

Internet of Things

Bräutigam / Kraul

2021

ISBN 978-3-406-74898-1

C.H.BECK

Internet of Things

Rechtshandbuch

Herausgegeben von

Prof. Dr. Peter Bräutigam

München

Dr. Torsten Kraul LL.M.

Berlin

Bearbeitet von den Herausgebern und

*Stefan Bauer LL.M., München; Dr. Alexander Birnstiel LL.M., München;
Prof. Dr. Dr. Walter Blocher, Kassel; Thomas Böhne, München; Dr. David Bomhard, München;
Dr. Steffen Burrer, München; Dr. Michael Denga LL.M., Berlin; Sebastian Dienst, München;
Prof. Dr. Christian Djefal, München; Andreas Egger, Augsburg; Dr. Wolfgang Feiel, Wien;
Dr. Korbinian Feller, München; Dr. Martin Geipel, Berlin; Janik Gößler LL.M., Frankfurt a. M.;
Dr. Korbinian Hartl, München; Prof. Dr. Dirk Heckmann, München; Martin Hedrich, Frankfurt
a. M.; Dr. Thomas Josef Heitzer, Düsseldorf; Prof. Dr. Dr. Kai-Michael Hings, Hamburg;
Prof. Dr. Ing. Dipl.-Inform. Joachim Hohmann, Kaiserslautern; Ingo Hüttemeyer, Düsseldorf;
Prof. Dr. Johannes Kreile, München; Tobias Kugler, Frankfurt a. M.; Christian Alexander Mayer,
München; Dr. Ralph Nack, München; Dr. Anne Paschke, Berlin; Dr. Mansur Pour Rafsendjani,
München; Dr. Louis Püschel, Bayreuth; Dr. Michael Reiling, München; Dr. Thomas Roth,
Frankfurt a. M.; Prof. Dr. Maximilian Röglinger, Bayreuth; Dr. Daniel Rücker LL.M., München;
Dr. Bärbel Sachs LL.M., Berlin; Prof. Dr. Joachim Schrey, Frankfurt a. M.; Dr. Nico Schur, Düsseldorf;
Dr. Klaus M. Steinmaurer MBA, Wien; Dr. Thomas Thalhofer, München; Olaf Vogel, Bonn;
Dr. Nikolai Warneke, Frankfurt a. M.; Prof. Dr. Andreas Wiebe LL.M., Göttingen*

2021




beck-shop.de
DIE FACHBUCHHANDLUNG

www.beck.de

ISBN 978 3 406 74898 1

© 2021 Verlag C.H. Beck oHG

Wilhelmstraße 9, 80801 München

Druck und Bindung: Westermann Druck Zwickau GmbH
Crimmitschauer Straße 43, 08058 Zwickau

Satz: 3w+p GmbH, Rimpar

Umschlaggestaltung: Druckerei C.H. Beck, Nördlingen



chbeck.de/nachhaltig

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Vorwort

„... When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole“

Nicola Tesla, 30. 1. 1926

Die vor fast 100 Jahren formulierte Vision von Nicola Tesla (zum Zitat → § 3 Rn. 24) wird mit dem Internet of Things zur Realität. Und das Potenzial ist enorm – geht es doch nicht mehr nur um die Vernetzung der Computer (Internet der Computer), die von voluminösen Mainframes zu kleinen Personal Computer und weiter zu noch viel kleineren/handlichen Smartphones schrumpften, sondern um die Vernetzung der Dinge (Internet der Dinge), und zwar nicht nur physischer, sondern auch virtueller Dinge.

Ermöglichte der Buchdruck überhaupt erst den Austausch menschengenerierter Information, der durch das Internet auf Echtzeit („any time“ und „any place“) beschleunigt wurde, so revolutioniert und erweitert das Internet of Things diesen Austausch auf maschinengenerierte Daten („anything“). Das Internet ist damit überall.

Damit geht ein enormes ökonomisches Potenzial einher. Zum stationären Handel, dem E- und M-Commerce, kommt nun der „IoT-Commerce“, bei dem es nicht mehr der Mensch ist, der seinen Bedarf erkennt und durch Bestellung befriedigt, sondern direkt das autonom agierende smarte Gerät. Dies geschieht sowohl im industriellen, also im Unternehmenskontext („Industrial IoT“, Industrie 4.0), als auch im Verhältnis zum Verbraucher („Consumer IoT“).

Die Konzeption des vorliegenden Handbuchs folgt geübter juristischer Herangehensweise. So wird denn auch zunächst der Sachverhalt aufgearbeitet, bevor eine rechtliche Einordnung und Beurteilung unternommen wird. Dem folgend beschäftigt sich der 1. Teil des Handbuchs mit den Grundlagen des Internet of Things, also der Definition, den ökonomischen Erwartungen und den grundlegenden Fragestellungen. Ganz im Mittelpunkt steht dabei das smarte Gerät, also das IoT-Device, das mit seinen Sensoren, Aktoren und der eingebetteten Datenverarbeitung die Fähigkeit zur Interaktion und zur Erbringung digitaler Services besitzt. Im 2. Teil werden die technischen Strukturen, vor allem die Kommunikations- und die IT-Infrastruktur (5G-Standard, Schmalband, Cloud Computing, Edge Computing, Plattform und Applications) beleuchtet. Der 3. und 4. Teil sind dann der juristischen Aufarbeitung des Internet of Things und seiner Merkmale gewidmet. Diese erfolgt gleichermaßen im Lichte des nationalen und des EU-Rechts. Gerade dem EU-Recht kommt besondere Bedeutung zu, prägt es doch unmittelbar oder mittelbar den rechtlichen Rahmen vieler Aspekte des Internet of Things. Bei näherer Beschäftigung mit der Materie kristallisiert sich heraus, dass zwischen allgemeinen rechtlichen Themen, die bei allen IoT-Systemen relevant sein können, und speziellen sektor- und branchenspezifischen Fragestellungen unterschieden werden kann. Deshalb bildet der 3. Teil – wenn man so will – den allgemeinen Teil der juristischen Subsumtion und setzt sich mit den grundlegenden rechtlichen Fragestellungen wie dem Daten(schutz)recht, der Vertragsgestaltung, der Haftung, dem IT-Sicherheits-, Vertriebs-, Patent- und Kartellrecht sowie dem Telekommunikations- und Exportkontrollrecht auseinander. Darüber hinaus werden in diesem Teil mit den Themen Künstliche Intelligenz und Blockchain wichtige Bestandteile des IoT rechtlich betrachtet.

Im 4. Teil werden schließlich ausgewählte Rechtsprobleme wichtiger Sektoren/Branchen angerissen; behandelt werden die Automobilwirtschaft (Connected Cars), die Landwirtschaft (Smart Farming, Farm Management), die Energiewirtschaft (Smart Home, Smart Metering), Immobilien- und Gesundheitswirtschaft, Banken und Versicherungen, der Maschinenbau (Smart Factory), der Handel, der Verkehr (Ridepooling, Ridesharing) die Medien, die Telekommunikation und die öffentliche Verwaltung (Smart Country, Smart Cities). Weder bei den behandelten Sektoren noch bei den Fragestellungen innerhalb der einzelnen Sektorenkapitel erhebt das Handbuch Anspruch auf Vollständigkeit.

Vorwort

Das wäre bei dieser Materie, die sich mit großer Rasananz weiter entwickelt, auch unmöglich.

Das Werk konnte nur durch eine wunderbare Teamarbeit entstehen. Daher gilt es Dank zu sagen. Zunächst bedanken wir uns bei all unseren 40 Mitautoren sowie den Verantwortlichen beim C.H.Beck Verlag. Dank gilt dabei Herrn Dr. Wasmuth, mit dem auf dem Fest zum 85. Geburtstag des Verlegers Dr. Beck die Idee zu diesem Buch geboren wurde. Bedanken möchten wir uns weiter bei Frau Schrödl für die umsichtige Übernahme des Lektorats. Dank gilt auch den Mitgliedern des Smart Centers von Noerr sowie Frau Gümpelein und Frau Weber für die Betreuung und das Korrekturlesen der Manuskripte. Schließlich sagen wir unseren Familien und Freunden Dank für ihr Verständnis und ihren Langmut.

München/Berlin März 2021

*Peter Bräutigam
Torsten Kraul*



beck-shop.de
DIE FACHBUCHHANDLUNG

Bearbeiterverzeichnis

Stefan Bauer LL.M., Rechtsanwalt, München	§ 14
Dr. Alexander Birnstiel LL.M., Rechtsanwalt, München	§ 14
Prof. Dr. Dr. Walter Blocher, Universität Kassel	§ 12
Thomas Böhne, Rechtsanwalt, München	§ 22
Dr. David Bomhard, Rechtsanwalt, München	§ 23
Prof. Dr. Peter Bräutigam, Rechtsanwalt München	§ 1
Dr. Steffen Burrer, Rechtsanwalt, München	§ 8
Dr. Michael Denga LL.M. (London), Maître en Droit (Paris), Humboldt-Universität Berlin	§ 11
Sebastian Dienst, Rechtsanwalt, München	§ 6 Rn. 112–365
Prof. Dr. Christian Djeffal, Technische Universität München	§ 25
Andreas Egger, Universität Augsburg	§ 2
Dr. Wolfgang Feiel, Leiter Recht und Kommunikation Wien	§ 15 Rn. 1–136
Dr. Korbinian Feller, Rechtsanwalt, München	§ 22
Dr. Martin Geipel, Rechtsanwalt, Berlin	§ 18
Janik Goßler LL.M., Rechtsanwalt, Frankfurt a. M.	§ 16
Dr. Korbinian Hartl, Rechtsanwalt, München	§§ 5, 7 Rn. 430–599
Prof. Dr. Dirk Heckmann, Technische Universität München	§ 10
Martin Hedrich, Rechtsanwalt, Frankfurt a. M.	§ 26
Dr. Thomas Josef Heitzer, Rechtsanwalt, Düsseldorf	§ 28
Prof. Dr. Dr. Kai-Michael Hingst, Rechtsanwalt, Hamburg	§ 17
Prof. Dr. Ing. Dipl.-Inform. Joachim Hohmann, Technische Universität Kaiserslautern	§ 21
Ingo Hüttemeyer, Leiter Digital Excellence/IoT, Düsseldorf	§ 21
Dr. Torsten Kraul LL.M., Rechtsanwalt, Berlin	§ 4
Prof. Dr. Johannes Kreile, Rechtsanwalt, München	§ 24
Tobias Kugler, Rechtsanwalt, Frankfurt a. M.	§ 7 Rn. 127–429
Christian Alexander Mayer, Rechtsanwalt, München	§ 27
Dr. Ralph Nack, Rechtsanwalt, München	§ 13
Dr. Anne Paschke, Berlin	§ 10
Dr. Mansur Pour Rafsendjani, Rechtsanwalt, München	§ 20
Dr. Louis Püschel, Universität Bayreuth	§ 2
Dr. Michael Reiling, Rechtsanwalt, München	§ 9
Prof. Dr. Maximilian Röglinger, Universität Bayreuth	§ 2
Dr. Thomas Roth, Rechtsanwalt, Frankfurt a. M.	§ 19
Dr. Daniel Rücker LL.M., Rechtsanwalt, München	§ 6 Rn. 112–365
Dr. Bärbel Sachs LL.M., Rechtsanwältin, Berlin	§ 15 Rn. 137–223
Prof. Dr. Joachim Schrey, Rechtsanwalt, Frankfurt a. M.	§ 7 Rn. 127–429
Dr. Nico Schur, Düsseldorf	§ 6 Rn. 1–111

Dr. Klaus M. Steinmaurer MBA, Geschäftsführer Fachbereich Telekom und Post Rundfunk und Telekomregulierungs GmbH, Wien	§ 3
Dr. Thomas Thalhofer, Rechtsanwalt, München	§ 7 Rn. 1–126
Olaf Vogel MLE, MBA, Rechtsanwalt, Frankfurt a. M.	§ 26
Dr. Nikolai Warneke, Rechtsanwalt, Frankfurt a. M.	§ 17
Prof. Dr. Andreas Wiebe LL.M., Universität Göttingen	§ 6 Rn. 1–111

The logo for beck-shop.de features the text 'beck-shop.de' in a bold, lowercase, sans-serif font. Above the 'i' in 'shop' are three red circles of varying sizes, arranged in a slight arc. Below the main text, the words 'DIE FACHBUCHHANDLUNG' are written in a smaller, uppercase, sans-serif font.

beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsverzeichnis

Vorwort	I
Bearbeiterverzeichnis	VII
Abkürzungsverzeichnis	XXI

1. Teil. Grundlagen

§ 1 IoT – Definition und Fragestellungen

I. Vom Internet der Personal Computer zum Internet der Dinge	2
II. Begriffsdefinition und Merkmale des Internets der Dinge	4
1. Smart Objects/smarteres Gerät/IoT-Device	5
2. Vernetzung	7
3. Das Internet der Dinge als technisches Funktionsbündel	12
4. Das Internet der Dinge aus wirtschaftlicher Perspektive	13
5. Die dynamische Semantik des Begriffs des Internets der Dinge	15
III. Ungeklärte Rechtsfragen im Zusammenhang mit dem Internet der Dinge	16
1. Das „Recht des Internets der Dinge“ als Querschnittsmaterie	16
2. Besondere rechtliche Herausforderungen	17

§ 2 Ausgangslage und ökonomische Erwartungen an das Internet der Dinge

I. Einleitung	26
II. Das smarte Gerät als Grundbaustein des Internets der Dinge	27
1. Der grundlegende Aufbau von smarten Geräten	27
2. Kurze Einordnung in bestehende smarte Geräte-Architekturen	28
3. Eine Taxonomie für smarte Geräte	28
4. Typische Gruppen von am Markt existierenden smarten Geräten	36
5. Innovative Interaktionsmuster ermöglicht durch das IoT	38
III. Vom smarten Gerät zum smarten Ökosystem	42
1. Smarte Ökosysteme und deren Komponenten	42
2. Design-Prinzipien für smarte Ökosysteme	51
IV. Das ökonomische Potenzial des Internets der Dinge	57
1. Das IoT und dessen Potenzial im Konsumentenbereich	57
2. Das IoT und dessen Potenzial im industriellen Kontext	58
3. Das IoT und dessen unternehmensübergreifendes Potenzial – B2B- und B2C-Bereich	61
V. Zusammenfassung und Einordnung der wesentlichen Erkenntnisse	66

2. Teil. Strukturen

§ 3 Kommunikationsnetze und Devices

I. Kommunikationsnetze/Infrastruktur/Devices	70
1. Einleitung	70
2. Definition IoT aus der Infrastrukturperspektive	74
3. IoT – technische und ökonomische Rahmenbedingungen	76
4. IoT-Anwendungsfelder im Überblick	80
II. Netzwerke und Konnektivität	81
1. IoT-Netzwerktechnologie	81
2. IoT-Netzwerkarchitektur	82
3. Narrowband (NB)-IoT	84

4. 5G – eine Netzwerktechnologie für das „Allesnetz“	85
5. Die Möglichkeiten von 5G für das Internet of Things	87
6. Smart Cell-Technologie und ihre Bedeutung für IoT	89
III. Herausforderungen für IoT-Services in öffentlichen Netzwerken	92
1. Spektrum	92
2. Adressierung und Identifikation	96
3. Roamingbeschränkungen	98
4. Interoperabilität von Netzen und Devices und Dienstportabilität	100
5. Netzneutralität	104
6. Netzsicherheit	105
IV. Exkurs: IoT-Device	109
1. Definition	109
2. Anwendungsbereiche	110
3. Nutzen und Risiko von IoT-Devices	112
4. Datenschutz – ein zentrales Thema für IoT-Devices	114
V. Schlussbemerkungen	115

§ 4 IT-Infrastruktur

I. Übersicht	118
1. Einführung	118
2. Cloud Computing	119
3. Edge Computing	120
II. Schichten der IT-Infrastruktur	121
1. Infrastruktur	121
2. Plattform	124
3. Anwendungen/SaaS-Schicht	137
4. User-Interfaces	143

§ 5 Ökosysteme

I. Der Begriff „Ökosystem“	146
II. Bedeutung und Ausblick	146
III. Vorteile aus Sicht der Endnutzer und Bedeutung von Apps	148
IV. „App-Ökosysteme“ – Die verschiedenen Akteure	148
1. Übersicht der beteiligten Akteure	149
2. Branchenspezifische Ausgestaltungsoptionen	149
3. Das Verhältnis von App-Entwickler und App-Anbieter	150
4. Der (App-)Plattformbetreiber	151

3. Teil. Besondere rechtliche Fragestellungen

§ 6 Daten

I. Rechte an Daten	158
1. Input und Ergebnisse	159
2. Daten-Auswertungsverträge	175
II. Datenschutz	192
1. Anwendbares Datenschutzrecht im IoT	192
2. Adressaten des Datenschutzrechts im IoT	206
3. Datenschutzkonforme Datenverarbeitung im IoT	209
4. Sicherstellung der Betroffenenrechte im IoT	224
5. Handhabung von Datenschutzverletzungen im IoT	232
6. Folgen bei Verstößen gegen Datenschutzrecht	236

§ 7 Vertragsgestaltung

I. Verträge mit Cloud Providern	242
1. Cloud Computing als Fundament des Internet of Things – Einleitung	242
2. Allgemeine Hinweise zur Gestaltung von Cloud-Computing-Verträgen	244
3. Anwendbares Recht	246
4. Vertragstypologie	247
5. Vertragsaufbau	248
6. Multi-Vendor-Szenarien	279
7. Probleme bei der Verbreitung von IoT	280
II. Kundenverträge (B2B und B2C)	281
1. IoT-Plattformverträge	281
2. Zurechnung der maschinell erzeugten Willenserklärung zu einer natürlichen Person	307
3. Abgabe und Zugang einer maschinell erzeugten Willenserklärung und Vertragsschluss	317
4. Vernichtung einer maschinell erzeugten Willenserklärung durch Anfechtung und deren Rechtsfolgen	321
5. Vertragliche Regelungen beim Einsatz autonomer Systeme	324
III. App-Plattform-Verträge	331
1. Terminologie und Übersicht der verschiedenen Akteure	331
2. App-Entwicklerverträge	331
3. Der Vertrag zwischen App-Anbieter und Plattformbetreiber	338
4. Der Vertrag zwischen Endkunde und Plattformbetreiber	365
5. App-Überlassungsverträge	366

§ 8 Haftung

I. Grundlagen: Verantwortlichkeiten im IoT	370
1. Das IoT als „digitales Ökosystem“ mit Verantwortlichkeiten der Systemteilnehmer	372
2. Verantwortlichkeiten als Vertragspartner	373
3. Verantwortlichkeiten als Hersteller eines IoT-fähigen Produkts bzw. von IoT-Software	373
4. Verantwortlichkeit des Diensteanbieters	374
5. Verantwortlichkeiten als Betreiber/Nutzer von IoT-Produkten und -Systemen	374
II. Vertragliche Haftung im IoT	374
1. Arten von IoT-Nutzungsverträgen	376
2. Mängelhaftung	380
3. Vertragliche Sekundärrechte	383
4. Entwurf der Richtlinie über bestimmte vertragliche Aspekte der Bereitstellung digitaler Inhalte – voraussichtliche Auswirkungen auf die geltende Rechtslage	385
III. Produkt- und Produzentenhaftung	389
1. Grundlagen und Entwicklungen	389
2. Deliktsrechtliche Produzentenhaftung – Flexibilität und Grenzen richterlicher Rechtsfortbildung	395
3. Produkthaftung nach dem Produkthaftungsgesetz	403
4. Resilienz vor Angriffen von außen als Frage der Produktsicherheit	405
IV. Betreiber-/Benutzerhaftung	407
1. Haftpflichtgesetz – intelligente Fabrik	407
2. Kfz-Halterhaftung	407
3. Arbeitsschutz	409
4. Deliktische Haftung des Betreibers/Benutzers	409

V. Plattformprivileg für Cloud-Computing-Plattformen?	410
1. Was steckt hinter dem sog. Plattformprivileg?	410
2. Voraussetzungen für ein Plattformprivileg für Cloud-Computing-Plattformen	411
VI. Haftungsdurchsetzung – prozessuale Fragen	412
1. Beweislast und beweisrechtliche Probleme	412
2. Substantiierung des Vortrags	413
3. Prozessuale Auskunftsrechte	414
4. Beweiswert von Datenpaketen	414
5. Auswertung der Daten durch das Gericht und Mitwirkungspflichten des Herstellers	415
6. Geheimnisschutz und Zeugnisverweigerungsrechte	415
7. Probleme mit nationalen Prozessregelungen angesichts internationaler Vernetzung	417
VII. Rechtspolitischer Ausblick	417

§ 9 Vertrieb

I. Einführung	421
1. Vertikale Vorwärtsintegration und Herstellerabhängigkeit	421
2. Herausforderungen im Vertriebskartellrecht	423
II. Vertriebsmittler von IoT-Produkten	424
1. Vorbemerkung	424
2. Der Handelsvertreter	425
3. Der Vertragshändler	437
4. Der Kommissionsagent	446
III. Vertriebskartellrecht	449
1. Kartellverbot	449
2. Spürbarkeit des Wettbewerbsverstoßes	449
3. Ausnahmen vom Kartellverbot	450
4. Freistellung	453

§ 10 IT-Sicherheit

I. Begriff, Funktionen und Ziele der Gewährleistung von IT-Sicherheit	459
1. IT-Sicherheit als Rechtsbegriff	459
2. Funktionen von IT-Sicherheit im rechtlichen Kontext	460
3. IT-Sicherheitsziele im Kontext des Internet of Things	461
II. Gefährdungspotenzial von und durch IoT-Systeme(n)	464
1. Gefährdungen von IoT-Systemen	464
2. Gefährdungen durch IoT-Systeme	467
III. IT-Sicherheitsregulierung	470
1. De lege lata	470
2. De lege ferenda	476
IV. Maßnahmen zur IT-Sicherheitsgewährleistung im Internet of Things	478
1. Staatliche Maßnahmen	478
2. Maßnahmen der Wirtschaft	481
V. Eckpunkte eines IT-Unsicherheitsfolgenrechts	484
1. IT-Unsicherheit als Normalzustand	484
2. Staatliche Schutzpflichten zur IT-Sicherheitsgewährleistung	485
3. „IoT“-Sicherheit als Aufgabe des BSI	486
4. IT-Unsicherheit und Haftungsrecht	487
5. Versicherbarkeit von IT-Risiken	488
6. Katastrophenschutzrecht	488

§ 11 Künstliche Intelligenz

I. Grundlagen und Grundsätze der KI	492
1. Technische Grundlagen der KI	493
2. Rechtliche Leitmotive zur KI	496
II. Vertragsschluss – insbesondere automatisierte Verträge	499
1. Transaktionen im IoT unter Mitwirkung von KI	499
2. Besondere Rechtsprobleme	500
III. Haftung für autonom handelnde Gegenstände	505
1. Haftungsrelevanz der KI im IoT	505
2. Vertragliche Haftung der Anbieter von KI	505
3. Deliktshaftung von Hersteller und Zulieferer	508
4. Beweislast	513
5. Zusammenfassung	514
IV. Entstehung von Rechten geistigen Eigentums bei Einsatz von KI	514
1. Anwendungsfälle von Computerschöpfungen	514
2. KI-relevante Grundprinzipien geistigen Eigentums	515
3. Schutz für KI-Funktionen und KI-Schöpfungen	517

§ 12 Blockchain-Lösungen

I. Ein künftiges IoT-Szenario (Durchlässigkeit von Unternehmensgrenzen auf der Grundlage digitaler Zwillinge)	523
II. Blockchain als „Rückgrat“ für das Internet der Dinge	524
1. Von der Tontafel zur Blockchain	524
2. Das Internet der Dinge beflügelnde Eigenschaften von Blockchains	526
3. Technische Grundlagen und Funktionsweise am Beispiel der Bitcoin-Blockchain	527
4. Arten von Blockchains und Einsatzbereiche	536
5. Bedarf an Vertrauen trotz „trustless trust“	539
6. Das Internet der Dinge hemmende Eigenschaften von Blockchains	540
III. Für das Internet der Dinge optimierte Ausprägungen der Distributed Ledger Technology	541
1. Leichtgewichtige Blockchains	541
2. Gerichtete azyklische Graphen (IOTA)	541
IV. Smart Contracts	543
1. Grundlegende Ideen	543
2. Ethereum	544
3. Hyperledger, Corda und Co.	547
4. Abbildung von Treuhandschaft durch Atomic Swaps und Smart Contracts	548
5. Bedeutung und Problematik von „Oracles“	549
6. Problematik der Entscheidung auf der Grundlage qualitativer Eigenschaften oder lückenhafter Vereinbarungen	550
7. Umgang mit fehlerhaften Smart Contracts	551
8. Durchsetzung ohne staatliche Zwangsgewalt	551
9. Autonome M2M-Transaktionen (Austausch von Daten, Geld und anderen Assets zwischen Dingen)	553
V. Ausgewählte Anwendungsbeispiele	554
1. Dezentrale Energieversorgung	554
2. Container-Logistik	556
3. Smart Locks	556
VI. Fazit und Ausblick	557

§ 13 Patentrecht

I. Patentlandschaft im Bereich Internet der Dinge	560
1. Überblick: Standardessenzielle Patente (SEPs) und nicht SEPs	560
2. Technische Standards und SEPs im Bereich Datenübertragung und Datenverarbeitung	560
3. Nicht standardessenzielle Patente	564
4. Patentinhaber	564
II. Patentrisiken des Herstellers und Betreibers von IoT-Komponenten und Anwendungen	565
1. Überblick	565
2. Einzelheiten zum Unterlassungsanspruch	566
3. Einzelheiten zum Vernichtungsanspruch	567
4. Einzelheiten zum Auskunfts- und Schadensersatzanspruch	567
5. Einzelheiten zu SEPs und FRAND-Lizenzen	569
6. Verschärfung der Risiken durch die Trennung zwischen Verletzungs- und Nichtigkeitsverfahren	581
7. Ausblick: Das Einheitliche Patentgericht	583
III. Strategische Reaktionsmöglichkeiten auf die Patentrisiken	585
1. FTO-Analyse als Voraussetzung sämtlicher Strategien	585
2. Offensive Strategien	586
3. Defensive Strategien	586
4. Flankierende Maßnahmen	587
IV. Zusammenfassung	587

§ 14 Kartellrecht

I. Einführung	590
1. Digitale Märkte – neue Herausforderungen für das Kartellrecht	590
2. Kartellrecht und das Internet of Things	591
II. Marktdefinition und Marktmacht – Besonderheiten bei digitalen Märkten – erste Überlegungen	593
1. Herkömmliche Betrachtung	593
2. Aktualisierungen der Marktdefinition erforderlich?	594
III. Das Kartellverbot (Art. 101 AEUV, § 1 GWB)	596
1. Wesentlicher Inhalt des Kartellverbots	596
2. Gruppenfreistellungen und Einzelfreistellung	597
3. Besonderheiten bei der Anwendung des Kartellverbots im IoT-Kontext ...	598
IV. Das Missbrauchsverbot (Art. 102 AEUV, §§ 19ff. GWB)	614
1. Marktbeherrschende Stellung	614
2. Missbrauch der marktbeherrschenden Stellung	615
3. Marktstarke Unternehmen (§ 20 GWB)	617
4. Besonderheiten bei der Anwendung des Missbrauchsverbots im IoT-Kontext	617
V. Folgen von Kartellrechtsverstößen	647
1. Bußgelder	648
2. Zivilrechtliche Folgen	648
VI. Anwendbarkeit	648
VII. Fusionskontrolle	649
1. Formelle Fusionskontrolle	649
2. Materielle Fusionskontrolle	651

§ 15 Besondere Regulierungsfragen

I. Telekommunikationsrecht	655
1. IoT aus rechtlicher Sicht	655

2. Kein europäisches IoT-Gesetzbuch	656
3. IoT im Telekommunikationsrecht	658
4. M2M als elektronischer Kommunikationsdienst	660
5. Betreiben von IoT-Übertragungsdiensten: Allgemeingenehmigung	664
6. Konnektivität für IoT-Anwendungen	667
7. Aspekte der Nummerierung bei IoT-Anwendungen	672
8. Sicherheit von Netzen und Diensten	674
9. Spezifischer Datenschutz	676
10. Roaming und IoT	680
11. Netzneutralität und IoT	681
12. IoT-bezogene Aspekte im spezifischen Verbraucherschutz	684
13. Zusammenfassung und Ausblick	686
II. Handelsbeschränkungen/Exportkontrolle	688
1. Bedeutung der Exportkontrolle für IoT	688
2. Vorgaben des deutschen und europäischen Exportkontrollrechts an IoT-Anwendungen	689
3. Relevante Listen	691
4. Erfasste Software	692
5. Erfasste Technologie	695
6. Erfasste Transfervorgänge	697
7. Sonderfall: Cloud Computing	698
8. Ausführer	700
9. Genehmigungen	700
10. Exkurs: Das US-Reexportkontrollrecht	701
11. Ausblick: Umgang mit exportkontrollrechtlichen Vorgaben in der Praxis	702
4. Teil. Sektorspezifische Anwendungsbereiche	
§ 16 Automobilwirtschaft	
I. Überblick	704
II. Autonomes Fahren/Connected Cars	704
1. Änderung des StVG – Rahmenbedingungen der Zulassung autonomer Fahrzeuge	706
2. Zukünftige Rechtsfragen des autonomen Fahrens	712
3. Datenerfassung und -übertragung durch Fahrzeuge (Connected Cars)	719
III. Produktion und Regress	722
1. Prozessuale Ausgangslage	722
2. Klassische Aufgabenteilung zwischen Hersteller und Zulieferer	723
3. Neue Kooperationsformen in der Automobilindustrie	724
4. Änderungen aufgrund fortschreitender Digitalisierung	725
IV. Internationale Bezüge	725
1. USA	725
2. Großbritannien	726
3. Weitere Länder	727
§ 17 Banken und Finanzinstitute	
I. Überblick	728
II. Anwendungen des IoT im Bank- und Finanzsektor (Use Cases)	730
1. Optimierung des klassischen Kreditgeschäftes von Banken und Finanzinstituten durch IoT	730
2. Machine-to-machine-Payments	733
3. Weitere Anwendungsfälle für IoT im Bank- und Finanzsektor	735

III. Besondere rechtliche Rahmenbedingungen für IoT im Bank- und Finanzsektor	736
1. IoT und Finanzierungen	736
2. IoT und Aufsichtsrecht	743
IV. Internationale Bezüge	748
1. Harmonisierung des Kreditsicherungsrechts und Außenhandelsfinanzierung	748
2. EU-Pass für erlaubnispflichtige IoT-Anwendungen	749

§ 18 Energie

I. Überblick	750
II. Branchenbeschreibung: Energiewirtschaft	751
III. Ausgewählte Use Cases im Energiebereich	752
1. Smart Home	752
2. Smart Metering	759
IV. Internationale Bezüge	766

§ 19 Gesundheitswirtschaft

I. Die praktische Bedeutung des Internets der Dinge in der Gesundheitswirtschaft im Überblick	768
1. Verbesserung der stationären und ambulanten Gesundheitsversorgung	769
2. Prävention durch das Internet der Dinge	770
3. Verbesserung der Lebensqualität durch das Internet der Dinge	770
4. Optimierung von nicht-medizinischen Prozessen im Gesundheitswesen	771
5. Neue Krankenversicherungstarife durch das Internet der Dinge?	771
II. Beispiele für Anwendungen des Internets der Dinge in der Gesundheitswirtschaft	772
1. Telemedizinische Methoden in der Diagnostik, Gesundheitsversorgung und Rehabilitation	772
2. Die Eroberung des Gesundheitsmarktes durch Technologie-Konzerne wie Apple und Alphabet	773
III. Besondere rechtliche Rahmenbedingungen des Internets der Dinge in der Gesundheitswirtschaft	774
1. Bedeutung des Arzneimittelrechts und Medizinproduktrechts	774
2. Internet der Dinge in der Gesundheitswirtschaft und gesetzliche Krankenversicherung	776
3. Datenschutzrecht auf der Grundlage der DS-GVO	777
4. Mögliche Auswirkungen der zukünftigen Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-VO)	788
5. Gesetze über die Sicherheit in der Informationstechnik	790
6. Besonderheiten des Vertragsrechts und Haftungsrechts im Internet der Dinge in der Gesundheitswirtschaft	791
IV. Internationale Bezüge des Internets der Dinge in der Gesundheitswirtschaft	792

§ 20 IoT im Handel

I. Überblick	796
1. Begriff des Handels	796
2. Einsatz von Smart Devices im Handelssektor	797
3. Verkauf und Erwerb von IoT-Geräten	797
4. Einsatz von KI im Handel	798
5. Einsatz von IoT in der Logistik und der Supply Chain	798
6. IoT-Chance für den stationären Handel	799
7. Vorteile von IoT im Handelssektor	800

8. Hindernisse und Herausforderungen	800
II. Rechtliche Aspekte beim Erwerb und Verkauf von IoT-Geräten	800
1. Parteien	801
2. Verträge	801
III. Rechtliche Aspekte beim Einsatz von IoT-Geräten im Handel	803
1. Automatisierter Vertragsschluss/Computer-Erklärung	803
2. Vertragsschluss aufgrund autonom agierender Systeme	803
3. Einsatz von Smart Contracts	806
4. Service-Button/Dash-Button	807
5. Smart Shelves und digitale Preisschilder	808
6. Digitale Einkaufsassistenten	808
7. Invisible Payments	809
8. IoT-basierte Marketingkonzepte	811
IV. Fazit	816
§ 21 Anwendungsbereiche von IoT in der Immobilienwirtschaft	
I. Einführung	817
1. Überblick	817
2. IoT im Immobilien- und Facility-Management	818
3. IoT im Bürogebäude The LAB in Düsseldorf	819
II. Use Cases	822
1. Management physischer Arbeitsplätze	822
2. Intelligente Gebäude	824
3. Reinigungsmanagement	827
4. Hospitality	831
III. Der Business Case	833
IV. Fazit und Ausblick	834
§ 22 Landwirtschaft	
I. Überblick IoT im landwirtschaftlichen Betrieb in den Bereichen Feld, Stall und Hof	836
II. Maschinen-Management-Software in der Feldwirtschaft (Smart Farming)	837
1. Funktionsweise	837
2. Rechtliche Rahmenbedingungen	838
III. Tier-Sensorik in der Stallwirtschaft (Monitoring-Systeme)	844
1. Funktionsweise	845
2. Rechtliche Rahmenbedingungen	846
IV. Zusammenführende Prozessauswertung und -steuerung auf dem Hof (Farm-Management-System)	849
1. Funktionsweise	849
2. Rechtliche Rahmenbedingungen	850
V. Zusammenfassung und Ausblick: Feld, Stall und Hof als vollautonomes System	853
§ 23 Maschinenbau und Smart Factory	
I. Einführung	856
1. Begriff der Smart Factory	856
2. Wertschöpfung in der Smart Factory	857
3. Strategische Ausgliederung des datenbasierten Geschäftsmodells	857
II. Datennutzung in der Smart Factory	858
1. Spannungsfeld Datennutzung	858
2. Notwendigkeit von Datennutzungsverträgen	860
3. Ausgestaltung von Datennutzungsverträgen	861

III. Softwarenutzung in der Smart Factory	868
1. Softwarenutzung im Wandel	868
2. Bemessung nach Nutzern	868
3. Bemessung nach Nutzung	872
4. Weitere Arten der Lizenzbemessung	878
IV. Sicherheit und Gesundheit in der Smart Factory	879
1. Enge Mensch-Roboter-Kollaboration	879
2. Produktsicherheit bei Robotern	879
3. Betrieblicher Arbeitsschutz in der Smart Factory	880
4. IT-Sicherheit in der Smart Factory	882
V. Steuerung von Mitarbeitern in der Smart Factory	885
1. KI-Weisung und Menschenwürde	885
2. KI-Weisung und Direktionsrecht	886
3. KI-Weisung und Datenschutz	886
VI. Digital Twin	888
1. Begriff des digitalen Zwillinges	888
2. Produkthaftung und -sicherheit	889
3. Datenschutz	889
4. Immaterialgüterrecht	890

§ 24 Medien

I. Überblick	894
1. Das Internet der Dinge und Medien	894
2. Öffentlich-rechtlicher Rechtsrahmen	895
II. Konkrete branchenspezifische Anwendungen	895
1. Künstliche Intelligenz und Medien	895
2. Algorithmische Sortiersysteme	896
3. Telemedien	897
III. Branchenspezifischer Rechtsrahmen im Bereich der Medien	897
1. Regulierung von Plattformen und Intermediären	897
2. Anbieter von Telemedien in sozialen Netzwerken	910
3. Social Bots	913
4. Netzwerkdurchsetzungsgesetz	919
5. Presserechtlicher Rahmen	922
6. Urheberrechtlicher Schutz für künstlich geschaffene Presseartikel	923
IV. Internationale Bezüge	925
1. Überblick	925
2. Audiovisuelle Mediendienste-Richtlinie der EU	925
3. Urheberrechts-Richtlinie der EU	926
4. Geoblocking von Inhalten	927
5. Der Ansatz nach britischem Recht	928

§ 25 Öffentliche Verwaltung und Smart Cities

I. Übersicht	930
II. Anwendungsfelder und Beispiele	931
1. Smart City und Smart Country	931
2. Verkehrsverwaltung	932
3. Sonstige Anwendungen	933
III. Besondere rechtliche Rahmenbedingungen	933
1. Herausforderung für die rechtsberatende Perspektive	934
2. Grundsätzliche rechtliche Rahmenbedingungen	935
3. Verhältnismäßigkeit	946
IV. Internationale Bezüge	946

V. Zusammenfassung	947
§ 26 Telekommunikation	
I. Überblick	949
II. Konkrete, branchenspezifische Anwendungen des Internets der Dinge (Use Cases)	950
1. Big-Data-Analysen	950
2. Datenquellen	951
3. Analyse	954
4. Anwendungsbeispiele	955
III. Besondere rechtliche Rahmenbedingungen	958
1. Datenschutzrechtliche Aspekte	958
2. Vertragsgestaltung	967
§ 27 Verkehr	
I. IoT im öffentlichen Verkehr	974
1. Einführung	974
2. Plattformdienste	975
3. Ridepooling/Ridesharing	980
4. Autonome Verkehrsdienstleistungen	983
5. Fazit	984
II. IoT in der Verkehrsleitung	984
1. Einführung	984
2. Automatisierte, autonome Leitung des öffentlichen Verkehrs	985
3. Private Fernsteuerung von Verkehrsinfrastruktur	986
4. Fazit	988
III. IoT in der Verkehrsüberwachung	989
1. Einführung	989
2. Rechtsgrundlagen für Überwachungsmaßnahmen	990
IV. Ausblick – die Mobilität der Zukunft	992
§ 28 Versicherungswirtschaft	
I. Einleitung	994
II. Anwendungsfälle des IoT in der Versicherungswirtschaft	996
1. Telematiktarife und Assistance-Leistungen	996
2. Vertrieb und Schadensmanagement unter Einsatz des IoT	1003
III. Outsourcing von IT-Dienstleistungen eines Versicherungsunternehmens	1006
1. Qualifizierung als Ausgliederung iSd § 32 VAG	1007
2. Konkrete Anforderungen an eine IT-Ausgliederung	1008
3. BaFin-Anforderungen an Beauftragungen von IT-Dienstleistungen, die keine Ausgliederung darstellen	1009
IV. Aufsichtsrechtliche Anforderungen an die IT von Versicherungsunternehmen	1010
V. Fazit	1011
VI. Ausblick	1011
Sachverzeichnis	1013