem Radar der Zusammenschlusskontrolle*“ hindurchsegeln könnte.[669]

b) Derzeitiger Rechtsrahmen

Sowohl die deutsche als auch die europäische Fusionskontrolle knüpfen bei den Aufgreifkriterien an die Umsätze der beteiligten Unternehmen an (vgl. § 35 Abs. 1 GWB, Art. 1 Abs. 2, 3 VO (EG) Nr. 139/2004 („FKVO“)). Daneben kann die Kommission einen Zusammenschluss, der die EU-Umsatzschwellen nicht erreicht, prüfen, wenn die beteiligten Unternehmen oder mindestens ein Mitgliedstaat dies beantragen und gewisse weitere Voraussetzungen erfüllt sind (vgl. Art. 4 Abs. 5, Art. 22 FKVO).

---

667 Vgl. Europäische Kommission, Beschl. v. 03.10.2014 im Fall Nr. COMP/M.7217 – *Facebook/WhatsApp*, Rz. 70, 188. Danach hat Google derzeit mit ca. 33% den größten Anteil an Nutzerdaten. Vgl. auch die Stellungnahme der Federal Trade Commission („FTC“) zu *Google/Doubleclick*, FTC File No. 071-0170, 20.12.2007, S. 12 f., im Internet abrufbar unter http://tinyurl.com/qhaemuq. Vgl. ferner *Lerner*, The Role of „Big Data“ in Online Platform Competition, 26.08.2014, im Internet abrufbar unter http://awards.concurrences.com/IMG/pdf/big.pdf.

668 Siehe dazu auch das „Recht auf Vergessenwerden“ (Art. 17) sowie das „Recht auf tät“ (Art. 18) in dem aktuellen Entwurf der Datenschutzgrundverordnung, im Internet abrufbar unter http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

669 *Zimmer*, WuW 2014, 923; *Monopolkommission* (Fn. 584), Rz. 453 ff.; *Körber*, WuW 2015, 120.

c) Reformbedarf?

Zur Anpassung der Fusionskontrolle an die Besonderheiten digitaler Märkte werden verschiedene alternative **Anknüpfungskriterien** diskutiert: Marktanteile;[670] Anzahl der Nutzer und die Bedeutung der Netzwerkeffekte;[671] sowie Transaktionsvolumen.[672] Während es sich bei den Umsatzschwellen um relativ klare Kriterien handeln, bringen die anderen vorstehend aufgelisteten Anknüpfungskriterien ein erhebliches Maß an Rechtsunsicherheit mit sich. Es sollte daher auch in diesem Zusammenhang sorgfältig geprüft werden, ob eine Anpassung tatsächlich erforderlich ist.

Weiterhin stellt sich die Frage, ob eine Anpassung lediglich auf EU-Ebene oder auch auf nationaler Ebene erfolgen sollte. Für eine Anpassung auf EU-Ebene spricht, dass die betroffenen digitalen Märkte in der Regel weiter als national abzugrenzen sein dürften und eine materielle Prüfung deshalb bei der Kommission angesiedelt werden sollte. Eine weitgehende Schließung der vermeintlichen Lücken wird dagegen nur erreicht, wenn die Anpassung auch auf nationaler Ebene erfolgt, da ansonsten Transaktion, die die EU-Schwelle nicht erreichen, (zumindest für Deutschland) weiterhin ungeprüft blieben.[673]

3. Internet der Dinge oder „Internet of Everything

a) Problemaufriss

Dem Zugang zu Daten kommt mittlerweile in den Bereichen der Produktentwicklung und -innovation zentrale Bedeutung zu.[674] Big-Data-Technologien dienen der Optimierung der eigenen Geschäftsprozesse und der Verbesserung des Geschäftsmodells. Big Data kann außerdem in der Forschung eingesetzt werden, z. B. in der Medizin. Im Rahmen der zunehmenden Digitalisierung traditioneller Wirtschaftsbereiche und der Entwicklung des „Internets der Dinge“[675] ermöglicht der Zugang zu Daten außerdem die Erschließung neuer Geschäftsbereiche. Google bietet z. B. seit März 2015 die Vermittlung von Kfz-Versicherungen an.[676] Ein weiteres Beispiel ist Apples Vorstoß in den „E-Health“ Bereich durch Verknüpfung von iPhone, Apple Watch und Gesundheits-App.[677]

In diesem Zusammenhang besteht die bereits oben angesprochene Gefahr, dass Unternehmen versuchen, sich einen Wettbewerbsvorteil zu verschaffen, indem sie anderen Unternehmen den Zugang zu „wesentlichen“ Daten verweigern.

---

670 Monopolkommission, XX. Hauptgutachten, 2012/2013, S. 69 f.

671 So *Europäisches Parlament* (Fn. 585), S. 60.

672 *Monopolkommission* (Fn. 584), Rz. 461, mit einem entsprechenden Vorschlag. Ähnlich wird in den USA die Anmeldepflicht nach dem sog. Hart-Scott-Rodino Act anhand des „Fair Market Value“ der Zielgesellschaft bestimmt.

673 Dafür *Monopolkommission* (Fn. 584), Rz. 463.

674 *Monopolkommission* (Fn. 584), Rz. 482.

675 „Internet der Dinge“ oder „Internet of Everything“ versteht man die Vernetzung physischer Objekte mit dem Internet, damit diese selbständig kommunizieren, Daten sammeln und austauschen können.

676 http://www.cash-online.de/versicherungen/2015/google-compare-2/252205.

677 Die Welt v. 12.06.2015, im Internet abrufbar unter http://tinyurl.com/njko8sn.

Darüber hinaus könnte ein Unternehmen seine durch Datenbestände vermittelte Marktmacht missbrauchen, indem es diese mittels einer Hebelwirkung auf einen anderen Markt überträgt.

b) Derzeitiger Rechtsrahmen

Die Verweigerung des Zugangs zu Daten könnte grundsätzlich als Lieferverweigerung bzw. unter Anwendung der *essential facilities* Doktrin vom Missbrauchsverbot nach §§ 19 ff. GWB, Art. 102 AEUV erfasst werden. Jedoch greift dieses nur bei Marktmacht. Dabei ist, wie bereits oben erläutert, im Zusammenhang mit Daten schon fraglich, wie der relevante Markt zu definieren ist und ob darauf Marktmacht besteht. Gerade Nutzerdaten werden von zahlreichen Unternehmen gesammelt; andererseits stellen Nutzer ihre Daten in der Regel auch nicht einem Unternehmen exklusiv zur Verfügung.

Die Übertragung von Marktmacht auf andere Märkte unter Ausnutzung einer Hebelwirkung wird ebenfalls vom Missbrauchsverbot erfasst. Allerdings fällt die Verwendung von Daten zur Erschließung neuer Märkte nicht unter die klassischen Fälle der Kopplung und der Bündelung.[678] Darüber hinaus dürfte auch hier die Abgrenzung danach schwer fallen, ob es sich noch um Leistungswettbewerb oder schon um einen Fall der illegalen Ausnutzung von Marktmacht handelt.

c) Reformbedarf?

Eventuell könnten Regelungen im Datenschutz- und im Verbraucherschutzrecht die wettbewerbsrechtlichen Bedenken beiseite räumen. Es sollte jedoch berücksichtigt werden, dass es sich bei der Nutzung von Daten zur Erschließung neuer Geschäftsbereiche grundsätzlich um innovative Geschäftsmodelle handelt. In diesem Zusammenhang sollte daher stets sorgfältig geprüft werden, ob ein regulatorischer Eingriff tatsächlich erforderlich ist.

IV. Herausforderung der digitalen Wirtschaft für das europäische Beihilferecht

Die Digitalisierung der Wirtschaft und die Vernetzung der Industrie bedeuten auch für das europäische Beihilfenrecht eine Reihe von neuen Herausforderungen, wobei es insoweit vor allem darum geht, überzeugende beihilferechtliche Antworten auf wettbewerbs- und industriepolitische Fragestellungen in den Zeiten einer zunehmend globalisierten Wirtschaft zu geben. Zusätzlich sind Sparanstrengungen öffentlicher Haushalte im Nachgang zur Finanz- und Wirtschaftskrise aus dem Jahre 2008 und den Folgejahren bzw. daraus resultierende Budgetbeschränkungen zu berücksichtigen.[679] Schon dieses Schlaglicht zeigt, dass es sich um ein komplexes Themenfeld mit vielfältigen Interessenlagen handelt. Der nachfolgende kurze Überblick versucht deshalb, zunächst die wesentlichen Herausforderungen zu

---

[678] Vgl. *Eilmansberger* in Streinz, EUV/AEUV, Art. 102 AEUV, Rz. 99 ff.

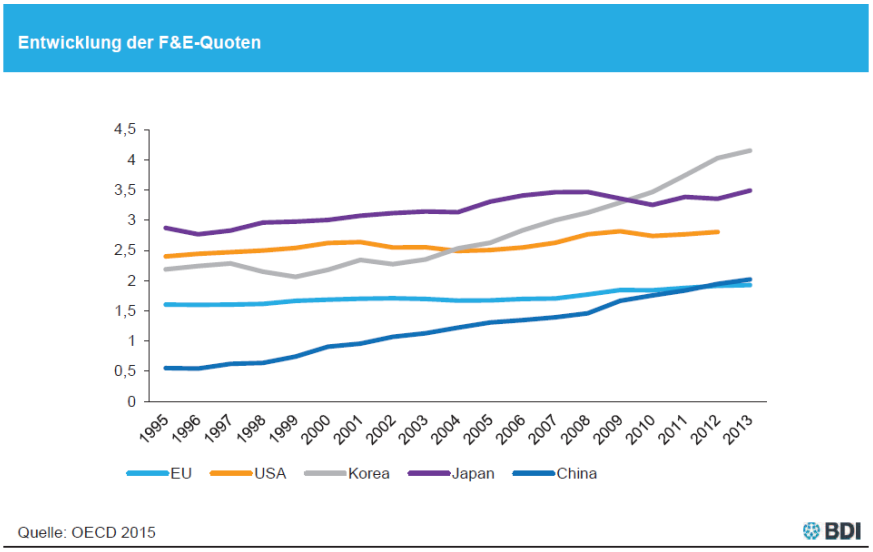
[679] Vgl. *Almunia*, Doing more with less – State aid reform in times of austerity: Supporting growth amid fiscal constraints, SPEECH 13/14, King's College – The modernisation of State aid rules, London, 11 January 2013.

benennen (1. Problemaufriss) und sodann die Leitprinzipien des europäischen Beihilfenrechts bzw. der europäischen Beihilfenpolitik zu skizzieren (2. Rechts- und Politikrahmen), um daran anschließend zu beleuchten, ob und inwieweit (legislativer) Handlungsbedarf besteht (3. Perspektiven und Lösungsansätze).

1. Problemaufriss

Nach der Lissabon-Strategie sollte die EU – übrigens bereits bis 2010 – zum *„wettbewerbsfähigsten und dynamischsten wissensbasierten Wirtschaftsraum der Welt“* werden. Dass dieses Ziel nicht erreicht werden konnte, liegt nicht nur an den Wirtschaftskrise aus dem Jahr 2008 und den Folgejahren. Vielmehr lässt sich feststellen, dass Produktionsanlagen zum Teil veraltet sind, der Infrastrukturausbau einschließlich der Erneuerung wichtiger Infrastrukturen nur langsam vorankommt und auch die Digitalisierung der Wirtschaft nicht so schnell wie erwartet stattfindet. Für die deutsche und die europäische Wirtschaft bedeutet das einen Verlust an Wettbewerbsfähigkeit und Wachstumspotential, für den deutschen Staat wie für die anderen EU-Mitgliedstaaten ein niedrigeres Niveau an Arbeitsplätzen und geringere Steuereinnahmen.

Dabei ist zu berücksichtigen, dass die deutschen und europäischen Unternehmen in vielen Bereichen in einem globalen Wettbewerb mit Unternehmen aus den USA, China, Japan, Korea, Indien und Brasilien stehen. Aufschlussreich ist deshalb ein Blick auf die F&E-Quoten im Verhältnis zur jährlichen Wirtschaftsleistung:



Aus der vorstehenden Graphik geht nicht nur hervor, dass die F&E-Quote in der EU mit einem Wert von ca. 2% noch erheblich von dem Ziel der Europa-2020-Strategie entfernt ist, das bei 3% liegt.[680] Vor allem aber zeigt sich, dass der Abstand zu wichtigen Wettbewerbern

[680] Vgl. http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/targets/index_de.htm.

wie Japan, Korea und den USA eher gewachsen ist als abgenommen hat und China, das lange Zeit zurücklag, die EU mittlerweile überholt hat.

Wie die nachfolgende Graphik zeigt, geht die Europäische Investitionsbank davon aus, dass der Investitionsbedarf pro Jahr in der EU für F&E ca. EUR 130 Mrd. beträgt. Der für die Digitalisierung benötigte Betrag liegt bei EUR 55 Mrd.

Jährlicher Investitionsbedarf in der Europäischen Union

Bereich	Benötigtes Investitionsvolumen in Mrd. Euro
Forschung und Entwicklung	130
Energienetze	100
Verkehrsnetze	50
Digitalisierung der Wirtschaft	55
Bildungseinrichtungen	10
Umwelt, Wasser und Klima	90

Quelle: EIB 2015a

BDI

Die vorstehenden Erwägungen belegen nicht nur, dass der Fokus auf die Digitalisierung der Wirtschaft und die Vernetzung der Industrie richtig ist, sondern auch, dass aus beihilferechtlicher Sicht Handlungsbedarf besteht, z.B. Anreize für eine Steigerung von F&E-Quoten zu setzen. An diesem Erfordernis müssen sich die bestehenden Regelungen messen lassen.

2. Rechtliche und politische Rahmenbedingungen

Die EU hat erst kürzlich eine Investitionsoffensive beschlossen; Beschäftigung, Wachstum und Investitionen zählen dabei zu den Prioritäten der Kommission.[681] Mittels des neu geschaffenen Europäischen Fonds für strategische Investitionen (EFSI) sollen insgesamt EUR 315 Mrd. für die Realwirtschaft bereitgestellt werden, um die Wettbewerbsfähigkeit zu steigern und Wachstum anzuregen. Hiervon stammen als Anschubfinanzierung EUR 21 Mrd. von der EU.[682] Unabhängig hiervon stellt die EU innerhalb ihres Forschungs- und Rahmenprogramms „Horizont 2020“ ca. EUR 80 Mrd. für die Periode 2014 – 2020 zur Verfügung.[683]

Aus beihilferechtlicher Sicht stehen seit der seit 2012 umfassend betriebenen Modernisierung des EU-Beihilfenrechts sog. „gute Beihilfen“, die auf die Behebung eines ausgewiesenen Marktversagens und auf die Förderung von im gemeinsamen Interesse liegenden Zielen ausgerichtet sind, im Fokus.[684] Dieser Ansatz ist im Zusammenhang mit der von der Kommission verfolgten Wettbewerbs- und Beihilfenpolitik zu sehen, welche die Förderung der

[681] http://ec.europa.eu/priorities/index_de.htm.
[682] http://ec.europa.eu/priorities/jobs-growth-investment/plan/efsi/index_de.htm.
[683] http://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020.
[684] Kommission 08.05.2012 – KOM(2012) 209 endg. (Mitteilung Modernisierung des EU-Beihilfenrechts).

Verbraucherwohlfahrt und einen positiven Beitrag zu Wachstum, Beschäftigung sowie Wettbewerbsfähigkeit zu zentralen Anliegen erklärt.[685] Nach der Kommission bilden Beihilfen ein Element zur Verwirklichung eines Binnenmarktes für das 21. Jahrhundert.[686] Im Hinblick auf die Ermessensausnahmen des Art. 107 Abs. 3 AEUV lässt sich dieser Ansatz der Kommission dahingehend verstehen, dass die Ermessensausnahmen vor allem unter Berücksichtigung eines *„more economic approach"* zur Behebung von Marktversagen genutzt werden sollen. Der damalige Wettbewerbskommissar Almunia hat dies in folgende Worte gekleidet: *„Of course, this does not mean that State aid is forbidden, quite the contrary. In our social-market economy, government intervention is justified – in fact, it is necessary in some case – to complement market forces when they fail to produce the desired outcomes."*[687]

Im hier gegebenen Kontext sind vor allem die folgenden rechtlichen Regelungen Beispiele für diese Schwerpunktsetzung der Kommission:

- die VO 651/2014 vom 17.06.2014 (Allgemeine Gruppenfreistellungsverordnung), vgl. insbesondere die Erläuterungen in Rz. 2, 39 und 45 ff. und 55 ff. der Erwägungsgründe, in denen auf den Stellenwert von F&E&I für ein nachhaltiges Wachstum und eine größere Wettbewerbsfähigkeit sowie die Strategie 2020 hingewiesen wird,[688]

- der Unionsrahmen für staatliche Beihilfen zur Förderung von Forschung, Entwicklung und Innovation, in dem bereits in der Einleitung Bezug auf die Wachstumsstrategie 2020 genommen und die Bedeutung von F&E für ein nachhaltiges Wachstum herausgestellt wird; außerdem wird die Notwendigkeit staatlicher Beihilfen zur Überwindung von Marktversagung bestätigt (2014/C 198/01),[689]

- die Mitteilung der Kommission zu den Kriterien für die Würdigung der Vereinbarkeit von staatlichen Beihilfen zur Förderung wichtiger Vorhaben von gemeinsamem europäischen Interesse mit dem Binnenmarkt, vgl. insbesondere die Beschreibung des gemeinsamen europäischen Interesses in Ziffer 3.2.1, die explizit die Europa-20-20 Strategie, aber auch die Digitale Agenda für Europa oder die Integrierte Industriepolitik für das Zeitalter der Globalisierung als Beispiele nennt (2014/C 188/02)[690].

Während aus unserer Sicht der wettbewerbspolitische Ansatz der Kommission (Ausrichtung an den Zielen der Europa-2020-Strategie, Betonung der Bedeutung von F&E&I für ein nach-

---

685 Bericht über die Wettbewerbspolitik (2011), SWD(2012) 141 final, S. 10 ff.

686 Mitteilung Europa 2020, S. 25: *„Auch die Beihilfenpolitik kann aktiv und positiv zu den Zielen von Europa 2020 beitragen, indem sie Initiativen zugunsten innovativerer, effizienterer und umweltfreundlicherer Technologien anregt und fördert und den Zugang zu staatlicher Förderung von Investitionen, Wagniskapital und Forschung und Entwicklung erleichtert."*

687 *Almunia*, Modernising State aid control, SPEECH/12/117, European Economic and Social Committee, Brussels, 23 February 2012.

688 ABl.EU 2014/L 187/1.

689 ABl.EU 2014/C 198/1.

690 ABl.EU 2014/C 188/4.

haltiges Wachstum, Beihilfen v.a. zur Behebung von Marktversagen und zur Stärkung der Wettbewerbsfähigkeit) grundsätzlich Zustimmung verdient, weisen die vorstehend genannten Regelungen einige Defizite auf, die insbesondere im Hinblick auf die erwünschte Digitalisierung der Wirtschaft kritisch zu bewerten sind. Zu Einzelheiten siehe sogleich den folgenden Abschnitt.

3. Kritikpunkte, Lösungsansätze und Perspektiven

So scheint es zunächst überlegenswert, ob die bislang in Rdn. 92 des Unionsrahmens für F&E&I und in Rdn. 34 der Mitteilung der Kommission zu den Kriterien für die Würdigung der Vereinbarkeit von staatlichen Beihilfen zur Förderung wichtiger Vorhaben von gemeinsamem europäischen Interesse mit dem Binnenmarkt enthaltene sel“ (d.h. die Berücksichtigung des Umstandes, wenn Wettbewerber außerhalb der Union in den vergangenen drei Jahren für vergleichbare Vorhaben direkt oder indirekt Beihilfen gleicher Intensität erhalten haben) nicht auch auf anderen Beihilfen wie z.B. Regionalbeihilfen ausgedehnt werden sollte; dabei könnte darauf abgestellt werden, ob es in dem betreffenden Bereich globalen Wettbewerb gibt. Da die Entsprechungsklausel bislang kaum jemals eine Rolle gespielt hat, wäre zudem zu ermitteln, woran dies liegt, um ihre praktische Anwendbarkeit sicherzustellen.

In Bezug auf die Förderung wichtiger Vorhaben von gemeinsamem europäischen Interesse erscheint die Voraussetzung, dass in der Regel mehr als ein Mitgliedstaat beteiligt sein muss, als eng und restriktiv; wünschenswert ist insoweit, dass die Kommission in ihrer Fallpraxis hier zu einer Auslegung gelangt, die berücksichtigt, dass auch bei Beteiligung nur eines Mitgliedstaates wegen der materiellen Zielsetzung des Vorhabens ggf. eine europäische Dimension haben kann. Ferner dürfte die im Rahmen der Vereinbarkeitsprüfung vorgesehene ausführliche Darstellung und Beschreibung der kontrafaktischen Fallkonstellation Mitgliedstaaten und Unternehmen gerade in diesem Bereich vor nicht unerhebliche praktische Schwierigkeiten stellen, etwa wenn es kein alternatives Vorhaben gibt. Abhilfe könnten insoweit Best-Practice-Beispiele der Kommission sein, die Mitgliedstaaten und Unternehmen als Orientierung dienen können.

Im Rahmen dieser Darstellung kann nicht auf sämtliche Kritikpunkte eingegangen werden. Die Beispiele zeigen aber, dass die von der Kommission im Rahmen der Modernisierung des EU-Beihilfenrechts erlassenen Regelungen an der ein oder anderen Stelle weiterhin verbesserungsbedürftig erscheinen. Aus unserer Sicht kommt es deshalb vor allem darauf an, dass die EU-Kommission bei der Anwendung der neuen Regelungen hinreichend flexibel agiert, um die allseits geteilten Ziele einer Digitalisierung der Wirtschaft und der Vernetzung der Industrie in enger Kooperation mit den Mitgliedstaaten bestmöglich umzusetzen. Daneben sind gemeinsame Anstrengungen der Unternehmen und der Politik erforderlich, sei es bei der Definition wichtiger Vorhaben von gemeinsamem europäischen Interesse, der Identifikation von Bereichen, in denen konkret Marktversagen droht, und dem entsprechenden “Design” von staatlichen Maßnahmen, mit denen dem Marktversagen abgeholfen werden

kann. Dabei sollte sichergestellt werden, dass die hierbei gemachten Erfahrungen zeitnah in einen weiter fortzuführenden Reformprozess des europäischen Beihilfenrechts eingebracht werden können, um eine noch bessere Anpassung an und Verzahnung mit den Europa-2020-Zielen zu erreichen.

Teil 15 Telekommunikationsrecht und Netzausbau *(Dr. Tobias Frevert, Dr. Michael Bergmann, Pascal Schumacher)*

Die Kommunikation von „Maschine zu Maschine“, wie sie prägend für die Industrie 4.0 ist, wird maßgeblich auf die (zumeist funktechnische) Einbindung von Industrieanlagen, Haushalts- und Gebrauchsgegenständen in eine Kommunikationsinfrastruktur angewiesen sein. Insofern liegt die Frage nach der Anwendbarkeit der Telekommunikationsregulierung (auch) auf die Hersteller der kommunizierenden Maschinen (sog. Connected Devices) nahe.

Der Regulierungsrahmen – wie er insbesondere durch das Telekommunikationsgesetz (TKG) vorgegeben wird – ist maßgeblich durch einen technologieneutralen und entwicklungsoffenen Ansatz geprägt. Dieser ermöglicht aus unserer Sicht schon heute eine Abgrenzung der telekommunikationsrechtlichen Verantwortlichkeiten von Herstellern, Netzbetreibern und Telekommunikationsdiensteanbietern mit dem gebotenen Maß an Rechtssicherheit. Grundsätzliche Schwierigkeiten für den Betrieb von Connected Devices sind – soweit sich Geschäftsmodelle schon heute abzeichnen – in der regulatorischen Ausgangslage nicht angelegt (dazu unter I.). Die begrenzten Nummernressourcen könnten perspektivisch allerdings die M2M-Kommunikation insgesamt erschweren (dazu unter II.). Als Hemmschuh könnte sich eine restriktive Regelung der Netzneutralität erweisen, die sich aktuell indes nicht abzeichnet (dazu unter III.). Wichtige Parameter daneben sind klare Haftungsregeln, ein zügiger Netzausbau und eine hinreichend vereinheitliche EU-weite Regulierungspraxis (dazu unter IV.-VI.).

I. Regulatorischer Rahmens

Nach inzwischen gefestigter Rechtsauffassung handelt es sich bei der Kommunikation von „Maschine zu Maschine“, wie sie zum Beispiel für Connected Cars und andere Anwendungsbereiche der digitalisierten Wirtschaft zum Einsatz kommt,[691] um Telekommunikation im Sinne des TKG.[692] Die zugrundeliegende Infrastruktur, also das Kommunikationsnetz, über welches Daten zwischen der Plattform des Herstellers und dem Connected Device ausgetauscht werden, ist zudem ein Telekommunikationsnetz, für welches grundsätzlich der Netzbetreiber verantwortlich ist. Schließlich ist auch der (technische) Transport von Steuersignalen über ein Telekommunikationsnetz als das Angebot eines Telekommunikationsdienstes einzustufen, welches der Regulierung unterfällt (§ 3 Nr. 24 TKG). Zu entscheiden ist daher im jeweiligen Einzelfall, wer den jeweiligen Dienst anbietet bzw. das eingesetzte Netz betreibt und dann Adressat der telekommunikationsrechtlichen Regulierung, aber auch der Kundenschutzvorschriften ist.

---

691 D.h. zwischen den Komponenten eines Connected Cars (Sensoren etc.) mit anderen Elementen der Verkehrsinfrastruktur (Verkehrszeichen, Parkplätze, andere Fahrzeuge etc.).

692 Vgl. nur *Grünwald/Nüßing*, MMR 2015, 378, 379 mit Verweis auf BVerfG, B. v. 12.10.1977 – 1 BvR 216/75,1 BvR 217/75, Rn. 66; BayOLG, U. v. 29.5.1979 – RReg 4 St 88/79, Rn. 10; LG Magdeburg, B. v. 3.2.2006 – 25 Qs 7/06, Rn. 8 ff.; BGH-Ermittlungsrichter, B. v. 21.2.2001 – 2 BGs 42/01, Rn. 10; *LG Ravensburg* NStZRR 1999, 84, 85.

Denkbar ist zum einen, dass allein der Mobilfunknetzbetreiber sowohl die Infrastruktur betreibt als auch die Signalübertragung übernimmt. Sein Kunde wäre dann entweder der Hersteller des Connected Device, zum Beispiel der Automobilhersteller, der in eine direkte Leistungsbeziehung mit dem Mobilfunknetzbetreiber eintritt.[693] Sein Kunde kann, je nach Vertragsgestaltung, aber auch der individuelle Nutzer sein, also beispielsweise der Fahrer eines Connected Car.

Aber auch der Hersteller eines Connected Device kann – ähnlich einem MVNO (also einem Weiterverkäufer von Telekommunikationsdienstleistungen unter Nutzung eines fremden Netzes) – TK-Diensteanbieter und ggfls. sogar Netzbetreiber sein. Letzteres insbesondere dann, wenn die zugrundeliegende Kommunikationsinfrastruktur nicht über Mobilfunk realisiert wird, sondern – wie derzeit bspw. von einigen Herstellern im Bereich der Connected Cars erwogen – über WLAN-ähnliche Technologie, die den Datenaustausch zwischen Autos und über fest im Straßenraum installierte „Points of Contact“ ermöglicht.

Auch der Betrieb einer M2M-Kommunikationsplattform kann im Einzelfall dazu führen, dass der Connected Device-Hersteller regulierungspflichtige Dienstleistungen anbietet. Das ist insbesondere dann der Fall, wenn er neben dem reinen Versand und Empfang von Steuersignalen zusätzlich eine – für den Dienst nicht ganz untergeordnete – Weiterleitung von Signalen (Routing) an Geräte vornimmt (z. B. Versendung von Befehlen zum Öffnen der Garage, eines Steuersignals zur Temperaturregelung im Smart Home oder einer SMS an einen Bekannten, dessen Smartwatch in der Nähe befindet).[694]

Reguliert wird grundsätzlich (nur) das Angebot *öffentlich* zugänglicher Telekommunikationsdienste i. S. d. §§ 3 Nr. 24, 6 TKG. Solange der Connected Device-Hersteller für die Telekommunikationsdienste auf das Angebot eines TK-Anbieters zurückgreift, unterfällt er selbst nicht der TK-Regulierung. Auch der automatische Aufbau von Notrufverbindungen, wie er beispielsweise im Rahmen des europäischen eCall-Systems stattfindet, das ab dem 31. März 2018 verpflichtend in der EU in alle neuen Modelle von Pkw und leichten Nutzfahrzeugen eingebaut werden muss,[695] ändert daran nichts. Zwar werden die automatisierten Notrufe durch die Bordelektronik abgesetzt, so dass der Fahrzeughersteller grundsätzlich auch die Funktionsherrschaft über diesen Telekommunikationsdienst hat. Allerdings setzt der eCall selbst auf der Notruffunktionalität des Mobilfunknetzes auf, so dass jedenfalls der Schwerpunkt dieser Dienstleistung beim Netzbetreiber, nicht beim Fahrzeughersteller liegt.[696] Etwas anderes würde allenfalls dann gelten, wenn der Automobilhersteller über die von ihm installierte Bordelektronik selbst Telekommunikationsdienste anbieten würde (Telefonie, Internet). Kommt der entsprechende Dienstleistungsvertrag mit dem Endkunden allerdings nicht mit dem Fahrzeughersteller, sondern mit dem Mobilfunkanbie-

---

[693] *Weisser/Färber*, MMR 2015, 506, 509 f.

[694] *Grünwald/Nüßing*, MMR 2015, 378, 380.

[695] Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG.

[696] *Weisser/Färber*, MMR 2015, 506, 509.

ter zustande, fällt auch in dieser Konstellation der Fahrzeughersteller aus der Regulierung heraus.

II. Begrenzte Nummernressourcen

Fachleute erwarten, dass Connected Devices und die M2M-Kommunikation in den kommenden Jahren zum wesentlichen Wachstumstreiber für die TK-Industrie werden. Prognosen zufolge werden die Zuwachsraten im M2M-Bereich um ein Vielfaches über denen der Sprachkommunikation liegen. Vor allem wird aber die Anzahl von Connected Devices rasant steigen.[697] Mit dieser Entwicklung Hand in Hand geht auch ein steigender Bedarf für mehr Rufnummernressourcen für Connected Device-Dienste. Denn die Verfügbarkeit von Nummern ist eine wesentliche Voraussetzung für den Betrieb einer M2M-Infrastruktur und entsprechende Dienste.

Zuständig für die Strukturierung und Ausgestaltung des Nummernraumes ist gem. § 66 TKG und der Telekommunikations-Nummerierungsverordnung (TNV) die Bundesnetzagentur. Im Rahmen ihrer Regelungskompetenz könnte die Regulierungsbehörde daher weitere Rufnummernblöcke für M2M-Dienste zuweisen, um einer künftigen Nummernknappheit frühzeitig entgegenzuwirken. Teilweise wird sogar ein eigener Nummernraum für M2M-Dienste gefordert.[698] Da Connected Devices typischerweise nicht nur im Inland sondern auch über Landesgrenzen hinweg gehandelt und genutzt werden, bietet sich unseres Erachtens sogar eine Lösung auf europäischer Ebene an. So sollte erwogen werden ob nicht perspektivisch EU-weit einheitliche M2M Rufnummern[699] in einem One-Stop-Shop Verfahren (bspw. über das Kooperationsgremium der nationalen Regulierer, GEREK) vergeben werden. So würde nicht nur den Marktentwicklungen und somit dem Rufnummernbedarf effektiv Rechnung getragen, sondern auch in technischer Hinsicht der grenzüberschreitende Einsatz und Handel von Connected Devices vereinfacht (insb. das Routing der Signale verbessert).

III. Netzneutralität

Die (Mit-)Nutzung vorhandener Mobilfunkinfrastruktur für den Betrieb von M2M-Kommunikation kann im Einzelfall hohe Anforderungen an Ausfallsicherheit, Übertragungsqualität und Übertragungsgeschwindigkeit stellen. Es müsste insbesondere vermieden werden, dass es zu Engpässen bei der Datenübertragung für zeitkritische Dienste wie Connected Cars durch andere, weniger kritische Dienste kommt. Das aktuelle TKG behandelt die Möglichkeit der Priorisierung von Diensten allenfalls kursorisch[700], den Gesetzgebungsvorstoß aus

---

[697] http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Rufnummern/M2M/M2M_node.html.

[698] VATM, Stellungnahme zu BNetzA Mitteilung Nr. 139/2011, abrufbar unter http://www.vatm.de/uploads/media/2011-04-20_VATM-Stellungnahme_M2M_pdf.pdf.

[699] Sog. Mobile Subscriber Integrated Services Digital Network Number (MSISDN).

[700] Vgl. Frevert, MMR 2012, 510.

2013[701] hat die Bundesregierung mit Verweis auf das Gesetzgebungsverfahren auf Ebene der EU[702] nicht weiter verfolgt[703].

Auf europäischer Ebene ist die Normsetzung mittlerweile abgeschlossen. Das EU-Parlament hat am 27. Oktober 2015 den Entwurf des Europäischen Rates für eine Verordnung „über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union“ nach zweiter Lesung verabschiedet. Die neuen Regelungen sehen die Möglichkeit der logischen Trennung von Netzen in unterschiedliche Bereiche vor. Ein Bereich, das offene Internet, folgt danach grundsätzlich dem „best effort“ Prinzip (alle Datenpakete werden mit gleicher Priorität behandelt). Ein anderer Bereich bleibt Spezialdiensten vorbehalten, die mit zuverlässiger Qualität abgewickelt werden und für die der Betreiber klare Qualitätsparameter versprechen kann.[704] Mit der Anwendung strenger Netzneutralität lediglich auf logische Teilkapazitäten scheinen die neuen Regeln grundsätzlich geeignet, den nötigen Rahmen für verlässliche Spezialdienste zu schaffen. Wie sich diese Unterscheidung in der Praxis bewährt, bleibt abzuwarten.

IV. Haftung

Nach § 44a TKG ist die Haftung des Anbieters von öffentlich zugänglichen Telekommunikationsdiensten für Vermögensschäden (nicht aber Personen- und Sachschäden) auf Euro 12.500 je Endnutzer und insgesamt Euro 10 Millionen je Ereignis beschränkt. Bei M2M-Anwendungen sind sehr viel höhere Vermögensschäden denkbar als in der klassischen Sprachtelefonie, die § 44a als Leitbild zugrunde liegt.[705] So wird bspw. bei Connected Cars das Auto zum Telekommunikationsendgerät, und ein Unfall kann neben Personen- und Sachschäden auch hohe Vermögensschäden (etwa Verdienstausfall) nach sich ziehen. Es ist fraglich, ob diese Haftungsbeschränkung sinnvoll ist, um Vertrauen in solche Dienste aufzubauen. Den Anbietern ist es indes unbenommen, auch eine höhere Haftung zu übernehmen, wobei sich dies im Preis des jeweiligen Dienstes niederschlagen wird. Gleichzeitig stellt sich die Frage, ob eine unbeschränkte Haftung für Personen- und Sachschäden gegenüber dem Endkunden nach dem Produkthaftungsgesetz dem flächendeckenden Einsatz von M2M-Kommunikation im Weg stehen kann.

So ließe sich bspw. erwägen, das telekommunikationsrechtliche Haftungssystem nach Vorbild des Stromnetzbetriebs (§ 18 der Niederspannungsanschlussverordnung, NAV) umzuge-

---

[701] Vgl. Frevert, ZRP 2013, 166.

[702] Koalitionsvertrag zwischen CDU, CSU und SPD zur 18. Legislaturperiode, Deutschlands Zukunft gestalten, S. 49.

[703] *Neitzel/Hofmann*, in: Spindler/Schuster, Recht der elektronischen Medien, § 41a Rn. 30.

[704] Siehe insbesondere Artikel 3 Ziffer 5 der Verordnung.

[705] Vgl. zur Normgenese unter Bezugnahme auf den Verweis des Bundesrates auf die „gängigen Tarife“ im Standardtelefoniegeschäft Kessel, in: Arndt/Fetzer/Scherer, TKG, 2008, § 44a Rn. 6, Fn. 11.

stalten, d.h. neben abgestuften relativen Haftungsgrenzen je Geschädigtem auch absolute Haftungshöchstgrenzen je Schadensereignis vorzusehen. Übersteigt die Summe der Einzelschäden die absolute Höchstgrenze, wären die Einzelansprüche dann anteilig zu kürzen (vgl. § 18 Abs. 5 NAV). Auf diese Weise könnte der Gesetzgeber die Interessen der Beteiligten im Dreieck zwischen TK-Anbieter, Geschädigtem sowie dem Interesse der übrigen Kunden an kostengünstigen Diensten angemessen zum Ausgleich bringen. Soweit im Rahmen einer solchen Neuregelung auch Haftungsbeschränkungen für Sach- und Personenschäden aufgenommen werden sollen, ist indes der Vorrang des Produkthaftungsrechts zu beachten.[706] Eine Haftungsbeschränkung wäre insoweit wohl auf Ebene der EU zu regeln.

V. Netzausbau

In hochentwickelten Staaten sind es heutzutage vor allem Investitionen in eine Modernisierung der Breitbandinfrastruktur, die zum Produktivitätswachstum der (zunehmend digitalisierten) Wirtschaft beitragen.[707] Die Verfügbarkeit von Breitbandanschlüssen in der Fläche und der Ausbau einer hochleistungsfähigen Netzinfrastruktur sind auch in Deutschland Schlüsselfaktoren für die Entwicklung der Industrie 4.0. Dies hat die Bundesregierung bereits früh erkannt. In ihrer Breitbandstrategie aus dem Jahr 2009[708] hat sich u.a. zum Ziel gesetzt, dass bis 2018 flächendeckend Anschlüsse mit mindestens 50 Megabit pro Sekunde zur Verfügung stehen. Erreicht werden soll dies mit einer Vier-Säulen-Strategie, die neben einer unterstützenden Frequenzpolitik, einer wachstums- und innovationsorientierten Regulierung und finanziellen Fördermaßnahmen auch die Nutzung von Synergien beim Infrastrukturausbau umfasst. Obwohl einige Maßnahmen bereits umgesetzt wurden, ist die Erfolgsbilanz bislang durchwachsen. Als Gründe für den stockenden Ausbau macht die Telekommunikationswirtschaft v.a. die hohen Ausbaukosten bei gleichzeitig rückläufigen Umsätzen geltend.

Mit dem Ziel die Ausbaukosten zu senken, hatte der Gesetzgeber daher 2012 die §§ 77a ff. in das TKG eingeführt.[709] Sie sollen den Netzbetreibern eine kostengünstige Mitnutzung von „alternativen Infrastrukturen“ (also Schienennetze, Wasserstraßen und Abwasserkanäle, Energieleitungen sowie Kabelkanäle in Straßen) ermöglichen. Über diese Infrastrukturen existiert häufig bereits ein Weg zum Kunden, der durch freie Leerrohrkapazitäten oder die Mitnutzung von vorhandenen Glasfasern für den Breitbandausbau nutzbar gemacht werden kann. Insgesamt bergen die Regelungen zur Mitbenutzung der alternativen Infrastruk-

---

[706] Einer nationalen Haftungsprivilegierung dürfte jedenfalls nach Auffassung des EuGH der Anspruch der Produkthaftungsrichtlinie auf Vollharmonisierung entgegenstehen, vgl. *Wagner*, in Münchener Kommentar BGB, 6. Auflage 2013, Einleitung Rn. 3 mwN in Fn. 18.

[707] Vgl. nur OECD, Broadband and Economy, Ministerial Background Report DSTI/ICCP/IE(2007)3/FINAL, 2008; Czernich et al., Economic Journal 2011, 505 ff.

[708] http://www.zukunft-breitband.de/SharedDocs/DE/Anlage/ZukunftBreitband/breitbandstrategie-der-bundesregierung.html?nn=126140.

[709] Vgl. dazu *Schramm/Schumacher*, in: Beck’scher Kommentar zum TKG, 4. Aufl. 2013, §§77a ff.; dies., MMR 2013, 571 ff; Beine, MMR 2013, 290 ff.; *Stelkens/Wabnitz*, MMR 2014, 730 ff.

turen durch TK-Unternehmen allerdings eine Vielzahl offener Rechtsfragen.[710] Zudem gewähren die aktuellen Regelungen TK-Anbietern keinen rechtsförmlichen Anspruch auf Zugang zu alternativen Infrastrukturen. Sie setzen vielmehr auf ein reines Verhandlungsregime, was sich in der Praxis häufig als Hemmschuh erweist.[711] Vor allem Energienetzbetreiber agieren zögerlich. Sie fürchten Interferenzen mit ihren Aufgaben im Rahmen der Energiewende. Zudem lehnte die Bundesnetzagentur bislang eine Anerkennung von Mitnutzungskosten und -einnahmen in der Entgeltregulierung ab und verwehrte ihnen so pekuniäre Anreize. Synergien blieben daher häufig ungenutzt.

Nun zeichnet sich eine neue Entwicklung ab. Zur Umsetzung der Richtlinie 2014/61/EU über „Maßnahmen zur Reduzierung der Kosten des Ausbaus von Hochgeschwindigkeitsnetzen für die elektronische Kommunikation“ (KostensenkungsRL) hat das Bundesministerium für Verkehr und digitale Infrastruktur am 11. September 2015 einen Gesetzentwurf zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze (DigiNetzG) vorgelegt. Neben einer Vielzahl weiterer Themen, die ähnlich – aber keineswegs identisch – auch in §§ 77 a-e TKG a.F. adressiert sind, sieht der DigiNetzG ausdrücklich rechtsförmliche Mitnutzungsansprüche vor, die deutlich über den aktuellen Gesetzesstand im TKG hinausgehen. Zusätzlich führt der DigiNetzG-E den sog. „Wohnungsstich“ ein (§ 77k TKG-E): Betreiber von Telekommunikationsnetzen sollen Netze „in den Räumen des Teilnehmers abschließen“ dürfen, soweit in dem betreffenden Gebäude hochgeschwindigkeitsfähige Infrastrukturen fehlen. Zudem sollen zukünftig Einnahmen aus der Mitnutzung von der Kostenbasis für die Entgeltregulierung im für den (Energie-)Netzbetreiber einschlägigen Regulierungsrecht (bspw. nach StromNEV) abgezogen werden können (§ 77f TKG-E). Damit gewährt der Gesetzentwurf den Unternehmen nun auch dringend benötigte finanzielle Anreize.

Kritisch ist gleichwohl anzumerken, dass der aktuelle Entwurf zum DigiNetzG keine Möglichkeit der Verlegung von Telekommunikationslinien in geringer Tiefe im Rahmen konventionellen Tiefbaus schafft und damit ein erhebliches Einsparpotential ungenutzt lässt. Gleiches gilt für den Vorrang der unterirdischen Verlegung von Telekommunikationslinien, den der DigiNetzG-E unberührt lässt. Hierdurch bleibt ein weiteres erhebliches Einsparpotential ungenutzt.

VI. EU-weite Vereinheitlichung der Regulierungspraxis

Neben den hohen Ausbaukosten hat die Europäische Kommission wiederholt auch eine zerklüftete Regulierungslandschaft, die allzu oft an nationalen Grenzen halt mache, als Hemmnis für grenzüberschreitende Investitionen in die Breitbandinfrastruktur kritisiert. Mit früheren Bestrebungen zur Schaffung einer zentralen EU-Regulierbehörde für Telekommu-

[710] Vgl. dazu ausf. *Schumacher*, RdE 2013, 213 ff.

[711] Vgl. nur *Koch*, in: Berliner Kommentar zum TKG, 3. Aufl. 2013, § 77b Rn. 2, der die Wirkkraft der Regelung als zu „schwach“ einschätzt. Ausf. zum Verhandlungsregime und den Vorstellungen des Gesetzgebers *Stelkens/Wabnitz*, MMR 2014, 730, 733 f.

nikation – bekannt bspw. von den europäischen Agenturen[712] (z.B. ACER und FRONTEX) oder der Europäischen Zentralbank[713] – war die Kommission allerdings nicht erfolgreich.[714] Sie sucht nun nach Alternativen, insb. über Koordinierungsregeln für eine Vereinheitlichung der nationalen Regulierungspraxis auf EU-Ebene.

Der Ansatz einer vollharmonisierten Regulierung des Telekommunikationsmarktes wird in Branchenkreisen oft kritisiert.[715] Tatsächlich bestehen in praktischer Hinsicht Überschneidungen mit anderen Rechtsgebieten, für die einem „europäischen Superregulierer" die innerstaatliche Kompetenz fehlen kann. Beim Breitbandausbau sind insb. die Überschneidungen zum Bauordnungsrecht groß. Im Bereich der Netzneutralität bestehen ferner Berührungspunkte zum Medienrecht. Für beides sind in Deutschland aber die Bundesländer, nicht der Bund zuständig. Einer konvergenten Behörde steht insoweit das verfassungsrechtliche Verbot der Mischverwaltung entgegen.[716] Zudem besteht die Gefahr der Entwicklung einer divergierenden Regulierungspraxis zwischen den telekommunikations- und medienrechtlichen Elementen der Netzneutralität bzw. den bauordnungsrechtlichen Aspekten des Netzausbaus, was sich nachteilig auf die Investitionssicherheit auswirken kann.

Grundlegender lässt sich ferner hinterfragen, ob das Ziel der Kommission, den europäischen Telekommunikationsmarkt einheitlich zu regulieren, überhaupt sinnvoll ist. Im ökonomischen Schrifttum wird darauf hingewiesen, dass die nationalen Marktgegebenheiten im TK-Bereich so unterschiedlich sind, dass man kaum von einem „Single Market" reden kann.[717] Grenzüberschreitende Märkte gibt es in der Telekommunikation nur in sehr begrenztem Umfang.[718] Je weiter die Regulierung aber europäisiert wird, desto eher drohen in konkreten Fällen nationale Gegebenheiten unberücksichtigt zu bleiben.[719] Dies kann sich negativ auf die Investitionsbereitschaft der Unternehmen auswirken.

---

712 Eine Übersicht über die aktuellen EU-Agenturen findet sich unter http://europa.eu/about-eu/agencies/index_de.htm.

713 Die EZB ist keine EU-Agentur im engeren Sinne, sondern ein Organ der Union. Der Sache nach ist sie aber ein Paradebeispiel für einen zentralen EU-Regulierer.

714 Vgl. zuletzt BBC News, EU plans single telecoms regulator, 14.08.2013, abrufbar unter http://www.bbc.co.uk/news/business-23695623 zu den erfolglosen Bestrebungen der Kommission in Vorgängerversionen zum Maßnahmenpaket „Connected Continent".

715 Vgl. nur VATM, EU-Kommission steuert in eine Sackgasse, Meldung vom 19.07.2013, abrufbar unter http://www.vatm.de/724.0.html?&tx_ttnews%5Btt_news%5D=1571&cHash=18d4fa90ce1e5fff81bf3f05d5f05853.

716 BVerfGE 32, 145, 156; 39, 96, 120; 41, 291, 311.

717 *Pelkmans/Renda*, Single eComms Market? No such thing, Communications & Strategies, 2011, 21 ff.; *Pelkmans/Luchetta*, Enjoying a single market for network industries?, 2013, S. 31.

718 Neben dem Roaming sind weitere Beispiele der Markt für Global Telecommunications Services, der die Herstellung grenzübergreifender Verbindungen im B2B-Bereich mit Sprach- und Datenkommunikationsdiensten (VPN, Fax, Konferenzen etc.) umfasst, und die Global Internet Connectivity (IP Transit und Peering).

719 Ein Beispiel ist der Streit zwischen der Bundesnetzagentur und der Kommission um den Maßstab zur Festlegung der Mobilfunkterminierungsentgelte (pureLRIC vs. KeL). Während die Kommission den pureLRIC-Kostenmaßstab europaweit einführen wollte, wollte die Bundesnetzagentur am bewährten KeL-

Vorzugswürdig erscheint aus unserer Sicht daher der aktuelle Ansatz des EU-Rechtsrahmens. Dieser ist eher vom Vorbild einer Harmonisierung der Regulierungspraxis „durch Verfahren“ geprägt. So sollen die Mitgliedstaaten bspw. gemäß Art. 19 Abs. 2 RRL zwar sicherzustellen, dass die nationalen Regulierer den Empfehlungen der Kommission „weitestgehend“ Rechnung tragen (vgl. auch § 123a Abs. 3 TKG). Hierbei handelt es sich letztlich aber nicht um eine starre Aussage zum Rangverhältnis zwischen nationaler Regulierungsbehörde und EU-Kommission. Beschließt die Bundesnetzagentur trotz der gesteigerten Berücksichtigungspflicht von einer Empfehlung der Kommission abzuweichen, so ist ihr dies nicht verwehrt.[720] Ein solches Abweichen muss der Kommission lediglich unter Angabe der Gründe mitgeteilt werden (was freilich einen gewissen Rechtfertigungsdruck bei der Bundesnetzagentur aufbaut). Dieses System belässt den Mitgliedstaaten hinreichende Spielräume für die Berücksichtigung nationaler Besonderheiten bei gleichzeitiger paneuropäischer Verzahnung der Regulierungsansätze.

Maßstab festhalten. Denn der pureLRIC lässt die Gemeinkosten unberücksichtigt, die in Deutschland rund die Hälfte der Gesamtkosten ausmachen.

[720] Vgl. nur *Groebel*, in: Berliner Kommentar zum TKG, § 123a Rn. 12; Kühling, in: MAH IT-Recht, Teil 7, Rn. 32.

Teil 16 Strafrecht *(Dr. Martin Schorn)*

I. (Teil-)Autonome Systeme und Strafrecht

Kern des Projekts Industrie 4.0 sind autonome Systeme. Hier geht es nicht allein um pilotiertes Fahren, sondern generell um die Entwicklung von intelligenten Systemen, die eigenständig in der Lage sind, sich zu vernetzen, Situationen zu erkennen, sich wechselnden Bedingungen anzupassen und mit Nutzern und anderen Objekten zu interagieren. Diese Fähigkeit wirft Fragen auf.

1. Grundüberlegungen zur strafrechtlichen Haftung bei autonomen Systemen

So die Frage nach der eigenen strafrechtlichen Verantwortung autonomer Systeme. Die Frage ist nicht abwegig. So ist eine Strafrechtsordnung, bei dem als Normadressat allein der Mensch im Mittelpunkt steht, nicht immer selbstverständlich gewesen. Es bestrafte nicht nur Perserkönig Xerxes nach der Zerstörung seiner Schiffe durch einen Sturm den Hellespont mit 300 Peitschenhieben,[721] auch dem mittelalterlichen und frühneuzeitlichen Strafrecht waren Strafen gegen Tiere nicht fremd.[722] Dann liegt auch die Abkehr vom strafrechtlichen Anthropozentrismus, hin zu einem Strafrecht für Maschinen, nicht völlig fern. Die im geltenden Schuldstrafrecht vorausgesetzte Willensfreiheit ist auch beim Menschen empirisch nicht belegbar,[723] sie wird als gesellschaftlich notwendiges Konstrukt begriffen, die – spätestens wenn ein Computer einen Turing-Test[724] bestehen wird – auch für autonom handelnde Maschinen zumindest nicht widerlegbar ist. Sieht man dann etwa „Umprogrammierung“ als mögliche Sanktionen für Maschinen vor, gleichsam als deren „Resozialisierung“, so wäre das ein weiterer Schritt hin zu einem pragmatisch-funktionalen Strafrecht. Diese Entwicklung ist schon angestoßen durch immer lauter werdende Rufe nach Einführung eines Verbandsstrafrechts:[725] Der Verband als soziales Konstrukt hat dann auch nicht mehr Willensfreiheit als ein autonomes System.

Freilich betrifft das eine nicht zu ferne Zukunft. Bis dahin ist zu konstatieren, dass das vorhandene Strafrecht eine eigenständige Haftung autonom handelnder Systeme nicht vorsieht. Strafrechtliche Verantwortung bleibt den die autonomen Systeme verantwortenden Menschen vorbehalten. Für diese gilt weiter das Schuldprinzip,[726] welches auch ein Zusam-

---

721 Nachweise bei Herodot 7, 35.

722 Vgl. die Beispiele von *Ziemann*, Wesen, Wesen seid’s gewesen? Zur Diskussion über ein Strafrecht für Maschinen, in *Hilgendorf*, Robotik und Gesetzgebung, 2013, S. 183 (186).

723 Allerdings auch nicht deren Fehlen, entgegen einiger Interpretationen der neueren neurologischen Forschung: Vgl. *Roth/Lück/Struber*, Willensfreiheit und strafrechtliche Schuld aus Sicht der Hirnforschung, in Lampe/Pauen/Roth, Willensfreiheit und rechtliche Ordnung, 2008, S. 126.

724 Also einen menschlichen Befrager anhand seiner Antworten davon zu überzeugen, dass es sich bei dem Computer um einen Menschen handelt.

725 Vgl. etwa den nordrhein-westfälischen Gesetzentwurf für ein Verbandsstrafgesetzbuch, abrufbar unter https://www.justiz.nrw.de/JM/justizpolitik/jumiko/beschluesse/2013/herbstkonferenz13/zw3/TOP_II_5_Gesetzentwurf.pdf.

726 Vgl. grundlegend BGH, Urt. v. 18.03.1952 - GSSt 2/51, BGHSt. 2, 194 (200).

menfallen von Tat und Täterschuld fordert.[727] Handelt etwa ein System völlig autonom und verletzt dabei ein strafrechtlich geschütztes Rechtsgut, führt also bspw. den Tod eines Menschen herbei, so wird es für die verantwortlichen Programmierer regelmäßig an einem Schuldanknüpfungspunkt bei der konkreten Tatausführung fehlen. Im Bereich der Fahrlässigkeitsstrafbarkeit kann zwar jede sorgfaltswidrig gesetzte Ursache, durch die ein tatbestandlicher Erfolg[728] herbeigeführt wird, erfasst werden, solange dieser Erfolg vorhersehbar war. Bei völlig autonom handelnden Systemen wird aber auch hier häufig der für eine objektive Zurechnung nötige Schutzzweckzusammenhang fehlen.[729] Dies gilt umso mehr, wenn strafrechtliche Haftung an eine konkrete Tathandlung anknüpft, etwa im Rahmen des § 315c Abs. 1 StGB an das „*Führen eines Kraftfahrzeugs*". Will man hier die verantwortlichen Programmierer haftbar machen, so muss man an dessen Handlung anknüpfen, einen Schuldanknüpfungspunkt also vorverlagern. Eine Vorverlagerung des Anknüpfungspunkts strafrechtlicher Schuld ist dem deutschen Strafrecht nicht unbekannt. So kann als mittelbarer Täter erfasst werden, wer die Tat (im Tatzeitpunkt) nicht selbst begeht, sondern durch einen anderen.[730] Ein weiterer – gesetzlich nicht ausdrücklich geregelter – Fall einer Vorverlagerung ist die sog. *actio libera in causa*. Bei dieser Rechtsfigur führt der Täter im Zustand der Schuldfähigkeit einen pathologischen Zustand herbei, in dem er als Schuldunfähiger bei vorsätzlicher *actio libera in causa* die vorher für möglich gehaltene und billigend in Kauf genommene,[731] bei Fahrlässigkeit vorhersehbare tatbestandsmäßige Handlung begeht.

Diese Rechtsfiguren sind *de lege lata* zwar nicht auf die Verantwortung für völlig autonom handelnde Systeme zu übertragen. Für die mittelbare Täterschaft liegt das daran, dass das autonome System wird nicht als „anderer" i.S.v. § 25 Abs. 1 2. Alt. StGB angesehen werden können. Die *actio libera in causa* findet ihre gegenwärtig vorherrschende Begründung in der sog. Vorverlegungslehre und erklärt die für die Rechtsgutsverletzung kausale Defektherbeiführung zur Tathandlung, auf die sich die Schuld bezieht,[732] sodass das Tatgeschehen als einheitliches zu werten ist.[733] Diese Begründung wird aber kaum auf ein autonom handelndes System Übertragung finden können, kann doch dessen Programmierung und ein möglicherweise viel späteres „Fehlverhalten" des Systems i.d.R. nicht mehr als einheitliches Tatgeschehen zu werten sein. Neue Zurechnungsformen dürften an Art. 103 Abs. 2 GG scheitern.

De lege ferenda besteht gleichwohl die Gefahr, dass eine Zurechnungsnorm geschaffen werden wird. Denkbar ist wegen der Komplexität der Programmierung autonomer Systeme eine Art Beweislastumkehr oder objektive Bedingung der Strafbarkeit, bei deren Vorliegen

---

[727] Sog. Koinzidenzprinzip. Vgl. etwa *Schild* in Kindhäuser/Neumann/Paeffgen, StGB, 4. Aufl. 2013, § 20 Rz. 104.

[728] Also Tod oder Verletzung eines Menschen, im Produktsicherheitsstrafrecht aber bspw. auch das fahrlässige Inverkehrbringen nicht verkehrsfähiger Produkte.

[729] Vgl. hierzu *Sternberg-Lieben/Schuster* in Schönke/Schröder, StGB, 29. Aufl. 2014, § 15 Rz.

[730] *Joecks* in Münchener Kommentar, StGB, 2. Aufl 2011, § 25 Rz. 105 ff.

[731] BGH, Beschl. v. 13. 09. 2001 – 3 StR 331/01, NStZ 2002, 28.

[732] BGH, Urt. v. 06.03.1986 – 4 StR 48/86, NJW 1986, 2384.

[733] *Schild* in Kindhäuser/Neumann/Paeffgen, StGB, 4. Aufl. 2013, § 20 Rz. 112.

eine Strafbarkeit gegeben wäre. Jedenfalls letztere ist dem deutschen Recht nicht unbekannt,[734] ersteres existiert in angelsächsischen Rechtsordnungen.[735] Träten erste Fälle eingestellter Verfahren auf, bei denen ein Verschulden bei der Programmierung deren Komplexität wegen nicht nachweisbar sein wird, werden Rufe nach Einführung solcher Haftungskonstruktionen vielleicht laut werden.

2. Besonderheiten bei der strafrechtlichen Produkthaftung

Strafrechtliche Produkthaftung ist in den haftungsauslösenden Anforderungen meist anspruchsvoller als die zivilrechtlichen. Anders als im Rahmen zivilrechtlicher Produkthaftung muss Verschulden positiv festgestellt werden, und zwar in Form einer zurechenbaren individuellen Pflichtwidrigkeit. Relevante Delikte sind dabei nicht nur fahrlässige Körperverletzung oder Tötung, sondern praktisch bedeutsamer das regelmäßig auch fahrlässig begehbare Inverkehrbringen nicht verkehrsfähiger Produkte.[736] Eine strafrechtliche Verantwortlichkeit wird – insbesondere wenn ein erforderlicher Produktrückruf nicht vorgenommen wurde – häufig in Form eines Unterlassens gegeben sein.[737] Für eine Unterlassungsstrafbarkeit ist eine sog. Garantenstellung erforderlich, also die Einstandspflicht des Herstellers zur Abwendung eines strafrechtlich relevanten Erfolges. Diese begründet der BGH bereits mit dem Inverkehrbringen des gesundheitsgefährdenden Produkts.[738] Bei Kollegialorganen trifft diese Pflicht regelmäßig alle Organmitglieder, also sämtliche Geschäftsführer oder Vorstände.[739] Aufhänger strafrechtlicher Produkthaftung ist regelmäßig der Produktfehler, i.d.R. beruhend auf oder einhergehend mit einer Sorgfaltspflichtverletzung. Sorgfaltspflichten können begründet werden durch normative Vorgaben, aufgrund konkreten Gefahrenverdachts oder durch Häufung von Beschwerden, Rückmeldungen aus dem Handel oder Erkenntnissen aus Produktbeobachtung.[740]

Für autonome Systeme wird dabei nichts anderes gelten. Eine strafrechtliche Haftung für fehlerhafte und zu Personenschäden führende Produkte wird weiterhin bestehen. Verstärken werden sich die Nachweisprobleme. Dies gilt insbesondere im Hinblick auf Kausalität und objektive Zurechnung bei Fabrikationsfehlern in der „Smart Factory“. Bei Fahrlässigkeitshaftung ist nämlich anerkannt, dass der Pflichtwidrigkeitszusammenhang und damit die objektive Zurechnung dann nicht besteht, wenn der tatbestandliche Erfolg bei rechtmäßigem Alternativverhalten entfiele.[741] Das ist jedenfalls zweifelhaft in den Fällen, in denen der Produktfehler nicht auf einem Fehler bei der Herstellung beruht, sondern auf einer selbständigen Anpassung der Produktspezifikation, z.B. aufgrund von Fertigungsinformatio-

---

[734] Vgl. exemplarisch die Nichterweislichkeit der Tatsache bei der Üblen Nachrede nach § 186 StGB.
[735] In Form der sog. *strict liability*, etwa in Section 7 UK Bribery Act.
[736] Vgl. etwa §§ 40 Abs. 1 Nr. 1 MPG, 95 AMG, 58 Abs. 1 Nr. 2 LFGB. Häufig bleibt es bei einer Verurteilung dafür, da der für ein Erfolgsdelikt notwendige Kausalitätsnachweis oft nicht gelingt.
[737] *Kuhlen* in Achenbach/Ransiek, Hdb. Wirtschaftsstrafrecht, 3. Aufl. 2012, Kapitel 2/1 Rz. 22.
[738] BGH, Urt. v. 06.07.1990 – 2 StR 549/89, NJW 1990, 2560 – Lederspray.
[739] *Kuhlen* in Achenbach/Ransiek, Hdb. Wirtschaftsstrafrecht, 3. Aufl. 2012, Kap. 2/1 Rz. 45 f.
[740] *Hilgendorf*, in Rotsch, Criminal Compliance, 2014, § 10 Rz. 37 ff.
[741] BGH, Urt. v. 13.11.2003 – 5 StR 327/03, NJW 2004, 237.

nen des Produkts selbst oder aufgrund von Kundenspezifikationen, die in Smart Factories möglich werden, bis hin zur Losgröße 1.

Auch ist anerkannt, dass im Rahmen einer Fahrlässigkeitshaftung der Zurechnungszusammenhang dann entfällt, wenn ein Dritter – eigenverantwortlich– dazwischentritt.[742] Maßstab für die Zurechnung des Erfolgs zum Erstverursacher ist die Frage der Vorhersehbarkeit des Drittverhaltens. Hier lässt sich vertreten, dass autonom oder vernetzt handelnde Systeme diesem Dritten gleichen. Diese Fallgruppe soll nämlich auch dann Anwendung finden, wenn der Dritte unbewusst handelt,[743] also vergleichbar autonomen Systemen ohne eigenes Bewusstsein. So ließe sich argumentieren, dass auch autonom handelnde Systeme durch eigene Fortentwicklung oder Einfluss mit ihnen vernetzter Systeme als eigenverantwortliche Dritte anzusehen wären, und damit den Zurechnungszusammenhang entfallen ließen, wenn die konkrete Systemreaktion außerhalb aller Erfahrung lag. In der Praxis wird diese Frage freilich nur eine geringe Rolle spielen, denn in den Fällen eines erwartungswidrig handelnden autonomen Systems wird es regelmäßig an der schon für die Fahrlässigkeitshaftung notwendigen objektiven Vorhersehbarkeit fehlen.

Fragen ergeben sich auch im Hinblick auf die Unterlassungshaftung, für die eine Garantenstellung erforderlich ist. Allein mit Ingerenz wird sich eine Garantenstellung nicht begründen lassen, wenn das in Verkehr gebrachte Produkt als solches nicht gefährlich ist, sondern erst durch Vernetzung mit anderen Produkten oder autonome Fortentwicklung gefährlich wird. Damit das Vorverhalten pflichtwidrig ist,[744] muss das Produkt zum Zeitpunkt des Inverkehrbringens bereits fehlerhaft sein. Entsteht der „Fehler“ aber erst durch Vernetzung mit anderen Produkten oder durch autonome Fortentwicklung, ist das Produkt im Zeitpunkt des Inverkehrbringens gerade nicht fehlerhaft; eine Garantenstellung kann dann nicht entstehen, will man die strafbarkeitsbegrenzende Funktion dieses Merkmals nicht völlig aushöhlen.[745] Eine Garantenstellung kann sich dann nur aus Übernahme einer Schutzfunktion oder der Pflicht zur Produktüberwachung ergeben. Diese kann aber nur die spezifischen Gefahren eines Produkts umfassen. Eine generelle strafrechtliche Pflicht des Herstellers, auch nicht vorhersehbare Gefahren durch Vernetzung mit anderen Produkten zu ermitteln und ggf. zurückzurufen, wird abzulehnen sein. Abzuwarten bleibt, wie die Rechtsprechung sich hier positionieren wird.

---

[742] Vgl. *Sternberg-Lieben/Schuster* in Schönke/Schröder StGB, 29. Aufl. 2014 § 15 Rz. 169.

[743] *Sternberg-Lieben/Schuster* in Schönke/Schröder StGB, 29. Aufl. 2014 § 15 Rz. 169.

[744] An diesem Merkmal zur Begründung einer Garantenstellung aus Ingerenz hält der BGH auch in der grundlegenden Lederspray-Entscheidung fest: Urteil vom 06.07.1990 – 2 StR 549/89, NJW 1990, 2560 (2563): „*Zumindest in diesem Rahmen besteht auch eine strafrechtliche Verantwortlichkeit für die Herstellung und den Vertrieb <u>fehlerhafter</u> Produkte*“ [Hervorhebung nur hier].

[745] So auch *Mayer*, PharmR 2008, 236 (245).

3. Algorithmen und Ethik: Abwägungsentscheidungen und Rechtfertigung

Im Rahmen autonomen Fahrens wird bisweilen – je nach Perspektive anschaulich oder polemisch – ein „Algorithmus des Todes“[746] diskutiert, nämlich die Programmierung bestimmter Reaktionsmuster des autonom fahrenden Fahrzeugs in Gefahrensituationen. Plakativ: Wie entscheidet ein autonomes Fahrzeug, wenn es bei einem sicher bevorstehenden Unfall durch allein noch mögliches Ausweichen nur die Wahl zwischen mehreren „Opfern“ hat. Die diskutierten Beispiele muten nicht immer realitätsnah an[747] und mögen in homöopathischen Wahrscheinlichkeiten auftreten, das Problem ist aber trotzdem da: Werden bislang unter Gesichtspunkten einer persönlichen Rechtfertigung abstrakt diskutierte Abwägungsentscheidungen dadurch realistischer, dass sie algorithmisch programmiert werden. Denn genauer betrachtet muten die bisherigen Lehrbuchbeispiele einer Güterabwägung auch konstruiert an: Anders als ein autonom handelndes Fahrzeug kann ein menschlicher Fahrer in Sekundenbruchteilen nämlich keine sinnhafte Entscheidung treffen; ein autonomes Fahrzeug schon eher. Traut man dem autonomen Fahrzeug das Erfassen der Situation zu so kann zwar nicht das Fahrzeug eine autonomere Entscheidung treffen, wohl aber derjenige, der für die Programmierung des entsprechenden Algorithmus verantwortlich ist. Diesem bieten sich folgende Alternativen:

- So kann in das Steuer wieder an den Fahrer übergeben werden.
- Zum zweiten kann eine Abwägung nach quantitativen Gesichtspunkten vorgenommen werden: Es wird immer die Alternative gewählt, die den geringsten Personenschaden nach sich zieht.
- Auch kann – dies käme einer menschlichen Reaktion vermutlich noch am nächsten – ein Zufallsgenerator die Letztentscheidung treffen,
- Weiter wäre – auch dies eine sehr menschliche Reaktion – denkbar, dass der Algorithmus stets die für die Fahrzeuginsassen sicherste Variante wählt, selbst um den Preis größeren Schadens unter Unbeteiligten.

Fall 1 dürfte jenseits von bloßen Fahrassistenten, die eine Letztentscheidung beim menschlichen Fahrer belassen, kaum praktikabel sein.[748] In der konkreten Situation bloßer Sekundenbruchteile wird ein abgelenkter Fahrer nicht übernehmen können. Fall 2 mag zwar pragmatisch daherkommen und für amerikanische Programmierer nach deren Rechtstradi-

---

[746] *Hilgendorf* in Hilgendorf/Hötitzsch, Das Recht vor den Herausforderungen der modernen Technik, 2015, S: 11 (20).

[747] Vgl. die Beispiele bei *Hilgendorf* in Hilgendorf/Hötitzsch, Das Recht vor den Herausforderungen der modernen Technik, 2015, S. 11 (21 ff.): Kleinkind, Fußgänger und entgegenkommendes Fahrzeug; mehrere Fußgänger und (für den eigenen Fahrer tödlicher) Betonpfeiler.

[748] In diesem Sinne aber *Nehm* in LTO vom 14.08.2015, abrufbar unter: http://www.lto.de/recht/hintergruende/h/autonome-autos-praesident-verkehrsgerichtstag-ueber-rechtliche-probleme-ethische-konflikte/2/.

tion vielleicht auch vorzugswürdig. Mit deutschem Rechtsdenken kantischer[749] Tradition ist ein solcher Pragmatismus schwer vereinbar.[750] Zudem lässt sich die quantitative Abwägung bei Bildung entsprechender Lebenssachverhalte immer pervertieren: Soll ein Kind überfahren werden statt zweier Erwachsener? Der Radfahrer mit Helm statt dem Radfahrer ohne Helm wegen höherer Überlebenswahrscheinlichkeit? Der Kleinwagen statt dem SUV? Benutzer (und Hersteller) von Fahrradhelmen und Kleinwagen wären nicht begeistert. Und entscheidend: Sollen im Extremfall unfreiwillig-heldenhaft die eigenen Fahrzeuginsassen geopfert werden.[751]

Damit ist man bei der Überlegung, auf den es ankommen wird, nämlich der, die am wirklichen oder mutmaßlichen Willen des Fahrers ansetzt: Ebenso wenig wie ein Navigationssystem den mündigen Fahrer bevormundet und nicht etwa aus Allgemeinwohlgründen die wirtschaftlichste Strecke wählt, sondern auf dessen Wunsch hin die schnellste, ökonomischste oder kürzeste, sollte dies auch ein Abwägungsalgorithmus tun. Denn das gesetzliche Leitbild einer Güterabwägung, wie es in §§ 34, 35 StGB zum Ausdruck kommt, stellt genau hierauf ab: auf den mündigen Normadressaten, der eine Abwägung anhand von Rechtsgütern trifft (§ 34 StGB), wobei er zwar nicht gerechtfertigt, aber immerhin persönlich entschuldigt ist, wenn er seine eigenen Rechtgüter (oder die Angehöriger) höher bewertet als eigentlich höherwertige Rechtsgüter Dritter (§ 35 StGB). Die gesetzliche Regelung geht – konstruiert und empirisch kaum belegbar – von dem Leitbild aus, dass er diese Entscheidung auch sinnhaft treffen kann, obwohl er in der konkreten Situation diese Zeit regelmäßig nicht haben wird. Ein autonomes System wäre aber in der Lage, solche Situationen zu antizipieren. Stellt ein autonomes System auf den Willen des (menschlichen) Fahrers ab, wird es diesem gesetzlichen Leitbild am ehesten gerecht, vielleicht mehr als die intuitive Entscheidung des Fahrers bei einem von ihm gesteuerten Fahrzeug. Anders der Programmierer, bliebe die Entscheidung bei ihm. Er wäre bei Bevorzugung der Fahrzeuginsassen nicht gerechtfertigt, denn deren Rechtsgüter überwögen nicht zwingend; entschuldigt wäre er aber ebenfalls nicht, da er keine Sonderverbindung zu den Fahrzeuginsassen hat. Denkbare Lösungsmöglichkeiten wären eine Vorabauswahl des (menschlichen) Fahrers in den Grundeinstellungen oder aber – und dann bestünde gesetzgeberischer Handlungsbedarf – die Aufwertung des § 35 StGB zu einem (verallgemeinerungsfähigen) Rechtfertigungsgrund, der dem mutmaßlichen Willen eines Dritten entsprechend wahrgenommen werden kann, nämlich dem der Fahrzeuginsassen. Die sollen das System schließlich nutzen (und kaufen). Das wäre legitim. Und es wäre ehrlich.

In den die Fahrzeuginsassen nicht betreffenden Fällen muss es nicht auf deren Entscheidung ankommen können; hier sind die Hersteller gefragt, bestimmte Formen einer Güterabwägung zu antizipieren. Diese bereitet keine Schwierigkeiten, solange das Gütergefälle

---

[749] Grundlegung zur Metaphysik der Sitten, 1785, Ausgabe von Weischdel, 1968, Bd. VII, S. 68.

[750] Das kantische Verständnis ist hochaktuell: Siehe BVerfG, Urt. v. 15.02.2006 – 1 BvR 357/05, NJW 2006, 751 (Rz. 118 ff.) zur Nichtigkeit von § 14 Abs. 3 LuftSG a.F., der im Eindruck des 11. September 2001 den Abschuss eines Passagierflugzeugs zur Rettung Vieler zuließ.

[751] Bspw. durch Kollision mit einem Betonpfeiler statt der Fußgängergruppe.

eindeutig ist, etwa Abwägung von Sachschaden gegenüber Personenschaden. In den übrigen Fällen einer Gleichrangigkeit von Rechtsgütern (Leben gegen Leben, körperliche Unversehrtheit gegen körperliche Unversehrtheit) wird auf die Grundsätze eines übergesetzlichen Notstandes abgestellt werden können, der im Rahmen richterlicher Rechtsfortbildung entwickelt und dessen Übertragung auf programmierte Güterabwägungen im Rahmen richterlicher Rechtsfortbildung wünschenswert wäre. Denkbar wäre in diesem Zusammenhang auch die Etablierung einer Ethikkommission, an die sich Softwareentwickler bei der Entwicklung entsprechender Algorithmen wenden können. Hierdurch könnte von vornherein Rechtssicherheit erzielt werden.

II. Strafrechtlicher Schutz gegen Angriffe in der digitalisierten Wirtschaft

1. Formen von Cyber-Kriminalität und Cyber-Aktivismus

Vernetze Systeme und Smart Factories sind besonders anfällig für Angriffe von außen. Der Schaden kann dabei immens sein. Denkbare Angriffe können in Form einfacher Cyber-Kriminalität oder als Cyber-Aktivismus vorkommen. Cyber-Aktivisten sind Angreifer, die auf einen politischen, gesellschaftlichen, sozialen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen („Hacktivism"). Cyber-Kriminelle wollen mithilfe der Informationstechnik auf illegalem Weg Geld verdienen. Zudem ist Cyber-Kriminalität in Form der Wirtschaftsspionage denkbar. Angriffe können dabei als Angriffe auf die Vertraulichkeit, auf die Datenintegrität sowie die Datenverfügbarkeit (etwa durch verteilte Denial of Service-Angriffe) vorkommen.

2. Bisheriger und geplanter Rechtsrahmen

Der bisherige strafrechtliche Rechtsrahmen schützt Daten vor solchen Angriffen sehr umfassend, prinzipiell auch in vernetzten Systemen. Geschützt sind die Datenvertraulichkeit,[752] die Datenintegrität[753] und die Datenauthentizität.[754] All diese Vorschriften legen den sehr weiten Datenbegriff des § 202a StGB zugrunde, der nicht auf personenbezogene Daten i.S.v. § 3 Abs. 1 BDSG beschränkt ist. Der Schutz der Datenintegrität enthält auch keine Beschränkung auf Daten, die gegen unberechtigten Zugang besonders gesichert sind, sondern erfasst das Löschen oder Verändern sämtlicher Daten auch in vernetzten Systemen.

Der nun veröffentlichte Gesetzentwurf zur Einführung einer Vorratsdatenspeicherung[755] sieht auch die Einführung eines Straftatbestands der Datenhehlerei vor. Strafbar soll nunmehr sein, wer Daten, die nicht allgemein zugänglich sind, und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem andern verschafft. Im Rahmen vernetzter und, d.h. Daten austauschender Systeme kann die Gefahr nicht ausgeschlossen werden,

[752] §§ 202a, 202b, 202c, 206 StGB, 17 UWG.
[753] §§ 303a, 303b StGB.
[754] §§ 269, 278, 270 StGB.
[755] Abrufbar unter https://netzpolitik.org/wp-upload/2015-05-15_BMJV-Referentenentwurf-Vorratsdatenspeicherung.pdf.

dass durch eine rechtswidrige Tat erlangte Daten auf eigene Systeme gespielt und damit „*verschafft*“ wurden. Die eigenen Daten wären damit – wie bei der Geldwäsche – kontaminiert. Zwar bieten Vorsatzerfordernis und die besonderen subjektiven Absichten (Bereicherungs- oder Nachteilszufügungsabsicht) einen gewissen Schutz vor Strafbarkeit. Jedoch ist die Schwelle eines Eventualvorsatzes vergleichsweise niedrig[756] Zudem wäre in dem Moment, in dem bekannt würde, dass bspw. von Zulieferern erhaltene Daten möglicherweise rechtswidrig verschafft wurden, der eigene Datenbestand, der selbständig diese Daten verarbeitet, kontaminiert und könnte – nach Kenntniserlangung – nicht weiterverwendet werden, ohne die kontaminierten Daten aufwändig auszusondern. Denn der Entwurf sieht als strafbar auch ein Verarbeiten der rechtswidrig erlangten Daten vor.

3. Gesetzgeberischer Handlungsbedarf

Für den Schutz autonomer Systeme dürfte das vorhandene Instrumentarium zum Schutz von Datenvertraulichkeit, -integrität und -authentizität ausreichen. Im Hinblick auf den Gesetzentwurf zur Datenhehlerei besteht die Gefahr überbordender Strafbarkeit durch Verarbeitung möglicherweise „bemakelter“ Daten in autonom kommunizierenden Systemen, die nur durch eine Überprüfung („*Third Party Due Diligence*“) des Bereitstellers der Daten auszuschließen ist. Hier kann gesetzgeberischer Nachbesserungsbedarf bestehen, etwa in Form eines Strafbarkeitsausschluss im Rahmen autonom stattfindenden Datenaustauschs.

III. Internet der Dinge, Wearables und Augmented Reality

Das „Internet der Dinge“ beschreibt zu Vernetzung intelligenter Gegenstände zum eigenständigen Informationsaustausch. Dazu kann intelligentes Supply Chain Management gehören ebenso wie intelligente Produkte, bspw. in Form von Wearables. Das führt zu einem zunehmenden Informationsaustausch zwischen realer und virtueller Welt und einer Erweiterung der Realitätswahrnehmung,[757] sog. Augmented Reality („AR“). Die Anwendungsbereiche von AR in Industrie und Produktion sind vielfältig, etwa durch virtuelle Anpassung von Prototypen oder Unterstützung bei der Produktions- und Anlagenplanung.

1. Kollision mit strafrechtlichem Schutz der Privatsphäre

Die Nutzung von Wearables kann in Konflikt mit dem strafrechtlichen Schutz der Privatsphäre, insbesondere nach §§ 201, 201a StGB, stehen. Benutzer von Wearables mit Aufnahmefunktion können sich strafbar machen: § 201 Abs. 1 Nr. 1 StGB lässt bereits die bloße Aufnahme jedes nichtöffentlich gesprochenen Wortes für eine Strafbarkeit genügen. § 201a StGB beschränkt den Schutz vor unbefugten Bildaufnahmen zwar auf die Wohnung und geschützte Räume, begründet aber innerhalb dieses Rahmens ein nicht unerhebliches Strafbarkeitsrisiko. Werden aber bspw. in der Produktion oder Entwicklung AR-Vorrichtungen

[756] Vgl. BGH, Beschl. v. 23.11.1999 – 4 StR 491/99, wistra 2000, 177: Täter muss die Tatbestandsverwirklichung als nicht ganz fernliegend erkannt und sich um des erstrebten Zieles willen mit ihr abgefunden haben.

[757] Definition von *Jones/Nobis/Röchner/Thal*, Internet der Zukunft, ein Memorandum, 2010, S. 98.

verwandt, die als Nebeneffekt zu Bildaufnahmen der Mitarbeiter führen, scheidet eine Strafbarkeit nach § 201a StGB aus, da es sich bei einer Betriebsstätte nicht um einen geschützten Raum i.S.v. § 201a StGB handelt.[758]

2. Wearables und §§ 90, 148 TKG

Eine besondere Bedeutung für auf Wearables, die Bild- oder Tonaufnahmen ermöglichen, besitzt die durch §§ 90 Abs. 1 Satz 1, 148 Abs. 1 Nr. 2 lit. b) TKG vorverlagerte Strafbarkeit. Hierfür genügt, dass Telekommunikationsanlagen hergestellt, vertrieben oder eingeführt werden, die mit Gegenständen des täglichen Gebrauchs verkleidet sind und aufgrund dessen oder aufgrund ihrer Funktionsweise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen unbemerkt abzuhören oder das Bild eines anderen unbemerkt aufzunehmen. Eine Verkleidung mit Gegenständen des täglichen Gebrauchs wird bei manchen Wearables, insbesondere Kameras und Aufnahmegeräten, zunehmend einfacher, vor allem wenn sie in die Kleidung integriert werden. Jedoch sind solche Geräte nicht bestimmt, unerlaubt Bild- oder Tonaufnahmen herzustellen, sodass ein Strafbarkeitsrisiko für Hersteller eher nicht besteht. Die Entwicklung gilt es aber zu beobachten.

3. Aufzeichnung von Gesundheitsdaten und deren strafrechtlicher Schutz

Wearables und mobile Geräte mit entsprechenden Apps zeichnen in zunehmendem Maße Gesundheitsdaten auf. Nach § 203 Abs. 1 Nr. 1 StGB besteht ein strafrechtlicher Geheimnisschutz für Gesundheitsdaten, wenn es sich um Gesundheitsdaten handelt, die einem Arzt anvertraut sind. Benutzt also ein Arzt bestimmte Apps zur Kommunikation mit dem Patienten oder setzt Apps zur Verwaltung von Patientendaten ein, so ist, wenn eine Kenntnisnahme dieser Daten durch den App-Betreiber möglich ist, eine entsprechende Einwilligung des Patienten erforderlich. Ansonsten besteht ein Strafbarkeitsrisiko nach § 203 StGB.

[758] *Lenckner/Eisele* in Schönke/Schröder StGB, 29. Aufl. 2014, § 101a Rz. 7.

Teil 17 Gesundheitswirtschaft 4.0 (Dr. Susanne Wende, LL.M.)

„Gesundheitswirtschaft 4.0“ im hier verstandenen Sinne umfasst verschiedene Nutzungen moderner Informations- und Kommunikationstechnologien im Gesundheitssystem. Dabei sind drei Hauptanwendungen zu unterscheiden: Zum einen können Apps und andere IT-Lösungen im Rahmen der Prävention, Diagnose oder Behandlung von Patienten selbst oder auch von Ärzten und anderen Berufsgruppen des Gesundheitssystems genutzt werden (im Folgenden zusammenfassend beschrieben als „Mobile-Health-Anwendungen“). Zum anderen ermöglichen die modernen Kommunikations- und Informationstechnologien auch eine qualitativ neuwertige Vernetzung und den elektronischen Austausch von Patientendaten zwischen verschiedenen Beteiligten (im Folgenden zusammenfassend beschrieben als „Gesundheits-Telematik“). Schließlich ermöglicht die moderne Informations- und Kommunikationstechnologie auch eine Ferndiagnose und -behandlung (im Folgenden zusammenfassend beschrieben als „Telemedizin“). Allen drei Anwendungsformen und vor allem ihrer Kombination wird sowohl auf deutscher als auch auf europäischer und internationaler Ebene großes Potential zur qualitativen Verbesserung, Kosteneinsparung sowie stärkerer Einbindung und Selbstverantwortung des Patienten zugemessen. Derzeit bestehen allerdings noch technische und rechtliche Hindernisse für die Weiterentwicklung und Nutzung.

I. Rechtliche Problemfelder im Zusammenhang mit Mobile Health Anwendungen

1. Unsicherheiten bei der rechtlichen Einordnung von Wearables, Health-Apps und weiteren Mobile Health-Anwendungen (als Medizinprodukte) und datenschutzrechtliche Herausforderungen im Rahmen der Anwendung

Es gibt verschiedene Formen von Mobile Health-Anwendungen. Zum einen sind die Lifestyle-Apps zu nennen, die zusammen mit den entsprechenden Endgeräten (Smartphone und Wearables) eine Vielzahl von Funktionen anbieten, um durch Erfassung und Auswertung gesundheitsrelevanter Körperdaten Informationen zur individuellen Steigerung des körperlichen Wohlbefindens bereitzustellen. Dazu gehören z.B. Anwendungen, die die täglich absolvierten Schritte messen, der Aufzeichnung von Ernährungsgewohnheiten dienen oder auch Unterstützung bei Fitness-Workouts bieten.

Davon zu unterscheiden sind Health Apps mit einem offensichtlich deutlich stärkeren medizinischen Bezug, die tatsächlich medizinische Funktionen erfüllen und daher auch in Krankenhäusern und Arztpraxen genutzt werden können. Beispiele hierfür sind mit einem Smartphone kombinierbare Fieberthermometer[759] oder Apps zur Messung und Verwaltung von Puls oder Blutzuckerspiegel.

[759] Z.B. https://kinsahealth.com/.

Diese Apps werden teilweise in Kombination mit sogenannten Wearables als haptische Endgeräte benutzt, z.B. einer Smart Watch oder auch mit speziellen Kontaktlinsen, die den Blutzuckerspiegel messen und die Daten an ein Smartphone übertragen[760].

Für all diese Mobile Health-Anwendungen stellt sich die Frage, ob sie als Medizinprodukte zu klassifizieren sind. Medizinprodukte müssen insbesondere gem. § 6 Medizinproduktegesetz („MPG") vor dem Inverkehrbringen ein gesetzlich vorgeschriebenes Konformitätsbewertungsverfahren durchlaufen und mit der CE-Kennzeichnung versehen werden. Dabei sind unterschiedliche Konformitätsbewertungsverfahren für verschiedene Klassen von Medizinprodukten vorgesehen. Außerdem unterliegt der Hersteller, sein Bevollmächtigter oder der Einführer eines Medizinprodukts einer besonderen Produktbeobachtungs- und Gefahrabwendungspflicht gem. § 5 MPG i.V.m. der Medizinprodukte-Sicherheitsplanverordnung („MPSV").

Der Hersteller von Mobile Health-Anwendungen steht demnach vor zwei Herausforderungen: Er muss zum einen entscheiden, ob sein Produkt ein Medizinprodukt ist und zum anderen auch bestimmen, in welche Klasse das jeweilige Produkt fällt, um das gesetzlich geforderte Konformitätsbewertungsverfahren zu ermitteln.

Im europäischen und deutschen Recht gibt es keine eindeutige Abgrenzung für Einzelfälle, welche der oben beschriebenen Anwendungen als Medizinprodukte zu werten sind und damit den entsprechenden Produktregulierungen unterfallen. Eine Klarstellung der Klassifizierung wird von der Europäischen Kommission als wesentlicher Aspekt gewertet, um Softwareentwicklern und -herstellern die weitere Entwicklung zu erleichtern.[761]

a) Aktueller Rechtsrahmen

Die Klassifizierung von Wearables, Health-Apps und weiteren Mobile Health-Anwendungen als Medizinprodukt richtet sich nach § 3 MPG, der die entsprechende Definition aus Art. 1 Abs. 2 der europäischen Richtlinie 93/42/EWG[762] („**Medizinprodukte-Richtlinie**") in deutsches Recht umsetzt. Nach dieser Definition ist neben den Merkmalen der physiologischen Komponente und des Wirkmechanismus für die Klassifizierung als Medizinprodukt vor al-

[760] Es gibt technisch bereits die Möglichkeit, mit einer speziellen Kontaktlinse den Blutzuckerspiegel zu messen und die Werte aufzuzeichnen und den Benutzer bei Schwankungen zu warnen, vgl. http://www.aerztezeitung.de/medizin/krankheiten/diabetes/article/853384/high-tech-auge-googles-kontaktlinse-diabetiker.html. Denkbare Erweiterungen der Funktionalität liegen in einer Übersendung der Daten an den Arzt oder sogar der Steuerung einer Insulinpumpe durch die gemessenen Werte.

[761] *Europäische Kommission*, Grünbuch über Mobile-Health-Dienste („mHealth") vom 10.4.2014, COM(2014) 219 final, S. 13.

[762] Richtlinie 93/42/EWG vom 14.06.1993, zuletzt geändert durch Richtlinie 2007/47/EG. Um die Übersichtlichkeit zu erhalten, wird in diesem Beitrag nur auf die Medizinprodukte-Richtlinie abgestellt. Der Vollständigkeit halber ist aber auf die europäische Richtlinie 98/79/EG vom 27.10.1998 über In-vitro-Diagnostika hinzuweisen, die für diese speziellen Medizinprodukte besondere Regelungen enthält.

lem die medizinische Zweckbestimmung entscheidend.[763] § 3 Abs. 1 Nr. 1 MPG zählt folgende medizinische Zwecke auf:

- Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,
- Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,
- Untersuchung, Ersetzung oder Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs
- Empfängnisregelung

Nach dem ausdrücklichen Wortlaut der gesetzlichen Definition kann auch Software ein Medizinprodukt sein, wenn sie eine solche medizinische Zweckbestimmung hat.[764]

b) Zweckbestimmung durch den Hersteller

Die im Rahmen der Klassifizierung als Medizinprodukt entscheidende Zweckbestimmung des Produktes ergibt sich nach den Regelungen in § 3 Nr. 10 und Nr. 15 MPG aus den Angaben des Herstellers.[765] Es genügt nach der Rechtsprechung des EuGH nicht die reine Eignung zu medizinischen Zwecken.[766] Der BGH hat in der Folge dieser EuGH-Rechtsprechung ergänzend klargestellt, dass der Hersteller bei der Zweckbestimmung einem Willkürverbot unterliegt.[767]

c) Abgrenzung der Zweckbestimmung

Vor dem Hintergrund des oben skizzierten aktuellen Rechtsrahmens stellen sich im Einzelfall schwierige Abgrenzungsfragen, bei welchen Mobile Health-Anwendungen die medizinische Zweckbestimmung zu bejahen ist. Die einschlägigen Auslegungsdokumente der Europäischen Kommission[768] geben hierzu Hinweise und Hilfestellungen, die aber eine Reihe von Abgrenzungsfragen offen lassen.

In der juristischen Literatur wird unter Berücksichtigung der Definition in § 3 MPG und der verfügbaren Auslegungsdokumente hauptsächlich darauf abgestellt, ob die Mobile Health-

---

[763] Zur Definition insgesamt Spickhoff/*Lücker*, Medizinrecht, 2. Auflage 2014, MPG § 3 Rn. 2.

[764] Es ist hierbei dogmatisch zwischen „embedded software“ und „stand alone software“ zu unterscheiden, da die Klassifizierung von „embedded software“ stets der Klassifizierung des Hauptproduktes folgt, während „stand alone software“ selbst die Voraussetzung der medizinischen Zweckbestimmung erfüllen muss.

[765] Vgl. hierzu auch *Heimhalt/Rehmann*, MPR 2014, 197 (201); .

[766] EuGH, Urt. v. 22.11.2012, Rs. C-219/11, MPR 2012, 191 – Brain Products GmbH/BioSani.

[767] BGH, Urt. v. 18.04.2013, I ZR 53/09, MPR 2014, 60 – Messgeräte II.

[768] Europäische Kommission, MEDDEV 2.1/6 zur Klassifizierung von Stand Alone Software: Hier werden Apps nicht direkt aufgeführt, die dortigen Kriterien lassen sich z.T. aber auf Apps übertragen; Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps, SWD(2014) 135 final.

Anwendungen eine diagnostische Funktion haben oder eine Diagnose unterstützen. Dann seien sie als Medizinprodukt zu klassifizieren. Handele es sich hingegen nur um Datenverwaltung oder Informationsvermittlung (z.B. das Anzeigen in der Nähe gelegener Arztpraxen), sei die Eigenschaft als Medizinprodukt abzulehnen.[769]

Schwierig ist die Abgrenzung bei Mobile Health-Anwendungen im Grenzbereich zwischen reiner Informationsvermittlung/Datenverwaltung und medizinischer Prävention, z.B. eine App mit Ernährungshinweisen – ggf. sogar unter Auswertung der Ernährungsgewohnheiten des Benutzers. Es ist unklar, wann die reine Verbesserung der Befindlichkeit in eine Verhütung von Krankheiten übergeht. Ein weiteres schwierig einzuordnendes Beispiel ist eine elektrische Zahnbürste, die Qualität und Quantität des Zähneputzens misst und anschließend die Daten an eine spezielle App auf dem Smartphone kommuniziert: Zahnbürsten und Zubehör werden im europäischen Recht grundsätzlich als Kosmetika qualifiziert.[770] Bei dieser speziellen Zahnbürste ist aber ein medizinischer Verwendungszweck im Hinblick auf einen Beitrag zur Verhütung, Behandlung oder Linderung von Zahnkrankheiten durchaus denkbar. Es kommt dabei auch auf die konkrete Ausgestaltung der Anwendung und die Darstellung gegenüber dem Adressatenkreis an.

Diese Abgrenzungsschwierigkeiten setzen sich bei der Zuordnung des jeweiligen Produktes nach den Klassifizierungsregeln des Anhangs IX der Medizinprodukte-Richtlinie fort. Der finanzielle und organisatorische Aufwand des Konformitätsbewertungsverfahrens unterscheidet sich erheblich zwischen den einzelnen Klassen.

Für eine Konkretisierung der Klassifizierungskriterien lohnt ggf. ein Blick den Katalog in der von der U.S.-amerikanischen Aufsichtsbehörde FDA erstellten Empfehlung zur Klassifizierung von Mobile Apps als Medizinprodukte in der dortigen Produktregulierung[771].

d) Datenschutzrechtliche Herausforderungen

Durch die zunehmende Vernetzung von Software-Medizinprodukten – also auch durch Mobile Health-Anwendungen – wird die Patientenbehandlung immer datenzentrierter. Daher gehört zur Sicherheit dieser Produkte neben dem ordnungsgemäßen Funktionieren auch die Informations- und Datensicherheit.[772]

Hier ergeben sich zum einen die in Teil 3 dieses Gutachtens ausführlich behandelten datenschutzrechtlichen Probleme. Besondere Bedeutung haben dabei der Grundsatz der Daten-

---

[769] *Heimhalt/Rehmann*, MPR 2014, 197, 202; *Backmann*, MPR 2011, 73.

[770] Vgl. die Definition in Art. 2 Abs. 1 lit. a) VO (EG) Nr. 1223/2009 (einschlägig wenn der ausschließliche oder überwiegende Zweck des Produktes die Reinigung, der Schutz oder die Erhaltung des guten Zustands der Zähne ist; vgl. hierzu auch *Heimhalt/Rehmann*, MPR 2014, 197 (202).

[771] FDA, Mobile Medical Application Guidance for Industry and Food and Drug Administration Staff, 25.09.2013, http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf (zuletzt aufgerufen am 27.8.2015), hierzu ausführlich unter Abschnitt Teil 17VIII.3.

[772] *Kempka*, MPR 2015, 31 (33).

minimierung und Zweckbindung sowie *Privacy by Design*. Darüber hinaus sind Besonderheiten der Gesundheitswirtschaft zu berücksichtigen:

Gesundheitsdaten, die bei der Nutzung von Mobile Health-Produkten regelmäßig erfasst, ggf. auch verarbeitet werden, sind als eigene Kategorie in § 3 Abs. 9 BDSG aufgeführt. Sie stellen personenbezogene Daten i.S.v. § 3 Abs. 1 BDSG dar. Adressat der datenschutzrechtlichen Pflichten ist die verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG. Gem. § 9 BDSG i.V.m. § 13 Abs. 4 TMG ist die verantwortliche Stelle verpflichtet, organisatorische und technische Maßnahmen zu ergreifen, um Datensicherheit zu gewährleisten. Dabei sind nach der Anlage zu § 9 S. 1 BDSG u.a. Zugangs-, Zugriffs- und Weitergabekontrollen erforderlich.

Aufgrund der denkbar weiten gesetzlichen Definition der verantwortlichen Stelle in § 3 Abs. 7 BDSG kommen Server- und Netzwerkbetreiber, Software-Entwickler, Hersteller der Endgeräte[773] und Betriebssysteme, App-Stores, Krankenversicherungen, medizinisches Personal und andere Beteiligte als Adressaten der Pflichten in Betracht. Hier ist vertieft zu prüfen, ob eine gesundheitswirtschaftsspezifische klarere Abgrenzung der Verantwortlichkeiten notwendig ist.

Die Erhebung, Verarbeitung und Nutzung der Daten ist nur mit Ermächtigung zulässig. Neben den bereits in Teil 3 dieses Gutachtens aufgeführten Ermächtigungen gilt für Gesundheitsdaten das besondere Regime des § 28 Abs. 6 bis 8 BDSG. Zulässig ist die Verwertung danach ohne Ermächtigung, wenn dies – neben weiteren Voraussetzungen – zum Schutz lebenswichtiger Interessen, zur Durchsetzung rechtlicher Ansprüche oder zur Durchführung wissenschaftlicher Forschung erforderlich ist oder der Betroffene die Daten offenkundig öffentlich gemacht hat. Daneben gibt es spezialgesetzliche Vorschriften zum Umgang mit Gesundheitsdaten in Landeskrankhaus- und Gesundheitsdatenschutzgesetzen.[774] Da es zunehmend technisch möglich ist, Mobile Health-Anwendungen mit medizinischen Telematik-Strukturen zu verknüpfen, sind auch die Vorgaben des § 291a SGB V zu berücksichtigen. Eine doppelte Verpflichtung der verantwortlichen Stelle folgt aus § 39 BDSG i.V.m. § 9 MBO-Ä, wenn die Daten aus der Mobile Health-Anwendung der ärztlichen Schweigepflicht unterliegen und damit auch strafrechtlich geschützt sind.

Die Frage, ob dieser aktuelle Rechtsrahmen das erforderliche Vertrauen der Patienten in die technischen Möglichkeiten der Gesundheitswirtschaft 4.0 schaffen und gleichzeitig eine effektive Nutzung der neuen Technologien ermöglichen kann, bedarf einer vertieften Auswertung der Wechselwirkungen zwischen den verschiedenen Vorschriften. Im Moment gibt es dazu durchaus kritische Stimmen, teilweise aber mit sehr pauschalen Begründungen[775]. Auch zu berücksichtigen wird dabei der weitere Fortgang der Gesetzgebungsinitiativen auf

[773] Teilweise wird § 2 Abs. 4 MPG als Rechtsgrundlage für eine entsprechende Pflicht des Herstellers zum Datenschutz diskutiert, vgl. hierzu einen Überblick bei *Kempka*, MPR 2015, 31 (33).
[774] *Rübsamen*, MedR 2015, 485 (488).
[775] Z.B. *Jensen*, ZD-Aktuell 2015, 04617.

deutscher und auf europäischer Eben sein, vor allem der derzeitige Entwurf eines E-Health-Gesetzes.[776]

e) Transparenz und Sicherheit bei Mobile Health-Anwendungen

Noch ungeklärt ist die Frage, wie bei schon jetzt mehr als 97.000 M-Health-Apps, die weltweit verfügbar sind,[777] sichergestellt werden kann, dass der Patient sichere und funktionierende Apps auswählt. Es gibt hierzu Ansätze in internationalen Normen, z.B. der internationalen Norm IEC 82304-1 mit Anforderungen an Software, die als Medizinprodukt gilt und gleichzeitig auch in einem breiteren Anwendungsfeld von Gesundheit und Wellness genutzt werden kann. In einigen EU-Mitgliedstaaten gibt es bereits nationalen Zertifizierungssysteme, z.B. die Health Apps Library des britischen NHS, die alle Apps einer Überprüfung auf Sicherheit und Einhaltung der Datenschutzvorschriften unterzieht oder die Auszeichnung „AppSaludable“ der Agencia de Calidad Sanitaria de Andalucía (Andalusische Agentur für Qualität im Gesundheitswesen). Dies sind allerdings nationale Insellösungen, die im Hinblick auf die europäische Warenverkehrs- und Dienstleistungsfreiheit auf ihre Vereinbarkeit mit dem europäischen Recht zu untersuchen sind. Der europäische Gesetzgeber sieht hier harmonisierenden Handlungsbedarf.[778]

2. Regelungsdefizite im Rahmen der Behandlung medizinischer Software – Klassifizierung als Medizinprodukt?

Relevant ist die Einordnung als Medizinprodukt auch für eine Reihe von Stand Alone-Software, die z.B. zur Aufbereitung, Auswertung und Archivierung von MRT-Aufnahmen in Krankenhäusern angeboten wird. Software könnte in Zukunft auch verschiedene, über die Möglichkeiten der Telemedizin eingeholte, Expertenmeinungen zu Röntgenaufnahmen auswerten und so die Befundsicherheit z.B. bei Tumoren signifikant erhöhen.[779] Die Europäische Kommission hat hierzu die Auslegungshinweise in MEDDEV 2.1/6 erarbeitet, die einige Kriterien zur Abgrenzung an die Hand geben. Als Medizinprodukt wird danach Stand Alone-Software klassifiziert, wenn sie die Diagnose unterstützt oder die Therapie beeinflusst. Nicht als Medizinprodukt klassifiziert wird hingegen reine Verwaltungssoftware. Auch hier können – ähnlich wie bei der Klassifizierung von Mobile Health-Anwendungen – in Grenzfällen Auslegungsschwierigkeiten verbleiben.

---

[776] Vgl. hierzu ausführlich unten Abschnitt Teil 17IV.

[777] Europäische Kommission, Europäische Kommission, Grünbuch über Mobile-Health-Dienste („mHealth“) vom 10.4.2014, COM(2014) 219 final, S. 13.

[778] Europäische Kommission, Grünbuch über Mobile-Health-Dienste („mHealth“) vom 10.4.2014, COM(2014) 219 final, S. 13.

[779] Vgl. hierzu *Müller-Jung*, Schwarmintelligenz könnte helfen, in FAZ v. 01.09.2015, http://www.faz.net/aktuell/wissen/medizin/schwarmintelligenz-koennte-bei-brustkrebs-diagnose-helfen-13767058.html (zuletzt aufgerufen am 01.09.2015).

II. Rechtliche Problemfelder im Zusammenhang mit der Gesundheits-Telematik

1. Interoperable IT- und Medizintechniksysteme zur Vermeidung technischer „Insellösungen“ in Krankenhäusern und Arztpraxen

Die Potentiale der technischen Möglichkeiten für die Gesundheitswirtschaft können derzeit vor allem wegen Defiziten in der notwendigen Infrastruktur[780] nicht vollständig ausgeschöpft werden. So lag das Wirtschaftswachstum der Gesundheits-IT-Branche in Deutschland im Jahr 2012 mit 3,2% unter dem Wachstum der Software-Branche allgemein mit 3,5%.[781]

a) Interoperabilität in Deutschland

In Deutschland gibt es bereits verschiedene – vom Internet getrennte – Netze, die für den Informationsaustausch zwischen verschiedenen Beteiligten der Gesundheitsversorgung angeboten werden, z.B. KV-Safe Net, gevko[782] („Bestandsnetze“). Diese sind nicht vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert.[783]

Der aktuelle, von der Bundesregierung bereits beschlossene Entwurf des E-Health-Gesetzes sieht die fristgebundene Einführung einer einheitlichen Telematik-Infrastruktur („TI“) und eines Interoperabilitätsverzeichnisses vor. [784]

b) Interoperabilität auf europäischer Ebene

Auf europäischer Ebene stellt sich das gleiche Problem: Es existiert eine Vielzahl unterschiedlicher Gesundheitsinformationssysteme, die von nationalen Behörden, Krankenhäusern und Ärzten eingerichtet wurden. Die Europäische Kommission hat sich zum Ziel gesetzt, diese Systeme so zu vereinheitlichen, dass elektronische Gesundheitsdienste und Mobile-Health-Dienste EU-weit miteinander kommunizieren können.[785] Das aufgrund der Richtlinie 2011/24/EU über Patientenrechte eingerichtete europäische Gesundheitstelematiknetz[786] wirkt federführend an der Entwicklung von EU-Leitlinien für elektronische Gesundheitsdienste mit. Ziel ist die Verbesserung der Interoperabilität der elektronischen Gesundheitssysteme und die Gewährleistung des Zugangs zu einer sicheren und hochwertigen Gesundheitsversorgung. Das Gesundheitstelematiknetz hat im November 2013 bereits Leitlinien

---

[780] Europäische Kommission, Grünbuch über Mobile-Health-Dienste („mHealth“) vom 10.4.2014, COM(2014) 219 final, S. 18; als zweites großes Hindernis wird die fehlende Vergütungsregelung gesehen, hierzu unten Abschnitt Teil 17III.2.

[781] Bundesverband Gesundheits-IT, Branchenbericht IT-Lösungen im Gesundheitswesen 2014, S. 4.

[782] http://www.aok-systems.de/newsletter/ausgabe-eins-2012/gesundheit-und-politik.html

[783] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), Stellungnahme zum Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) vom 11.02.2015, S. 2.

[784] Siehe hierzu ausführlich unter Abschnitt Teil 17IV.3.

[785] Europäische Kommission, Studie über den europäischen Interoperabilitätsrahmen für elektronische Gesundheitsdienste, http://ec.europa.eu/isa/actions/documents/isa_2.12_ehealth1_workprogramme.pdf.

[786] eHealth Network, http://ec.europa.eu/health/ehealth/policy/network/index_en.htm.

zur grenzübergreifenden Verwendung der Daten angenommen.[787] Diese Prozesse sind bei der Weiterentwicklung des Rechtsrahmens in Deutschland zu berücksichtigen.

2. Einhaltung berufsrechtlicher und vertragsarztrechtlicher Archivierungs-pflichten bei elektronischer Datenverwaltung und Nutzung innovativer IT- und Medizintechniksysteme (in Krankenhäusern und Praxen)

Bei der weiteren Ausgestaltung der TI sind Wechselwirkungen mit den berufsrechtlichen Dokumentations- und Archivierungspflichten gem. § 630f BGB (und § 10 MBO-Ä) zu berücksichtigen. Soll eine Pflicht zur doppelten Aktenführung vermieden werden, müssen insbesondere die Rechte für Zugriff auf und Veränderung der Datensätze auf der elektronischen Gesundheitskarte und der elektronischen Patientenakte abgestimmt werden – vor allem weil eine Nichterfüllung der Dokumentationspflicht zu einer Beweislastumkehr gem. § 630h BGB im Hinblick auf die Nichtvornahme gebotener medizinischer Maßnahmen führen kann.

III. Rechtliche Hindernisse im Bereich der Telemedizin als heilberufliche Leistung

1. Fehlende Grundlagen der Erstattungsfähigkeit telemedizinischer Leistungen nach SGB V, EBM und GOÄ

Der Einsatz von Telemedizin kann zur Kostensenkung im Gesundheitssystem beitragen. Bisher sind diese Dienste allerdings nicht in die Regelversorgung der gesetzlichen Krankenversicherung integriert. Gem. § 87 SGB V vereinbart die kassenärztliche Bundesvereinigung mit dem Spitzenverband Bund der Krankenkassen durch Bewertungsausschüsse einen einheitlichen Bewertungsmaßstab für ärztliche und zahlärztliche Leistungen („EBM“). Nur die darin aufgeführten Leistungen sind bei den gesetzlichen Krankenkassen abrechenbar. Trotz eines entsprechenden gesetzlichen Auftrags (§ 87 Abs. 2a S. 8 SGB V) hat der Bewertungsausschuss bislang nur eine Rahmenvereinbarung mit den zu überprüfenden Eckpunkte geschlossen.[788]

Bei den privaten Krankenversicherungen ist eine Abrechnung telemedizinischer Leistungen schon nach der aktuellen Gesetzeslage einfacher, da § 6 Abs. 2 GOÄ die Möglichkeit eröffnet, diese durch eine Analogie in die Abrechnung mit aufzunehmen.

Diese aktuelle gesetzliche Lage stellt ein Hindernis für die weitere Entwicklung und Nutzung von telemedizinischen Leistungen dar. Der aktuelle Entwurf eines E-Health-Gesetzes enthält hierzu weitergehenden Regelungen, die unter Abschnitt IV. ausführlich dargestellt werden. In anderen EU-Mitgliedstaaten haben nationale Gesundheitsdienste bereits mit der Einfüh-

[787] http://ec.europa.eu/health/ehealth/docs/guidelines_patient_summary_en.pdf.

[788] Rahmenvereinbarung zwischen der Kassenärztlichen Bundesvereinigung und dem GKV-Spitzenverband als Trägerorganisationen des Bewertungsausschusses gemäß § 87 Abs. 1 Satz 1 SGB V zur Überprüfung des Einheitlichen Bewertungsmaßstabes gemäß § 87 Abs. 2a Satz 8 SGB V zum Umfang der Erbringung ambulanter Leistungen durch Telemedizin.

rung von innovativen Erstattungsmodellen begonnen, z. B. in Form von Anreizprogrammen.[789]

2. Berufsrechtliche Hürden (MBO-Ä) und heilmittelwerberechtliche Beschränkungen (HWG)

a) Verbot der Fernbehandlung in § 7 Abs. 4 MBO-Ä

Die deutsche (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte („MBO-Ä") verbietet in ihrem § 7 Abs. 4 eine ärztliche Behandlung und Beratung ausschließlich über Print- und Kommunikationsmedien. Auch bei einer telemedizinischen Behandlung muss gem. § 7 Abs. 4 S. 2 MBO-Ä eine unmittelbare Behandlung gewährleistet sein. Es gibt bereits Ansätze in der Literatur, die das Fernbehandlungsverbot vor dem Hintergrund der Möglichkeiten der Telemedizin kritisch hinterfragen.[790]

Einige telemedizinische Leistungen sind aber nach der Rechtsprechung durchaus zulässig. Zusammenfassend stellt die Rechtsprechung dabei darauf ab, ob es sich um eher allgemeine Informationen, Hinweise auf typische Krankheiten bei den geschilderten Symptomen oder um eine individuell auf den einzelnen Patienten abgestellte Diagnose oder Therapieempfehlung handelt.[791] In der juristischen Literatur wird auch eine Notfallbehandlung in Form der Fernbehandlung für zulässig gehalten.[792] Auch werden Ausnahmen für das Telemonitoring z.B. eines chronisch kranken Patienten erwogen. Spezielle Regelungen gibt es aber nur für die Teleradiologie.[793] Es bedarf einer vertieften Prüfung und Auswertung, ob diese Lösungsansätze eine Nutzung der Telemedizin im rechtspolitisch gewollten Umfang ermöglichen oder ob das Fernbehandlungsverbot insgesamt kritisch überdacht werden muss.

b) Heilmittelwerberechtliche Beschränkungen

Gem. § 9 des Gesetzes über die Werbung auf dem Gebiete des Heilwesens (Heilmittelwerbegesetz, „HWG") ist die Werbung für Fernbehandlung verboten. Es stellen sich hier die unter Abschnitt Teil 17III.2.a) aufgeführten Abgrenzungsfragen, die teilweise schon durch die Rechtsprechung adressiert worden sind.[794]

---

[789] *Dixon-Fyle/Kowallik*, „Engaging consumers to manage health care demand", Januar 2010, http://www.mckinsey.com/insights/health_systems_and_services/engaging_consumers_to_manage_health_care_demand (zuletzt aufgerufen am 27.08.2015).

[790] Z.B. *Bergmann/Pauge/Steinmeyer/Sobotta*, Das gesamte Medizinrecht, MBO-Ä § 7 Rn. 4.

[791] Z.B. OLG München, Urt. v. 02.08.2012, 29 U 1471/12, GRUR-RR 2012, 435 (436); Ärztliches BerufsG Nds, Urt. v. 07.03.2012, BG 6/11, MedR 2012, 839.

[792] *Spickhoff/Scholz*, Medizinrecht, 2. Aufl. 2014, MBO § 7 Rn. 16; *Stüwe/Hauenschild,* Deutsches Ärzteblatt 2011, A-729.

[793] *Spickhoff/Scholz*, Medizinrecht, 2. Aufl. 2014, MBO § 7 Rn. 17.

[794] Z.B. OLG München, Urt. v. 2. 8. 2012, 29 U 1471/12, GRUR-RR 2012, 435.

IV. Der aktuelle Regierungsentwurf zum „E-Health-Gesetz“: Fortentwicklung von Telematik-Infrastruktur, Telemedizin und der elektronischen Gesundheitskarte (§ 291a SGB V)

Um den Ausbau und die Nutzung der neuen Technologien im Gesundheitswesen zügig voranzutreiben, hat die Bundesregierung den Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen („E-Health-Gesetz“) beschlossen.[795] Dieser adressiert hauptsächlich datenschutzrechtliche Themen und Infrastrukturprobleme durch Ergänzung und Neuregelungen der relevanten Vorschriften des SGB V. Er enthält auch eine Reihe von Anreizen zur zügigen flächendeckenden Einführung von telemedizinischen Anwendungen.

1. Die elektronische Gesundheitskarte („eGK“) und Stammdatenmanagement

Ein zentrales Element des im E-Health-Gesetz fortgeschriebenen Konzepts der Nutzung moderner Informations- und Kommunikationstechnologien im Gesundheitswesen[796] ist die elektronische Gesundheitskarte („**eGK**“).

Seit 1.1.2015 hat die eGK bereits die frühere Krankenversichertenkarte zum Nachweis des Versicherungsschutzes der gesetzlichen Krankenversicherung abgelöst. Neben den bereits jetzt darauf gespeicherten administrativen Daten soll die eGK schrittweise um weitere Datensätze, wie z.B. Notfalldaten (ab 2018) und einen Medikationsplan[797], erweitert werden. Als Anreiz für die zügige Erstellung dieser Datensätze wird dem Bewertungsausschuss die Pflicht auferlegt, innerhalb bestimmter Fristen spezielle Vergütungssätze hierfür festzulegen.

Ab 2016 soll ein modernes Stammdatenmanagement mit regelmäßiger Prüfung und Aktualisierung von Versichertenstammdaten eingeführt werden. Ab 1. Juli 2018 sind pauschale Kürzungen der Vergütung für Ärzte und Zahnärzte vorgesehen, wenn diese nicht an der Online-Prüfung der Versichertenstammdaten teilnehmen.

2. Telemedizin

Gerade im ländlichen Raum ergeben sich mit der Telemedizin neue Möglichkeiten, vor allem bei der Überwachung von Schlaganfall-, Diabetes- und chronisch herzkranken Patienten. Wie bereits in Abschnitt III. aufgeführt, stehen der stärkeren Nutzung der Möglichkeiten der Telemedizin derzeit vor allem berufsrechtliche Regelungen (Fernbehandlungsverbot) und die fehlende Abrechenbarkeit entgegen.

---

[795] Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendung im Gesundheitswesen, BT-Drs. 18/5293.

[796] Dieses Konzept war bereits im Versorgungsstrukturgesetz vom 22.11.2011, BGBl. 2011 I, S. 1983, angelegt. Die dort festgeschriebenen Maßnahmen wurden bisher aber nur teilweise umgesetzt.

[797] Patienten, die drei oder mehr Medikamente gleichzeitig einnehmen müssen, sollen schon ab Oktober 2016 einen Anspruch auf einen solchen Medikationsplan in Papierform haben.

Der Entwurf des E-Health-Gesetzes sieht vor, dass ab April 2017 Telekonsile für Röntgenbefunde vergütet werden. Die Selbstverwaltung wird fristgebunden zur Erarbeitung der entsprechenden Vergütungssätze verpflichtet. Bei Nichteinhaltung dieser Pflichten drohen Haushaltskürzungen.[798] Die Selbstverwaltung erhält zudem den Auftrag, zu prüfen, welche weiteren Leistungen telemedizinisch erbracht und vergütet werden können.

An dieser Regelung wird kritisiert, dass sie nicht weit genug gehe, da die Prüfung und Erarbeitung von Vergütungssätzen für telemedizinische Leistungen außerhalb der Radiologie nicht mit Sanktionen belegt sei.[799]

3. Gesundheits-Telematik und Telematik-Infrastruktur

Zur Schaffung der technischen Voraussetzungen und für die Einführung der digitalen Infrastruktur im Gesundheitswesen ist die von der Selbstverwaltung[800] getragene Gesellschaft für Telematik („Gematik GmbH“) zuständig. Ihre Aufgabe ist es, den sicheren Datenaustausch in Form einer einheitlichen Telematikinfrastruktur („TI“) weiter aus- und aufzubauen. Dazu gehört auch die behördliche Zulassung von Dienstleistern und Dienstleistungen, die im Rahmen der TI angeboten werden. Bei Nichteinhalten der hierfür im Entwurf des E-Health-Gesetzes gesetzten Fristen, gibt es ein gestuftes Sanktionsverfahren, das auch zur Kürzung der Haushaltsmittel führen kann.

Die Wirksamkeit dieser Maßnahmen wird z.T. bezweifelt, da durch die geplante, vorübergehende Anreizvergütung auch Parallelstrukturen und -netze, wie sie in der Vergangenheit von Einrichtungen der Selbstverwaltung aufgebaut wurden, weiter gefördert würden.[801] Es wird daher gefordert, gesetzlich festzulegen, dass die Bestandsnetze vom BSI zertifiziert und schrittweise in die TI überführt werden müssen.[802]

Daneben soll die Gematik GmbH ein Interoperabilitätsverzeichnis einrichten, um die von den verschiedenen IT-Systemen im Gesundheitswesen verwendeten Standards transparent zu machen und für mehr Standardisierung auf freiwilliger Basis zu sorgen. Ob dieses auf Freiwilligkeit basierende System tatsächlich eine Vereinheitlichung der technischen Parameter herbeiführen kann, bleibt abzuwarten.[803]

---

[798] So z.B. in Art. 1 Nr. 10e)aa) des Gesetzentwurfs, der bei Verabschiedung § 291 SGB V wird; vgl. hierzu auch Pressemitteilung des Bundesministeriums für Gesundheit vom 3.7.2015, http://www.bmg.bund.de/presse/pressemitteilungen/pressemitteilungen-2015-3/e-health-bundestag.html (zuletzt aufgerufen am 27.8.2015).

[799] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), Stellungnahme zum Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) vom 11.02.2015, S. 8.

[800] GKV-Spitzenverbände, Kassenärztliche Bundesvereinigung und Kassenzahnärztliche Bundesvereinigung.

[801] *BITKOM*, Stellungnahme zum E-Health Gesetz vom 11.02.2015, S. 2.

[802] *BITKOM*, Stellungnahme zum E-Health Gesetz vom 11.02.2015, S. 4

[803] Kritisch: *BITKOM* Stellungnahme zum E-Health Gesetz vom 11.02.2015, S. 13.

4. Datenschutzrechtliche Aspekte

Der Entwurf des E-Health-Gesetzes enthält einige Ergänzungen und Änderungen der datenschutzrechtlichen Vorgaben zur Gesundheitswirtschaft 4.0, die in §§ 291a ff. SGB V eingearbeitet werden sollen. Es werden dabei vor allem die entsprechenden gesetzlichen Ermächtigungen zur Erstellung, Verarbeitung und Verwendung der Datensätze auf der eGK und in der elektronischen Patientenakte aufgegriffen. So soll z.B. auf den Notfalldatensatz auch ohne Autorisierung des Patienten zugegriffen werden können. Zu den Regelungen gibt es einige Kritikpunkte verschiedener Interessengruppen.[804] Besonders wird dabei das Zugriffsrecht des Patienten selbst diskutiert, das von einer IT-technischen Autorisierung abhängig gemacht wird. Als weiterer Kritik-Schwerpunkt wird die Gefahr eines faktischen Zwangs zur Preisgabe von Daten gesehen.[805] Ob diese Kritikpunkte im Hinblick auf einen ausreichenden Patientendatenschutz, bedarf einer vertieften Auseinandersetzung mit den verschiedenen Aspekten des komplexen Regelungsgefüges. Hierbei wird z.B. zu prüfen sein, ob die existierende Rechtsprechung zum Patienteneinsichtsrecht und zur Einschränkung der Pflicht zur Datenpreisgabe in der Gesundheitsversorgung[806] zu überzeugenden Lösungen bei etwaigen Lücken führen kann.

V. Rechtsprobleme im Rahmen der Personalized Medicine – Individualisierung von Medizinprodukten (u.a. durch 3D-Druck)

Der Begriff „Personalized Medicine“ hat zwei verschiedene Hintergründe: Er umfasst zum einen die mit neuen Technologien mögliche Ausrichtung medizinischer Prävention und Behandlung sehr viel stärker anhand der individuellen Voraussetzungen des jeweiligen Patienten. Wesentliche Bausteine dieses Aspekts der Personalized Medicine sind Gendiagnostik und Auswertung von Biomarkern.[807] Bei der diagnostischen Seite der Personalized Medicine können wiederum Apps und andere Mobile Health-Anwendungen genutzt werden, wodurch alle bereits oben (Abschnitt I.) aufgeworfenen Rechtsfragen hierzu relevant werden.

Personalized Medicine umfasst aber auch die therapeutische Seite des Gesundheitssystems. Mit Hilfe moderner Produktionstechniken, wie z.B. dem 3D-Druck, können auf Grundlage der nunmehr möglichen, sehr individuellen Diagnose auch ganz individuelle Medizinprodukte zur Therapie entwickelt und hergestellt werden. So könnten z.B. bei der Herstellung einer Prothese oder eines Hörgerätes die individuellen Diagnosewerte in die Konstruktion

---

[804] Vgl. hierzu zusammenfassend *Jensen*, ZD-Aktuell 2015, 04617.

[805] Vgl. hierzu auch die Kleine Anfrage der Fraktion DIE LINKE im Bundestag (BT-Drs. 18/3633) im Hinblick auf die Gefahr einer faktischen Pflicht zur Preisgabe diverser persönlicher Daten und die Versicherungspflicht nach § 5 Abs. 1 SGB V und die Antwort der Bunderegierung (BT-Drs. 18/3849).

[806] Vgl. nur BVerfG, Beschluss v. 17.7.2013, 1 BvR 3167/08, ZD 2014, 84; BGH Urt. v. 26.02.2013, VI ZR 359/11, ZD 2014, 87, jeweils auch unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und der ärztlichen Schweigepflicht.

[807] Vgl. hierzu eingehend *Eberbach*, MedR 2014, 449 (458); *von Hardenberg/Wilman*, MedR 2013, 77.

des konkreten Produktes einfließen, das dann beim Arzt – oder sogar beim Patienten – mit dem 3D-Drucker ausgedruckt wird.

Es stellen sich dabei schon bei konventionell hergestellten Medizinprodukten schwierige Fragen, inwieweit eine individuelle Anpassung/Einstellung des jeweiligen Medizinproduktes die verantwortliche medizinisch geschulte Person zum Hersteller macht. Im europäischen Medizinprodukterecht gibt es bereits Ansätze zur differenzierten Behandlung von Produkten, die speziell für jeden Patienten angepasst werden müssen und können.[808] Die Rechtsfrage der Herstellereigenschaft hat aber nicht nur Bedeutung für die öffentlich-rechtliche Medizinprodukte-Regulierung, sondern auch Auswirkungen auf die zivilrechtliche Haftung. Hierzu gibt es für konventionell hergestellte Medizinprodukte bereits Rechtsprechung[809], die auf ihre Übertragbarkeit als Lösungsmöglichkeit für Rechtsfragen im Zusammenhang mit Personalized Medicine vertieft zu untersuchen ist.

VI. Haftungsrechtliche Aspekte der Gesundheitswirtschaft 4.0

Die Europäische Kommission weist darauf hin, dass Mobile-Health-Dienste beim Einsatz in der Telemedizin eine stärkere Einbindung und selbstverantwortliche Teilnahme des Patienten an medizinischer Vorsorge und Behandlung ermöglicht.[810] Gleichzeitig werden – anders als bei der klassischen unmittelbaren Behandlung – neben Arzt und Patient weitere Akteure in diese Form der Behandlung einbezogen, wie z.B. die Entwickler der verwendeten Software. Hiermit geht ggf. einher, dass die Grenzen zwischen der herkömmlichen Behandlung durch einen Arzt einerseits und der Behandlungsanteile anderer Mitwirkender verwischt werden.[811] Die Wahrnehmung dieses Phänomens als mögliches Hindernis der Nutzung telemedizinischer Möglichkeiten ist auch vor dem Hintergrund zu sehen, dass der Markt der im Rahmen der Telemedizin verwendeten Anwendungen von Einzelpersonen oder kleinen Unternehmen dominiert wird,[812] die mit derartigen Haftungsrisiken bisher nicht konfrontiert waren.

Eine Haftung für Schäden, die durch Fehler in der Gesundheitswirtschaft 4.0 entstehen, kann aus vertraglichen und deliktsrechtlichen Ansprüchen sowie aus dem Produkthaftungsgesetz hergeleitet werden. Als Beispiel für einen sicherheitsrelevanten Fehler ist die jüngst zurückgerufene App, für die damit geworben wurde, dass sie durch Erfassen und Auswer-

---

808 Europäische Kommission, MEDDEV 2.1/1, April 1994, Abschnitt IV, http://ec.europa.eu/health/medical-devices/files/meddev/2_1-1___04-1994_en.pdf

809 Vgl. z.B. KG Berlin, Urt. v. 03.04.2014, 20 U 253/12, MPR 2014, 120 zur Produkthaftung des Arztes beim Austausch einzelner Komponenten einer implantierten Prothese im Rahmen einer OP.

810 Europäische Kommission, Grünbuch über Mobile-Health-Dienste („mHealth“) vom 10.4.2014, COM(2014) 219 final, S. 6.

811 Europäische Kommission, Aktionsplan für elektronische Gesundheitsdienste 2012–2020 – innovative Gesundheitsfürsorge im 21. Jahrhundert, S. 9–10; Europäische Kommission, Grünbuch über Mobile-Health-Dienste („mHealth“) vom 10.4.2014, COM(2014) 219 final; Entschließung des Europäischen Parlaments vom 14. Januar 2014 zum Aktionsplan für elektronische Gesundheitsdienste 2012–2020: innovative Gesundheitsfürsorge im 21. Jahrhundert, 14.1.2014.

812 Europäische Kommission, Grünbuch über Mobile-Health-Dienste („mHealth“) vom 10.4.2014, COM(2014) 219 final, S. 8.

ten der Fotos von Hautstellen analysieren könne, ob es sich um ein bösartiges Melanom handele. In 60% der Fälle diagnostizierte die App allerdings bösartige Melanome als harmlos.[813]

Zur vertraglichen Haftung für Softwaremängel gelten die in Teil 7I. dieses Gutachtens dargestellten Überlegungen. Zu berücksichtigen sind dabei allerdings die speziellen Vorgaben der §§ 630a ff. BGB.

Im Rahmen der deliktsrechtlichen und produkthaftungsrechtlichen Verantwortlichkeit kommen neben Diagnose- und Behandlungsfehlern auch Aufklärungsfehler als Anknüpfungspunkt der Haftung in Betracht. Ob eine gesetzgeberische Klarstellung der Haftungsverteilung speziell für die Gesundheitswirtschaft 4.0 notwendig ist, muss vertieft untersucht werden. Dabei sind neben den bereits in Teil 7II. dieses Gutachtens adressierten Aspekten und der ganz eigenen deliktsrechtlichen Systematik der Haftung bei Behandlungsfehlern[814] drei Besonderheiten der Gesundheitswirtschaft 4.0 zu beachten:

1. Nichtfunktionieren als Produktfehler

Zum einen ist zu berücksichtigen, dass das Nichtfunktionieren eines Produktes grundsätzlich keinen sicherheitsrelevanten Produktfehler darstellt, der produkthaftungsrechtliche Schadenersatzansprüche auslösen kann. Vielmehr ist der Geschädigte auf die vertraglichen Gewährleistungs- und Schadenersatzansprüche beschränkt. Anders ist dies nach der Rechtsprechung zu § 823 Abs. 1 BGB allerdings, wenn das Produkt gerade eine bestimmte Schutzfunktion hat, auf die sich der Benutzer berechtigterweise verlässt und in der Konsequenz auf andere Schutzmaßnahmen verzichtet.[815] Eine Übertragung dieser Rechtsprechung auf bestimmte Mobile-Health-Anwendungen und andere medizinische Software kommt durchaus in Betracht. So kann z.B. die Nichtverfügbarkeit oder der Ausfall einer solchen Anwendung zu einer Verletzung des behandelten Patienten führen. Für die produkthaftungsrechtliche Bewertung wird es jeweils darauf ankommen, mit welchen Angaben und an welchen Adressatenkreis (Patient oder Arzt?) die App in Verkehr gebracht wurde und wie die Rechtsprechung das Zusammenspiel der Herstellerverantwortung und der Verantwortung des behandelnden Arztes ausgestaltet. Zu berücksichtigen sind dabei auch die medizinproduktespezifischen Vorgaben der §§ 4 und 14 MPG.

2. Besonders hohe berechtigte Sicherheitserwartung des Patienten

Aufgrund der jüngsten Rechtsprechung des EuGH[816] zur europäischen Produkthaftungsrichtlinie 85/73/EWG (die durch das Produkthaftungsgesetz („ProdHaftG“) in deutsches Recht umgesetzt wird) muss unter Umständen eine besonders hohe Sicherheitserwartung

---

[813] Beispiel bei *Rübsamen*, MedR 2015, 485 (489).
[814] Vgl. zum Überblick Jauernig/*Teichmann*, BGB, 15. Aufl. 2014, Rn. 108.
[815] BGH, Urt. v. 17.03.1981, VI ZR 191/79, NJW 1981, 1603 – *Derosal*; Urt. v. 17.03.1981, VI ZR 286/78, NJW 1981, 1606 – *Benomyl.*
[816] EuGH, Urteil vom 05.03.2015, Rs. C - 503/13 und C - 504/13 - Herzschrittmacher

des Patienten angenommen werden, bei deren Nichterfüllung Schadenersatzansprüche gem. § 1 ProdHaftG entstehen. In dem konkreten, vom EuGH entschiedenen Fall ging es um implantierte Herzschrittmacher, die zu einer Gruppe von Geräten mit erhöhter Ausfallwahrscheinlichkeit gehörten, ohne dass am einzelnen Gerät ein Fehler nachgewiesen werden konnte. Der EuGH entschied hierzu, dass wegen der besonders hohen Sicherheitserwartung der Patienten schon der Fehlerverdacht einen Fehler i.S.d. § 3 ProdHaftG begründen könne. Diese Rechtsprechung ist bei Weitem nicht auf alle Medizinprodukte übertragbar, sondern muss zunächst als Einzelfallrechtsprechung zu einer speziellen Gruppe von Medizinprodukten gesehen werden.[817] Es bedarf aber einer vertieften Prüfung, welche Auswirkung diese Rechtsprechung auf die Haftung für Fehler an Mobile-Health-Anwendungen und damit auch für Software- und Algorithmus-Fehler hat.

3. Haftung bei Kombinationsrisiken

Relevant wird bei Haftungsfragen der Mobile-Health-Anwendungen auch die besondere Konstellation der Kombinationsrisiken. Grundsätzlich haftet der Hersteller im Rahmen des § 823 Abs. 1 BGB nur für Schäden, die durch sein fehlerhaftes Produkt verursacht werden. Die Rechtsprechung hat diese Produzentenhaftung - unter engen Voraussetzungen - ausgedehnt auf Schäden, die gerade durch das Zusammenwirken zweier Produkte verursacht werden (sog. Kombinationsrisiken). Im Hinblick auf solche Kombinationsrisiken kann dem Hersteller eine Produktbeobachtungs- und ggf. Gefahrabwendungspflicht obliegen.[818]

Aus dieser Rechtsprechung entnimmt ein großer Teil der sich damit auseinandersetzenden Literatur, dass eine Haftung für Kombinationsrisiken insbesondere dann in Betracht kommt, wenn ein Produkt notwendigerweise mit einem anderen kombiniert werden muss um funktionsfähig zu sein.[819]

Es liegt nahe, mobile Endgeräte und Apps, die für eine bestimmte Funktion zwingend miteinander kombiniert werden müssen, als derart ergänzungsbedürftig zu bewerten. Gerade aus der Kombination können sich neue Gefahren ergeben, die besonderes Augenmerk für die jeweiligen Schnittstellen und Interoperabilität erfordern. Für die genaue Bewertung der Verkehrssicherungspflichten der einzelnen Wirtschaftsakteure der Wertschöpfungskette müssen die jeweilige Anwendung vertieft untersucht werden.

VII. Versicherbarkeit neuer Haftungsrisiken in der vernetzten Gesundheitswirtschaft

Wie oben aufgezeigt, bringt die vernetzte Gesundheitswirtschaft neue Haftungsrisiken mit sich, vor allem weil die Aufteilung der Haftung zwischen den verschiedenen Beteiligten nach den Maßstäben des geltenden Rechts nicht eindeutig ist. Ob und wie diese Risiken versicherbar sind, wird der Markt zeigen. Dabei werden voraussichtlich die Versicherungen

---

[817] *Mäsch*, JuS 2015, 556 (558); *Wende*, mrl aktuell 2015, Heft III, 24 (26).
[818] BGH, Urt. v. 09.12.1986, VI ZR 65/86, NJW-RR 1987, 603 – Lenkerverkleidung.
[819] *Foerste/Graf v. Westphalen*, Produkthaftungshandbuch, 3. Aufl. 2012, § 25, Rn. 184; *Helmig*, PHi 2004, 92 (100); MüKo/*Wagner*, 6. Aufl. 2014, § 823 Rn. 663; a.A. *Bamberger/Roth/Spindler*, § 823 Rn. 513.

die rechtlichen Risiken selbst bewerten und ggf. entsprechende Policen für die einzelnen Beteiligten anbieten. Ob diese dann Absatz am Markt finden, wird vor allem davon abhängen, ob sich die Risikobewertung der Versicherungen mit derjenigen der einzelnen Wirtschaftsakteure in der Gesundheitswirtschaft 4.0 deckt. Durch eine Klärung der Haftungsrisiken durch den Gesetzgeber ließe sich die Versicherbarkeit vor diesem Hintergrund ggf. steuern, vgl. hierzu auch Teil 7III. dieses Gutachtens und den Hinweis auf die vorgeschlagenen Pflicht zum Abschluss einer Produkthaftungsversicherung unter Abschnitt VIII.1.

VIII. Europäische/internationale Dimension

1. Gesetzgebungsprozesse auf EU-Ebene: Auswirkungen der Medical Devices Regulation (MDR) auf die Gesundheitswirtschaft 4.0

Das in der Medizinprodukte-Richtlinie angelegte System der herstellereigenen Konformitätsbewertung – ggf. unter Hinzuziehung einer benannten Stelle – soll nach dem derzeitigen Entwurf einer Medical Device Regulation[820] auch in Zukunft beibehalten werden. Der Entwurf enthält Ergänzungen und Klarstellungen der Definition des Medizinproduktes und der Abgrenzung zu anderen Produktkategorien, z.B. Kosmetika. Diese Änderungen betreffen allerdings eher Kombinationsprodukte und Produkte ohne medizinische Zielrichtung (z.B. ästhetische Implantate) als Mobile Health-Anwendungen.

Für die Gesundheitswirtschaft 4.0 relevant sind hingegen die Einführung des Unique Device Identification System („UDI“) zur weltweit kompatiblen Registrierung von Medizinprodukten im Sinne einer individuellen Rückverfolgbarkeit und der Vorschlag des Europäischen Parlaments, für Hersteller von Medizinprodukten eine Pflicht zum Abschluss einer Produkthaftpflichtversicherung mit ausreichender Mindestdeckung aufzunehmen. Insbesondere der letztgenannte Aspekt muss in seinen Auswirkungen auf die Einführung und Nutzung von Mobile-Health-Diensten näher untersucht werden, da er die Teilhabe der am Entwicklungsprozess in großem Umfang beteiligten Einzelunternehmer und KMU ggf. beeinträchtigen kann.[821] Darüber hinaus enthält Anhang I des Entwurfs in seiner Ziffer 14 Anforderungen an Software im Zusammenhang mit mobilen Computerplattformen, z.B. im Hinblick auf Zuverlässigkeit und Leistung. Diese Regelungen helfen nicht bei der medizinprodukterechtlichen Klassifizierung von Software und Apps, sind aber für die weitere Ausgestaltung des deutschen Rechtsrahmens zu berücksichtigen.

---

[820] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Medizinprodukte und zur Änderung der Richtlinie 2001/83/EG, der Verordnung(EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 vom 26.09.2012, COM(2012) 542 final.

[821] Vgl. hierzu *Hegendörfer*, MPR 2013, 181, 184.

2. Strategien auf EU-Ebene: Inhalt und Auswirkungen des Grünbuchs der Kommission zu Mobile-Health-Diensten (mHealth) und des Aktionsplans für elektronische Gesundheitsdienste 2012 – 2020 (eHealth Action Plan)

a) Grünbuch Mobile-Health-Dienste

Im Grünbuch Mobile-Health-Dienste[822] werden einige Bereiche als besonders relevant für die möglichst effektive Anwendung von Mobile-Health-Diensten identifiziert. Dazu gehören datenschutzrechtliche Probleme unter Berücksichtigung von Fragen des Cloud Computing und Big Data Analysen sowie Patientensicherheit und Transparenz, Interoperabilität, Erstattungsmodelle, Haftungsfragen und internationale Zusammenarbeit. Zu diesen Bereichen werden Fragen aufgeworfen, die von den relevanten Interessenträgern beantwortet werden sollen. Es bleibt abzuwarten, wie sich die weitere Entwicklung der gesetzgeberischen Tätigkeit auf europäischer Ebene nach Eingang und Auswertung der Antworten gestaltet. Dabei sind die Gebiete der Produktregulierung und des Datenschutzrechts insgesamt stärker europarechtlich geprägt als z. B. Fragen der zivilrechtlichen Haftung.

b) Aktionsplan für elektronische Gesundheitsdienste 2012-2020

Der Aktionsplan für elektronische Gesundheitsdienste 2012-2020 führt den bereits 2004 beschlossenen Aktionsplan für elektronische Gesundheitsdienste fort. Mit dem Erlass der Richtlinie über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung und der Einrichtung des Netzwerks für elektronische Gesundheitsdienste sind seit 2004 bereits einige Schritte in Richtung einer förmlichen Zusammenarbeit im Bereich der elektronischen Gesundheitsdienste ergriffen worden mit dem Ziel, den sozialen und wirtschaftlichen Nutzen durch die Herstellung der Interoperabilität und durch die Einführung elektronischer Gesundheitssysteme zu maximieren.[823] Diese Maßnahmen und die weitere Fortentwicklung – auch aufgrund der Ergebnisse des europäischen epSOS-Projektes[824] zur Schaffung einer Infrastruktur zum grenzüberschreitenden, elektronischen Austausch von Gesundheitsdaten – sind bei der vertieften Untersuchung der rechtlichen Hindernisse für die Gesundheitswirtschaft 4.0 und der Entwicklung von Lösungsmöglichkeiten zu berücksichtigen, auch wenn Deutschland sich an dem Projekt nicht beteiligt hat.

3. Looking abroad: Internationale Initiativen am Beispiel der US-amerikanischen FDA-Guidelines zu Mobile Medical Applications (HealthApps) sowie zu Safety and Security bei Medizinsystemen

Das US-amerikanische Medizinprodukterecht ist strukturell etwas anders aufgebaut als der europäische Regulierungsrahmen. Die risikobasierte Einstufung in Klassen erfolgt anhand

---

[822] Europäische Kommission, Grünbuch über Mobile-Health-Dienste („mHealth“) vom 10.4.2014, COM(2014) 219 final.

[823] Europäische Kommission, Aktionsplan für elektronische Gesundheitsdienste 2012–2020 – innovative Gesundheitsfürsorge im 21. Jahrhundert, COM(2012) 736 final, S. 3.

[824] European Patients Smart Open Services, http://www.epsos.eu/home/about-epsos.html.

von Vergleichsprodukten, die in einer von der US-amerikanische Food and Drug Administration („FDA“) geführten Liste bereits aufgeführt sind. Für die Risikoklassen II und III besteht eine Pflicht zur Anzeige oder behördlichen Zulassung der Produkte vor dem Inverkehrbringen.[825] Eine solche behördliche Vormarktkontrolle gibt es im europäischen Medizinprodukterecht nicht. Im Hinblick auf neuartige Medizinprodukte – wie z.B. Mobile Health-Anwendungen – kennt das US-amerikanische System eine sog. „de novo classification“, die die Rechtssicherheit des Herstellers vor dem Inverkehrbringen erhöhen kann: Im Rahmen eines vereinfachten Verfahrens können risikoarme Produkte freigegeben werden. Im Rahmen eines solchen Verfahrens hat die FDA z.B. eine App zur kontinuierlichen Überwachung von Blutzuckerwerten über einen implantierten Sensor als Klasse II-Medizinprodukt freigegeben.[826]

Die FDA hat bereits 2013 ein Auslegungspapier zur Klassifizierung von Mobile Health-Anwendungen als Medizinprodukte herausgegeben.[827] Das Dokument enthält neben allgemeinen Abgrenzungskriterien auch nicht erschöpfende Listen mit Beispielen, welche Anwendungen als regulierte Medizinprodukte zu klassifizieren sind und welche nicht (Anhänge A und B). Die grundsätzlichen Abgrenzungskriterien sind dabei durchaus ähnlich wie diejenigen des deutschen und europäischen Medizinprodukterechts, geben aber in Zweifelsfällen dem Hersteller größere Rechtssicherheit durch Auflistung der konkreten Beispiele.

4. Auswirkungen der Transatlantischen Handels- und Investitionspartnerschaft (TTIP)

Das derzeit zwischen Vertretern der EU und der USA verhandelte Freihandelsabkommen TTIP enthält einige Bestimmungen zu Medizinprodukten, die bei der vertieften Untersuchung der rechtlichen Hindernisse für die Gesundheitswirtschaft 4.0 auch zu berücksichtigen sind. Die Kernpunkte des TTIP im Zusammenhang mit der Gesundheitswirtschaft 4.0 sind derzeit das UDI-System, die Harmonisierung der Zulassungsvoraussetzungen für Medizinprodukte und die einheitliche Zertifizierung von Qualitätsmanagementsystemen.[828] Da das TTIP im Falle seiner Ratifizierung sowohl den europäischen als auch den deutschen Gesetzgeber bindet, sind die weiteren Verhandlungen zu diesen Punkten zu beobachten. Insbesondere die vorgesehene Erleichterung des elektronischen Datenaustauschs zwischen Behörden auch über Geschäftsgeheimnisse der Wirtschaftakteure und die gegenseitige Anerkennung der unterschiedlichen Prüf- und Zertifizierungssysteme für Medizinprodukte können dabei rechtliche Probleme aufwerfen.[829]

---

825 Zum Überblick: *Rübsamen*, MedR 2015, 485 (487).

826 Pressemitteilung der FDA vom 23.01.2015, http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm431385.htm.

827 Aktuelle Fassung: FDA, Mobile Medical Application, Guidance for Industry and Food and Drug Admninistration Staff, 09.02.2015, http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf (zuletzt aufgerufen am 28.08.2015).

828 *Grinblat*, MPR 2014, 158.

829 *Grinblat*, MPR 2014, 158 (159).

IX. Zusammenfassung und Ausblick

Zusammenfassend ist festzustellen, dass die aktuelle Rechtslage in Deutschland einige (potentielle) Hindernisse und Hemmnisse für die Einführung und/oder stärkere Nutzung der technischen Möglichkeiten einer Gesundheitswirtschaft 4.0 enthält. Besonders relevant sind dabei das Verbot der Fernbehandlung und die fehlende Aufnahme elektronischer Gesundheitsdienstleistungen in den EBM (Abschnitt III.). Faktisch ist auch der fehlende technische und rechtliche Rahmen für eine operable TI (Abschnitt II.) ein großes Hindernis. Aus datenschutzrechtlicher Sicht lässt sich noch nicht abschließend bewerten, ob der Entwurf des E-Health-Gesetzes in seiner aktuellen Fassung geeignet ist, Patientendaten tatsächlich zu schützen und auch das erforderliche Patientenvertrauen herzustellen. Für die Neu- und Weiterentwicklung von Mobile-Health-Anwendungen ist insbesondere eine Klarstellung der Klassifizierung im deutschen und europäischen Medizinprodukterecht relevant, um hier einen Wettbewerbsnachteil ggü. anderen Rechtsregionen (z.B. den USA) zu verhindern (Abschnitt I.1.). Auch haftungsrechtliche Fragen stellen sich im Zusammenhang mit der Gesundheitswirtschaft 4.0, die für die an der Entwicklung maßgeblich beteiligten Einzelpersonen und kleinen Unternehmen gewiss eine große Herausforderung darstellen.

Teil 18 Energy *(Dr. Cornelia Kermel)*

Die automatische Erfassung von Verbrauchsdaten durch sog. Smart Meter bzw. intelligente Messsysteme[830] nahezu ohne Zeitversatz und die flexible Steuerung von industriellen Produktionsabläufen auf der Grundlage energiewirtschaftlicher Daten ermöglichen eine weitreichendere und engere Verzahnung von Energiewirtschaft und Industrie als bisher. Diese Verzahnung bietet sowohl für die Energiewirtschaft als auch für die Industrie erhebliche Vorteile und Chancen. So können z. B. Energieerzeugung und -verbrauch mittels entsprechender Steuereinrichtungen zukünftig besser aneinander angepasst werden. Auch die Netze lassen sich durch die Nutzung digitaler Infrastrukturen bedarfsgerechter betreiben.

In einer voll vernetzten (Energie-)Wirtschaft, deren Steuerungsmechanismen u. a. auf Verbrauchsdaten basiert, die beim Energieverbraucher erhoben werden, ergeben sich aus Sicht der energieverbrauchenden Industrie indes datenschutzrechtliche Fragen. Daneben führt die umfassende, digitalisierte und dadurch oft automatisch ablaufende Koordination aller Beteiligten entlang der energiewirtschaftlichen Wertschöpfungskette auch dazu, dass ein größeres „Störpotential“ im Gesamtsystem existiert. Für die Industrie, die auf die ständige Verfügbarkeit von Energie angewiesen ist, stellt sich vor diesem Hintergrund insbesondere die Frage, wie die Versorgungssicherheit auch in einer digitalisierten Energiewirtschaft sichergestellt werden kann. Die in Zukunft noch weiter voranschreitende Digitalisierung der Energiewirtschaft wirft nicht zuletzt die Frage auf, wer die Kosten für die Installation der erforderlichen technischen Systeme und für andere, mittelbar mit dieser Digitalisierung in Zusammenhang stehende (Reform-)Vorhaben trägt.

I. Erhebung, Verarbeitung und Nutzung von Daten

Die geplante Ausstattung von Energieverbrauchern mit Smart Metern eröffnet neue Möglichkeiten, die Energieerzeugung und den Energieverbrauch zu steuern. Smart Meter bzw. intelligente Messsysteme sind über ein sog. Smart Meter Gateway in ein Kommunikationsnetz eingebundene moderne Messeinrichtungen, die den Energieverbrauch und die Nutzungszeit erfassen und aufgrund ihrer technischen Ausrüstung und kommunikativen Einbindung eine Vielzahl von Anwendungen ermöglichen. Denkbar wäre vor allem die Nutzung von aktuellen Daten, um die Erzeugung auf den Stromverbrauch abzustimmen oder – andersherum – den Stromverbrauch in Abhängigkeit von der aktuellen Stromerzeugung zu steuern. In Betracht käme etwa auch, die Vorhersagen für den Stromverbrauch durch genauer aufgelöste historische Verbrauchsdaten zu präzisieren und so die Bilanzkreissteuerung zu verbessern. Im Strom- und Gasbereich könnten auf diese Weise auch Beschaffungsstrategien optimiert werden.

Im aktuell geltenden Rechtsrahmen ist bereits angelegt, dass ein „Upgrade“ der bestehenden Messsysteme auf intelligente Messsysteme stattfinden wird (§§ 21b bis 21h Energiewirtschaftsgesetz – EnWG). Die entsprechenden Regelungen sind indes nicht umfassend

[830] Im Folgenden werden diese Begriffe synonym verwendet.

und lassen noch viele Fragen bei der Erhebung und Nutzung von Daten offen. Der Gesetzgeber plant gegenwärtig, ein Gesetz zur Digitalisierung der Energiewende zu erlassen, mit dem der erforderliche umfassende Rechtsrahmen geschaffen werden soll. Nachdem das Bundesministerium für Wirtschaft und Energie am 21.09.2015 einen Referentenentwurf vorgelegt hatte, liegt nunmehr der Gesetzesentwurf vom 06.11.2015 vor.[831] Der Gesetzesentwurf enthält u. a. in Artikel 1 das Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG)[832] Im weiteren Gesetzgebungsverfahren, das bis Mai 2016 abgeschlossen sein soll, sind einzelne Änderungen an dem vorgeschlagenen Rechtsrahmen selbstverständlich noch möglich.

1. Eindeutige Regelung zur Erhebung, Verarbeitung und Nutzung aller erhobenen Daten

Bei den in intelligenten Messsystemen erhobenen und gesammelten Verbrauchsdaten handelt es sich in der Regel um sensible Daten, die z. B. Rückschlüsse auf die Auslastung und die Produktionsabläufe eines Industriestandortes zulassen können. Im Einzelfall kann es sich daher bei den erhobenen Daten um sog. Geschäfts- und Betriebsgeheimnisse handeln, die auch einem besonderen grundrechtlichen Schutz (Art. 14 Abs. 1 und Art. 12 Abs. 1 GG) unterfallen. Der Schutz dieser Daten vor unberechtigtem Zugriff spielt aus Sicht der betroffenen Unternehmen eine überragend wichtige Rolle.

Im aktuell geltenden Rechtsrahmen regelt § 21g EnWG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die aus bzw. mit Hilfe von Messsystemen gewonnen werden. § 21g EnWG sieht diesbezüglich vor, dass eine Nutzung ausschließlich durch zum Datenumgang berechtigte Stellen und ausschließlich auf Grundlage des EnWG erfolgen darf, soweit dies für die in § 21g EnWG definierten Zwecke erforderlich ist.

Gemäß der Begriffsdefinition des § 3 Abs. 1 des Bundesdatenschutzgesetzes (BDSG), die im Rahmen von § 21g EnWG Anwendung findet, handelt es sich bei personenbezogenen Daten um *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“*. Diese Daten dürfen ausschließlich gemäß der Vorgaben des § 21g EnWG erhoben, verarbeitet und genutzt werden. Regelungen in Bezug auf nichtpersonenbezogene Daten enthält § 21g EnWG aber nicht. Die derzeit geltende Regelung zur Erhebung, Verarbeitung und Nutzung der in intelligenten Messsystemen erhobenen Daten in § 21g EnWG gewährleistet den Schutz von Geschäfts- und Betriebsgeheimnissen deswegen nicht.

Diese Regelungslücke soll über das geplante Messstellenbetriebsgesetz geschlossen werden. Dieses enthält im Teil 3 Regelungen zur Schaffung eines bereichsspezifischen, in Bezug auf

[831] BR-Drs. 543/15

[832] In diesem Gesetz finden sich technische Vorgaben, die in Teil 2 im Kapitel 3 zusammengefasst sind. Diese Regelungen wurden notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (kodifizierter Text, vormals 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998).

intelligente Messsysteme abschließenden Datenschutzrechts, das nicht auf personenbezogene Daten im Sinne des BDSG beschränkt ist, sondern alle in den intelligenten Messsystemen erhobenen Daten zum Gegenstand hat. Der geplante Rechtsrahmen für die in intelligenten Messsystemen erhobenen Daten soll abschließend regeln, wer zu welchem Zweck mit den erhobenen Daten umgehen darf sowie den zulässigen Umfang der Datenerhebung. Genauso soll festgelegt werden, in welchem Umfang bzw. unter welchen Voraussetzungen ein Datenaustausch zwischen den verschiedenen Akteuren stattfinden darf. Auch soll gesetzlich geregelt werden, wie und wie lange die erhobenen Daten zu speichern und wann sie vom Datenumgangsberechtigten unwiderruflich zu löschen sind.

In dem nunmehr im Entwurf vorliegenden Gesetz zur Digitalisierung der Energiewende und insbesondere in dem darin enthaltenen Messstellenbetriebsgesetz werden die wesentlichen Fragestellungen in Bezug auf die Erhebung und Nutzung von nicht personenbezogenen Daten aufgegriffen und in einer eigenständigen Vorschrift geregelt.[833] Zum Schutz der erfassten Daten enthält der Gesetzesentwurf umfassende technische Vorgaben für die Einrichtung der intelligenten Messsysteme und die Übermittlung und Verarbeitung der betreffenden Daten. Der Kreis der Personen, die zum Umgang mit den Daten berechtigt sind, umfasst dabei zunächst die Akteure aus dem Energiesektor, also neben den Messstellenbetreibern etwa die Netzbetreiber, Energielieferanten, Direktvermarktungsunternehmen und Bilanzkreisverantwortlichen. Darüber hinaus besteht aber auch die Möglichkeit, weiteren Stellen durch eine schriftliche Einwilligung des Anschlussnutzers den Umgang mit den Daten zu gestatten. Dies würde es etwa Drittanbietern ermöglichen, Dienstleistungen zur Energieoptimierung anzubieten.

2. Mehrwertdienste müssen möglich sein

Über die intelligenten Messsysteme sollen möglichst viele energiewirtschaftliche Anwendungsfälle bedient werden. Hierzu gehören die Kommunikation von Stromverbrauchs- und Erzeugungswerten und anderen netzdienlichen Informationen sowie die Umsetzung von Last- und Erzeugungsmanagementmaßnahmen. Anlagen zur Stromerzeugung (insbesondere Erneuerbare-Energien-Anlagen), Elektromobile, Wärmepumpen und Energiespeicher könnten in das intelligente Energienetz integriert werden, um eine flächendeckende Vernetzung aller Wertschöpfungsstufen und Marktakteure zu erreichen. In einer zukunftsweisenden Ausrichtung soll die dem Smart Meter zugeordnete Kommunikationsplattform, das Smart Meter Gateway, als Datenplattform für Messwerte aller möglicher Sparten dienen. Sowohl der gegenwärtige Rechtsrahmen als auch der Entwurf des Messstellenbetriebsgesetzessehen eine Reihe von Anwendungen vor, für die die Daten der Smart Meter genutzt werden können.

Im Gegensatz zum gegenwärtigen Rechtsrahmen sieht der Gesetzesentwurf vor, dass mehr Akteure der Energiewirtschaft auf die Daten zugreifen können. So sollen zukünftig etwa auch Direktvermarktungsunternehmer einbezogen werden, die die Daten zur Steuerung der

[833] Siehe § 50 MsbG-E

Stromproduktion aus erneuerbaren Energien und zur Portfoliooptimierung nutzen können. Das dürfte die Marktintegration der erneuerbaren Energien voranbringen. Weiterhin ist die Durchführung von Mehrwertdiensten auf Veranlassung des Anschlussnutzers in dem vorgeschlagenen neuen Rechtsrahmen ausdrücklich als zulässiger Zweck für den Umgang mit Daten genannt. Das könnte innovative Geschäftsmodelle fördern, die etwa durch die Auswertung und den Abgleich einer Vielzahl von Daten neue Optimierungsstrategien im Energiebereich aufzeigen können.

II. Gewährleistung der Versorgungssicherheit

Die zunehmende Digitalisierung der Energiewirtschaft geht mit einer bisher unerreichten Akteursvielfalt einher, was die „Störanfälligkeit" des Gesamtsystems erhöht und damit Versorgungssicherheit gefährden kann. Darüber hinaus erfordert die Aufrechterhaltung der Versorgungssicherheit insbesondere einen umfassenden Schutz der neuen digitalen Systeme auf allen Wertschöpfungsstufen gegen Angriffe von außen, um zu verhindern, dass unberechtigte Personen über die mit Kommunikationsnetzen verbundene energiewirtschaftliche Infrastruktur Zugriff z. B. auf Produktionsanlagen erhalten.

1. Klare Abgrenzung der Verantwortungsbereiche im Zusammenhang mit dem Einbau und dem Betrieb von intelligenten Messsystemen

Um einerseits den zügigen Roll-out von Smart Metern zu fördern und andererseits die hohe Sicherheit der Energieinfrastrukturen nicht zu gefährden, sollten die Verantwortungsbereiche bei der Ausstattung und dem Betrieb von Smart Metern klar abgegrenzt werden.

a) Möglichkeit zur Übertragung der Aufgabe des Messstellenbetriebs auf einen Dritten muss geschaffen werden

Der Gesetzgeber hat in den im Rahmen der Energierechtsnovelle 2011 eingefügten §§ 21c ff. EnWG die breit angelegte verpflichtende Einführung von Messsystemen als Grundlage für intelligente Netze geregelt. Zur Erreichung dieses Ziels wird das Recht der Messstellenbetreiber, über die Art der von ihnen zu betreibenden Messeinrichtungen zu bestimmen, eingeschränkt. Sie werden vielmehr verpflichtet, in den in § 21c Abs. 1 EnWG geregelten Fallgestaltungen und unter den dort geregelten Voraussetzungen Messsysteme im Sinne von § 21d EnWG einzubauen.

Verpflichtet zum Einbau der Messsysteme ist grundsätzlich der jeweilige Betreiber des Energieversorgungsnetzes. Dieser ist nach derzeitiger Rechtslage Messstellenbetreiber im Sinne des Gesetzes, soweit nicht auf Wunsch des Anschlussnutzers der Messstellenbetrieb durch einen Dritten durchgeführt wird (vgl. § 21b Abs. 1 EnWG).

Mit der Rolle des Messstellenbetreibers sind indes erhebliche Verpflichtungen und finanzielle Belastungen verknüpft. Damit ist zu erwarten, dass aus personellen oder finanziellen Gründen (insbesondere bei Vorgabe von Kostenobergrenzen) der ein oder andere Netzbe-

treiber die Funktion des grundzuständigen Messstellenbetreibers nicht wird ausfüllen können. Nach den geltenden Regelungen kann der Netzbetreiber seine Rolle als grundzuständiger Messstellenbetreiber aber nicht auf einen Dritten übertragen.

In dem Entwurf des Messstellenbetriebsgesetzes wird dem Netzbetreiber, der nicht in der Lage oder Willens ist, die Funktion des grundzuständigen Messstellenbetreibers auszuüben, daher nunmehr die Möglichkeit eingeräumt, im Wege der Ausschreibung diese Funktion auf ein anderes Unternehmen zu übertragen, was zu begrüßen ist. Denn auf diese Weise kann eine zügige Verbreitung von Smart Metern gefördert werden.

b) Verantwortlichkeit und Haftung des Messstellenbetreibers muss eindeutig geregelt und eine Rückfallzuständigkeit festgelegt werden

Mit der Einführung des sog. intelligenten Messstellenbetreibers wurde bereits nach dem geltenden Recht eine neue Marktrolle eingeführt, die die Komplexität der Kommunikation zwischen Messstellenbetreiber, Netzbetreiber, Energielieferant und Anschlussnutzer bzw. Anschlussnehmer erhöht hat. Diese Komplexität würde durch die eben beschriebene Möglichkeit, die Funktion des grundzuständigen Messstellenbetreibers im Wege der Ausschreibung zu übertragen, weiter zunehmen.

Insbesondere mit Blick auf die Versorgungssicherheit stellen sich aus Sicht der Energieverbraucher hier Fragen nach einer Rückfallzuständigkeit, d. h. die Zuständigkeit bei einem Ausfall des durch Ausschreibung ermittelten Messstellenbetreibers. In Betracht kommt dabei zum einen, dem ursprünglichen Netzbetreiber eine Rückfallzuständigkeit aufzubürden. Zum anderen könnte aber etwa auch der Netzbetreiber bei Ausfall des Messstellenbetreibers in die Pflicht genommen werden, der in einem bestimmten geografischen Gebiet die meisten Messstellen betreibt.

Daneben muss geregelt werden, wie die Ausübung der Rechte des Netzbetreibers, der nicht Messstellenbetreiber ist, insbesondere in Bezug auf die Durchführung von notwendigen Unterbrechungen (z. B. nach §§ 17, 24 der Niederspannungsanschlussverordnung - NAV) sichergestellt werden kann. Das gleiche gilt auch in Bezug auf die Rechte der anderen Marktteilnehmer wie etwa die Bilanzkreisverantwortlichen. Die genannten Akteure müssen ihren Aufgaben auch dann nachkommen können, wenn der Messstellenbetrieb nicht (mehr) in der Verantwortung des Netzbetreibers liegt, sondern in der Verantwortung eines durch Ausschreibung ermittelten Dritten. Denn nur wenn die Aufgabenwahrnehmung beim Messstellenbetrieb sichergestellt ist, kann auch die Versorgungssicherheit gewährleistet werden.

c) Implementierung des Smart Meter Gateway Administrators in das energiewirtschaftliche System erforderlich

Neben dem Betrieb der Smart Meter muss auch der Datenaustausch über die Kommunikationsplattform, das Smart Meter Gateway, zuverlässig funktionieren. Dafür ist der Smart Meter Gateway Administrator verantwortlich. Sein Aufgabenfeld betrifft die Bereitstellung

des Smart Meter Gateway und der informationstechnischen Anbindung von Messgeräten sowie anderer an das Smart Meter Gateway angebundenen technischen Einrichtungen.

Die neu geschaffene Marktrolle des Smart Meter Gateway Administrators ist für das Funktionieren des Gesamtsystems von erheblicher Bedeutung, da jegliche Kommunikation zwischen der digitalen Infrastruktur über das Smart Meter Gateway stattfindet. Deswegen muss sichergestellt werden, dass dieser neue Akteur so in das energiewirtschaftliche Gesamtsystem eingefügt wird, dass dieses System nicht beeinträchtigt wird und die Versorgungssicherheit, trotz der zukünftigen weiter gesteigerten Akteursvielfalt, ständig gewährleistet werden kann.

Dazu ist eine genaue Definition der Verantwortungsbereiche der verschiedenen Akteure erforderlich. Darüber hinaus muss die Zusammenarbeit der Marktteilnehmer und insbesondere der Informationsaustausch zwischen diesen detailliert festgeschrieben werden, um einen reibungslosen Datenaustausch zu ermöglichen.

2. Schutz digitaler Energieinfrastruktur gegenüber Angriffen von außen

Eine flächendeckend mit dem Telekommunikationsnetz verbundene Energieinfrastruktur bietet eine Vielzahl von Angriffspunkten, die es Dritten ermöglichen könnten, Einfluss auf die Steuerung von Erzeugungs-, Verbrauchs- oder netztechnischen Infrastruktureinrichtungen zu nehmen. Dies erfordert eine technische Ausstattung der digitalen Systemkomponenten, die höchsten technischen Sicherheitsanforderungen genügt.

a) Technische Sicherheitsanforderungen an den Betrieb von Energienetzen umfassend geregelt

Der Gesetzgeber hat im Rahmen der EnWG-Novelle 2011 die Vorschrift des § 11 Abs. 1a in das EnWG eingefügt. Danach umfasst der Betrieb eines sicheren Energieversorgungsnetzes insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen bzw. für einen sicheren Netzbetrieb notwendig sind. Unter Sicherheit wird damit sowohl die technische Anlagensicherheit als auch die Versorgungssicherheit verstanden.

Der Bundesnetzagentur (BNetzA) kommt in diesem Zusammenhang die Aufgabe zu, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Katalog von Sicherheitsanforderungen zu erstellen zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Dazu hat die BNetzA am 12.08.2015 einen IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG veröffentlicht. Der Geltungsbereich dieses Sicherheitskataloges umfasst alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind. Enthalten sind demnach zumindest alle TK- und EDV-Systeme des Netzbetreibers, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Daneben sind auch TK- und EDV-Systeme im

Netz betroffen, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte. Darunter fallen z. B. Messeinrichtungen an Trafo- oder Netzkoppelstationen. Solange und soweit Messsysteme nach § 21d EnWG zu netzbetrieblichen Zwecken (z. B. Ermittlung von Netzzustandsinformationen, Ermöglichung von Last- und Erzeugungsmanagement) eingesetzt werden, hat der Netzbetreiber sicherzustellen, dass hinsichtlich dieses Teilbereichs Sicherheitsstandards eingehalten werden, die dem IT-Sicherheitskatalog zumindest gleichwertig sind.

Zur Gewährleistung eines angemessenen Sicherheitsniveaus für TK- und EDV-Systeme, die für einen sicheren Netzbetrieb notwendig sind, sieht der IT-Sicherheitskatalog zahlreiche Maßnahmen vor, die von den Netzbetreibern umzusetzen sind. So haben die Netzbetreiber ein sog. Informationssicherheits-Managementsystem zu implementieren, das den Anforderungen der DIN ISO/IEC 27001 in der jeweils geltenden Fassung genügt und bestimmte, in dem Sicherheitskatalog näher beschriebene Systeme umfasst.

b) Geplante Vereinheitlichung der Schutzprofile und Technischen Richtlinien in Bezug auf intelligente Messsysteme

Vom Geltungsbereich des zuvor dargestellten IT-Sicherheitskatalogs ausgenommen sind Messsysteme nach § 21d EnWG, soweit sie nicht zu netzbetrieblichen Zwecken eingesetzt werden (z. B. zur Ermittlung von Energieverbräuchen). Ungeachtet dessen gelten für alle Messsysteme die Schutzanforderungen gemäß §§ 21e, 21i EnWG und den auf dieser Basis erlassenen Rechtsverordnungen einschließlich der vom BSI erarbeiteten Schutzprofilen und Technischen Richtlinien.

Nach § 21e Abs. 2 Nr. 1 EnWG dürfen insofern zur Datenerhebung, -verarbeitung, -speicherung, -prüfung, -übermittlung ausschließlich solche technischen Systeme und Bestandteile eingesetzt werden, die den Anforderungen von Schutzprofilen nach der nach § 21i EnWG zu erstellenden Rechtsverordnung entsprechen. § 21i Abs. 1 Nr. 12 EnWG berechtigt die Bundesregierung mit Zustimmung des Bundesrates Schutzprofile und Technische Richtlinien für Messsysteme im Sinne von § 21d Abs. 1 EnWG zu regeln.

Diese in § 21i Abs. 1 Nr. 12 EnWG genannten Schutzprofile und die erwähnten Technischen Richtlinien wurden bereits durch das BSI erarbeitet und sind auf der Internetpräsenz des BSI abrufbar.[834] So existiert bereits heute z. B. ein Schutzprofil für die Kommunikationseinheit und das Sicherheitsmodul eines intelligenten Messsystems für Stoff- und Energiemengen. Die Technische Richtlinie TR-03109-2 enthält Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls eines Smart Meter Gateways, die Technische Richtlinie TR-03109-3 kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen.

[834] https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html.

Diese Schutzprofile und die Technischen Richtlinien werden gemäß § 22 Abs. 2 des im Entwurf vorliegenden Messstellenbetriebsgesetzes vereinheitlicht, indem die Einhaltung des Standes der Technik vermutet wird, wenn die vom BSI entwickelten Schutzprofile in der jeweils geltenden Fassung eingehalten werden.

III. Verteilung der Kosten für die Digitalisierung der Energiewirtschaft

Die Digitalisierung der Energiewirtschaft ist mit Kosten für die Installation und den Betrieb der digitalen Infrastruktur verbunden. Es stellt sich die Frage, wer diese Kosten trägt. Aber auch andere energiewirtschaftliche (Reform-)Vorhaben, die mittelbar im Zusammenhang mit den aufgezeigten Digitalisierungsbestrebungen stehen, sind ggf. mit Kosten für die Energieverbraucher und damit auch für die Industrie verbunden.

1. Begrenzung der Kosten für den Einbau intelligenter Messsysteme

Der Einbau und Betrieb intelligenter Messsysteme verursacht regelmäßig höhere Kosten beim Messstellenbetreiber als bei „gewöhnlichen“ analogen Messsystemen. Diese höheren Kosten werden über entsprechende Entgelte an die Energieverbraucher weitergereicht. Dabei ist allerdings zu berücksichtigen, dass diesen Mehrkosten Energieeinsparpotenziale auf Seiten der Energieverbraucher gegenüber stehen, die sich insgesamt kostensenkend auswirken können. Das Einsparpotenzial auf Verbraucherseite hängt dabei im Ergebnis erheblich von der Menge der bezogenen Energie ab.

Vor diesem Hintergrund erscheint es sachgerecht, das vom Messstellenbetreiber zu erhebende Entgelt für den Einbau und den Betrieb intelligenter Messsysteme so festzulegen, dass es sich der Höhe nach am Verbrauch des jeweiligen Abnehmers und damit an dem von bestimmten Verbrauchergruppen zu erzielenden Einsparungspotenzial orientiert. So kann verhindert werden, dass es zu einer Benachteiligung bzw. Überforderung solcher Energieverbraucher kommt, die durch den Einbau eines intelligenten Messsystems wegen ihres geringen Verbrauchs absolut betrachtet nur unterdurchschnittlich profitieren.

Diesen Ansatz verfolgt auch der Entwurf des Messstellenbetriebsgesetzes. Danach sollen die Kosten für die Verbraucher in Abhängigkeit zum Energieverbrauch begrenzt und entsprechende Preisobergrenzen festgelegt werden, die sich an dem durchschnittlich zu erzielenden Einsparpotenzial unter Zugrundlegung von Sowieso-Kosten orientieren.[835]

2. Weitere ggf. kostenrelevante (Reform-)Vorhaben

Auch andere, derzeit diskutierte Vorhaben im Bereich der Energiewirtschaft, die mittelbar mit der Digitalisierung der Energiewirtschaft zusammenhängen, können sich zukünftig kostenmäßig bei den Energieverbrauchern auswirken.

[835] Siehe §§ 29 ff. MsbG-E

So stellt sich u. a. die Frage, wie der für die Integration der erneuerbaren Energien erforderliche Ausbau insbesondere auch der Verteilernetze bzw. die dadurch entstehenden Kosten gleichmäßig auf alle Netznutzer und damit letztlich auf die Verbraucher verteilt werden kann. Denn nach der derzeit geltenden Netzentgeltsystematik tragen diese Kosten ausschließlich die Netznutzer, die an die vom Ausbau betroffenen Netze angeschlossen sind. Eine Verteilung auf alle Netznutzer in Deutschland oder eine Umlegung auf die Einspeiser könnte dabei zu Kostenveränderungen bei den jeweils zu entrichtenden Netzentgelten führen.

Die Installation intelligenter Messsysteme könnte aber auch Auswirkungen auf die bestehende Netzentgeltsystematik insgesamt haben. Denn die Installation intelligenter Messsysteme bzw. die darin erhobenen Daten bieten die Möglichkeit, energiewirtschaftliche Kenndaten bei allen Verbrauchern bei der Berechnung der Netznutzungsentgelte zu berücksichtigen und so z. B. auch diejenigen Netznutzer stärker an der Finanzierung der Netzinfrastruktur zu beteiligen, die bisher an den Kosten nur unterdurchschnittlich beteiligt waren, weil sie sich z. B. selbst mit Energie versorgen und nur als Notfalloption über einen Netzanschluss verfügen – was nach derzeitiger Entgeltsystematik zu einem geringen Netzentgelt führt, obwohl von der Netzinfrastruktur profitiert wird.

Letztlich kann die zunehmende Digitalisierung sich auch auf das mögliche Erfordernis eines sog. Kapazitätsmarktes auswirken, da die Knappheit der Erzeugungskapazitäten und die Auswirkungen auf die Stromnachfrage durch die digitale Infrastruktur genau ermittelt werden könnten. Auch die mit der Digitalisierung zusammenhängende Flexibilisierung sowohl der Erzeugung als auch des Verbrauchs kann dabei Auswirkungen auf das mögliche Erfordernis eines Kapazitätsmarktes haben.