

Inhaltsübersicht

Vorwort	V
Inhalt	IX
Einleitung	1
A. Problemaufriss und Ziel der Arbeit	1
B. Gang der Untersuchung	3
C. Stand der Forschung	4
1. Teil Grundlagen und technischer Hintergrund von KI-Systemen	7
A. Einführung Künstliche Intelligenz	7
B. Technischer Hintergrund Deep Learning	18
C. Schutzwürdige Komponenten eines KI-Systems	26
D. Technologische Trends und Besonderheiten von KI-Systemen	38
2. Teil Schutzfähigkeit von KI-Komponenten nach alternativen Schutzinstrumenten	49
A. Schutzfähigkeit von KI-Systemen nach dem Gesetz zum Schutz von Geschäftsgeheimnissen	50
B. Schutzfähigkeit von KI-Systemen nach dem lauterkeitsrechtlichen Leistungsschutz	80
3. Teil Betrachtung des Schutzniveaus des Gesetzes zum Schutz von Geschäftsgeheimnissen für KI-Systeme	103
A. Vergleich zur Schutzfähigkeit nach Patent- und Urheberrecht von KI-Systemen	105
B. Betrachtung der geschäftsgeheimnisrechtlichen Schranken und Ausnahmen in Bezug auf KI-Systeme	161
C. Betrachtung des Umfangs und der Reichweite des Geschäftsgeheimnisschutzes von KI-Systemen	203
4. Teil Bewertung und Reformvorschläge eines Geschäftsgeheimnisschutzes für KI-Systeme	239
A. Bewertung des geschäftsgeheimnisrechtlichen Schutzes für KI-Komponenten	240
B. Verbesserungen, Modifizierungen und Reformen des Geschäftsgeheimnisschutzes	246
Zusammenfassende Schlussbetrachtung in Thesen	289
Abkürzungen	295
Literatur	299
Sachregister	327

Inhalt

Vorwort	V
Inhaltsübersicht	VII
Einleitung	1
A. Problemaufriss und Ziel der Arbeit	1
B. Gang der Untersuchung	3
C. Stand der Forschung	4
1. Teil Grundlagen und technischer Hintergrund von KI-Systemen	7
A. Einführung Künstliche Intelligenz	7
I. Kurzabriss der Geschichte von Künstlichen Intelligenz	7
II. Begrifflichkeiten und Wesensmerkmale im Bereich KI	9
1. Künstliche Intelligenz	10
2. Maschinelles Lernen	11
a) Begriffsannäherung	11
b) Vorgehensweise bei maschinellen Lernverfahren	13
aa) Erste Phase: Die Schritte der Datenaufbereitung und -sammlung	13
bb) Zweite Phase: Auswahl, Training und Anwendung der jeweiligen Methode des maschinellen Lernens	15
3. Künstliche neuronale Netze und Deep Learning	16
4. Zwischenergebnis: Einführung	17
B. Technischer Hintergrund Deep Learning	18
I. Funktionsweise und wesentliche Bestandteile von künstlichen neuronalen Netzen	18
1. Aufbau und wesentliche Bestandteile	18
2. Grundlegende Funktionsweise	20
II. Der Entwicklungsprozess bis zum trainierten KI-Modell	22
1. Das Framework für die Entwicklung eines KI-Modells	22
2. Erstellung einer Topologie	22
3. Training des KI-Modells	24
4. Ergebnis des Trainingsvorgangs: Trainiertes KI-Modell	25
III. Zwischenergebnis: Der Entwicklungsprozess bis zum trainierten KI-Modell	26
C. Schutzwürdige Komponenten eines KI-Systems	26
I. Beurteilungsmaßstab	27
1. Technische Erwägungen	28
2. Schützenswerte Leistungen bei der Entwicklung von KI-Systemen	28
a) Inhalt und Umfang der Investitionsleistung	29
b) Inhalt und Umfang der Entwicklungsleistung	31

Inhalt

II.	Festlegung von schutzwürdigen KI-Komponenten	32
1.	KI-Modell	32
2.	KI-Trainingsdatenset	33
3.	KI-Algorithmen	36
4.	KI-Gesamtanwendung	37
III.	Zwischenergebnis: Schutzwürdige Komponenten eines KI-Systems	37
D.	<i>Technologische Trends und Besonderheiten von KI-Systemen</i>	38
I.	Geschäftsmodelle und allgemeine IT-Trends	38
II.	Besonderheiten von KI-Systemen im Vergleich zu regelbasierter Software	44
III.	Zwischenergebnis: Technologische Trends und Besonderheiten von KI-Systemen	47
2. Teil	Schutzfähigkeit von KI-Komponenten nach alternativen Schutzinstrumenten	49
A.	<i>Schutzfähigkeit von KI-Systemen nach dem Gesetz zum Schutz von Geschäftsgeheimnissen</i>	50
I.	Grundprinzipien des Geschäftsgeheimnisschutzes	50
1.	Historische Entwicklung bis zum Gesetz zum Schutz von Geschäftsgeheimnissen	51
2.	Allgemeine Charakteristika eines Geschäftsgeheimnisschutzes nach der EU-Reform 2016	53
3.	Wirtschaftliche Bedeutung von Geschäftsgeheimnissen	55
II.	Schutzfähigkeit nach dem Gesetz zum Schutz von Geschäftsgeheimnissen	57
1.	Geheimnischarakter der jeweiligen KI-Komponente	57
a)	Informationscharakter	57
aa)	Informationscharakter des KI-Modells	58
bb)	Informationscharakter des KI-Trainingsdatenset	59
cc)	Informationscharakter weiterer KI-Komponenten	61
b)	Geheimnischarakter	61
aa)	Geheimnischarakter des KI-Modells	62
(1)	Verlust des Geheimnischarakters bei der Nutzung von Cloudinfrastruktur	63
(2)	Verlust des Geheimnischarakters bei Kooperationsverhältnissen	63
(3)	Verlust des Geheimnischarakters bei der Nutzung von Open Source-Software	65
bb)	Geheimnischarakter des KI-Trainingsdatensets	68
cc)	Geheimnischarakter der KI-Algorithmen	71
dd)	Geheimnischarakter der KI-Gesamtanwendung	72
2.	Wirtschaftlicher Wert	73
3.	Angemessene Geheimhaltungsmaßnahmen	76
4.	Berechtigtes Interesse an der Geheimhaltung	78
III.	Zwischenergebnis: Schutzfähigkeit von KI-Systemen nach dem Gesetz zum Schutz von Geschäftsgeheimnissen	79
B.	<i>Schutzfähigkeit von KI-Systemen nach dem lauterkeitsrechtlichen Leistungsschutz</i>	80
I.	Grundprinzipien des lauterkeitsrechtlichen Leistungsschutzes	81

II.	Lauterkeitsrechtlicher Leistungsschutz von KI-Systemen	83
1.	Ware oder Dienstleistung im lauterkeitsrechtlichen Sinne	84
2.	Angebot einer nachgeahmten KI-Komponente	87
3.	Wettbewerbliche Eigenart einer KI-Komponente	89
4.	Unlauterkeit der Nachahmung	95
a)	Vermeidbare Herkunftstäuschung in Bezug auf KI-Modell und KI-Gesamtanwendung	95
b)	Rufausbeutung und -beeinträchtigung in Bezug auf das KI-Modell und KI-Gesamtanwendung	96
c)	Unredliche Erlangung des KI-Modells und der KI-Gesamtanwendung	97
5.	Unlauterkeit durch eine Behinderung in Form der systematischen Leistungübernahme	98
III.	Unmittelbarer Leistungsschutz von KI-Systemen	99
IV.	Zwischenergebnis: Lauterkeitsrechtlicher Schutz von KI-Systemen	102
3. Teil	Betrachtung des Schutzniveaus des Gesetzes zum Schutz von Geschäftsgeheimnissen für KI-Systeme	103
A.	<i>Vergleich zur Schutzfähigkeit nach Patent- und Urheberrecht von KI-Systemen</i>	105
I.	Urheberrechtliche Schutzfähigkeit von KI-Systemen	106
1.	Computerprogrammschutz	108
a)	Computerprogramm	109
aa)	KI-Modell	110
(1)	Kein Computerprogramm	110
(2)	Erweitertes Begriffsverständnis Computerprogramm	111
(3)	Stellungnahme: KI-Modell als Computerprogramm	113
bb)	KI-Algorithmen	113
cc)	KI-Gesamtanwendung	114
b)	Eigene geistige Schöpfung	115
aa)	KI-Modell	116
(1)	Der Voranknüpfungsansatz	116
(2)	Ablehnung einer eigenen, geistigen Schöpfung	118
(3)	Stellungnahme: Eigene, geistige Schöpfung des KI-Modells	120
bb)	KI-Gesamtanwendung	123
2.	Datenbankherstellerrecht in Bezug auf die KI-Komponenten	124
a)	Unabhängigkeit und einzelne Zugänglichkeit der Elemente einer Datenbank	124
aa)	KI-Modell	125
bb)	KI-Trainingsdatenset	126
b)	Systematisch oder methodisch angeordnet	126
c)	Bezugsplatz der berücksichtigungsfähigen Investition	127
d)	Wesentlichkeit der Investition	132
3.	Zwischenergebnis: Urheberrechtlicher Schutzfähigkeit von KI-Systemen	132
II.	Patentrechtliche Schutzfähigkeit von KI-Systemen	133
1.	Technizität der KI-Komponenten	136
a)	KI-Modell	137
b)	KI-Trainingsdatenset	142
c)	KI-Algorithmen	143

Inhalt

d) KI-Gesamtanwendung	144
2. Erfinderische Tätigkeit in Bezug auf die KI-Gesamtanwendung	145
a) Weitere technische Wirkung	146
b) Naheliegen aus dem Stand der Technik	148
c) Menschlicher Anteil an der erforderlichen Tätigkeit	149
3. Neuheit der KI-Gesamtanwendung	150
4. Gewerbliche Anwendbarkeit der KI-Gesamtanwendung	153
5. Hinreichende Offenbarung der KI-Gesamtanwendung	153
a) Hinreichende Beschreibung	154
b) Ermöglichung der Reproduzierbarkeit	157
6. Zwischenergebnis: Patentrechtlicher Schutz von KI-Systemen	159
III. Zwischenergebnis: Vergleich zur Schutzfähigkeit nach Urheber- und Patentrecht	160
 <i>B. Betrachtung der geschäftsgeheimnisrechtlichen Schranken und Ausnahmen in Bezug auf KI-Systeme</i>	161
I. Eigenständige Entdeckung oder Schöpfung	164
II. Reverse Engineering	167
1. Reverse Engineering allgemein	168
a) Technischer Hintergrund des Reverse Engineering bei KI-Systemen	168
b) Geschäftsgeheimnisrechtlicher Rahmen des Reverse Engineering	170
aa) Reverse Engineering nach Markteintritt	171
bb) Reverse Engineering vor Markteintritt	173
2. Reverse Engineering in Bezug auf die KI-Komponenten	174
a) Reverse Engineering des KI-Modells	174
b) Reverse Engineering des KI-Trainingsdatensets	178
c) Reverse Engineering von KI-Algorithmen	180
d) Reverse Engineering der KI-Gesamtanwendung	181
3. Reverse Engineering im Falle einer Schutzrechtskumulation	181
a) Verhältnis zu den urheberrechtlichen Regelungen des Reverse Engineering	181
aa) Ausgangssituation der urheberrechtlichen Reverse Engineering-Regelungen	182
bb) Verhältnis von GeschGehG und Softwareurheberrecht im Bereich des Reverse Engineering	183
(1) Situation vor Markteintritt	184
(2) Situation nach Markteintritt	185
b) Verhältnis zu einem patentrechtlichen Schutz	189
c) Verhältnis zur Datenschutzgrundverordnung	189
4. Zwischenergebnis: Reverse Engineering	191
III. Arbeitnehmerwechsel	191
1. KI-Komponenten und die Zuordnung zu Arbeitnehmern	192
a) Originäre Zuordnung von KI-Komponenten als Geschäftsgeheimnisse an Arbeitnehmer?	193
b) KI-Komponenten als Erfahrungswissen der Arbeitnehmer	193
2. Uber vs. Waymo als Fallbeispiel	194
3. Zunehmende Automatisierung der KI-Entwicklung	197
4. Zwischenergebnis: KI-Komponenten und Arbeitnehmerwechsel	198
IV. Ausnahmen	199

V.	Zwischenergebnis: Betrachtung der geschäftsgeheimnisrechtlichen Schranken und Ausnahmen in Bezug auf KI-Systeme	202
C.	<i>Betrachtung des Umfangs und der Reichweite des Geschäftsgeheimnisschutzes von KI-Systemen</i>	203
I.	Zuordnung der Rechtsinhaberschaft	204
1.	Rechtezuordnung im Hinblick auf KI-Komponenten	206
2.	Zwischenergebnis: Zuordnung der Rechtsinhaberschaft	212
II.	Reichweite der Handlungsverbote	213
1.	Unerlaubte Erlangung von KI-Komponenten	214
2.	Unerlaubte Nutzung oder Offenlegung von KI-Komponenten	217
3.	Von Dritten erlangte Information und KI-Komponenten	220
4.	Zwischenergebnis: Reichweite der Handlungsverbote	226
III.	Durchsetzung und Nachweis von Ansprüchen aufgrund geheimnisrechtlicher Rechtsverletzungen	226
1.	Ansprüche nach dem Gesetz zum Schutz von Geschäftsgeheimnissen	227
a)	Beweisprobleme hinsichtlich der Geschäftsgeheimnisverletzung bei KI-Komponenten	228
b)	Aktiv und Passivlegitimation bei Ansprüchen nach dem Gesetz zum Schutz von Geschäftsgeheimnissen	230
2.	Einreden nach dem Gesetz zum Schutz von Geschäftsgeheimnissen	233
3.	Grundzüge verfahrensrechtlicher Aspekte	234
4.	Zwischenergebnis: Durchsetzung und Nachweis geheimnisrechtlicher Verletzung	236
IV.	Zwischenergebnis: Betrachtung der Reichweite des Geschäftsgeheimnisschutzes von KI-Systemen	236
4. Teil	Bewertung und Reformvorschläge eines Geschäftsgeheimnisschutzes für KI-Systeme	239
A.	<i>Bewertung des geschäftsgeheimnisrechtlichen Schutzes für KI-Komponenten</i> . .	240
B.	<i>Verbesserungen, Modifizierungen und Reformen des Geschäftsgeheimnisschutzes</i>	246
I.	Ausgewählte Stärkung und Verbesserung des Geschäftsgeheimnisschutzes	247
1.	Weite Auslegung des Tatbestandsmerkmals »geheime Information«	248
2.	Verbesserungen der Zuordnung der Rechtsinhaberschaft	252
a)	Ein Geschäftsgeheimnisregister für KI-Komponenten?	253
aa)	Das partiell konstitutive Geschäftsgeheimnisregister	253
bb)	Das fakultative Geschäftsgeheimnisregister und Blockchain-Lösungen	255
b)	Weitere Maßnahmen: Leitlinien und Standardvertragsklauseln	257
c)	Die besondere Rolle der Arbeitnehmer bei der Rechtezuordnung	259
3.	Verbesserungen bei der Rechtsdurchsetzung von KI-Komponenten als Geschäftsgeheimnisse	261
a)	Nachweis einer Geschäftsgeheimnisverletzung bei KI-Komponenten . .	262
b)	Reformansatz speziell für die Durchsetzung von KI-Komponenten im Zivilprozess	265

Inhalt

c) Stärkere Verankerung von Zero Knowledge Beweis-Verfahren im Geschäftdgeheimnisrecht	266
II. Partielle Modifizierung des Ausnahmen- und Schrankensystems	270
1. Anpassung der erlaubten Handlungen nach § 3 GeschGehG	270
2. Öffnung der Ausnahmen aus § 5 GeschGehG für weitere Interessen der Allgemeinheit	272
a) Datennutzungsrechte für Wettbewerber	272
b) Weitere berücksichtigungsfähige Allgemeininteressen	273
III. Reform der Reichweite des Geschäftdgeheimnisrechts	274
1. Beschränkung der Rechtsverfolgungsansprüche	275
a) Adressatenkreis, insbesondere Intermediärhaftung	275
b) Reichweite des § 4 Abs. 3 GeschGehG	277
2. Zugangsansprüche zu KI-Komponenten	280
a) Datenzugangsansprüche im Kartellrecht	281
aa) Zugang zu Daten als wesentliche Einrichtung	281
bb) Zugang bei relativer Marktmacht	282
cc) Zwangslizenzen nach FRAND-Standard	282
b) Geschäftdgeheimnisse als objektive Rechtfertigung der Zugangsverweigerung	283
IV. Zwischenergebnis: Reform des Geschäftdgeheimnisschutzes	286
Zusammenfassende Schlussbetrachtung in Thesen	289
Abkürzungen	295
Literatur	299
Sachregister	327