

Digitale Wirtschaft und Industrie 4.0

herausgegeben von

Mag. Philip Raffling

Mag.³ Sofie Schock

mit Beiträgen von

Mag. Lukas Disarö, Dr. Alexander Forster, Dr. Silke Graf, LL.M.,
Dr. Alexander Hiersche, LL.M., Dr. Patricia Kaindl, LL.M.,
Dr. Rainer A. Lassel, MA, Dr. Hasan Pasalic, Mag. Philip Raffling,
Mag. Sofie Schock, Mag. Mirjam Tercero
und Prof. Mag. Dr. Manfred Wöhrl

MANZä?

Inhaltsverzeichnis

Vorwort	III
Verzeichnis der Autorinnen und Autoren	XIII
Abkürzungsverzeichnis	XV
Einleitung	
I. Definitionen und Zusammenhang zwischen digitaler Wirtschaft und Industrie 4.0	1
A. Industrie 4.0	2
B. Kundenorientierung	3
C. Digitale Wirtschaft	3
II. Potenziale und Herausforderungen digitaler Technologien	4
Vertragsabschluss im E-Commerce und im Internet of Things	
I. Einleitung	7
II. Elektronische Verträge – Vertragsabschluss unter Einsatz von EDV-Kommunikation	8
A. Zustandekommen des Vertrages	9
B. Anfechtung des Vertrages	12
III. Computererklärungen – automatisierter Vertragsabschluss	13
A. Zustandekommen des Vertrages	13
B. Anfechtung des Vertrages	13
IV. Autonome Verträge – Vertragsabschluss durch intelligente Software-Agenten	14
A. Zustandekommen des Vertrages	16
B. Anfechtung des Vertrages	19
V. Allgemeines zum Vertragsabschluss im E-Commerce und im IoT	20
A. Aspekte des Verbraucherschutzes	20
B. Weitere E-Commerce-rechtliche Informationspflichten	24
C. Formvorschriften	25
D. Einbeziehung von AGB	26
EU-Zivilrecht im Bereich Robotik	
I. Allgemein	29
II. Hintergrund	30

III. Ethische Fragen	31
IV. öffentliche Konsultation und Aussicht	32

Neue Technologien und Datenschutz

I. Allgemeines	35
II. Räumlicher Anwendungsbereich	36
III. Zweckbindung	37
IV. Benachrichtigung über Sicherheitsverletzungen	38
V. Privacy by default und privacy by design	38
VI. Einzelne ausgewählte Bereiche	40
A. Beschränkungen für Profiling	40
B. Big Data: Begriffsbestimmung und charakteristische Merkmale	41
1. Allgemein	41
2. Wesentliche Voraussetzungen bei der Verarbeitung von Big Data	43
3. Zweckbindung	43
C. Online Behavioral Targeting / Profilerstellung	44
D. Neue Technologien im Gesundheitswesen	45
E. Cloud-Computing	47
1. Datenverkehr vom und zum Cloud-Anbieter	47
2. Anwendbarkeit der Datenschutzrichtlinie für die elektronische Kommunikation	50
3. Stellungnahme der Artikel-29-Datenschutzgruppe zum Cloud-Computing	50
4. Nicht verbindliche Stellungnahmen mit Relevanz für das Cloud-Computing	52
F. Rechtsfragen iZm Drohnen	52
G. Geolokalisierungsdienste von intelligenten mobilen Endgeräten	55
H. Apps auf intelligenten Endgeräten	56
I. Datenschutz und IoT	57
1. Allgemein	57
2. Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter	58
3. IoT-Sicherheitsarchitektur	59
4. Art 5 Abs 3 der Datenschutzrichtlinie für die elektronische Kommunikation	60

Die Cloud

I. Was versteht man unter der „Cloud“?	63
II. Arten von Clouds	64
A. Public Cloud	64
B. Community Cloud	64
C. Private Cloud	64
D. Hybride Cloud	65
III. Die Cloud in internationaler rechtlicher Hinsicht	65

IV. Die Cloud in nationaler rechtlicher Hinsicht	67
V. Serverstandorte	69
VI. Haftung Dritten gegenüber bei Datenpannen	70
VII. Auf was ist bei AGB zu achten?	70
VIII. Auswirkungen der DSGVO?	71
IX. Zusammenfassung	73

Der 3D-Drucker

I. Allgemeines	75
II. Europäische Tendenzen	76
III. Nationales Urheberrecht	77
IV. Nationales Marken- und Patentrecht	78
V. Kommerzieller 3D-Druck	79
VI. Nationales Wettbewerbsrecht	80
VII. Zusammenfassung und Ausblick	80

Rechte an Daten im Kontext von Industrie 4.0 – ausgewählte Fragestellungen

I. Allgemein	83
II. Datenbegriff	85
III. Schutz der Daten als Betriebsgeheimnis?	85
IV. Erwerb neugeschaffener Daten durch sachenrechtliche Zuordnung?	85
V. Vertragliche Regelung	86
VI. Exkurs: Digitale Güter	88

Der Schutz von Geschäftsgeheimnissen

I. Allgemeines	91
II. Was ist ein Geschäftsgeheimnis?	92
III. Wie schütze ich meine Geschäftsgeheimnisse angemessen?	93
A. Organisatorisch und technisch	94
B. Vertraglich	95
IV. Wovor sind meine Geschäftsgeheimnisse geschützt?	96
V. Welche Rechtsbehelfe stehen zur Wahl?	97
VI. Was ist zu tun?	98

Kartellrecht in digitalen Märkten

I. Einleitung	99
II. Beschränkungen im Online-Vertrieb	101
A. Selektivvertrieb	101
B. Beschränkungen des Online-Verkaufs und der Online-Werbung	103
1. Allgemeines	103
2. Beschränkungen des Online-Handels	105

Inhaltsverzeichnis

3. Insbesondere: Beschränkungen für den Verkauf über Online-Marktplätze („Drittplattformverbote“)	107
4. Geoblocking – neue Regelungen	108
C. Hotelbuchungsplattformen und Bestpreisklauseln	111
III. Algorithmen und Daten als Herausforderungen für das Wettbewerbsrecht	112
A. Allgemeines	112
B. Algorithmen im Kontext vertikaler Vereinbarungen	113
C. Algorithmen im Kontext horizontaler Vereinbarungen	114
1. Umsetzung von Absprachen durch Algorithmen	114
2. Sternkartelle und „price signalling“	115
3. Markttransparenz durch konstantes Preismonitoring und die Möglichkeit stillschweigender Abstimmungen	117
IV. Marktmacht im digitalen Zeitalter	118
A. Allgemeines	118
1. Netzwerkeffekte	118
2. Wechselaufwand und Trägheit der Verbraucher	119
3. Größenvorteile	120
4. Zugang zu Daten	120
5. Wettbewerbsdruck durch Innovation	120
V. Neuerungen in der Zusammenschlusskontrolle	121
VI. Fazit	122

Arbeitsrechtliche Implikationen der Digitalisierung

I. Crowdwork	125
A. Was ist Crowdwork?	125
B. Die Vertragsverhältnisse	126
C. Die Frage nach der Arbeitnehmereigenschaft	127
D. Liegen Kettenarbeitsverträge vor?	129
E. Arbeitskräfteüberlassung	130
F. Crowdworker als Heimarbeiter?	130
II. Mitbestimmung und Betriebsrat in der digitalen Arbeitswelt	131
A. Allgemeines	131
B. Maßnahmen nach § 96 ArbVG	132
1. Personalfragebögen	133
2. Kontrollmaßnahmen, die die Menschenwürde berühren	134
C. Maßnahmen nach § 96a ArbVG	136
1. Personaldatensysteme	136
2. Mitarbeiterbeurteilungssysteme	137
D. Informationsrechte des Betriebsrates	137
III. Bring your own device	138
A. Vereinbarung notwendig?	140
B. Kostentragung	140
IV. Arbeitszeitmanagement	141

A. Aufzeichnungspflicht	142
B. Gleitzeit und Vertrauensarbeitszeit	143
C. Work on Call	143
V. Arbeitnehmerschutz	144
VI. Der Datenschutzbeauftragte nach der DSGVO	144
A. Allgemeines	144
B. Wann muss ein Datenschutzbeauftragter bestellt werden?	144
1. Was ist unter systematischer oder regelmäßiger Überwachung zu verstehen?	145
2. Wann beginnt die umfangreiche Verarbeitung „sensibler“ Daten?	146
C. Stellung und Aufgaben des Datenschutzbeauftragten	147
D. Persönliche Verantwortung des Datenschutzbeauftragten?	150

Strafrechtliche Aspekte

I. Einleitung	151
II. Strafrechtliche Haftung für (teil)autonome Systeme	152
A. Grundlagen	152
B. Wer haftet?	153
1. Lenker, Hersteller, Programmierer	153
2. Verbandsverantwortlichkeit	154
C. Sorgfaltsanforderungen	155
D. Relevante Straftatbestände	157
III. Strafrechtlicher Schutz gegen Angriffe auf (teil)autonome Systeme	158
A. Grundlagen	158
B. Relevante Straftatbestände	159
1. Daten- und Systemschädigungen	159
2. Betrug und betrugsähnliche Angriffe	160
3. Indiskretionsbezogene Angriffe	161
C. Vor- und Nachteile eines Strafverfahrens für den Geschädigten	162
IV. Conclusio	163

Ausgewählte rechtliche Aspekte der Blockchain-Technologie

I. Einleitung	165
II. Wie funktioniert die Blockchain-Technologie?	165
A. Funktionsweise	166
B. Arten von Blockchains	167
III. Welche Vor- und Nachteile birgt die Blockchain-Technologie?	169
IV. Welche Anwendungsfälle können auf der Blockchain-Technologie basieren?	171
A. Allgemeines	171
B. Internet of Things	172
C. Smart Contracts	173
D. Virtuelle Währungen	174

Inhaltsverzeichnis

E. Decentralised Autonomous Organisations	175
F. Energiesektor	175
V. Welche Rechtsprobleme können sich durch die Blockchain-Technologie ergeben?	176
A. Allgemeines	176
B. Datenschutz	178
C. Vertragsrecht	180
D. Verantwortlichkeit/Haftung in distribuierten Systemen	182
E. Strafrecht	186
F. Urheberrecht	186
G. Register	187
H. Anwendbares Recht	188
I. Gesellschaftsrecht	189
J. Normen und Standards	189

Normen und Standards

I. Einleitung	191
II. Normung als regulierte Selbstregulierung	192
III. Eigenschaften und Arten von Normen	194
IV. Überstaatliche Normung	195
A. Internationale Normung	195
B. Europäische Normung	196
C. Koordinierung	198
V. Österreichische Normen	198
A. Die Zuständigkeit zur Normsetzung	198
B. Das Verfahren der Normsetzung	200
C. Abänderung bestehender Normen	203
D. Widerspruch zwischen Normen und staatlichen Rechtsakten	204
E. Finanzierung der Normung	204
VI. Rechtswirkungen der Normen	205
A. Allgemeines	205
B. Dynamische Verweise und Technik Klauseln	206

IT-Security und das Internet der Dinge

I. Einleitung	209
A. Erste industrielle Revolution	209
B. Zweite industrielle Revolution	209
C. Dritte industrielle Revolution	210
D. Vierte industrielle Revolution	210
II. Basistechnologien	210
A. Internet	210
1. Aus der Geschichte lernen	211
2. Die Zukunft: Blockchain	211

B. Datenverschlüsselung	212
1. Ein historischer Rückblick	212
2. Verschlüsselung & Kryptisierung	212
3. Zertifikate	214
4. Anwendung: sicherer Webzugang	215
5. Anwendung: VPN	215
6. Kryptisierung & Quantencomputing	216
C. Safety & Security	216
1. Informationssicherheit	216
2. Security: Technische Sicherheit	216
3. Firewalls: Wandel im Einsatz	217
4. Safety: Sicherer Betrieb	218
D. Cloud	218
E. Big Data	219
1. Zahlen und Fakten	219
2. Wo liegen die Daten?	219
III. Was ist IoT?	220
A. Grundbegriffe	220
B. IoT & Cloud	221
C. Cyber Physical Systems (CPS)	222
D. IIoT/Industrie 4.0	222
IV. IoT & Big Data	222
A. IoT als Datenlieferant	223
B. IoT und personenbezogene Daten	223
V. IoT & Normen	223
VI. IoT & Smart City	224
VII. IoT & Security	224
A. Distributed Denial of Service (DDoS)	224
B. Blackout	225
C. Verfügbarkeit eines IoT-Services	226
VIII. Zukunftsaspekte	228
A. IoT & künstliche Intelligenz (KI)	228
B. IoT & Security by Design	229
C. Kognitive Security	229
Stichwortverzeichnis	231