

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	IX
Abkürzungsverzeichnis	XVII
Autorenverzeichnis	XXIII

Teil 1: Auf dem Weg zur Industrie 4.0 – Einführung

Auf dem Weg zur Industrie 4.0	1
-------------------------------------	---

Teil 2: Allgemeiner rechtlicher Rahmen

A. Schutz von maschinengenerierten Daten	27
B. Forschung und Entwicklung sowie Kooperationen	53
C. Haftungsfragen bei vernetzten und autonomen Systemen	69
D. Anforderungen des Telekommunikationsrechts	85
E. Datenschutz und IT-Sicherheit	140
F. Kartellrechtlicher Rahmen	183
G. Arbeitsrecht – Realität und Herausforderungen	211

Teil 3: Besonderheiten bei Vertragsschluss und -gestaltung

A. Vertragsschluss beim IoT Rechtsgeschäft	239
B. Anforderungen bei Verbraucherverträgen	267
C. Vertragstypen und Herausforderungen der Vertragsgestaltung	291

Teil 4: Besonderheiten ausgewählter Branchen

A. Digitalisierung des Gesundheitswesens (eHealth)	333
B. Automatisiertes Fahren (Automotive)	361
C. Digitalisierung des Energiesektors (Smart Grids)	385
D. Digitalisierung der Versicherungswirtschaft (Insurance)	404
E. Digitalisierung der Elektroindustrie (Smart Factory)	420
F. Digitalisierung der Bankenwelt (FinTech)	437

Teil 5: Europäische und amerikanische Perspektiven

A. Zukünftige Regulierung des Internet of Things in Europa: Ein Überblick	479
B. Regulation and Self-Regulation of the Internet of Things in the United States ...	504
Stichwortverzeichnis	527

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Abkürzungsverzeichnis	XVII
Autorenverzeichnis	XXIII

Teil 1: Auf dem Weg zur Industrie 4.0 – Einführung

Auf dem Weg zur Industrie 4.0	1
I. Einführung	3
II. Einordnung	5
III. Ökonomische Relevanz der Industrie 4.0	8
1. Treiber und Wirkungen	8
2. Neue Wertschöpfungsketten	9
3. Branchen	10
4. Beispiel Telekommunikation	11
5. Umsetzung	13
6. Potenziale	16
IV. Politische und öffentliche Diskussion	16
V. Herausforderung Rechtsrahmen	17
VI. Ausgewählte Schwerpunkte für rechtliche Fragestellungen	19
1. Daten	19
2. Konnektivität	21
3. Standardisierung und Interoperabilität	22
4. Arbeitswelt	24
5. Rechtssicherheit	25
VII. Ausblick	25

Teil 2: Allgemeiner rechtlicher Rahmen

A. Schutz von maschinengenerierten Daten	27
I. Einführung	28
1. Begriffsbestimmung	29
2. Abgrenzung zum Datenschutzrecht	29
II. Schutz maschinengenerierter Daten – an den Grenzen der Gesetze	30
1. Schutz durch IP-Rechte	30
2. Lauterkeitsrechtlicher Schutz von maschinengenerierten Daten	36
3. Strafrechtliche und kapitalmarktrechtliche Ansätze	41
III. Maschinengenerierte Daten – Ansätze der Grenzverschiebung	42
1. Scheitern von sachenrechtlichen Begründungen	43
2. Vorschlag eines „Rechts des Datenerzeugers“	44
IV. Derzeitige Lösung: Vertragliche Konstruktion eines „immateriellen Gutes“	46
1. Kategorisierung von maschinengenerierten Daten	46
2. Vereinbarungen über Datennutzungen	48
B. Forschung und Entwicklung sowie Kooperationen	53
I. Erscheinungsformen der Kooperationen	54
1. Unterscheidung nach Dimensionen	55
2. Unterscheidung nach der Bestimmbarkeit des Teilnehmerkreises	56

II. Vertragsgestaltung	56
1. Semi-offene Innovationsprozesse	57
2. Offene Innovationsprozesse	64
III. Kartellrecht	66
IV. Rechtspolitischer Handlungsbedarf	67
C. Haftungsfragen bei vernetzten und autonomen Systemen	69
I. Einführung	70
II. Vertragliche Haftung	70
III. Produkt- und Produzentenhaftung	71
1. Die deliktsrechtliche Produzentenhaftung	71
2. Produkthaftung nach dem Produkthaftungsgesetz	75
IV. Sonderprobleme der Produkt-/Produzentenhaftung im Zusammenhang mit Industrie 4.0	76
1. Neue Produktrisiken durch neue Funktionen	76
2. Produktsicherheit und IT-Sicherheit – Produktfehler bei Cyber-Angriffen?	76
3. Apps und Software	78
4. Das Nichtfunktionieren als Produktfehler	79
5. Bestimmung des Herstellers beim Einsatz innovativer Produktionstechnologien	80
6. Abgrenzung von Verantwortungsbereichen in der Produktions- und Lieferkette	81
7. Haftungsrechtliche Verantwortung bei Weiterentwicklung des Produktes nach Inverkehrbringen, insbesondere bei maschinellem Lernen	82
V. Betreiber-/Benutzerhaftung	82
1. Haftung nach dem HaftPflG	83
2. Kfz-Halterhaftung	83
3. Deliktische Haftung des Benutzers	83
VI. Zusammenfassung der haftungsrechtlichen Herausforderungen	83
D. Anforderungen des Telekommunikationsrechts	85
I. Anwendbarkeit der Regelungen des Telekommunikationsgesetzes	87
1. Geschäftsmodelle und regulatorische Anknüpfungspunkte	87
2. Connectivity Service Provider	88
3. IoT Service Provider	92
4. IoT User	94
5. Fallbeispiele	95
6. Zwischenergebnis und Ausblick	96
II. Meldung und Aufsicht durch die Bundesnetzagentur	97
III. Kundenschutz	98
1. Vertragliche Informationspflichten und Vertragsdauer	98
2. Auswirkung der Regelungen zur sogenannten Routerfreiheit	99
3. Haftung für Vermögensschäden	100
4. Fragen der Abrechnung	101
5. Sperre von Nutzern	103
IV. Nummerierung und Nummernnutzung	104
1. (Ruf-)Nummern für IoT Dienste	104
2. Adressierung von ortsfesten IoT Endgeräten	107
3. Adressierung von mobilen IoT Endgeräten	107
4. Zuteilung von Nummern durch die Bundesnetzagentur	110
5. Zuteilung von IP-Adressen	111
6. Anbieterwechsel und Rufnummernportierung bei IoT Diensten	111
V. Fernmeldegeheimnis und Datenschutz	114
1. Fernmeldegeheimnis bei IoT Diensten	114

2. Telekommunikationsdatenschutz	116
VI. Öffentliche Sicherheit	120
1. In der Regel keine Notrufverpflichtung bei IoT Anwendungen	120
2. eCall Verpflichtung	121
3. Schutz der Systeme und Daten bei IoT Anwendungen	122
4. Telekommunikationsbevorrechtigung für IoT User und IoT End-User	127
5. Behördenbeauskunftung und Überwachungsmaßnahmen	127
VII. Roaming von IoT Anwendungen	133
1. Hintergrund des Roamings bei IoT Anwendungen	133
2. Anwendbarkeit der Roamingverordnung auf IoT Anwendungen	134
3. Roamingentgelte	134
VIII. Netzneutralität und IoT Dienste	135
IX. Ansprüche und Schlichtung	135
1. Ansprüche von Kunden, Verbraucherverbänden und Mitbewerbern	135
2. Schlichtung	136
X. Übernahme der Verpflichtungen durch den Connectivity Service Provider	136
XI. Zwischenergebnis	138
E. Datenschutz und IT-Sicherheit	140
I. Einführung	141
1. Datenschutz	142
2. IT-Sicherheit	142
II. Datenschutz	143
1. Bestimmungen zum Datenschutz	143
2. Personenbezogene Daten	147
3. Räumlicher Anwendungsbereich datenschutzrechtlicher Regelungen	150
4. Datenschutzrechtliche Verantwortlichkeiten	152
5. Informationspflichten, Rechte der Betroffenen	155
6. Technische und organisatorische Datenschutzmaßnahmen	161
7. Folgen bei Datenschutzverstößen	167
III. IT-Sicherheit	173
1. Bedrohungs- und Angriffsszenarien	173
2. Ordnungsrecht	174
3. IT-Sicherheit vs. Datenschutz – Erfordernis eines Ausgleichs	181
F. Kartellrechtlicher Rahmen	183
I. Einführung	184
II. Der Kartellrechtsrahmen im Überblick	186
1. Grundsatz, Verhaltenskontrolle und Fusionskontrolle	186
2. Kartellverbot und Gruppen- oder Einzelfreistellung	187
3. Missbrauchsverbot	190
4. Fusionskontrolle	191
5. Marktdefinition als Ausgangspunkt jeder wettbewerblichen Beurteilung	192
III. Einzelfragen	193
1. Kartellrechtliche Erfassung von Plattform-Geschäftsmodellen	193
2. Marktmacht und Daten	198
3. Probleme des Kartellverbotes	201
4. Technische Standards/Normen	206
IV. Zusammenfassende Bewertung	210
G. Arbeitsrecht – Realität und Herausforderungen	211
I. Einführung	212
II. Arbeitsrecht 4.0? – Realität und Anpassungsbedarf	213
1. Neue Arbeitsformen – Plattformökonomie und „Crowdworking“	214
2. Auswirkungen auf den Arbeitsort	216
3. Arbeitszeitfragen	221

4. „Entpersonalisierte Arbeitsverhältnisse“ – Ausübung von Weisungsrechten in der Industrie 4.0	224
5. Kündigungsgrund „Digitalisierung“ – Arbeitsplatzverlust infolge von Digitalisierung und Automatisierung	226
6. Betriebliche Mitbestimmung in der Industrie 4.0	228
7. Technischer Arbeitsschutz und Gesundheitsschutz in der Industrie 4.0	232
8. Arbeitnehmerdatenschutz und Mitarbeiterkontrolle	233

Teil 3: Besonderheiten bei Vertragsschluss und -gestaltung

A. Vertragsschluss beim IoT Rechtsgeschäft	239
I. Einführung und Fallbeispiel	240
II. Allgemeine Grundzüge des Vertragsschlusses	241
1. Prinzipien	241
2. Der Softwareagent im Rechtsverkehr	247
3. Zusammenfassung	256
III. Internet of Things und Allgemeine Geschäftsbedingungen	257
1. Ausgangspunkt: Strenge des deutschen AGB-Rechts	259
2. Interessenslage für Hersteller und Betreiber von M2M-Kommunikationssystemen und Softwareagenten	264
3. Handlungsbedarf für den Gesetzgeber	265
IV. Praxistipps	266
B. Anforderungen bei Verbraucherverträgen	267
I. Die Anwendbarkeit der fernabsatzrechtlichen Regelungen	269
1. IoT als Teil der besonderen Betriebsformen, §§ 312 ff. BGB	269
2. Bereichsausnahmen	270
3. Außerhalb von Geschäftsräumen geschlossener Vertrag oder Fernabsatzvertrag	272
4. Vertrag im elektronischen Geschäftsverkehr	274
II. Informationspflichten bei Verbraucherverträgen	275
1. Vorvertragliche Informationspflicht	275
2. Nachvertragliche Informationspflicht	278
3. Einzelne Informationspflichten aus Art. 246a § 1 EGBGB	278
4. Weitere Pflichten im elektronischen Geschäftsverkehr	285
III. Gestaltung von IoT Modellen in der Praxis	288
1. Vorhandene Modelle („Dash Button“, „amazon echo“ et al.)	288
2. Anforderungen an die Gestaltung von IoT Geschäftsmodellen <i>de lege lata</i>	289
3. Zusammenfassung und Ausblick	290
C. Vertragstypen und Herausforderungen der Vertragsgestaltung	291
I. Einführung	292
II. Vertragsgegenstand	294
1. Arten von Verträgen	294
2. Vertragsstruktur	295
3. Vertragstypologische Einordnung	297
III. Hauptleistungspflichten	298
1. Leistungsbeschreibung	298
2. Wesentliche Hauptleistungen	298
IV. Allgemeine Beschaffenheitsvereinbarungen	314
1. Software ist nie fehlerfrei	314
2. IT-Sicherheit	315
3. Frei von Rechten Dritter	316
V. Gewährleistung	317
1. Mangelbegriff	317

2. Mängelrechte	320
VI. Service Level Agreements	321
1. Qualität der Leistung	321
2. Messung von Service Level Agreements	322
3. Sanktionen für Service Level Agreement Verletzungen	322
VII. Haftung	323
1. Begriff der Haftung	324
2. Haftungstatbestände	324
3. Haftungsbeschränkungen	325
VIII. Informations- und Datenschutz	327
1. Umgang mit vertraulichen Informationen	327
2. Umgang mit personenbezogenen Daten	327
3. Umgang mit sonstigen Informationen	327
IX. Zusammenfassung	329
X. Checkliste Vertragsgestaltung	330

Teil 4: Besonderheiten ausgewählter Branchen

A. Digitalisierung des Gesundheitswesens (eHealth)	333
I. Einführung	334
1. Nutzungsmöglichkeiten	334
2. Regulatorische Aspekte	334
3. Datenschutz	335
4. Haftungsfragen	335
II. Gesundheitswesen und Krankenkassen	336
1. Die Ziele und Regelungsbereiche des eHealth-Gesetzes	336
2. Digitale Technologien in der vertragsärztlichen Versorgung	338
3. Patientendaten	341
III. Krankenhäuser und Ärzte	342
1. Krankenhausinformationssysteme	342
2. Telemedizin	343
3. Datenschutz und Datensicherheit im Bereich der Telemedizin	345
4. Haftung im Bereich der Telemedizin	345
IV. Forschung und klinische Prüfung	346
1. Recruiting	346
2. Aufklärung und Informed Consent	347
3. Datensammlung	349
V. Gesundheitsprodukte, insb. Digitalisierung der Arzneimitteltherapie	351
1. Abgrenzungsfragen (Medizinprodukte)	352
2. Digitale Technologien zur Therapiesicherung beim Arzneimitteleinsatz	354
3. Haftungsfragen, Produkt- und Datenverantwortung	357
VI. Ausblick	359
B. Automatisiertes Fahren (Automotive)	361
I. Einführung	363
II. Begriffliche Schärfung	363
1. Nomenklatur der Bundesanstalt für Straßenwesen zur Fahrzeugautomatisierung	363
2. StVG-Änderungsgesetz	364
III. Zulassungsrechtlicher Rahmen für automatisierte Fahrzeuge	366
1. Fahrzeugzulassung und -genehmigung	366
2. EG-Typengenehmigung	366
3. (Keine) Auswirkungen des StVG-Änderungsgesetzes auf die Fahrzeugzulassung	370

IV. Haftungsrechtliche Implikationen der Fahrzeugautomatisierung entlang der Lieferkette	370
1. Haftung des Fahrzeughalters	371
2. Haftung des Fahrzeugführers	373
3. Haftung des Fahrzeugherstellers	377
V. Ausblick	383
C. Digitalisierung des Energiesektors (Smart Grids)	385
I. Die Energiewende als aktuell größtes nationales IT-Projekt	386
1. Transformation zu erneuerbaren Energien	387
2. Energieeffizienz	388
3. Digitalisierung der Energiewende	388
II. Herausforderungen und Chancen für die Energiewirtschaft	389
1. Erzeugung und Speicherung	389
2. Übertragung und Verteilung (Smart Grids)	389
3. Messwesen (Smart Metering)	390
4. Vertrieb und Marketing	390
III. Chancen und Herausforderungen für die Industrie (Verbraucher)	391
IV. Rechtlicher Rahmen	391
1. Gesetz zur Digitalisierung der Energiewende	392
2. EEG	399
3. Strommarktgesetz	400
V. Praxisbeispiele	401
1. Virtuelles Kraftwerk	402
2. Elektromobilität – Autos als Energiespeicher	402
VI. Zusammenfassung und Ausblick	403
D. Digitalisierung der Versicherungswirtschaft (Insurance)	404
I. Digitalisierung der Versicherungsbranche	404
II. Versicherungsvertrieb	406
1. Einleitung	406
2. Zulässigkeit der Versicherungsvermittlung	407
3. Zivilrechtliche Vorgaben	409
III. Versicherungsprodukte	412
1. Einleitung	412
2. Kfz-Versicherung (Telematik-Tarife)	414
3. Berufsunfähigkeits- und Lebensversicherung	415
4. Cyber-Versicherungen	417
E. Digitalisierung der Elektroindustrie (Smart Factory)	420
I. Rolle der Elektroindustrie im Rahmen der industriellen Digitalisierung	420
II. Schlüsselrolle der Normung und Standardisierung	422
III. Anwendungsbeispiele aus der Praxis	423
1. Eine exemplarische Auswahl von Szenarien	428
2. Exkurs: Anwendbares Recht und Streitbeilegungsmechanismen	434
IV. Zusammenfassung	435
F. Digitalisierung der Bankenwelt (FinTech)	437
I. Einführung	439
1. Begriffsbestimmung	439
2. Wesentliche Eigenschaften von FinTech Unternehmen	440
3. Kategorisierung des FinTech Markts	440
4. Wirtschaftliche Bedeutung und Ausblick	441
5. Verhältnis zwischen FinTech Unternehmen und traditionellen Anbietern	442
II. Europäische und deutsche Finanzaufsichtsbehörden	442
1. Europäisches System der Finanzaufsicht	443
2. Deutsches System der Finanzaufsicht	444

III. Wesentliche aufsichtsrechtliche und sonstige rechtliche Rahmenbedingungen	444
1. KWG	445
2. ZAG	452
3. Weitere relevante Vorschriften	454
4. Aktuelle rechtliche Entwicklungen	456
IV. Europäischer Pass	456
1. Europäischer Pass nach §§ 24a und 53b KWG	457
2. Europäischer Pass nach §§ 25 und 26 ZAG	457
V. Beteiligung an FinTech Unternehmen mit einer Erlaubnis nach KWG bzw. ZAG	458
VI. Das Verhältnis der BaFin zu FinTech Unternehmen	459
VII. Aufsichtsrechtliche Strategien für FinTech Unternehmen	460
1. Vorteile	460
2. Nachteile	460
VIII. FinTech Geschäftsmodelle	461
1. Alternative Bezahlverfahren	461
2. Virtuelle Währungen	463
3. Crowdfunding – Allgemein	465
4. Crowdinvesting	465
5. Crowdlending oder Peer-2-Peer Lending	469
6. Robo Advisor	472
7. Social Trading	474
IX. Aktuelle FinTech Trends	475
1. Blockchain	475
2. Smart Contracts	475
3. Internet of Things	477

Teil 5: Europäische und amerikanische Perspektiven

a. Zukünftige Regulierung des Internet of Things in Europa: Ein Überblick	479
I. Einführung	480
1. Europäische Strategie für einen digitalen Binnenmarkt	481
2. Roadmap der Maßnahmen – Rahmen für die digitale Wirtschaft	483
II. Vorbedingung für einen wachstumsorientierten digitalen Binnenmarkt	485
1. Konnektivität und Netzabdeckung	486
2. Funkspektrum	486
3. Ausschöpfung des Wachstumspotentials der digitalen Wirtschaft	488
III. Wettbewerb	488
1. Big Data	489
2. Online-Plattformen	490
IV. Vertragsschluss, Verantwortung und Haftung	492
1. Vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte	493
2. Online-Warenhandel	495
3. Urheberrechte auf dem digitalen Binnenmarkt	497
V. Standardisierung und Interoperabilität	497
1. 5G-Mobilfunknetze	498
2. Internet of Things, Machine-to-Machine und Cloud-Computing	498
3. Cybersicherheit	500
4. Fazit und Ausblick	500
VI. Vertrauen und Sicherheit	501
1. Datenschutz	501
2. Datensicherheit	502

VII. Ausblick und Zusammenfassung	502
B. Regulation and Self-Regulation of the Internet of Things in the United States	504
I. Introduction	505
II. Federal Trade Commission	505
1. Relevant Enforcement Activity	506
2. FTC Staff Reports and Public Workshops	509
III. Other US Federal Government Efforts	514
1. Federal Communications Commission	514
2. National Institute of Standards and Technology	515
3. Department of Commerce	517
4. Department of Transportation	519
5. Food and Drug Administration	519
6. Department of Homeland Security	520
7. White House	521
8. Congressional Landscape	521
IV. Self-Regulatory and Voluntary Frameworks and Guidance Materials	522
1. IoT Cybersecurity Certifications	524
2. Online Trust Alliance Internet of Things Framework	525
3. The Open Web Application Security Project	525
4. Interoperability Standards	525
V. Conclusion	526
Stichwortverzeichnis	527