

Inhalt

Vorwort	V
Inhaltsübersicht	VII
Einleitung	1
§ 1 <i>Problemstellung und praktische Bedeutung</i>	1
§ 2 <i>Stand der Forschung und Gegenstand der Untersuchung</i>	4
§ 3 <i>Gang der Untersuchung</i>	7
Teil I Grundlagen	9
§ 4 <i>Daten</i>	9
I. Definition des Datums	9
1. Wortherkunft	9
2. Vergleich von Definitionen aus verschiedenen Disziplinen	9
3. Zwischenergebnis	13
II. Abgrenzung von digitalen und analogen Daten	14
III. Abgrenzung von Daten und Informationen anhand der informationswissenschaftlich-semiotischen Aufteilung von Informationen	15
IV. Abgrenzung von flüchtigen und dauerhaft verfügbaren Daten	17
V. Fazit	17
§ 5 <i>Technischer Hintergrund</i>	18
I. Grundbegriffe von Datenverarbeitungsprozessen	18
II. Hardware	20
III. Software	22
IV. Rechnernetze	24
V. Internet	26
§ 6 <i>Eigenschaften von Daten</i>	27
I. Immateriellität	27
II. Nicht-rivalisierend	27
III. Nicht-exklusiv	29
IV. Nicht-Abnutzbarkeit	29
V. Räumliche Ungebundenheit	30
VI. Fazit	31
§ 7 <i>Anwendbares Recht</i>	31
I. Territorialitäts- und Schutzlandprinzip im Immaterialgüterrecht	31
II. Anknüpfung	32
1. Globale Sachverhalte	33
2. Anknüpfungsmomente	33

a)	Die Belegenheit des Datenträgers und das Sendelandprinzip	34
b)	Ort der erstmaligen Datenerhebung	35
c)	Handlungsort des Datennutzers	36
III.	Fazit	36
§ 8	<i>Klassifizierung</i>	37
I.	Personenbezogene Daten	38
1.	Historische Entwicklung des Datenschutzes	38
2.	Sinn und Zweck des Datenschutzes	40
II.	Technische Daten/Maschinendaten	40
III.	Abgrenzung von personenbezogenen und technischen Daten	41
1.	Die betroffene Person	41
2.	Wann ist eine betroffene Person identifiziert oder identifizierbar?	42
a)	Identifikation	42
b)	Identifizierbarkeit	42
c)	Absolute oder relative Bestimmbarkeit	43
3.	Zwischenergebnis	44
IV.	Besondere Abgrenzungsfälle	45
1.	Pseudonymisierung	45
a)	Definition und Ziel der Pseudonymisierung	45
b)	Voraussetzungen der Pseudonymisierung	46
c)	Rechtsfolge der Pseudonymisierung	47
aa)	Die anonymisierende Wirkung der Pseudonymisierung	48
bb)	Die risikomindernde Wirkung der Pseudonymisierung	48
cc)	Die irrelevante Wirkung der Pseudonymisierung	48
d)	Zwischenergebnis	49
2.	Anonymisierung	49
a)	Definition und Ziel der Anonymisierung	49
b)	Anonymisierungstechniken	50
c)	Rechtsfolge der Anonymisierung	51
3.	Big Data	51
a)	Begriffserläuterung von Big Data	51
b)	Volume, Variety, Velocity, Value und Veracity	52
c)	Risiko der Re-Identifizierung	54
V.	Datengenerierung	55
VI.	Rohdaten und kultivierte Daten	56
VII.	Fazit	58
Teil II	Schutzsystem von nicht-personenbezogenen Daten de lege lata	61
§ 9	<i>Urheberrecht und Leistungsschutzrechte</i>	61
I.	Daten als möglicher Schutzgegenstand des Urheberrechts	61
II.	Urheberrechtliche Grundlagen	62
1.	Sinn und Zweck des Urheberrechts	62
2.	Die verschiedenen Werkarten	62
3.	Der Urheber und sein Verhältnis zum Werk	63
4.	Die Leistungsschutzrechte im UrhG	63
III.	Urheberrechtlicher Schutz von Daten als Werk	64

1. Eine persönliche geistige Schöpfung als Voraussetzung eines urheberrechtlichen Schutzes	64
a) Persönliches Schaffen	64
b) Geistiger Gehalt	64
c) Wahrnehmbare Form	65
d) Schöpferische Eigentümlichkeit	65
2. Daten als Werk	66
a) Daten als etwas persönlich Geschaffenes	66
b) Die wahrnehmbare Form von Daten	67
c) Daten als etwas geistig Geschaffenes	67
d) Zwischenergebnis	68
IV. Schutz von Computerprogrammen als Sprachwerke	68
V. Schutz von Datenbanken im Urheberrechtsgesetz	69
VI. Schutz als Datenbankwerk	69
1. Aufbau der Norm	69
2. Sammelwerk	71
a) Die Voraussetzungen des Sammelwerks	71
aa) Sammlung von Elementen	71
bb) Auswahl und Anordnung der Elemente als persönliche geistige Schöpfung	72
b) Schutzmfang	73
3. Datenbankwerk	74
a) Voraussetzungen	74
aa) Systematisch oder methodisch angeordnet	74
bb) Einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich	75
cc) Persönliche geistige Schöpfung	75
b) Inhaber	76
c) Schutzmfang	76
d) Schutz einzelner Daten	77
aa) Datenbankwerke mit technischen Daten	77
bb) Auswirkung auf den Schutz einzelner Daten	78
4. Zwischenergebnis	78
VII. Schutz als Datenbankherstellerrecht	80
1. Historische Entwicklung des Datenbankherstellerrechts	80
2. Überblick über das Datenbankherstellerrecht und dessen Verhältnis zum Datenbankwerk	81
3. Voraussetzungen	82
a) Datenbank	82
b) Wesentliche Investition	83
aa) Berücksichtigungsfähige Investitionen	83
(1) Investition in die Beschaffung	83
(2) Investitionen in die Erzeugung der Daten	84
(3) Investition in die Überprüfung	85
(4) Investition in die Darstellung	85
bb) Wesentlichkeit der Investition	86
4. Datenbankhersteller	88
a) Initiative zum Aufbau der Datenbank	88

b) Investitionsrisiko	89
c) Mehrheit von Datenbankherstellern	90
5. Schutzmfang	90
a) Vervielfältigungsrecht	91
b) Verbreitungsrecht	93
c) Recht der öffentlichen Wiedergabe	93
d) Gesamtheit der Datenbank oder eines wesentlichen Teils	94
aa) Quantitativ wesentlicher Teil	94
bb) Qualitativ wesentlicher Teil	95
e) Umgehungstatbestand	96
f) Erschöpfung	98
g) Schranken	99
aa) Vervielfältigung wesentlicher Teile zum privaten Gebrauch	100
bb) Vervielfältigung wesentlicher Teile zu Zwecken der wissenschaftlichen Forschung	100
cc) Vervielfältigung wesentlicher Teile zur Veranschaulichung des Unterrichts und der Lehre	101
dd) Vervielfältigung wesentlicher Teile vor Gerichten oder Behörden	101
h) Verletzungshandlungen	101
i) Verletzungshandlungen im Zusammenhang mit Big Data und Scraping Sachverhalten	103
6. Schutz einzelner Daten	106
7. Schutzdauer	107
a) Bestimmung der Schutzdauer bei einer wesentlichen Änderung der Datenbank	108
b) Stellungnahme	109
8. Fazit	110
VIII. Schutz als Computerprogramm	112
1. Überblick und historische Entwicklung	112
2. Schutzgegenstand	114
a) Das Computerprogramm	114
b) Eigene geistige Schöpfung	116
3. Schutzmfang	117
a) Vervielfältigungsrecht	118
b) Umarbeitungsrecht	118
c) Verbreitungsrecht	118
d) Recht der öffentlichen Wiedergabe	119
e) Schranken	119
4. Schutz einzelner Daten	120
IX. Fazit: Schutz Daten durch das Urheberrechtsgesetz de lege lata	121
<i>§ 10 Patentrecht</i>	123
I. Einführung in das Patentrecht	123
1. Sinn und Zweck des Patentrechts	123
2. Die materiellen Voraussetzungen des Patents	124
3. Der Erfinder und das Recht auf das Patent	125
4. Die Rechte aus dem Patent	126
5. Die Schutzdauer	127

II.	Daten als patentierbare Erfindung	127
1.	Technizität	127
2.	a) Die Voraussetzungen des Rote Taube-Leitsatzes	129
	b) Die Anwendung des Rote Taube-Leitsatzes auf Daten	129
2.	Neuheit	130
3.	Fazit	130
III.	Schutz über eine computerimplementierte Erfindung	131
1.	Schutz von Daten als Bestandteil einer computerimplementierten Erfindung	132
2.	Schutz von Daten als Erzeugnis einer computerimplementierten Erfindung	133
3.	Schutz der Daten als Erzeugnis eines Verfahrenspatents betreffend eine computerimplementierte Erfindung	133
	a) Sinn und Zweck des Schutzes von unmittelbaren Verfahrenserzeugnissen	133
	b) Der Einfluss der Digitalisierung auf den derivativen Erzeugnisschutz	134
	c) Die Voraussetzungen des derivativen Erzeugnisschutzes	135
	aa) Herstellungsverfahren	135
	bb) Körperlichkeit	135
	cc) Unmittelbarkeitszusammenhang	136
	(1) Streit um die Bestimmung der Unmittelbarkeit	136
	(2) Stellungnahme	137
	d) Daten als Gegenstand des derivativen Erzeugnisschutzes	138
	aa) Die Vorgaben aus den BGH-Entscheidungen MPEG-2-Video-signalcodierung und Rezeptortyrosinkinase II	138
	bb) Der Ausschluss der Wiedergabe von Informationen aus dem Patentschutz	140
	cc) Die Anwendung der Voraussetzungen auf Daten	142
IV.	Fazit: Schutz und Zuordnung von Daten durch das Patentrecht de lege lata	143
<i>§ 11 Geschäftsgeheimnisrecht</i>		144
I.	Einführung in das Geschäftsgeheimnisrecht	144
1.	1. Sinn und Zweck des Geschäftsgeheimnisrechts	145
	2. Historische Entwicklung	146
II.	Die Rechtsnatur von Geschäftsgeheimnissen	148
1.	1. Gesetzesmaterialien	148
2.	2. Die Voraussetzungen eines Immaterialgüterrechts	149
	a) Immaterielles Gut	150
	b) Positiver Zuweisungsgehalt	150
	c) Absolutes Abwehrrecht	152
	d) Fazit	157
III.	Anforderungen an das Geschäftsgeheimnis	157
1.	1. Information	159
2.	2. Geheimnisqualität	159
	a) Allgemein bekannt	160
	b) Ohne weiteres zugänglich	161
3.	3. Wirtschaftlicher Wert	162
4.	4. Angemessene Geheimhaltungsmaßnahmen	163
	a) Geheimhaltungsmaßnahmen	164

b) Angemessen	165
c) Verantwortlichkeit für die Geheimhaltungsmaßnahmen	166
5. Geheimhaltungsinteresse	166
IV. Schutz von Daten als Geschäftsgeheimnis	167
1. Daten auf syntaktischer Ebene als Geschäftsgeheimnisse	167
2. Daten auf semantischer Ebene als Geschäftsgeheimnisse	168
a) Vereinbarkeit mit Zielsetzung der Arbeit, Daten unabhängig ihrer Bedeutung zu betrachten	168
b) Erfüllen der Anforderungen an ein Geschäftsgeheimnis	169
aa) Information	169
bb) Geheimnisqualität	169
cc) Wirtschaftlicher Wert	170
dd) Angemessene Geheimhaltungsmaßnahmen	171
ee) Geheimhaltungsinteresse	171
ff) Zwischenergebnis	172
3. Inhaber des Geschäftsgeheimnisses	172
a) Natürliche oder juristische Person	172
b) Rechtmäßige Kontrolle über das Geschäftsgeheimnis	173
aa) Kontrolle	173
bb) Rechtmäßig	174
c) Lizenznehmer als Geheimnisinhaber	174
d) Besonderheiten im kontextuellen Zusammenhang	176
4. Schutzmfang	176
a) Handlungsverbote	177
b) Ansprüche bei Rechtsverletzungen	178
V. Fazit: Schutz und Zuordnung von Daten durch das Geschäftsgeheimnisrecht de lege lata	178
 § 12 Lauterkeitsrecht	180
I. Einführung in das Lauterkeitsrecht	180
1. Der Schutzzweck des UWG	181
a) Schutz der Mitbewerber	181
b) Schutz der Verbraucher, der sonstigen Marktteilnehmer und der Allgemeinheit	182
2. Historische Entwicklung	183
II. Schutz von Daten durch den wettbewerbsrechtlichen Leistungsschutz	184
1. Schutzzweck des wettbewerbsrechtlichen Leistungsschutzes	184
2. Verhältnis zum Urheberrecht, den verwandten Leistungsschutzrechten und dem Patentrecht	186
a) Gleichrang zwischen dem Sonderrechtsschutz und dem lauterkeitsrechtlichen Nachahmungsschutz	186
b) Wettbewerbsrechtlicher Leistungsschutz und Urheberrecht	187
c) Wettbewerbsrechtlicher Leistungsschutz und Patentrecht	188
3. Tatbestandsvoraussetzungen	189
a) Anbieten von Waren oder Dienstleistungen	189
aa) Ware oder Dienstleistung	190
bb) Auf dem Markt anbieten	191
b) Nachahmung	192
c) Wettbewerbliche Eigenart	194

d) Besondere, unlauterkeitsbegründende Umstände	197
aa) Vermeidbare Herkunftstäuschung (lit. a)	197
bb) Unangemessene Ausnutzung oder Beeinträchtigung der Wertschätzung des nachgeahmten Produkts (lit. b)	199
cc) Unrechtmäßige Erlangung von Kenntnissen oder Unterlagen (lit. c)	200
e) Daten als Gegenstand des wettbewerbsrechtlichen Leistungsschutzes	201
aa) Daten als Waren	201
bb) Daten als Dienstleistungen	203
cc) Nachahmung	204
dd) Wettbewerbliche Eigenart von Daten	205
(1) Die wettbewerbliche Eigenart von Daten in der Rechtsprechung	206
(2) Kombination der Daten selbst mit der Besonderheit der Dienstleistung	206
ee) Unlauterkeitsbegründende Merkmale	208
f) Sonderfall: Schutz von Daten in Erzeugnissen	208
4. Schutzzumfang/Rechtsfolge	210
5. Zuordnung	211
III. Schutz von Daten durch den unmittelbaren Leistungsschutz	212
1. Die Herleitung des unmittelbaren Leistungsschutzes	212
a) Argumente für einen unmittelbaren Leistungsschutz	213
b) Argumente gegen einen unmittelbaren Leistungsschutz	214
2. Die Anwendung des unmittelbaren Leistungsschutzes auf Daten nach <i>Becker</i>	215
IV. Fazit	216
<i>§ 13 Allgemeines Zivilrecht</i>	218
I. Versuch der Herleitung eines Dateneigentums	218
1. Daten als Sachen	218
2. Daten als Gegenstände	219
3. Herleitung über das Eigentum am Datenträger	220
4. Herleitung über eine analoge Anwendung des § 903 BGB	220
5. Herleitung über strafrechtliche Vorschriften	221
6. Daten als Sachfrüchte oder Gebrauchsvoerteile	222
II. Deliktsrechtlicher Schutz als sonstiges Recht	224
1. Deliktsrechtlicher Schutz des Datenträgers	224
2. Deliktsrechtlicher Schutz für Daten als sonstiges Recht	225
a) Absolutes, subjektives Recht an Daten als sonstiges Recht	226
aa) Zuweisungsfunktion	226
bb) Ausschlussfunktion	227
b) Rechtspolitische Diskussion um die Anerkennung eines sonstigen Rechts an Daten	228
3. Anerkennung eines Rahmenrechts am Datenbestand	230
III. Fazit	230
<i>§ 14 Verwertung</i>	231
I. Bedeutung und Voraussetzungen der Verkehrsfähigkeit	232
1. Gut	233
2. Subjektives Recht	233

3. Gesetzgeberische Entscheidung	234
II. Verkehrsfähigkeit der jeweiligen subjektiven Rechte an Daten	234
1. Verkehrsfähigkeit des Datenbankwerks	234
2. Verkehrsfähigkeit des Datenbankherstellerrechts	235
3. Verkehrsfähigkeit des Verfahrenserzeugnisses	235
4. Verkehrsfähigkeit des Geschäftsgeheimnisses	236
III. Datenhandel auf faktischer Grundlage	237
IV. Fazit: Verwertung von Daten	238
 <i>§ 15 Zusammenfassung: Schutz, Zuordnung und Verwertung von Daten de lege lata</i>	239
 Teil III Schutz, Zuordnung und Verwertung von Daten durch das Vertragsrecht	245
 <i>§ 16 Tatsächliche Rahmenbedingungen</i>	246
I. Art des Vertrages und Bedeutung der Datenüberlassung	246
II. Terminologie	246
III. Vertragsparteien	247
 <i>§ 17 Typologische Zuordnung des Datenüberlassungsvertrags</i>	247
I. Ziel und Kriterien der typologischen Zuordnung	247
II. Die Digitale-Inhalte-Richtlinie	249
III. Der typengemischte Vertrag und der atypische Vertrag als Alternativen zu einer typologischen Zuordnung sowie deren Normenwendungsbefehl	250
1. Der typengemischte Vertrag	250
2. Der atypische Vertrag	251
IV. Vorüberlegungen zur typologischen Zuordnung des Datenüberlassungsvertrags	251
1. Dauerschuldverhältnis oder punktueller Leistungsaustausch?	251
2. Die typologische Qualifikation des Lizenzvertrages	252
a) Die Lizenz	253
b) Die Lizenz als Kaufvertrag?	253
c) Die Lizenz als Mietvertrag?	254
d) Die Lizenz als Pachtvertrag?	254
aa) Das Pflichtenprogramm	255
bb) Das gesetzliche Leitbild	255
e) Die Lizenz als atypischer Vertrag	256
V. Typologische Zuordnung des Datenüberlassungsvertrags	257
1. Der Datenüberlassungsvertrag als Kauf- oder Werkvertrag	257
2. Der Datenüberlassungsvertrag als Mietvertrag	258
3. Der Datenüberlassungsvertrag als Pachtvertrag	259
a) Das Pflichtenprogramm	259
aa) Der Vertragsgegenstand	260
(1) Die Rechtspacht	260
(2) Streit um die Pacht unkörperlicher Gegenstände	260
bb) Die Fruchtziehung	262
(1) Die Datenauswertung als Fruchtziehung	262
(2) Der Ertrag aus der Weitergabe der Daten als Fruchtziehung ..	262

(3) Die Informationsgenerierung infolge einer Datenauswertung als Fruchtziehung	263
b) Das gesetzliche Leitbild	264
aa) Das gesetzliche Leitbild der Pacht	264
bb) Die Übertragbarkeit der Regelungen zu Leistungsstörungen	264
cc) Die Übertragbarkeit der Regelungen zur Vertragsbeendigung	266
c) Zwischenergebnis	267
4. Einordnung als Vertrag sui generis	267
VI. Fazit	269
§ 18 Berücksichtigung der Grundsätze der EU-Kommission	269
I. Transparenz in der Vertragsgestaltung	270
II. Minimierung der Datenabhängigkeit von einem Anbieter	271
§ 19 Berücksichtigung AGB-rechtlicher Vorgaben	272
I. Überraschende und mehrdeutige Klauseln	272
II. Unangemessene Benachteiligung	272
1. Transparenzgebot	272
2. Vereinbarkeit mit den wesentlichen Grundgedanken der gesetzlichen Regelung	273
3. Gefährdung der Erreichung des Vertragszwecks	273
4. Ausformung eines Leitbildes nach Hennemann	274
III. Rechtsfolgen AGB-rechtlicher Vorgaben	275
§ 20 Inhaltliche Regelungspunkte	276
I. Anwendungsbereich	276
1. Definition der Daten	277
2. Kategorisierung der Daten	277
3. Ausschluss personenbezogener Daten	277
II. Vergütung	278
III. Zuordnung der Daten	278
IV. Vereinbarung der Nutzungsrechte	279
V. Gewährleistungsrechte, Haftung und Vertragslaufzeit	280
VI. Nebenabreden	281
§ 21 Einbezug (möglicherweise) bestehender absoluter Rechtspositionen	282
I. Datenbestand enthält bekanntermaßen Schutzrechte	283
II. Infolge der Datenauswertung entstehen Schutzrechte	283
III. Datenbestand enthält wider Erwarten Schutzrechte	284
IV. Fazit	284
§ 22 Muster Datenüberlassungsvertrag	285
§ 23 Grenzen, Vor- und Nachteile einer vertraglichen Regelung	293
I. Grenzen	293
1. Relativität der Schuldverhältnisse	293
2. Kartellrechtliche Grenzen	293
II. Nachteile	296
1. Relativität der Schuldverhältnisse	296
2. Kartellrechtsrisiken	296
3. Missbrauchsrisiken infolge fehlender Kontrollmöglichkeiten	297

4. Nichtigkeitsrisiken	297
5. Komplexität der Sachverhalte	298
III. Vorteile	298
1. Flexibilität	298
2. Globale Sachverhalte	299
IV. Fazit	299
<i>§ 24 Zusammenfassung: vertragliche Nachbildung eines Ausschließlichkeitsrechts?</i>	299
Teil IV Gesetzgeberischer Handlungsbedarf	301
<i>§ 25 Lösungsmodelle in Wissenschaft und Gesetzgebung</i>	301
I. Absolutes Recht an Daten	301
1. Anknüpfungspunkt	302
a) Sacheigentum	303
b) Investition	303
c) Skripturakt	304
2. Inhalt eines möglichen Datenrechts	304
3. Bewertung des Vorschlags	306
a) Anwendung der Patentrechtstheorien	306
aa) Die Anspornungstheorie	306
bb) Die Offenbarungstheorie	307
b) Schaffen neuer Märkte und Erleichterung des Datenhandels	308
c) Klärung der originären Zuordnung des Datennutzens	309
d) Die wirtschaftliche Bedeutung von Daten	309
e) Rechtssicherheit und Transparenz	310
f) Wettbewerb	310
g) Eingriff in die Berufs- und Wettbewerbsfreiheit	311
h) Praktische Probleme in der Umsetzung	311
4. Fazit	312
II. Zugangsrechte	313
III. Status quo belassen	316
Teil V Schlussbetrachtungen	317
<i>§ 26 Lösungsvorschlag</i>	317
I. Schutz, Zuordnung und Verwertung durch einschlägige absolute Rechte als Schutzzinseln	317
II. Ergänzende Anwendung des Vertragsrechts	318
III. Ausgleich der Nachteile des Vertragsrechts	319
1. Kombination vertraglicher Maßnahmen mit der faktischen Exklusivität	319
2. Anpassung der TT-GVO	319
3. Standardvertragsklauseln	320
<i>§ 27 Ergebnis</i>	321
<i>§ 28 Zusammenfassung in Thesen</i>	321
I. Definition und Eigenschaften von Daten	321
II. Die Bestimmung des anwendbaren Rechts	322

III.	Daten als unmittelbares Erzeugnis eines patentierten Herstellungsverfahrens	322
IV.	Das Geschäftsgeheimnis als Immaterialgüterrecht	322
V.	Schutz, Zuordnung und Verwertung von Daten durch absolute Rechte de lege lata	323
VI.	Es gibt kein Dateneigentum	323
VII.	Der Datenüberlassungsvertrag ist ein Vertrag sui generis	323
VIII.	Kein Bedarf zur Schaffung eines umfassenden Ausschließlichkeitsrechts	324
IX.	Die Regelungen de lege lata sind geeignet, einem rechtlichen Umgang mit Daten zu ermöglichen.	324
X.	Folgerungen für die Praxis	324
Abkürzungen		327
Literatur		331
Sachregister		355