

Rechtshandbuch Industrie 4.0 und Internet of Things

Praxisfragen und Perspektiven der digitalen Zukunft

Herausgegeben von

Dr. Thomas Sassenberg, LL.M.

Rechtsanwalt in Frankfurt

Dr. Tobias Faber

Rechtsanwalt in Frankfurt

Bearbeitet von den Herausgebern und

Prof. Dr. Benjamin von Böchingen, LL.M., Professor in Heilbronn sowie Rechtsanwalt in Frankfurt am Main; *Prof. Dr. Felix Buchmann*, Rechtsanwalt in Stuttgart; *Dr. Anne-Kathrin Drettmann, LL.M.*, Rechtsanwältin (Syndikusrechtsanwältin) in Hamburg; *Dr. Iris Henseler-Unger*, Geschäftsführerin in Bad Honnef; *Dr. David Jahn*, Rechtsanwalt in Frankfurt am Main; *Dr. Thomas Jochheim*, Rechtsanwalt in Frankfurt am Main; *Dr. Gerd Kiparski, MBA*, Head of Legal in Montabaur; *Christian Knß, LL.M.*, Rechtsanwalt in Köln; *Dr. Reto Mantz*, Dipl.-Inf., Richter am Landgericht Frankfurt am Main; *Jan Paul Marscholke*, Executive M.B.L.-HSG, Rechtsanwalt, Senior Legal Counsel & Compliance Officer in Frankfurt am Main; *Dr. Kerstin Neighbotr*, Rechtsanwältin in Frankfurt am Main; *Paul Otto*, Rechtsanwalt in Washington, D.C.; *David Reichwein, LL.B.*, Rechtsanwalt in Berlin; *Christian Rein*, Rechtsanwalt in Stuttgart; *Dr. Andreas Sattler, LL.M.*, Akademischer Rat a.Z., Ludwig-Maximilians-Universität in München; *Dr. Henning Schaloske*, Rechtsanwalt in Düsseldorf; *Dr. Jörg Schicken*, Rechtsanwalt in München; *Prof. Dr. Robert Schönau*, Professor in Hof; *Dr. Stefan Schuppert, LL. M.*, Rechtsanwalt in München; *Dr. Matthias M. Schweiger*, Rechtsanwalt in München; *Jatt Spittka*, Rechtsanwalt in Köln; *Dr. Martin Sura*, Rechtsanwalt in Düsseldorf; *Lukas Wagner, MSc*, Rechtsanwalt in Düsseldorf; *Philipp Weber*, Rechtsanwalt in Frankfurt am Main; *Jan-Hendrik vom Wege*, MBA, Rechtsanwalt in Hamburg; *Dr. Susanne Wende, LL.M.*, Rechtsanwältin in München; *Dr. Matthias Winter*, Rechtsanwalt in Frankfurt am Main; *Marc Wirivas*, Rechtsanwalt (Syndikusrechtsanwalt) in Espelkamp

2. Auflage 2020

C.H.BECK

Inhaltsverzeichnis

Vorwort zur zweiten Auflage	V
Inhaltsübersicht	VII
Abkürzungsverzeichnis	XIX
Autorenverzeichnis	XXV
Bearbeiterverzeichnis	XXVII

Kapitel 1 Einführung

§ 1 Auf dem Weg zur Industrie 4.0 und zum Internet of Things	1
I. Einführung	3
II. Einordnung	6
III. Ökonomische Relevanz der Industrie 4.0	10
1. Treiber und Wirkungen	10
2. Neue Wertschöpfungsketten	11
3. Branchen	13
4. Beispiel Telekommunikation	15
5. Umsetzung	17
6. Potenziale	20
IV. Politische und öffentliche Diskussion	22
V. Herausforderung Rechtsrahmen	23
VI. Ausgewählte Schwerpunkte für rechtliche Fragestellungen	25
1. Daten	25
2. Konnektivität	27
3. Standardisierung und Interoperabilität	29
4. Arbeitswelt	31
5. Rechtssicherheit	31
VII. Ausblick	32

Kapitel 2 Typische Rechtsfragen

§ 2 Schutz von maschinengenerierten Daten	35
I. Einführung	37
1. Begriffsbestimmung	39
2. Abgrenzung zum Datenschutzrecht	39
II. Schutz maschinengenerierter Daten – an den Grenzen der Gesetze	40
1. Schutz durch IP-Rechte	41
2. Schutz maschinengenerierter Daten als Geschäftsgeheimnis	50
3. Lauterkeitsrechtlicher Schutz von maschinengenerierten Daten	60
4. Kein besitzrechtlicher Schutz von maschinengenerierten Daten	62
5. Strafrechtliche und kapitalmarktrechtliche Ansätze	63
III. Maschinengenerierte Daten – Ansätze der Grenzverschiebung	65
1. Scheitern von sachenrechtlichen Begründungen	65
2. Vorschlag eines „Rechts des Datenerzeugers"/„Datenherstellerrechts“	66
IV. Vertragliche Konstruktion eines immateriellen Gutes	68
1. Kategorisierung von maschinengenerierten Daten	69
2. Vereinbarungen über Datennutzungen	70
§ 3 Forschung und Entwicklung sowie Kooperationen	76
I. Erscheinungsformen der Kooperationen	77
1. Unterscheidung nach Dimensionen	78

Inhaltsverzeichnis

2. Unterscheidung nach der Bestimmbarkeit des Teilnehmerkreises	79
II. Vertragsgestaltung	80
1. Semi-offene Innovationsprozesse	80
2. Offene Innovationsprozesse	88
III. Kartellrecht	90
IV. Rechtspolitischer Handlungsbedarf	91
§ 4 Haftungsfragen bei vernetzten und autonomen Systemen	93
I. Einführung	94
II. Vertragliche Haftung	95
III. Produkt- und Produzentenhaftung	95
1. Die deliktsrechtliche Produzentenhaftung	96
2. Produkthaftung nach dem Produkthaftungsgesetz	100
IV. Sonderprobleme der Produkt-/Produzentenhaftung im Zusammenhang mit Industrie 4.0	103
1. Neue Produktrisiken durch neue Funktionen	103
2. Produktsicherheit und IT-Sicherheit – Produktfehler bei Cyber-Angriffen?	103
3. Apps und Software	111
4. Das Nichtfunktionieren als Produktfehler	112
5. Bestimmung des Herstellers beim Einsatz innovativer Produktionstechnologien	113
6. Abgrenzung von Verantwortungsbereichen in der Produktions- und Lieferkette	114
7. Haftung für KI	115
V. Betreiber-/Benutzerhaftung	119
1. Haftung nach dem HaftPflG	119
2. Kfz-Halterhaftung	119
3. Deliktische Haftung des Benutzers	119
4. Haftungrechtliche Berücksichtigung des Einsatzes von automatisierten Systemen	120
VI. Möglichkeiten der Haftungsbeschränkung für Hersteller	120
VII. Zusammenfassung der haftungsrechtlichen Herausforderungen	121
§ 5 Anforderungen des Telekommunikationsrechts	122
I. Anwendbarkeit der Regelungen des Telekommunikationsgesetzes	125
1. Geschäftsmodelle und regulatorische Anknüpfungspunkte	125
2. Connectivity Service Provider	125
3. IoT Service Provider	131
4. IoT User	132
5. Fallbeispiele	134
6. Zwischenergebnis und Ausblick	135
II. Meldung und Aufsicht durch die Bundesnetzagentur	136
III. Kundenschutz	137
1. Vertragliche Informationspflichten und Vertragsdauer	137
2. Auswirkung der Regelungen zur sogenannten Routerfreiheit	139
3. Haftung für Vermögensschäden	139
4. Fragen der Abrechnung	140
5. Sperre von Nutzern	142
6. Neuregelung durch den europäischen Telekommunikations-Kodex ...	144
IV. Frequenzen	146
1. Hintergrund	146
2. 5G-Spektrum	147
3. Frequenzuteilung	148

4. Anzeigepflicht, Kosten und Widerruf	151
5. Zuteilungsgebiet	152
V. Nummerierung und Nummernnutzung	154
1. (Ruf-)Nummern für IoT Dienste	154
2. Adressierung von ortsfesten IoT Endgeräten	156
3. Adressierung von mobilen IoT Endgeräten	157
4. Zuteilung von Nummern durch die Bundesnetzagentur	161
5. Zuteilung von IP-Adressen *	162
6. Anbieterwechsel und Rufnummemportierung bei IoT Diensten	162
VI. Fernmeldegeheimnis und Datenschutz	166
1. DSGVO und TK-Datenschutz	166
2. Fernmeldegeheimnis bei IoT Diensten	168
3. Telekommunikationsdatenschutz	170
VII. Öffentliche Sicherheit	174
1. In der Regel keine Notrufverpflichtung bei IoT Anwendungen	174
2. eCall Verpflichtung	175
3. Schutz der Systeme und Daten bei IoT Anwendungen	177
4. Telekommunikationsbevorrechtigung für IoT User und IoT End-User	183
5. Behördenbeauskunftung und Überwachungsmaßnahmen	183
VIII. Roaming von IoT Anwendungen	191
1. Hintergrund des Roamings bei IoT Anwendungen	191
2. Anwendbarkeit der Roamingverordnung auf IoT Anwendungen	191
3. Roamingentgelte	191
IX. Netzneutralität und IoT Dienste	192
X. Ansprüche und Schlichtung	193
1. Ansprüche von Kunden, Verbraucherverbänden und Mitbewerbern ...	193
2. Schlichtung	193
XI. Übernahme der Verpflichtungen durch den Connectivity Service Provider	194
XII. Zwischenergebnis	196
§ 6 Datenschutz und IT-Sicherheit	197
I. Einführung	199
1. Datenschutz	199
2. IT-Sicherheit	199
II. Datenschutz	200
1. Systematik des Datenschutzrechts	201
2. Personenbezogene Daten	204
3. Räumlicher Anwendungsbereich datenschutzrechtlicher Regelungen	208
4. Datenschutzrechtliche Verantwortlichkeiten	211
5. Rechtmäßigkeit der Datenverarbeitung	214
6. Informationspflichten, Rechte der Betroffenen	217
7. Technische und organisatorische Datenschutzmaßnahmen	223
8. Folgen bei Datenschutzverstößen	229
III. IT-Sicherheit	236
1. Bedrohungs- und Angriffsszenarien	236
2. Ordnungsrecht	237
3. IT-Sicherheit vs. Datenschutz – Erfordernis eines Ausgleichs	246
§ 7 Kartellrechtlicher Rahmen	248
I. Einführung	249
II. Der Kartellrechtsrahmen im Überblick	252
1. Grundsatz, Verhaltenskontrolle und Fusionskontrolle	252

Inhaltsverzeichnis

2. Kartellverbot und Gruppen- oder Einzelfreistellung	253
3. Missbrauchsverbot	256
4. Fusionskontrolle	256
5. Marktdefinition als Ausgangspunkt jeder wettbewerblichen Beurteilung	258
III. Einzelfragen	259
1. Kartellrechtliche Erfassung von Plattform-Geschäftsmodellen	259
2. Marktmacht und Daten	264
3. Probleme des Kartellverbotes	267
4. Technische Standards/Normen	272
IV. Zusammenfassende Bewertung	276
§ 8 Arbeitsrecht – Realität und Herausforderungen	277
I. Einführung	280
II. Arbeitsrecht 4.0? – Realität und Anpassungsbedarf	281
1. Neue Arbeitsformen – Plattformökonomie und „Crowdworking“	281
2. Auswirkungen auf den Arbeitsort	284
3. Arbeitszeitfragen	291
4. „Entpersonalisierte Arbeitsverhältnisse“ – Ausübung von Weisungsrechten in der Industrie 4.0	295
5. Kündigungsgrund „Digitalisierung“ – Arbeitsplatzverlust infolge von Digitalisierung und Automatisierung	298
6. Betriebliche Mitbestimmung in der Industrie 4.0	301
7. Technischer Arbeitsschutz und Gesundheitsschutz in der Industrie 4.0	305
8. Arbeitnehmerdatenschutz und Mitarbeiterkontrolle	307
9. Die Arbeit des Betriebsrats in der Industrie 4.0	312
10. Arbeitskampf in der Industrie 4.0	313
§ 9 Gesellschaftsrecht	315
I. Problemstellung	315
II. Charakteristika einer Personengesellschaft und Abgrenzungsfragen	316
1. Vorliegen einer Personengesellschaft	317
2. Erscheinungsformen von Personengesellschaften	318
3. Abgrenzung von anderen Vertragstypen	322
III. Beispiele regelungsbedürftiger Inhalte vor Beginn eines Projekts	324
1. Eigentumsverhältnisse und Nutzungsrechte	325
2. Höchstpersönliche Gesellschafterstellung; Übertragbarkeit von Anteilen	325
3. Ausscheiden eines Gesellschafters	326
IV. Personengesellschaften im internationalen Kontext	326
Kapitel 3: Besonderheiten bei Vertragsschluss und -gestaltung	
§ 10 Vertragsschluss beim IoT Rechtsgeschäft	329
I. Einführung und Fallbeispiel	330
II. Allgemeine Grundzüge des Vertragsschlusses	332
1. Prinzipien	332
2. Der Softwareagent im Rechtsverkehr	338
3. Zusammenfassung	348
III. Internet of Things und Allgemeine Geschäftsbedingungen	349
1. Ausgangspunkt: Strenge des deutschen AGB-Rechts	351
2. Interessenslage für Hersteller und Betreiber von M2M-Kommunikationssystemen und Softwareagenten	357
3. Handlungsbedarf für den Gesetzgeber	358

IV. Praxistipps	358
§ 11 Besonderheiten bei Verbraucherverträgen	360
I. Die Anwendbarkeit der fernabsatzrechtlichen Regelungen	362
1. IoT als Teil der besonderen Betriebsformen, §§ 312ff. BGB	362
2. Bereichsausnahmen	363
3. Außerhalb von Geschäftsräumen geschlossener Vertrag oder Fernabsatzvertrag	366
4. Vertrag im elektronischen Geschäftsverkehr	368
II. Informationspflichten bei Verbraucherverträgen	368
1. Vorvertragliche Informationspflicht	368
2. Nachvertragliche Informationspflicht	371
3. Einzelne Informationspflichten aus Art. 246a § 1 EGBGB	372
4. Weitere Pflichten im elektronischen Geschäftsverkehr	379
III. Gestaltung von IoT-Modellen in der Praxis	382
1. Verwendete Modelle („dash button“, „amazon echo“ et al.)	382
2. Anforderungen an die Gestaltung von IoT-Geschäftsmodellen de lege lata	384
3. Zusammenfassung und Ausblick	385
§ 12 Vertragstypen und Herausforderungen der Vertragsgestaltung	387
I. Einführung	389
II. Vertragsgegenstand	391
1. Arten von Verträgen	391
2. Vertragsstruktur	391
3. Vertragstypologische Einordnung	393
III. Hauptleistungspflichten	394
1. Leistungsbeschreibung	394
2. Wesentliche Hauptleistungen	394
IV. Allgemeine Beschaffenheitsvereinbarungen	410
1. Software ist nie fehlerfrei	410
2. IT-Sicherheit	411
3. Frei von Rechten Dritter	412
4. Sollbeschaffenheit von Daten und Informationen	413
5. Indirekte Nutzung von Software	415
V. Gewährleistung	417
1. Mangelbegriff	417
2. Mängelrechte	420
VI. Service Level Agreements	421
1. Qualität der Leistung	421
2. Messung von Service Level Agreements	422
3. Sanktionen für Service Level Agreement Verletzungen	422
VII. Haftung	423
1. Begriff der Haftung	424
2. Haftungstatbestände	424
3. Haftungsbeschränkungen	425
VIII. Informations- und Datenschutz	427
1. Umgang mit vertraulichen Informationen	427
2. Umgang mit personenbezogenen Daten	427
3. Umgang mit sonstigen Informationen	427
IX. Zusammenfassung	429
X. Checkliste Vertragsgestaltung	430

Kapitel 4 Besonderheiten ausgewählter Technologien

§ 13 Künstliche Intelligenz und Machine Learning	433
I. Einführung'	434
1. Begriffsbestimmung und technischer Hintergrund	434
2. Typische rechtliche Fragestellungen	436
II. Ethische Fragen der automatisierten Entscheidungsfindung	437
1. Funktion ethischer Prinzipien	437
2. Ethische Grundprinzipien	438
3. Rechtliche Bedeutung der ethischen Prinzipien	441
III. Künstliche Intelligenz und Datenschutz	441
1. Verbot automatisierter Entscheidungen	441
2. Informationspflichten	443
3. Datenrichtigkeit und Prognoseentscheidungen	444
4. Datenschutzfolgenabschätzung	445
5. Speicherbegrenzung und Datenminimierung	446
IV. Schutz von KI-Systemen und deren Schöpfung	446
1. Patentschutz des KI-Systemen	446
2. Schutz von KI und Algorithmus als Computerprogramm	448
3. Schutz der Weights	449
5. Schutz des Analyseergebnisses	449
6. Zwischenergebnis und Ausblick	450
V. Accountability und Diskriminierungsverbot	450
1. Accountability	450
2. Diskriminierungsverbot	451
V. Vertraglicher Regelungsbedarf	452
1. Dogmatische Einordnung des Vertrags	452
2. Verantwortung für Entscheidungen	455
3. Rechte an Daten	455
VI. Zusammenfassung	457
VII. Checkliste für KI-Projekte	457
§ 14 Blockchain	459
I. Einführung	461
1. Hintergründe der Blockchain-Technologie	461
2. Bedeutung der Blockchain-Technologie	462
3. Geschichte der Blockchain	462
4. Arten und Funktionsweise einer Blockchain	463
5. Rechtliche Fragen der Blockchain-Nutzung	466
II. Urheberrechtliche Einordnung der Blockchain und Fragen des gewerblichen Rechtsschutzes	466
1. Allgemeines	466
2. Blockchain	466
3. Einzelne Elemente einer Blockchain	473
4. Client-Software	474
III. Datenschutzrechtliche Einordnung der Blockchain	475
1. Allgemeines	475
2. Vorliegen personenbezogener Daten	476
3. Datenschutzrechtliche Verantwortlichkeit innerhalb einer Blockchain	477
4. Auftragsverarbeitung innerhalb der Blockchain	480
5. Rechtmäßigkeit der Datenverarbeitung und Betroffenenrechte	481
IV. Zivilrechtliche Fragen im Zusammenhang mit der Blockchain-Technologie	483
1. Zivilrechtliche Rahmenbedingungen der Blockchain	483

2. Haftung der Nutzer der Blockchain	483
3. Ausgestaltung der Nutzungsbedingungen	486
4. Sonstige Anforderungen	487
V. Zivilprozessuale Fragestellungen	487
1. Erkenntnisverfahren	487
2. Vollstreckungsverfahren	488
VI. Smart Contracts	489
1. Allgemeines	489
2. Störungen bei der Vertragsdurchführung	490
3. Streitschlichtungsmechanismen	491
VII. Strafrechtliche Bewertung der Blockchain-Nutzung	492
1. Allgemeine Grundsätze der strafrechtlichen Verantwortlichkeit der Nutzer	492
2. Sonderfälle	493
VIII. Ausgewählte Erscheinungsformen und Einsatzgebiete	493
1. Kryptowährungen	493
2. Initial Coin Offerings	495
3. Nachverfolgbarkeit innerhalb von Lieferketten	495
4. „Blockchain Grundbuch“ und digitales Handelsregister	496
Kapitel 5 Besonderheiten ausgewählter Branchen	
§ 15 Digitalisierung des Gesundheitswesens	497
I. Einführung	498
1. Nutzungsmöglichkeiten	498
2. Regulatorische Aspekte	499
3. Datenschutz	500
4. Haftungsfragen	501
II. Gesundheitswesen und Krankenkassen	501
1. Digitalisierung in der Gesetzgebung	501
2. Digitale Technologien in der vertragsärztlichen Versorgung	505
3. Patientendaten	510
III. Krankenhäuser und Ärzte	512
1. Krankenhausinformationssysteme	512
2. Telemonitoring und Telemedizin	513
3. Datenschutz und Datensicherheit im Bereich des Telemonitoring und der Telemedizin	516
4. Haftung im Bereich der ärztlichen Nutzung digitaler Technologien ...	517
IV. Forschung und klinische Prüfung	518
1. Recruiting	519
2. Aufklärung und Informed Consent	520
3. Datensammlung	521
V. Gesundheitsprodukte, insbes. Digitalisierung der Arzneimitteltherapie	524
1. Abgrenzungsfragen (Medizinprodukte)	526
2. Digitale Technologien zur Therapiesicherung beim Arzneimitteleneinsatz	528
3. Haftungsfragen, Produkt- und Datenverantwortung	532
VI. Ausblick	536
§ 16 Automatisiertes Fahren (Automotive)	537
I. Einführung	539
II. Begriffliche Schärfung	540
1. Nomenklatur der Bundesanstalt für Straßenwesen zur Fahrzeugautomatisierung	540

Inhaltsverzeichnis

2. Achten StVG-Änderungsgesetz	541
III. Zulassungsrechtlicher Rahmen für automatisierte Fahrzeuge	542
1. Fahrzeugzulassung und -genehmigung	542
2. EG-Typengenehmigung	543
3. (Keine) Auswirkungen des Achten StVG-Änderungsgesetzes auf die Fahrzeugzulassung	546
IV. Haftungsrechtliche Implikationen der Fahrzeugautomatisierung entlang der Lieferkette	547
1. Haftung des Fahrzeughalters	547
2. Haftung des Fahrzeugflüherers	550
3. Haftung des Fahrzeugherstellers	553
V. Ausblick	560
§ 17 Digitalisierung des Energiesektors (Smart Grids)	563
I. Die Energiewende als aktuell größtes nationales IT-Projekt	564
1. Transformation zu erneuerbaren Energien	565
2. Energieeffizienz	566
3. Digitalisierung der Energiewende	567
II. Herausforderungen und Chancen für die Energiewirtschaft	568
1. Erzeugung und Speicherung	568
2. Übertragung und Verteilung (Smart Grids)	568
3. Messwesen (Smart Metering)	569
4. Vertrieb und Marketing	569
III. Chancen und Herausforderungen für die Industrie (Verbraucher)	570
IV. Rechtlicher Rahmen	571
1. Gesetz zur Digitalisierung der Energiewende	571
2. Erzeugungsanlagen EEG und KWKG	579
3. Strommarktgesetz	580
V. Praxisbeispiele	581
1. Virtuelles Kraftwerk	581
2. Elektromobilität – Autos als Energiespeicher	582
VI. Zusammenfassung und Ausblick	583
§ 18 Digitalisierung der Versicherungswirtschaft (InsurTech)	585
I. Bestandsaufnahme und Begriffsbestimmung	585
II. Neue Technologien und neue Formen von Versicherung	590
III. Versicherungsvertrieb	593
1. Einleitung	593
2. Zulässigkeit der Versicherungsvermittlung	594
3. Zivilrechtliche Vorgaben	596
IV. Versicherungsprodukte	601
1. Einleitung	601
2. Kfz-Versicherung (Telematik-Tarife)	603
3. Berufsunfähigkeits- und Lebensversicherung	605
4. Cyber-Versicherungen	607
§ 19 Digitalisierung der Elektroindustrie (Smart Factory)	611
I. Rolle der Elektroindustrie im Rahmen der industriellen Digitalisierung	611
II. Schlüsselrolle der Normung und Standardisierung	613
III. Anwendungsbeispiele aus der Praxis	615
1. Eine exemplarische Auswahl von Szenarien	620
2. Exkurs: Anwendbares Recht und Streitbeilegungsmechanismen	627
IV. Zusammenfassung	627

§ 20 Digitalisierung der Bankenwelt (FinTech)	629
I. Einführung	631
1. Begriffsbestimmung	631
2. Wesentliche Eigenschaften von FinTech Unternehmen	632
3. Kategorisierung des FinTech Markts	632
4. Wirtschaftliche Bedeutung und Ausblick	633
5. Verhältnis zwischen FinTech Unternehmen und traditionellen Anbietern	634
II. Europäische und deutsche Finanzaufsichtsbehörden	635
1. Europäisches System der Finanzaufsicht	635
2. Deutsches System der Finanzaufsicht	636
III. Wesentliche aufsichtsrechtliche und sonstige rechtliche Rahmenbedingungen	636
1. KWG	637
2. ZAG	644
3. Weitere relevante Vorschriften	647
4. Aktuelle rechtliche Entwicklungen	648
IV. Europäischer Pass	649
1. Europäischer Pass nach §§ 24a und 53b KWG	649
2. Europäischer Pass nach §§ 38 und 39 ZAG	650
V. Beteiligung an FinTech Unternehmen mit einer Erlaubnis nach KWG bzw. ZAG	650
VI. Das Verhältnis der BaFin zu FinTech Unternehmen	651
VII. Aufsichtsrechtliche Strategien für FinTech Unternehmen	653
1. Vorteile	653
2. Nachteile	653
VIII. FinTech Geschäftsmodelle	654
1. Alternative Bezahlverfahren	655
2. Virtuelle Währungen	656
3. Crowdfunding – Allgemein	658
4. Crowdfunding	659
5. Crowdlending oder Peer-2-Peer Lending	663
6. Robo Advisor	666
7. Social Trading	667
IX. Aktuelle FinTech Trends	668
1. Blockchain	668
2. Smart Contracts	669
3. Internet of Things	670
4. Künstliche Intelligenz (AI)	671
§ 21 Aviation – Unbemannte Luftfahrzeuge	672
I. Einführung	672
II. Arten und Rechtsgrundlagen für unbemannte Luftfahrzeuge	675
1. Einteilung der unbemannten Luftfahrzeuge nach technischen Kriterien	675
2. Europäischer und deutscher Rechtsrahmen	678
III. Rechtsfragen im Umgang mit unbemannten Luftfahrzeugen	684
1. Herstellung von unbemannten Luftfahrzeugen	684
2. Betrieb von unbemannten Luftfahrzeugen	687
3. Kennzeichnungspflicht der unbemannten Luftfahrzeugsysteme und Registrierungspflicht der Betreiber	698
4. Infrastruktur für unbemannte Luftfahrzeuge	699
5. Finanzierung von unbemannten Luftfahrzeugen	702

Inhaltsverzeichnis

IV. Internationaler Vergleich der Drohnenregulierung	704
V. Ausblick in die Zukunft	707
Kapitel 6 Europäische und amerikanische Perspektiven	
§ 22 Zukünftige Regulierung des Internet of Things in Europa: Ein Überblick	715
I. Einführung	717
1. Europäische Strategie für einen digitalen Binnenmarkt	718
2. Roadmap der Maßnahmen – Rahmen für die digitale Wirtschaft	721
II. Verbesserung des Zugangs zu digitalen Gütern und Dienstleistungen für Verbraucher und Unternehmen	723
1. Vertragsschluss, Verantwortung und Haftung	725
2. Verbraucherschutz	730
3. Urheberrechte im digitalen Binnenmarkt	731
4. Modernisierung der Mehrwertsteuer für den grenzüberschreitenden elektronischen Handel	735
III. Schaffung optimaler Rahmenbedingungen für die Entwicklung digitaler Netze und Dienste	735
1. Konnektivität und Netzabdeckung	738
2. Funkspektrum	738
3. Optimale Rahmenbedingungen für die Entwicklung digitaler Netze und Dienste in Europa	741
4. Wettbewerb	741
IV. Bestmögliche Ausschöpfung des Wachstumspotentials der digitalen Wirtschaft	746
1. Standardisierung und Interoperabilität	748
2. Vertrauen und Sicherheit	751
V. Ausblick und Zusammenfassung	754
§ 23 Regulation and Self-Regulation of the Internet of Things in the United States	756
I. Introduction	757
II. Federal Trade Commission	757
1. Relevant Enforcement Activity	758
2. FTC Staff Reports and Public Workshops	762
III. Other US Federal Government Efforts	766
1. Federal Communications Commission	766
2. National Institute of Standards and Technology	767
3. Department of Commerce	769
4. Department of Transportation	771
5. Food and Drug Administration	771
6. Department of Homeland Security	772
7. White House	773
8. Congressional Landscape	773
IV. Self-Regulatory and Voluntary Frameworks and Guidance Materials	775
1. IoT Cybersecurity Certifications	776
2. Online Trust Alliance Internet of Things Framework	777
3. The Open Web Application Security Project	777
4. Interoperability Standards	778
V. Conclusion	778
Stichwortverzeichnis	780