

digital | recht

Schriften zum Immaterialgüter-, IT-,
Medien-, Daten- und Wettbewerbsrecht

Pablo Schumacher

Schutzfähigkeit Künstlicher Intelligenz

Die immaterialgüterrechtliche Schutzfähigkeit von
KI-Technologien

Band 15

Pablo Schumacher

Schutzfähigkeit Künstlicher Intelligenz

Die immaterialgüterrechtliche Schutzfähigkeit von
KI-Technologien

digital | recht

Schriften zum Immaterialgüter-, IT-, Medien-, Daten- und Wettbewerbsrecht

Herausgegeben von Prof. Dr. Maximilian Becker,
Prof. Dr. Katharina de la Durantaye, Prof. Dr. Franz Hofmann,
Prof. Dr. Ruth Janal, Prof. Dr. Anne Lauber-Rönsberg,
Prof. Dr. Benjamin Raue, Prof. Dr. Herbert Zech

Band 15

Pablo Schumacher, geboren 10.12.1991, Studium der Rechtswissenschaften in Basel, Volontariate in Basel-Stadt und Basel-Landschaft, Advokaturexamen in Basel-Stadt, Advokat in Basel, seit 2023 Referent für Digital Content & Recht beim Bitkom e.V., das Werk gibt die persönliche Meinung des Verfassers wieder.

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dieses Buch steht gleichzeitig als elektronische Version über die Webseite der Schriftenreihe: <http://digitalrecht-z.uni-trier.de/> zur Verfügung.

Dieses Werk ist unter der Creative-Commons-Lizenz vom Typ CC BY-ND 4.0 International (Namensnennung, keine Bearbeitung) lizenziert:

<https://creativecommons.org/licenses/by-nd/4.0/deed.de>

Von dieser Lizenz ausgenommen sind Abbildungen, an denen keine Rechte der Autorin/des Autors oder der UB Trier bestehen.

Umschlaggestaltung von Monika Molin

ISBN: 9783758439339

URN: urn:nbn:de:hbz:385-2023112308

DOI: <https://doi.org/10.25353/ubtr-8fd4-5e49-0b08>



© 2023 Pablo Schumacher, Berlin

Die Schriftenreihe wird gefördert von der Universität Trier und dem Institut für Recht und Digitalisierung Trier (IRDT).

Anschrift der Herausgeber: Universitätsring 15, 54296 Trier.

 UNIVERSITÄT
TRIER

IRDT Institut für
Recht und Digitalisierung
Trier

Für meine Familie
und für Annka

Vorwort

Vorliegende Arbeit wurde im Herbst 2023 von der Juristischen Fakultät der Humboldt-Universität zu Berlin als Dissertation angenommen. Stand der Literaturangaben und sonstigen Ver- und Nachweise ist Frühjahr 2023.

Für die Inspiration zur Themenfindung danke ich meinem Doktorvater, Prof. Dr. Herbert Zech. Nicht nur, weil er die Arbeit betreut hat, sondern vor allem, weil er durch seine damalige Lehrtätigkeit an der Universität Basel meine Begeisterung für das Immaterialgüterrecht bei mir weckte.

Fachlicher Dank gebührt einer Vielzahl von Menschen: Dr. Andrea Linhart für Ihre so geschätzten inhaltlichen Anregungen und das Korrekturlesen des Manuskriptes, Lukas Seiling für die wertvollen Ratschläge vor allem technischer Art und das Lektorat des technischen Teils, Dr. Ferdinand Müller als Leidensgenosse und Co-Seminarleiter für die (Streit-)Gespräche fachlicher und menschlicher Art sowie Lisa Markschies, Mariam Sattorov und Melina Braun für die Unterstützung bei der Literaturbeschaffung und Formatierung.

Meiner Freundin Lea Ludmilla Ossmann-Magiera gebührt zum einen fachlicher Dank: Als Doktorandin zur Regulierung von KI war und ist sie mein wichtigster fachlicher Sparringspartner. Zum anderen und noch viel mehr gilt ihr mein menschlicher Dank: Als Freundin war und ist sie mir mein Antrieb, Rückhalt und Ruhepol.

Dr. Annka Dietrich möchte ich dafür danken, dass sie mir als juristische Mentorin und als Mensch stets mit Rat und Tat zur Seite steht und mein juristisches Denken und Handeln maßgeblich geprägt hat.

Meiner Schwester Paloma Ilona Schumacher danke ich für Ihre schwesterliche Liebe, ihren Rückhalt, ihren Rat und vor allem ihre Ehrlichkeit – nicht nur während der Entstehung dieser Arbeit. Schließlich gilt mein größter Dank meinen Eltern, Susanne und David Schumacher, die mir meinen Lebens- und Ausbildungsweg überhaupt erst ermöglicht haben.

Berlin, im Dezember 2023

Pablo Schumacher

Inhaltsverzeichnis

Abkürzungsverzeichnis	XIII
<i>Einleitung in die Untersuchung</i>	1
A. Gegenstand der Untersuchung	1
B. Forschungsstand	4
C. Gang der Untersuchung	7
<i>Teil 1</i>	
<i>Begriffe und Funktionsweisen</i>	11
<i>Kapitel 1</i>	
<i>Einführung in die Begriffe</i>	13
A. Digitale Systeme	13
B. Intelligente digitale Systeme	16
I. Intelligenz durch Lernfähigkeit	19
II. Autonomie durch Intelligenz	20
C. Zwischenergebnis zum Intelligenzbegriff in der digitalen Welt	21
D. KI-Technologie	23
E. Algorithmus	24
F. Exkurs: Starke und schwache KI	25
<i>Kapitel 2</i>	
<i>Technische Besonderheiten von KI-Technologien</i>	27
A. Die trainierende Person als neues Subjekt im Entwicklungsprozess	27
B. Daten als conditio sine qua non	30
C. Funktionsweise intelligenter digitaler Systeme anhand dreier Beispiele	31
I. Expertensysteme	32

II. Künstliche Neuronale Netze	34
III. Evolutionäre und genetische Algorithmen sowie genetische Programme	44
IV. Zwischenergebnis.....	55
 <i>Teil 2</i>	
<i>Das Immaterialgüterrecht und dessen Rechtfertigung.....</i>	<i>57</i>
<i>Kapitel 3</i>	
<i>Begriff und Wesen des Immaterialgüterrechts</i>	<i>59</i>
<i>Kapitel 4</i>	
<i>Rechtfertigungsansätze im Immaterialgüterrecht.....</i>	<i>61</i>
A. Deontologische Theorien.....	62
B. Utilitaristische Theorien.....	65
C. Zwischenergebnis	67
 <i>Teil 3</i>	
<i>Ökonomische Analyse und Schutzbedürftigkeit von KI-Technologien</i>	<i>69</i>
<i>Kapitel 5</i>	
<i>Von der ökonomischen Analyse des Rechts zur Rechtspolitik.....</i>	<i>71</i>
A. Marktversagensgründe	76
I. Marktmacht.....	76
II. Externe Effekte	77
III. Informationsasymmetrie	78
IV. Nicht private Güter/öffentliche Güter	79
B. Volkswirtschaftliche Ziele	80
I. Ziel der hohen Produktion – dynamische Effizienz	81
II. Ziel der weiten Verbreitung – statische Effizienz	83
III. Niedrige Kosten im Umgang.....	85

C. Zusammenfassung	86
--------------------------	----

Kapitel 6

<i>Markt für KI-Technologien</i>	89
--	----

A. Marktdynamik und potenzielle Marktzutrittsschranken	89
B. Treiber des Marktes	91
C. Produkte des Marktes	95
D. Ineffizienzen des Marktes?	99
I. Ineffizient hohe Kosten.....	99
II. Unterbleibende Güterverbreitung – statische Ineffizienz	105
III. Fehlende Transparenz.....	106
E. Schlussfolgerung: Indizien für Schutzbedürfnis	107

Teil 4

<i>Schutzrecht an KI-Technologien de lege lata</i>	111
--	-----

Kapitel 7

<i>Patentrechtlicher Schutz von KI-Technologien</i>	113
---	-----

A. Grundlagen des Patentrechts	113
I. Materielle Voraussetzungen des Patentschutzes	113
II. Formelle Voraussetzungen des Patentschutzes	116
III. Ausschluss von mathematischen Methoden und Computerprogrammen vom Patentschutz.....	117
B. Prüfung der patentrechtlichen Schutzfähigkeit von KI-Technologien ...	122
I. Die erforderliche Technizität und erfinderische Tätigkeit.....	123
II. Erfinderbegriff.....	126
III. Hinreichende Offenbarung	132
IV. Mangelnde Schutzfähigkeit von Trainingsdatensätzen.....	136
V. Exkurs: selbständige Weiterentwicklungen intelligenter digitaler Systeme.....	136
VI. Zwischenergebnis.....	137

Kapitel 8

<i>Urheberrechtlicher Schutz von KI-Technologien</i>	139
--	-----

A. Grundlagen des Urheberrechts	139
I. Voraussetzungen des urheberrechtlichen Schutzes nach UrhG...	139

II. Inhalt des Urheberrechts.....	142
III. Voraussetzungen für den Computerprogrammenschutz insbesondere	145
IV. Leistungsschutzrechte.....	148
B. Prüfung der urheberrechtlichen Schutzfähigkeit von KI-Technologien.	149
I. Expertensysteme.....	150
II. Genetische Programme.....	152
III. Künstliche Neuronale Netze als Computerprogramme nach §§ 69a ff. UrhG.....	158
IV. Künstliche neuronale Netze als sonstige Werke nach § 2 UrhG..	172
V. Schutz der Trainingsdaten.....	175
VI. Zwischenergebnis zum urheberrechtlichen Schutz von KI- Technologien.....	177

Kapitel 9

<i>Schutz von KI-Technologien als Geschäftsgeheimnisse.....</i>	<i>179</i>
A. Grundlagen des Know-How- bzw. Geschäftsgeheimnisschutzes.....	179
B. Anwendung des GeschGehG auf KI-Technologien.....	182
I. KI-Technologien als Geheimnis.....	182
II. Trainingsdaten als Geheimnis.....	184
III. Sperrige Natur der Geheimhaltungsmaßnahmen.....	186
IV. Gesetzliche Offenlegungspflichten als Hindernis?.....	186
C. Erlaubte Handlungen nach GeschGehG.....	188
I. Erlaubte Handlungen und ihre Auswirkungen auf die Natur des Geheimnisschutzes.....	189
II. Reverse Engineering im Besonderen.....	193
III. Zwischenergebnis.....	204

Kapitel 10

<i>Schutzlücken beim Schutz von KI-Technologien.....</i>	<i>207</i>
A. Würdigung des Schutzniveaus und Schutzlücken.....	207
I. Würdigung des patentrechtlichen Schutzes.....	208
II. Würdigung des urheberrechtlichen Schutzes.....	212
III. Würdigung des Geschäftsgeheimnisschutzes.....	217

B. Ergebnis: Schutzlücken	219
C. Weitere Argumente für die Einführung eines neuen Schutzrechts	223
<i>Teil 5</i>	
<i>Schutzrecht an KI-Technologien de lege ferenda</i>	227
<i>Kapitel 11</i>	
<i>Offenlegungsanreize</i>	229
<i>Kapitel 12</i>	
<i>Schutzvoraussetzungen und Rechtsinhaber</i>	233
<i>Kapitel 13</i>	
<i>Schutznatur, -umfang und -dauer</i>	237
<i>Kapitel 14</i>	
<i>Verortung des Schutzrechts</i>	241
<i>Kapitel 15</i>	
<i>Zwischenergebnis</i>	243
<i>Ergebnisse der Untersuchung</i>	245
Literaturverzeichnis	253
Materialien	263

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingung
AIA-Entwurf.	Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM (2021) 206 final)
BeckOK	Beck'sche Online-Kommentare
BGBI	Bundesgesetzblatt
BGH	Bundesgerichtshof
CR	Computer und Recht
Diss.	Dissertationsschrift
E.	Erwägungsgrund
EG .	Erwägungsgründe
EPA	Europäisches Patentamt
EPÜ	Übereinkommen über die Erteilung europäischer Patente (Europäisches Patentübereinkommen) vom 5. Oktober 1973 in der Fassung der Akte zur Revision von Artikel 63 EPÜ vom 17. Dezember 1991 und der Akte zur Revision des EPÜ vom 29. November 2000
EU	Europäische Union
f.	folgend
ff.	folgende
GA	Genetic Algorithm
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBI. I S. 466)
GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-

	-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 u. 2 Satz 2 des Gesetzes vom 29. September 2020 (BGBl. I S. 2048) geändert worden ist
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
Habil.	Habilitationsschrift
Harv. J.L. & Tech	Harvard Journal of Law & Technology
Hrsg.	Herausgeber
ICLR	International Conference on Learning Representations
ijEP	International Journal of Engineering Pedagogy
IJSN	International Journal of Security and Networks
JZ	JuristenZeitung
Kap.	Kapitel
KNN	Künstliches Neuronales Netz
MPI	Max-Planck-Institut
NeurIPS.	Conference on Neural Information Processing Systems
NJW	Neue Juristische Wochenschrift
PatG	Patentgesetz in der Fassung der Bekanntmachung vom 16. Dezember 1980 (BGBl. 1981 I S. 1), das zuletzt durch Artikel 4 des Gesetzes vom 8. Oktober 2017 (BGBl. I S. 3546) geändert worden ist
PCT	Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens, unterzeichnet in Washington am 19. Juni 1970, geändert am 28. September 1979, am 3. Februar 1984 und am 3. Oktober 2001
PVÜ	Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums vom 20. März 1883
RD <i>i</i>	Recht Digital
UrhG	Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 1 des Gesetzes vom 28. November 2018 (BGBl. I S. 2014) geändert worden ist

Einleitung in die Untersuchung

Künstliche Intelligenz und die damit zusammenhängenden Technologien sind allgegenwärtig. Spätestens als *OpenAI* den „intelligenten“ Chatbot *ChatGPT* am 30. November 2022 veröffentlichte, ist Künstliche Intelligenz definitiv in der Mitte unserer Gesellschaft angekommen.¹

Es existiert kaum noch ein Industriezweig oder Gesellschaftsbereich, in welchem nicht auf Systeme künstlicher Intelligenz oder zumindest auf lernfähige Algorithmen zurückgegriffen wird. Aber auch auf Gebieten der Kunst in Form von kunstwerkerschaffender Robotik oder Software sowie im Alltag als Staubsaugerroboter sind Technologien der künstlichen Intelligenz (nachfolgend: KI-Technologien) anzutreffen.

Je nach Anwendungsbereich in der Industrie können solche Systeme zu gewichtiger Effizienzsteigerung führen. Die Entwicklung von als intelligent geltenden Programmen ist je nach Einsatzbereich äußerst kostenintensiv. Dies liegt vor allem – aber nicht nur – an der benötigten Datenmenge und deren Aufbereitung.² Deshalb drängt sich aus Investitionsschutzüberlegungen die Frage nach der Schutzfähigkeit von trainierter Künstlicher Intelligenz auf: Wer viel investiert, möchte aus dem Investitionsobjekt auch entsprechend profitieren bzw. die Investition zumindest amortisieren. Dieser Frage nach der Schutzfähigkeit von KI-Technologien wird in vorliegender Arbeit nachgegangen.

A. Gegenstand der Untersuchung

Will man die Schutzfähigkeit eines Rechtsguts untersuchen, ist es notwendig, dieses Rechtsgut klar zu beschreiben. Im Rahmen dieser Arbeit wird die Schutzfähigkeit von KI-Technologien untersucht. Was ist aber mit Künstlicher Intelligenz gemeint? Was mit Technologie?

¹ <https://openai.com/blog/chatgpt>, zuletzt besucht am 9. Mai 2023.

² Statt vieler: KI & Recht kompakt-HOPPE, S. 18; unten Kap. 2., B.

Unter KI-Technologien werden im Rahmen dieser Arbeit Softwareebenen von intelligenten digitalen Systemen verstanden. Digitale Systeme sind Systeme, die in der Lage sind, Information künstlich – genauer: technisch – zu verarbeiten.³ Solche Systeme weisen eine Zweiteilung auf: Sie sind in eine Hardwareebene und in eine Softwareebene aufgeteilt.⁴ Die Hardwareebene ist die physikalische Struktur, auf welcher die Informationsverarbeitung erfolgt. Auf der Softwareebene sind in einer für das digitale System verständlichen Form bzw. Sprache die Regeln festgehalten, nach welchen die Informationsverarbeitung erfolgt.⁵ Ein digitales System gilt nach dem vorliegenden Verständnis als intelligent, wenn seine Softwareebene intelligent ist. Eine Softwareebene gilt als intelligent, wenn sie die Regeln der Informationsverarbeitung im Rahmen ihrer Entwicklung nicht gänzlich von Programmierer:innen vorgegeben erhält, sondern sich diese selbst aneignet oder zumindest die direkt vorgegebenen Regeln autonom weiterentwickelt.⁶ Bei diesen Softwareebenen handelt es sich also um Technologien zur Informationsverarbeitung, die das Forschungsgebiet der Künstlichen Intelligenz hervorgebracht hat. Solche Softwareebenen werden im Rahmen dieser Arbeit als KI-Technologien verstanden und sind damit Untersuchungsgegenstand. Da herkömmliche (nicht intelligente) Rechenmaschinen ebenfalls Systeme zur künstlichen Informationsverarbeitung sind, gilt es diese herkömmlichen (nicht intelligenten) digitalen Systeme von den intelligenten zu unterscheiden, deren Softwareebene Gegenstand vorliegender Untersuchung ist.⁷

Das intelligente digitale System als Ganzes – oder ungenau „KI-System“ – ist hingegen nicht Untersuchungsgegenstand dieser Arbeit. Die Hardwareebene – mit oder ohne Sensorik oder Robotik ausgestattet – wird vorliegend nicht untersucht. Die Hardwareebene fließt nur insofern in die Untersuchung mit ein, als dass sie für die Schutzfähigkeit der Softwareebene ausschlaggebend sein kann.⁸

³ Siehe unten Kap. 1, B.

⁴ Siehe unten Kap. 1, B.

⁵ Siehe unten Kap. 1, B.

⁶ Siehe unten Kap. 1, B., I, II.

⁷ Siehe dazu unten Kap. 1, B., Kap. 2, A.

⁸ Vor allem bei der patentrechtlichen Untersuchung in Kapitel 7.

Stellt man sich also ein mit Sensorik und Robotik ausgestattetes intelligentes digitales System („KI-System“) als intelligenten Organismus vor, interessiert im Rahmen dieser Arbeit stark vereinfacht und ungenau gesprochen lediglich „das Gehirn“ dieses KI-Systems.

Oft schwingt in der Diskussion rund um die Schutzfähigkeit von KI-Technologien auch die Schutzfähigkeit der Erzeugnisse von KI-Technologien mit. Die Untersuchung der Schutzfähigkeit von KI-Erzeugnissen wird für die vorliegende Arbeit soweit möglich ausgeschlossen. Das Charakteristikum der Intelligenz⁹ der untersuchten Technologien bringt es aber mit sich, dass die Thematik rund um KI-Erzeugnisse nicht gänzlich ausgeblendet werden kann. Dies betrifft vor allem die Entwicklung von KI-Technologien. Indem sie sich ab einem bestimmten Zeitpunkt die Regeln selbständig aneignen, erzeugen die Technologien Regeln.¹⁰ Dieser Umstand ist ausschlaggebend dafür, dass die Diskussion um die Schutzfähigkeit von maschinengenerierten Erzeugnissen nicht gänzlich von vorliegender Untersuchung ausgeschlossen werden kann. Dabei wird sich aber lediglich auf den aktuellen Forschungsstand in dieser Diskussion gestützt und auf die Grundsätze der mehrheitlich einstimmigen Lehrmeinungen zurückgegriffen.¹¹

Die Untersuchung der Schutzfähigkeit von KI-Technologien soll Aufschluss darüber geben, inwiefern KI-Technologien Gegenstand eines Schutzrechtes sein können. Es werden sowohl relative als auch absolute Schutzrechte untersucht. Aufgrund des immateriellen Charakters von KI-Technologien drängen sich die Immaterialgüterrechte des Patent- und Urheberrechts als absolute Schutzrechte auf. Der Geschäftsgeheimnisschutz wird ebenfalls in einer Zwischenstellung zwischen absolutem und relativem Schutz untersucht.¹²

⁹ Bzw. der Lernfähigkeit und damit der Autonomie.

¹⁰ Siehe unten Kap.1, B., II.

¹¹ Siehe bspw. unten Kap.8, B., II., 2.

¹² Siehe dazu genauer unten Kap. 9.

B. Forschungsstand

Rechtliche Abhandlungen zu Themen auf dem Gebiet der Künstlichen Intelligenz beginnen, sich zu etablieren, sodass auf gewisse Aspekte dieser Beiträge und bereits bestehende Abhandlungen teilweise zurückgegriffen werden kann. Die bestehenden Abhandlungen weisen verschiedene Schwerpunkte auf. Diese reichen von Haftungs¹³- und Regulierungsfragen¹⁴ über privatrechtliche Probleme beim Einsatz von KI-Technologien¹⁵ bis hin zu Untersuchungen im Schnittstellenbereich zwischen Künstlicher Intelligenz und Immaterialgüterrecht.

Letztere fokussieren aber vorwiegend auf Fragen der Schutzfähigkeit von KI-Erzeugnissen. Hervorzuheben sind dabei die Dissertationen von MAAMAR, GRÄTZ, LINKE und MUHR. Gewisse Überlegungen zur Thematik der Schutzfähigkeit von KI-Erzeugnissen lassen sich *cum grano salis* auch als Anhaltspunkte für vorliegende Arbeit heranziehen. Dies betrifft vor allem einzelne Argumentationen aus der ökonomischen Analyse des KI-Marktes bei MAAMAR.¹⁶ Zu den Dissertationen von GRÄTZ, MAAMAR, LINKE und MUHR gesellen sich noch vereinzelt Abhandlungen zur Schutzfähigkeit von KI-Erzeugnissen in Zeitschriftenaufsätzen und Sammelband- und Handbuchbeiträgen.¹⁷

¹³ Vgl. dazu v.a. ZECH, Gutachten, *passim*.

¹⁴ HACKER/ENGEL/MAURER, *passim*.

¹⁵ MÜLLER, *passim*.

¹⁶ Siehe dazu unten Teil 3.; die ökonomischen Ausführungen von MUHR, S. 101 ff. lassen sich weniger gut für die vorliegende Untersuchung heranziehen. Wo jedoch Überlegungen übertragbar sind, werden sie an entsprechender Stelle jedoch aufgeführt. Ihre Ausführungen gehen von Prämissen betreffend das technische Verständnis sowie betreffend die Schutzfähigkeit von KI-Technologien aus, die hier nicht geteilt werden. Das überrascht jedoch nicht. Ihre Stoßrichtung und Herangehensweise orientiert sich an einem anderen Untersuchungsgegenstand: die Schutzfähigkeit von KI-Erzeugnissen. Dementsprechend anders ist ihre ökonomische Analyse geprägt.

¹⁷ EHINGER/STIEMERLING, CR 2018, 761 ff.; GRÄFE/KAHL, MMR 2021, 121 ff.; HARTMANN/PRINZ; Rechtshandbuch-AI-Kaulartz/Braegelmann/TOCHTERMANN, Kap. 7.3; LAUBER-RÖNSBERG/HETMANK, GRUR Int. 2019, 641 ff.; NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 336 ff.; PAPAŞTEFANOU, CR 2019, 209 ff.; SCHAUB, JZ 7/2017, 342 ff.; SÖBBING, MMR 2021, 111 ff.

Es existieren auch bereits vereinzelte Untersuchungen zur Schutzfähigkeit von KI-Technologien als solche. Dies betrifft unter anderem und vor allem die Dissertationen von GRÄTZ, LINKE und MUHR, die neben der Schutzfähigkeit von KI-Erzeugnissen auch die Schutzfähigkeit von KI-Technologien untersuchen. Allerdings beschränken sich GRÄTZ und MUHR in ihren Untersuchungen auf eine Technologie: die künstlichen neuronalen Netze. In der vorliegenden Arbeit werden aber auch andere KI-Technologien untersucht. So soll versucht werden, ein technologieübergreifendes bzw. -unabhängiges Verständnis der immaterialgüterrechtlichen Schutzfähigkeit zu erhalten. LINKE untersucht demgegenüber zwar verschiedene Technologien¹⁸, beschränkt sich aber auf die Untersuchung der urheberrechtlichen Schutzfähigkeit – weitere Schutzrechte werden nicht untersucht. Die verschiedenen Schutzrechte im Immaterialgüterrecht greifen aber ineinander.¹⁹ Ein generelles Verständnis der Schutzfähigkeit kann nur mittels Betrachtung verschiedener Immaterialgüterrechte erfolgen. LINKE geht summarisch von einem Schutzbedürfnis von KI-Technologien aus.²⁰ Es wird jedoch nicht ausführlich dargelegt, welche Aspekte der Entwicklung und des Wesens von KI-Technologien genau für ein Schutzbedürfnis sprechen. Eine solche genaue Darlegung des Schutzbedürfnisses ist jedoch Voraussetzung, um ein eventuell vorhandenes Schutzniveau überhaupt anhand eines entsprechenden Maßstabs würdigen zu können. Erst aus einer solchen Würdigung ist ein allfälliger politischer Handlungsbedarf eruiierbar.

Die Zeitschriftenaufsätze von EHINGER/STIEMERLING sowie APEL/KAULARTZ lassen sich bei GRÄTZ einordnen: Sie untersuchen jeweils nur eine Technologie. Auch die Arbeit von PAPASTEFANOU wählt keinen übertechnologischen Ansatz. Letzterer untersucht im Unterschied zu den Erstgenannten genetische Algorithmen und nicht neuronale Netze.

Es existiert demnach keine Untersuchung der Schutzfähigkeit von KI-Technologien, die die Schutzfähigkeit verschiedener Technologien unter verschiedenen Schutzrechten beleuchtet. Ein übertechnologischer Ansatz ist aber notwendig, um einen realitätsnahen Gesamtüberblick über die Schutzfähigkeit

¹⁸ Wenn auch vor allem der Untersuchungsgegenstand des Algorithmus unklar bleibt. Siehe dazu in vorliegender Arbeit unten Kap. 1, E.

¹⁹ So selbst auch LINKE, S. 32.

²⁰ LINKE, S. 134 ff. geht bei hohen Investitionsvolumen *eo ipso* von einem Schutzbedürfnis aus.

von KI-Technologien zu erhalten. Erst ein solcher Ansatz kann zusammen mit einer schutzrechtsübergreifenden Untersuchung vor einem ökonomischen Hintergrund eine realistische Einschätzung über das Genügen der Schutzmöglichkeit bzw. das Vorliegen von Schutzlücken liefern. Einen solchen Ansatz verfolgt die vorliegende Untersuchung. Hierfür ist jedoch eine vertiefte Auseinandersetzung mit den Gründen für ein Schutzbedürfnis erforderlich. Die Schutzfähigkeit *de lege lata* kann so überhaupt erst gewürdigt werden. Anhand dieser Würdigung lassen sich Schutzlücken aufzeigen, welche Anknüpfungspunkte für weitere Untersuchungen *de lege ferenda* darstellen. Die entsprechende vertiefte Würdigung des Schutzniveaus *de lege lata* findet zum ersten Mal im Rahmen dieser Arbeit statt.

Zentral wird auch die Abgrenzung zum Schutz von herkömmlichen (nicht intelligenten) Softwareebenen (herkömmliche Computerprogramme). Für diese Abgrenzung wird vorwiegend die Entwicklung in der Rechtsprechung herangezogen, um die ausschlaggebenden Charakteristika für den Schutz von Computerprogrammen herauszuarbeiten.

Ebenfalls neu an der vorliegenden Arbeit ist, dass ein Schwerpunkt auf den Geschäftsgeheimnisschutz gelegt wird. Insbesondere die nach GeschGehG erlaubten Handlungen zur Erlangung des geschützten Geheimnisses werden im Hinblick auf KI-Technologien vertieft betrachtet. Dabei wird ein weiterer Unterschied zu den bereits vorhandenen Arbeiten deutlich: Die vorliegende Untersuchung soll tiefer als die bisherigen Arbeiten in die technischen Grundlagen von KI-Technologien einführen. Ein tiefergehendes technisches Verständnis der untersuchten Technologien ist einerseits entscheidend für die Beurteilung der Schutzfähigkeit und andererseits für die Würdigung der Schutzmöglichkeiten *de lege lata* im Hinblick auf erlaubtes *reverse engineering*. Damit hängen erlaubte Nachahmungshandlungen und Trittbrettfahrer:innenproblematiken zusammen. Die vorliegende Arbeit argumentiert in Abgrenzung zu den vorhandenen Abhandlungen auch mit technischen und nicht bloß juristischen Thesen.

Für die technischen Grundlagen wird vorwiegend auf Literatur aus der Informatik zurückgegriffen. Für allgemeingültige und technologieübergreifende

Grundlagen dienen die Werke von RUSSEL/NORVIG als Grundlage und Anknüpfungspunkt. Einzelne interdisziplinäre Arbeiten zwischen Informatik und Rechtswissenschaften dienen ebenfalls als Grundlage. Das betrifft vor allem die Aufarbeitungen von KONERTZ/SCHÖNHOF.

Zu den Marktstrukturen des KI-Marktes existieren noch wenige Untersuchungen mit immaterialgüterrechtlichem Bezug. In diesem Zusammenhang dient die Untersuchung des MPI unter der Leitung von HILTY/HOFFMANN/SCHUEERER als Ausgangspunkt.

C. Gang der Untersuchung

Ziel der Arbeit ist ein technologieunabhängiges Gesamtbild der Schutzfähigkeit von KI-Technologien zu zeigen. Die Schutzfähigkeit *de lege lata* wird zudem gewürdigt. Für diese Würdigung wird ein innovationsökonomischer Maßstab herangezogen. Innovationsökonomik ergibt sich aus der Wohlfahrtsökonomie und hat Effizienzsteigerung der Gesamtgesellschaft zum Ziel. Diese innovationsökonomisch geprägte Würdigung wird betreffend KI-Technologien Schutzlücken deutlich machen. Aus diesen Schutzlücken wird ein rechtspolitischer Handlungsbedarf zur Schaffung eines KI-Schutzrechtes abgeleitet. Dieses Schutzrecht *de lege ferenda* kann nicht in einer juristischen Abhandlung abschließend vorgeschlagen bzw. ausformuliert werden. Vielmehr werden aus den gewonnen Erkenntnissen Eckpunkte des Schutzrechtes *de lege ferenda* skizziert. Diese können dort effizienzsteigernd eingreifen, wo die *lex lata* Effizienzpotenziale unausgeschöpft lässt. Diese Eckpunkte für ein Schutzrecht *de lege ferenda* können sodann Anknüpfungspunkte für weitere Untersuchungen darstellen.

Dazu werden im ersten Teil einerseits die Begrifflichkeiten definiert und andererseits die notwendigen technischen Grundlagen gelegt. Mithin wird im ersten Teil in die Disziplin der Informatik eingeführt. Der erste Schritt besteht darin, die Begriffe darzulegen, die im Fortgang der Untersuchung verwendet werden. Dabei wird nicht nur herausgearbeitet, was unter Begriffen wie Künstlicher Intelligenz, Algorithmus und Technologie zu verstehen ist, sondern auch der Untersuchungsgegenstand ein- und abgegrenzt. Es wird erläutert, was unter KI-

Technologie zu verstehen ist – dem Gegenstand der vorliegenden Untersuchung. Im zweiten Kapitel werden die Besonderheiten von KI-Technologien in Abgrenzung zu herkömmlichen Softwareebenen aufgezeigt. So wird auch deutlich, dass sich für nicht intelligente Softwareebenen bereits etablierte Grundsätze nicht ohne weiteres auf KI-Technologien übertragen lassen. Zu den Besonderheiten von KI-Technologien gehören neben dem Trainingsschritt sowie der Unabdingbarkeit von Trainings- oder Wissensdaten auch die Entwicklungs- und Funktionsweisen von KI-Technologien. Deshalb werden zum Abschluss des zweiten Kapitels die Entwicklungs- und Funktionsweisen von drei verschiedenen Technologien konkret dargelegt. Die genaue Darstellung der Entwicklungs- und Funktionsweisen ist erstens Voraussetzung für die Subsumtion der Technologien unter die bestehenden Schutzrechte. So zeigt sich beispielsweise, dass das anthropozentrische Verständnis im Patentrecht und im Urheberrecht aufgrund der technischen Grundlagen der einzelnen Technologien herausgefordert wird. Zweitens ermöglicht das genaue Aufzeigen der Entwicklungs- und Funktionsweisen das Eruiieren der Gemeinsamkeiten und Unterschiede verschiedener KI-Technologien. Diese Gemeinsamkeiten und Unterschiede werden bei der Würdigung der bestehenden Schutzmöglichkeiten und den Überlegungen *de lege ferenda* erneut herangezogen und berücksichtigt.

Während im ersten Teil der Arbeit das Faktische dargelegt wird, stellt der zweite Teil der Arbeit den Einstieg in die rechtliche Würdigung des Faktischen dar. Da KI-Technologien immaterielle Güter darstellen, bewegen wir uns bei der vorliegenden Arbeit auf dem Gebiet des Immaterialgüterrechts. Deshalb schafft der zweite Teil ein Grundverständnis des in Deutschland geltenden Immaterialgüterrechts. Neben Begriff und Wesen des Immaterialgüterrechts werden die Rechtfertigungsansätze des Immaterialgüterrechts in der gebotenen Kürze aufgezeigt. Es wird insbesondere das Spannungsverhältnis zwischen Persönlichkeitsschutz und wohlfahrtsfördernden rechtlichen Eingriffen aufgezeigt, wobei heutzutage die ökonomischen Rechtfertigungsargumente überwiegen dürften.

Anknüpfend an diese ökonomischen Rechtfertigungsansätze erfolgt im dritten Teil der Arbeit die ökonomische Analyse des Marktes für KI-Technologien. Die Einführung in die ökonomische Disziplin soll Aufschluss darüber geben, ob aus ökonomischer Perspektive ein Schutzbedürfnis für KI-Technologien überhaupt besteht. Dazu ist es in einem ersten Schritt notwendig, die Grundlagen

für die ökonomische Analyse zu legen. Es wird dargelegt, wie das Zusammenwirken von ökonomischer Analyse und Rechtspolitik funktioniert. Dazu wird das notwendige Grundverständnis der Wohlfahrtsökonomie geschaffen. Dabei wird in die Markttheorien eingeführt und insbesondere werden Marktversagensgründe erläutert, da ein Marktversagen hauptsächlicher Rechtfertigungsgrund für die Schaffung von Ausschließlichkeitsrechten an immateriellen Gütern ist. Eine Untersuchung des Marktes für KI-Technologien auf Marktversagensgründe würde jedoch den Rahmen einer rein juristischen Dissertation überstrapazieren. Dazu wären empirische Erhebungen notwendig, die sich dem traditionellen Gebiet der Rechtswissenschaften entziehen. Es liegen keine ausführlichen ökonomischen Studien zu einem potenziellen Marktversagen auf dem Markt für KI-Technologien vor.²¹ Deshalb werden im dritten Teil der Arbeit in einem nächsten Schritt aus den Marktversagensgründen normative Richtlinien abgeleitet, an denen das Funktionieren bzw. Nichtversagen eines Marktes bewertet werden kann. Diese Richtlinien sind die drei Effizienzziele der statischen und dynamischen Effizienz sowie der niedrigen Kosten im Umgang mit Gütern. Mit diesem Vorwissen wird im sechsten Kapitel der Markt für KI-Technologien konkret betrachtet. Dazu werden zunächst die Charakteristika des Marktes dargelegt, bevor dieser auf Ineffizienzen untersucht wird. Das Ergebnis dieser Untersuchung wird zeigen, dass vor allem im Bereich der statischen Effizienz Ineffizienzen vorliegen und dass die Kosten im Umgang mit KI-Technologien als Güter (ineffizient) hoch sind. In diesem Untersuchungsergebnis wird zumindest ein Indiz für die Schutzbedürftigkeit von KI-Technologien gesehen.

Im vierten Teil der Arbeit wird dieses Schutzbedürfnis mit der Schutzfähigkeit *de lege lata* verglichen. Dazu wird die Schutzfähigkeit von Expertensystemen, genetischen Programmen sowie Künstlichen Neuronalen Netzen getrennt für das Patentrecht, Urheberrecht und Geschäftsgeheimnisrecht betrachtet. Das Ergebnis der Schutzfähigkeitsprüfung wird zeigen, dass die Schutzfähigkeit das ökonomisch begründete Schutzbedürfnis nicht zu befriedigen vermag und sich deshalb Schutzlücken *de lege lata* ergeben. Diese Schutzlücken werden im zehnten Kapitel mittels Würdigung der einzelnen Schutzrechte in Bezug auf KI-

²¹ Eine Ausnahme bildet HILTY/HOFFMANN/SCHUEERER, Max Planck Institute for Innovation and Competition Research Paper 20-02.

Technologien genau umrissen und beschrieben. Es wird gezeigt, dass Entwickler:innen und Anbieter:innen von KI-Technologien über keine Möglichkeit verfügen, ihre Investitionen wohlfahrtsökonomisch effizient zu schützen und zu amortisieren.

Diese Schutzlücken im Hinblick auf einen wohlfahrtsökonomisch effizienten Investitionsschutz dienen im fünften und letzten Teil der Arbeit als Anhaltspunkte für einzelne Überlegungen *de lege ferenda*. Wie bereits erwähnt, kann das Aufzeigen einer konkreten, ausformulierten *de lege ferenda*-Lösung nicht Ziel einer ausschließlich juristischen Arbeit sein. Vielmehr werden mit dem wohlfahrtsökonomisch geprägten juristischen Maßstab einige Überlegungen für ein Schutzrecht angestellt, die an den Schutzlücken anknüpfen. Es handelt sich dabei um Vorschläge, wie diese Schutzlücken unter Berücksichtigung der vorliegenden Wertung gefüllt werden könnten.

Teil 1

Begriffe und Funktionsweisen

Kapitel 1

Einführung in die Begriffe

Technologien, die als künstlich intelligent gelten, sind heutzutage nicht nur in allen Lebens- und Wirtschaftsbereichen anzutreffen, sondern scheinen auch alltagsbestimmend bzw. gar das Wundermittel zur rationalen Lösung zahlreicher Probleme zu sein.¹ Sie prägten nicht nur die jüngste Vergangenheit, sondern in besonderem Maße die Gegenwart – politisch wie gesellschaftlich und auch rechtlich. „Künstliche Intelligenz“, „autonome/digitale/lernfähige Systeme“, „Algorithmen“ – diese Begriffe werden oft im selben Kontext, aber sehr unterschiedlich verwendet.² Umso wichtiger ist es, für den Rahmen dieser Arbeit die Begriffe „digitale Systeme“, „Künstliche Intelligenz“, „KI-Technologie“ und „Algorithmus“ zu trennen, zu definieren und einzuordnen.

A. Digitale Systeme

Digitale Systeme dienen dazu, Informationen technisch zu verarbeiten.³ Informationen können nach ZECH als das Gegenteil von Unbestimmtheit definiert werden.⁴ Die Informationsverarbeitung haben digitale Systeme und natürliche Intelligenzen gemeinsam – natürliche Intelligenzen verarbeiten Informationen mittels eines Organs wie dem Gehirn und digitale Systeme mithilfe eines informationstechnischen Systems.⁵ Um Informationen technisch und damit

¹ Siehe kritisch zu letzterem KEINER, *passim*.

² ZECH, Risiken, S. 7; MÜLLER/KIRCHNER/SCHÜSSLER, S. 86 sprechen gar von einer übermäßigen Verwendung des Begriffs.

³ VDI-Informatiklexikon, S. 196 ff.; ZECH, Gutachten, S. 18; vgl. ausführlich zum Begriff HAUGELAND, S. 52 ff.

⁴ ZECH, Information, S. 13.

⁵ VDI-Informatiklexikon, S. 196 ff.; ZECH, Gutachten, S. 18; siehe für die natürliche Informationsverarbeitung RUSSEL/NORVIG, 3. Auflage, S. 32 ff.; vgl. auch HAUGELAND, S. 52 ff.

künstlich verarbeiten zu können, bedarf es derer Maschinenlesbarkeit. Maschinenlesbarkeit setzt wiederum die Repräsentation der Informationen voraus. In dem sie repräsentiert sind, können Informationen auch kommuniziert werden. Diese Repräsentation ist auf dem Gebiet von KI-Technologien besonders erwähnenswert, da bei gewissen Technologien, wie bspw. den künstlichen neuronalen Netzen, Information implizit repräsentiert wird. Dies im Unterschied zu der klassischen symbolischen – expliziten – Repräsentation.⁶ Die technische Informationsverarbeitung ist es sodann auch, die das Gebiet der digitalen Systeme absteckt: Die Informationstechnologie (kurz „IT“) ist das Technikgebiet, welches sich mit der nicht-natürlichen bzw. künstlichen Generierung, Speicherung, Archivierung und Verwendung von Informationen – kurz: der künstlichen Informationsverarbeitung – befasst.⁷ Damit ahmen digitale Systeme die menschliche Fähigkeit des Rechnens nach.⁸ Mit anderen Worten handelt es sich bei digitalen Systemen um Maschinen, die automatisiert logische Schlüsse ziehen. Automatisiert ist dahingehend zu verstehen, dass die Schlussfolgerungen ohne menschliches Zutun erfolgen – sie verarbeiten Information aufgrund von Regeln. Automatisiert ist dabei von autonomisiert bzw. autonom zu unterscheiden.⁹ Das Schlussfolgern innerhalb von digitalen Systemen erfolgt anhand eines Programms. Das Programm gibt dem digitalen System die Regeln vor, nach welchen die Informationsverarbeitung erfolgen soll. Dieses automatisierte Schlussfolgern ist allen digitalen Systemen gemein – unabhängig davon, ob sie lediglich Informationen verarbeiten oder auch Hardware steuern.¹⁰ Sie zeichnen sich durch die Elemente Steuerung, Speicher, Rechner und elektronische Schaltkreise aus.¹¹ Sollen diese digitalen Systeme auch interaktionsfähig¹² sein, kommt noch ein von der eigentlichen Funktion der Informationsverarbeitung unabhängiges Attribut hinzu: die Kommunikation – also die Übertragung von codierter Information unter Einsatz von Elektrik oder Elektronik.¹³

⁶ Siehe dazu weiter unten Kap. 2, C., II., 4.

⁷ ZECH, Gutachten, S. 19; siehe auch VDI-Informatiklexikon, S. 350.

⁸ VDI-Informatiklexikon, S. 196 ff.; ZECH, Gutachten, S. 19.

⁹ Siehe dazu sogleich Kap. B., II.

¹⁰ VDI-Informatiklexikon, S. 196 ff., S. 545 ff.; ZECH, Gutachten, S. 19.

¹¹ CERUZZI, S. 9.

¹² Sowohl untereinander als auch im Verhältnis Benutzer:in-digitales System.

¹³ CERUZZI, ebenda.

Der Begriff des Systems muss ebenfalls umschrieben werden. Der Systembegriff ist Forschungsgegenstand zahlreicher Wissenschaften.¹⁴ Im Rahmen dieser Arbeit und für den Gegenstand der digitalen Systeme wird davon ausgegangen, dass sich Systeme dadurch auszeichnen, dass sie sich von ihrer Umwelt abgrenzen.¹⁵ Mit anderen Worten handelt es sich bei Systemen um Ausschnitte der Wirklichkeit.¹⁶ Zwar existieren rein gedankliche Systeme, doch diese interessieren im Rahmen dieser Arbeit nicht. Digitale Systeme bestehen aus einer Software- und einer Hardwareebene. Die Softwareebene ist mit der Programmebene gleichzusetzen.¹⁷ Es handelt sich also um die Ebene des digitalen Systems, auf welcher die Regeln repräsentiert sind, nach welchen die Informationsverarbeitung zu erfolgen hat.¹⁸ Die Hardwareebene stellt die physikalische Struktur dar, auf welcher die Informationsverarbeitung erfolgt.¹⁹ Die zunehmende Vernetzung digitaler Systeme und die abnehmende Greifbarkeit bzw. Nachverfolgbarkeit der effektiven Informationsverarbeitungsebenen (Stichworte cloud-computing, Serverfarmen, etc.) führen dazu, dass sich die Abgrenzung von digitalen Systemen als herausfordernd gestalten kann.²⁰ Diese Abgrenzung ist aber nicht unmöglich und bspw. für Haftungsfragen im Zusammenhang mit digitalen Systemen von zentraler Bedeutung.²¹ Besonders wenn es um KI-Systeme als Teilmenge von digitalen Systemen²² geht, ist es wesentlich, zu verstehen, dass auch KI-Systeme über eine physikalische Ebene verfügen – sei dies in Form eines Roboters, vernetzten Computers oder sonstiger Hardwarekomponenten. Mit anderen Worten sind KI-Systeme stets auf einer Hardwarekomponente implementiert.²³ Die schwierige Abgrenzbarkeit der Hardwareebene bei digitalen Systemen²⁴ impliziert sogleich auch, dass bei digitalen Systemen die einzelnen

¹⁴ Siehe bspw. für die Kybernetik KÜPPERS, S. 39 f.; für die Soziologie die Systemtheorie LUHMANNs.

¹⁵ KÜPPERS, S. 39; vgl. für die digitalen Systeme auch ZECH, Gutachten, S. 23 mit Verweis auf ZECH, Information, S. 15; vgl. schließlich auch LUHMANN, S. 68.

¹⁶ ZECH, Information, S. 15.

¹⁷ Siehe zum Programmelement eben hiervor, Kap. 1, A.

¹⁸ ZECH, Gutachten, S. 23 f.

¹⁹ ZECH, Gutachten, S. 24.

²⁰ Siehe auch ZECH, Gutachten, S. 23 f.

²¹ ZECH, Gutachten, 24.

²² Siehe dazu sogleich unten Kap. 1, B.

²³ SCHERER, Harv. J. L. & Tech, 2016, 362.

²⁴ ZECH, Gutachten, S. 24.

Ebenen der Hardware- und der Softwareebene ebenfalls gegeneinander abgegrenzt werden können. Im Zentrum dieser Arbeit steht die Softwareebene. Durch das Aufkommen lernfähiger bzw. autonomer Technologien ist die Informationsverarbeitung auf Softwareebene immer schwerer für den Menschen beschreib- sowie lesbar und schließlich verständlich.²⁵ Das hat vor allem zwei Gründe: Erstens setzen sich solche Systeme die Regeln eigenständig, indem ihnen lediglich das Ziel der Informationsverarbeitung vorgegeben wird.²⁶ Zweitens ist bei vielen solcher lernfähigen Technologien²⁷ die Informationsdarstellung implizit – nicht mehr explizit wie bei den klassischen Programmiermethoden.²⁸

B. Intelligente digitale Systeme

Es wurde aufgezeigt, was ein digitales System ist. Doch was macht ein digitales System intelligent? Wann zählen wir ein digitales System zur Künstlichen Intelligenz?

Künstliche Intelligenz ist ein Forschungsgebiet der Informatik²⁹ und fußt auf dem Versuch, natürliche Intelligenz mittels Technik nachzuahmen. Dies stellt sogleich die klassische Definition von künstlicher Intelligenz dar.³⁰ Das Teilgebiet der Informatik, welches sich mit künstlicher Intelligenz befasst, greift dabei zurück auf Erkenntnisse aus der Philosophie, Mathematik, Wirtschaft, Neurowissenschaften, kognitiven Wissenschaften, Psychologie, Computer Engineering, Kontrolltheorie sowie Kybernetik und Linguistik.³¹ Es wäre also genauer, die Künstliche Intelligenz als interdisziplinäres Forschungsgebiet aufzufassen, welches die Informatik – genauer die Informationstechnologie – mit ihren Technologien umzusetzen versucht. Eine allgemeingültige Definition von

²⁵ ZECH, Gutachten, S. 24 f.

²⁶ Siehe dazu unten Kap. 1, B., I. ff. und Kap. 2, C. zu den konkreten Funktionsweisen.

²⁷ Nicht bei genetisch programmierten Algorithmen.

²⁸ Vgl. dazu bspw. Kap. 2, C., III, 4.

²⁹ Bspw. Rechtshandbuch-AI-KAULARTZ/BRAEGELMANN, Kap. 1 Rn. 9.

³⁰ ZECH, Gutachten, S. 20.

³¹ RUSSEL/NORVIG, 4. Auflage, S. 23 ff.

Künstlicher Intelligenz existiert dabei nicht. Dies liegt einerseits daran, dass es aufgrund der immanenten Ungenauigkeiten als Schlagwort verwendet wird³² – oder um es noch pointierter auszudrücken: Der Begriff der KI wird inflationär verwendet.³³ Andererseits liegt dies an der Mannigfaltigkeit der Funktionsweisen von Technologien, die als Teil der Künstlichen Intelligenz gelten. Hinzu kommt, dass die Grenzen zwischen „herkömmlicher“ und „intelligenter“ Informationstechnologie fließend sind. So finden sich in der Literatur auch entsprechend verschiedene Ansätze, Künstliche Intelligenz zu definieren.³⁴ Auch für den Rahmen dieser Arbeit ist es notwendig, das Gebiet der Künstlichen Intelligenz genauer zu beschreiben, um Technologien zu eruieren, die als künstlich intelligent gelten.

Der Begriff der künstlichen Intelligenz ist keineswegs ein neuer Begriff. Er existiert als Übersetzung von „*artificial intelligence*“ bereits seit den 1950er Jahren. So sprachen MCCARTHY/MINSKY/ROCHESTER/SHANNON in ihrem Forschungsantrag für die *Dartmouth Conference* bereits 1955 von „*artificial intelligence*“.³⁵ Sie stellten die Theorie auf, dass jeder Aspekt des Lernens bzw. jedweder andere Wesenszug von Intelligenz so präzise beschrieben werden könne, dass eine Maschine in die Lage versetzt werden könne, diesen nachzuahmen bzw. zu simulieren. Damit definieren sie Künstliche Intelligenz im klassischen Sinn.³⁶ Allerdings dürfte eine solche Definition zu weit gefasst sein, zumal simple Rechenaufgaben ebenfalls als Nachahmung natürlicher Intelligenz gesehen werden können. Wahrscheinlich würde aber niemand eine durch einen Computer ausgeführte einfache Rechenaufgabe als Form der Künstlichen Intelligenz im heutigen Sinne sehen. Auch wenn MCCARTHY/MINSKY/ROCHESTER/SHANNON zweifelsohne Vordenkerarbeit leisteten, ist die informationstechnische Nachbildung natürlicher Intelligenz wie gesehen lediglich Merkmal von di-

³² So ZECH, Gutachten, S. 20.

³³ Vgl. auch MÜLLER/KIRCHNER/SCHÜSSLER, S. 86.

³⁴ Aufzählung bei Rechtshandbuch-AI-KAULARTZ/BRAGELEMANN, Kap. 1 Rn. 2 ff.

³⁵ MCCARTHY/MINSKY/ROCHESTER/SHANNON, *passim*. Wenn auch das Dartmouth College keine neuen Durchbrüche brachte, gilt es als Geburtsstunde der künstlichen Intelligenz (RUSSEL/NORVIG, 3. Auflage, S. 40 f.).

³⁶ RUSSEL/NORVIG, 3. Auflage, S. 40 f.; s. auch GROTH, K&R 2019, Heft 7-8, Beilage S. 3; soeben Kap. 1, B.

gitalen Systemen und damit höchstens Ausgangspunkt, nicht aber entscheidendes Kriterium zur Klassifizierung eines informationstechnischen Systems als ein solches künstlicher Intelligenz.³⁷ Somit ist festzuhalten, dass die Übernahme von menschlichen Aufgaben bzw. Fähigkeiten durch Maschinen ein Merkmal von digitalen Systemen im Allgemeinen ist.³⁸

Auch ALAN TURING orientierte sich an der Imitation natürlicher Intelligenz. TURING gilt als einer der Pioniere der KI-Forschung und entwickelte 1950 den sog. Turing-Test. Ziel des Tests ist die Determinierung eines Computersystems als intelligent. Dabei interagiert ein Mensch an einem Bildschirm mit einer Instanz via Text. Wobei der Mensch nicht weiß, ob es sich bei der Instanz um die zu testende Maschine oder einen anderen Menschen handelt. Gelingt es dem Menschen nicht herauszufinden, ob es sich bei der Instanz um eine Maschine oder einen Menschen handelt, gilt der Turing-Test als bestanden bzw. die zu testende Maschine als intelligent.³⁹

Unter anderem HERBERGER hinterfragt zwecks Einordnung des Begriffs der künstlichen Intelligenz berechtigterweise die Übersetzung des englischen „*intelligence*“ zu „Intelligenz“. ⁴⁰ Er stellt die Behauptung auf, das deutsche Verständnis des Wortes Intelligenz gehe im Vergleich zum englischen Wort „*intelligence*“ zu weit.⁴¹ LEGG/HUTTER versuchten Maschinenintelligenz zu definieren. Dafür untersuchten sie verschiedene Definitionen von „*intelligence*“.⁴² Im Ergebnis schließen sie, dass „*intelligence*“ am besten als „*ability to achieve goals in a wide range of environments*“ umschrieben wird.⁴³ Nach dem Verständnis von LEGG/Hutter ist also *intelligence* (bzw. Intelligenz) die „*Fähigkeit, in einem breiten Umfeld von Rahmenbedingungen Ziele zu erreichen*“.⁴⁴ Durch die Wahrneh-

³⁷ Ähnlich HERBERGER, NJW 2018, 2826, welcher die Definition „the science of making machines do things that would require intelligence if done by men“ als zirkuläre Definition bezeichnet, welche keinen Erkenntnisfortschritt zur Semantik von „*intelligence*“ bringe.

³⁸ So auch KI-Rechtshandbuch-HEINZE/ENGEL, §10 Rn. 2.

³⁹ TURING, Mind 1950, *passim*.

⁴⁰ HERBERGER, NJW 2018, 2826.

⁴¹ HERBERGER, NJW 2018, ebenda.

⁴² Auflistung in LEGG/HUTTER, 11.

⁴³ LEGG/HUTTER, 12.

⁴⁴ HERBERGER, NJW 2018, 2826.

mung des Umfelds und dadurch, dass sich die handelnde Instanz in diesem Umfeld zurechtfindet bzw. sich diesem anpasst und Ziele erreicht, kann ihr „Intelligenz“ zugesprochen werden.

I. Intelligenz durch Lernfähigkeit

Das Zurechtfinden in einem Umfeld und die damit einhergehende Anpassungsfähigkeit kann bei intelligenten digitalen Systemen auch auf ihre Softwareebenen übertragen werden. Auf der Softwareebene von digitalen Systemen kann dieses Zurechtfinden und die Anpassungsfähigkeit als Lernfähigkeit beschrieben werden. Diese Lernfähigkeit ist sodann auch der wesentliche Unterschied von herkömmlichen digitalen Systemen zu intelligenten digitalen Systemen.⁴⁵ Lernfähigkeit wird im Rahmen dieser Arbeit als Fähigkeit verstanden, sein Verhalten anzupassen und sich damit die Regeln der Informationsverarbeitung basierend auf Daten selbst aufzuerlegen. Während bei herkömmlichen Programmiermethoden die programmierende Person die Regeln der Informationsverarbeitung aufstellt und diese dem digitalen System direkt vorgibt, setzt sich ein intelligentes digitales System diese Regeln selbst.⁴⁶ Es erhält von der programmierenden oder trainierenden Person lediglich eine Vorgabe über das Ziel der Informationsverarbeitung vorgegeben. Darüber hinaus geben die Entwickler:innen in Form von einzelnen Rahmenbedingungen Richtungen und Einschränkungen betreffend die Lösungsfindung quasi als Leitlinien vor. Wie das System innerhalb dieser Leitlinien zum Ziel kommt, ist dem System vereinfacht gesagt selbst überlassen. Es legt die konkreten Rechnungsschritte bzw. die einzelnen Informationsverarbeitungsregeln anhand der ihm zur Verfügung stehenden Daten eigenständig fest bzw. modifiziert diese. Bei der Festlegung der einzelnen Rechenregeln und Lösungsschritte ist das System innerhalb der Rahmenbedingungen frei.⁴⁷

Die Interaktion mit dem Umfeld erfolgt bei intelligenten digitalen Systemen mittels Sammlung, Auswertung und Vergleich von Daten. Dieser Vorgang wird

⁴⁵ ERTEL, S. 191 ff.; KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 2; KI & Recht kompakt-HOPPE, S.5; vgl. auch ZECH, S. 31 ff. ZECH, Risiken, S. 27.

⁴⁶ ERTEL, S. 194.

⁴⁷ Statt vieler: ERTEL, S. 191 ff., insb. 194 ff.; vgl. ZECH, Gutachten, S. 31.

als *Data Mining* bezeichnet.⁴⁸ Hier eröffnet sich ein weiterer Unterschied zwischen künstlicher und natürlicher bzw. menschlicher Intelligenz: ein intelligentes digitales System ist in der Lage, in Daten relevante statistische Merkmale auf eine Art und Weise zu finden, derer sich der Mensch nicht bewusst ist bzw. die sich stark oder gar komplett vom menschlichen analytischen Denken unterscheidet. Anhand dieser Muster passt sich das intelligente digitale System so dann an. Als Beispiel für die andersartige Weise, analytisch Information zu verarbeiten sei das Expertensystem *Deep Blue* von *IBM* genannt. Es handelt sich um das erste Computerprogramm, das einen Schachweltmeister besiegte. Der Schachweltmeister Garry Kasparov beschrieb die Vorgehensweise des Computers als neuartige Intelligenz.⁴⁹ Ein weiteres Beispiel stellt das auf einem künstlichen neuronalen Netz und einer Baumsuche beruhende Programm *AlphaGo* dar, welches zum ersten Mal einen professionellen Go-Spieler schlug.

Das Wissen von intelligenten digitalen Systemen beruht somit auf den in den Trainingsdaten enthaltenen Informationen.⁵⁰ Die Maschine extrahiert dieses Wissen selbständig und lernt dabei.⁵¹ Dies steht im Gegensatz zu herkömmlichen digitalen Systemen, deren Wissen auf demjenigen der programmierenden Person beruht.⁵²

II. *Autonomie durch Intelligenz*

Ein weiterer Begriff, der sich zwischen die Schlagworte Künstliche Intelligenz, Digitalisierung, Big Data und Robotik einfügt, ist derjenige der Autonomie.⁵³ Autonomie heißt wörtlich übersetzt, sich Regeln selbst zu setzen. In Kap. 1, A. haben wir gesehen, dass bei digitalen Systemen die Regeln zur Informationsverarbeitung auf der Softwareebene dargestellt sind. Diese Regeln bestimmen das Verhalten des digitalen Systems. In Kap. 1, B., I. wurde gezeigt, dass

⁴⁸ Beim sog. *Data Mining* wird Wissen aus den Trainingsdaten extrahiert. Gestützt auf diesem Wissen passt sich das intelligente digitale System an und verbessert seine Funktionsfähigkeit, s. ERTEL, 195 f.; genauer zum Training unten Kap. 2, A.

⁴⁹ Vgl. dazu Rechtshandbuch-AI-STIEMERLING, Kap. 2.1 Rn. 12 und RUSSEL/NORVIG, 3. Auflage, S. 53.

⁵⁰ Statt vieler: ZECH, Gutachten, S. 34.

⁵¹ SPECHT/HEROLD, MMR 2018, 41.

⁵² So ZECH, Gutachten, S. 34.

⁵³ ZECH, Gutachten, S. 31.

sich intelligente digitale Systeme diese Regeln selbst schaffen. Indem sich intelligente digitale Systeme die Regeln zur Informationsverarbeitung selbst schaffen, sind sie auch autonom.⁵⁴

Die Autonomie von intelligenten digitalen Systemen ist jedoch nicht grenzenlos. Ebenso wenig ist Autonomie binär entweder gegeben oder nicht gegeben. Vielmehr lassen sich unterschiedliche Autonomiegrade von intelligenten digitalen Systemen ausmachen. Personen, die den Grad an Autonomie eines digitalen Systems beeinflussen können, sind die programmierende und die trainierende Person.⁵⁵ Die programmierende Person ist zuständig für die Architektur der Softwareebene. Es liegt in ihrer Hand, das System überhaupt erst als lernfähig zu gestalten bzw. kann sie durch ihr Schaffen die Grenzen der Lernfähigkeit festlegen.⁵⁶ Die trainierende Person hat auch durch die Wahl der Trainingsmethode Einfluss auf den Autonomiegrad. Je nachdem ob überwacht, unüberwacht oder verstärkend gelernt wird, verfügt das System über unterschiedliche Freiheiten beim Lernen aus Erfahrungen bzw. bei der Festlegung der einzelnen Regeln. Während beim überwachten Lernen die Freiheiten des Systems entsprechend begrenzt sind, sind die Freiheiten und damit die Menge an unerwarteten Lösungen des Systems betreffend die Regelsetzung beim unüberwachten Lernen groß.⁵⁷ Die Trainingsdaten haben einen signifikanten Einfluss auf das Trainingsergebnis und damit auf das fertige Modell. Allerdings erstreckt sich ihr Einfluss nicht darauf, wie autonom bzw. lernfähig das System schließlich ist.⁵⁸

C. Zwischenergebnis zum Intelligenzbegriff in der digitalen Welt

Als Zwischenergebnis kann somit festgehalten werden, dass ein digitales System dann als intelligent gilt, wenn es ausgehend von der Imitation menschlicher

⁵⁴ RUSSEL/NORVIG, 3. Auflage, S. 40; vgl. ZECH, Gutachten, S. 37 m.w.N.

⁵⁵ Vgl. ZECH, Gutachten, S. 38.

⁵⁶ Siehe zum Design der Architekturen weiter unten Kap- 2, C., II., 1. ff.; ZECH, Gutachten, S. 34 f.

⁵⁷ Siehe zu den Trainingsmethoden genauer unten Kap- 2, A.; vgl. ZECH, Gutachten, S. 36.

⁵⁸ Anders ZECH, Gutachten, S. 36.

Fähigkeiten in einem Umfeld Ziele *autonom* erreicht. Autonomie bedeutet dabei, dass sich das System die Regeln der Informationsverarbeitung selbst aneignet – einzig aber immerhin beschränkt durch die von den programmierenden und trainierenden Personen vorgegeben Schranken und Rahmenbedingungen. Nach diesen selbst auferlegten bzw. selbst angeeigneten Regeln richtet sich sodann das Verhalten des Systems in der Anwendungsphase. Sowohl in der Entwicklungs- wie auch der Anwendungsphase ist das intelligente digitale System auf Daten angewiesen; in der Entwicklungsphase, um aus den Daten die Programmierungsregeln zu lernen und in der Anwendungsphase, um die gewünschte Funktion zu erfüllen.⁵⁹ Je nach Ausgestaltung des Systems besitzt das

⁵⁹ Die Definitionen verschiedener Nationen oder Staatenbunde gehen in eine ähnliche Richtung, wenn auch Unterschiede auszumachen sind. So die Bundesregierung Deutschland, die künstliche Intelligenz als „[Techniken] zur Lösung konkreter Anwendungsprobleme auf Basis der Methoden aus der Mathematik und Informatik, wobei die entwickelten Systeme zur Selbstoptimierung fähig sind.“ definiert (KI-Strategie D, S. 4). Das Eidgenössische Departement für Wirtschaft, Bildung und Forschung machte fünf Wesensmerkmale der KI aus: die Fähigkeit, (1) Daten in Komplexität und Menge in einer Form auszuwerten, die mit anderen Technologien nach heutigem Stand nicht möglich wäre; (2) Vorhersagen als wesentliche Grundlage für (automatisierte) Entscheidungen zu erstellen; (3) Fähigkeiten nachzubilden, die mit menschlicher Kognition und Intelligenz in Verbindung gebracht werden; und (4) auf dieser Basis weitgehend autonom zu agieren (KI-Bericht CH, S. 7). Im Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM (2021) 206 final, ab nun: „AIA-Entwurf“) spricht die europäische Kommission von KI-Systemen, legt dabei den Schwerpunkt auf Software und behilft sich mit einer enumerativen Aufzählung: „System der künstlichen Intelligenz“ [...] [bezeichnet] eine Software, die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren“. Für die Verordnung des Europäischen Parlaments und des Rates über die Haftung für den Betrieb von Systemen mit künstlicher Intelligenz wurde aber wiederum folgende Definition gewählt: „KI-System“ bezeichnet ein softwaregestütztes oder in Hardware-Geräte eingebettetes System, das ein Intelligenz simulierendes Verhalten zeigt, indem es unter anderem Daten sammelt und verarbeitet, seine Umgebung analysiert und interpretiert und mit einem gewissen Maß an Autonomie Maßnahmen ergreift, um bestimmte Ziele zu erreichen.“

intelligente digitale System zudem die Fähigkeit, sich auch in der Anwendungsphase noch anzupassen und sich zu optimieren.⁶⁰ Was als „optimal“ gilt, hängt von der Zielsetzung des Systems ab: während bei einer Gedichts-KI möglicherweise lyrische Schönheit als Ziel vorgegeben wurde, ist Effizienzsteigerung das Ziel eines intelligenten digitalen Systems, welches zum Hochfrequenzaktienhandel eingesetzt wird. RUSSEL/NORVIG fassen dieses Zwischenergebnis weiter zusammen und beschreiben intelligente digitale Systeme als rationale Agenten.⁶¹

Aufgrund der Interdependenz zwischen Lernfähigkeit, Intelligenz und Autonomie lassen sich intelligente digitale Systeme auch als autonome oder lernfähige digitale Systeme bezeichnen.⁶² Vorliegend wird mit dem Begriff des intelligenten digitalen Systems fortgefahren, um in der Begrifflichkeit des KI-Gebietes zu bleiben.

D. KI-Technologie

Als KI-Technologien werden im Rahmen dieser Arbeit die Technologien verstanden, die auf der Softwareebene von intelligenten digitalen Systemen zum Einsatz kommen. Technologien also, die das als intelligent geltende Verhalten des Systems überhaupt ermöglichen. Im Rahmen dieser Arbeit ist die Softwareebene von intelligenten digitalen Systemen mit dem Begriff der KI-Technologie gleichzusetzen. Die Technologien, die auf dem Feld der KI zum Einsatz kommen, sind zahlreich und reichen von künstlichen neuronalen Netzen (KNN) über evolutionäre bzw. genetische Algorithmen oder Expertensysteme zu *support vector machines* hin zu zahlreichen anderen Technologien.⁶³ So unterschiedlich die verschiedenen Technologien sind, so unterscheiden sie sich auch in ih-

⁶⁰ Vgl. auch Rechtshandbuch-AI-STIEMERLING, Kap. 2.1 Rn. 3; RUSSEL/NORVIG, 3. Auflage, S. 41.

⁶¹ RUSSEL/NORVIG, 3. Auflage, S. 25 f.; KONERTZ/SCHÖNHOF, S. 32 ff.; vgl. auch Annex I AIA-Entwurf.

⁶² Vgl. Zech, Gutachten, *passim*; MÜLLER, *passim*; im Ergebnis wohl gleich LINKE, S. 127 f., welcher auch auf Lernfähigkeit abstellt, diese aber losgelöst von Intelligenz auffasst.

⁶³ Siehe dazu bspw. RUSSEL/NORVIG, 4. Auflage, Kapitel II bis Kapitel V.

ren Funktionsweisen. Zudem ist davon auszugehen, dass noch zahlreiche weitere Technologien entwickelt und dass bestehende Technologien weiterentwickelt werden.

E. Algorithmus

Ein weiterer im Kontext der Digitalisierung oft (ungenau) verwendeter Begriff ist derjenige des Algorithmus. Umso wichtiger ist es, dessen Bedeutung und das dieser Arbeit zugrunde gelegte Verständnis offenzulegen. Der Algorithmusbegriff wird auch losgelöst von Computerprogrammen verwendet. Im weitesten Sinne kann ein Algorithmus als eine „Beschreibung von Vorschriften [...] [verstanden werden], die sich nach vorgegebenen Schritten abarbeiten lassen.“⁶⁴ Damit stellen auch einfache Handlungsanweisungen wie bspw. Kochrezepte Algorithmen dar.⁶⁵ Auch wenn sich bislang keine allgemeingültige Definition von Algorithmus etabliert hat, überzeugt in der Informatik unter anderem die Definition von CORMEN/LEISERSON/RIVEST/STEIN: „Ein Algorithmus [ist] eine Folge von Rechenschritten, die die Eingabe in die Ausgabe umwandeln.“⁶⁶ Eingabe und Ausgabe erfolgen in Form von Daten. Daten sind Informationen. Damit sind wir beim Algorithmus-Begriff in der Informatik – sinnvollerweise – wieder bei der Informationsverarbeitung. Diese ist wiederum Wesensmerkmal von digitalen Systemen.⁶⁷ Damit ist auch offensichtlich, dass die Verwendung des Algorithmusbegriffes ohne klare Definition keinen Mehrwert schafft. Insbesondere ist die Abgrenzung von Algorithmen zu größer- oder kleinerteiligen Rechneranweisungen problematisch. So kann bspw. ein bestimmter Optimierungs- oder Sortieralgorithmus Teil eines neuronalen Netzes⁶⁸ sein. Gleichzeitig ist das ganze neuronale Netz für sich gesehen auch wieder ein Algorithmus im allgemeinen Sinn. Ein ganzes neuronales Netz kann aber kein Algorithmus im informatischen Sinne sein.⁶⁹

⁶⁴ KONERTZ/SCHÖNHOF, S. 53.

⁶⁵ KONERTZ/SCHÖNHOF, S. 53 mit Verweis auf GOOS, S. 23.

⁶⁶ CORMEN/LEISERSON/RIVEST/STEIN, S. 5.

⁶⁷ Vgl. oben Kap. 1, A.

⁶⁸ Siehe zu den neuronalen Netzen weiter unten Kap. 2, C., II.

⁶⁹ Siehe dazu unten Kap. 2, C., II, 3.; anders demgegenüber LINKE, S. 114 f.

Im Rahmen dieser Arbeit wird der Begriff „Algorithmus“ nur zurückhaltend verwendet und nicht mit Computerprogramm oder Software gleichgesetzt. Nach dem vorliegenden Verständnis sind Algorithmen kleinteiliger als Computerprogramme und Software bzw. sind Teile davon. „Algorithmus“ wird in dieser Arbeit vor allem dann verwendet, wenn es sich um einen *terminus technicus* betreffend eine KI-Technologie handelt. So bspw. „Optimierungsalgorithmus“ beim Training von neuronalen Netzen⁷⁰, „genetischer/evolutionärer Algorithmus“ bei den *genetic algorithms*⁷¹ oder „Builder- und Testalgorithmus“ bei der Entwicklung von genetischen Algorithmen.⁷²

F. Exkurs: Starke und schwache KI

Auf dem Gebiet der künstlichen Intelligenz wird weiter in schwache und starke künstliche Intelligenz unterteilt. Die starke künstliche Intelligenz gilt derzeit als Utopie und umfasst Systeme, welche mindestens dieselben intellektuellen Fähigkeiten besitzen wie ein Mensch. Die schwache künstliche Intelligenz hingegen kann bestimmte Anwendungsgebiete von menschlichem intelligentem Verhalten nachahmen.⁷³ Da die starke KI derzeit Utopie ist und die Begriffe starke vs. schwache KI darüber hinaus auch ungenau bzw. auf verwirrende Art und Weise verwendet werden, finden diese im Fortgang der Arbeit auch keine weitere Verwendung.

⁷⁰ Siehe dazu unten Kap. 2, C., II., 3.

⁷¹ Siehe dazu unten Kap. 2, C., III.

⁷² Siehe dazu unten Kap. 8, B., II.

⁷³ Statt vieler: KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 2 f.; vgl. ZECH, Gutachten, S. 21.

Kapitel 2

Technische Besonderheiten von KI-Technologien

Um die immaterialgüterrechtliche Schutzfähigkeit von KI-Technologien beurteilen zu können, muss in einem ersten Schritt ein Blick auf die Besonderheiten in Entwicklung und Funktionsweise solcher Technologien geworfen werden, die bei intelligenten digitalen Systemen zum Einsatz kommen.

A. Die trainierende Person als neues Subjekt im Entwicklungsprozess

Wie oben in Kapitel 1, C. gesehen, verleiht die Lernfähigkeit einem digitalen System Intelligenz und Autonomie. Diese Lernfähigkeit wird bei der Entwicklung von intelligenten digitalen Systemen beim Training eingesetzt. Nur durch die Lernfähigkeit ist die Entwicklung durch Training statt – bzw. ergänzend zu – Programmierung erst möglich.

Bevor das Training stattfinden kann, müssen die Grundlagen für die Lernfähigkeit gelegt werden. Mit anderen Worten muss das Programm lernfähig ausgestaltet werden. Es müssen also Lösungsstrategien gewählt werden, die das Lernen bzw. die autonome Repräsentation von Zusammenhängen überhaupt erst ermöglichen. Bei KI-Technologien besitzt der:die Programmierer:in weniger Kontrolle über bzw. Einfluss auf das Verhalten des Computerprogramms, während der:die Programmierer:in bei klassischer Programmierung die volle Kontrolle über das Verhalten des Systems behält. Dennoch können der Softwareebene von intelligenten digitalen Systemen durch die Auswahl der Programmarchitektur, deren Verfeinerung wie auch beim Training selbst Grenzen des Lernbaren gesetzt und so das Verhalten des Systems in einem gewissen Maße

bestimmt bzw. eingegrenzt werden.¹ Das Bewusstsein dieses Umstandes ist nicht nur für etwaige Haftungsfragen von Relevanz, sondern auch betreffend die Zuweisung der Schutzrechte.²

Zweck des Trainierens einer KI-Technologie ist, dass das intelligente digitale System später auch die gewünschte Funktion erfüllt. Anders als beim herkömmlichen Programmieren wird beim Training von KI-Technologien die Lösung des Problems nicht als Abfolge von Regelanwendungen auf Fakten dargestellt, sondern als automatisch zu bestimmende mathematische Funktion. Dabei soll die KI-Technologie die Eingaben in die passende Ausgabe umrechnen.³ Die Arten des maschinellen Lernverfahrens sind dabei unterschiedlich. So existieren neben dem überwachten und dem unüberwachten Lernen auch das Lernen durch Verstärkung (auch verstärkendes Lernen oder *Reinforcement Learning* genannt). Die Trainingsarten werden im Folgenden einzeln dargestellt.

Das überwachte Lernen ist die Trainingsart mit der „engsten“ Begleitung der Technologie durch einen Menschen. Bei ihr ist das Trainingsziel bereits bekannt und der:die Trainer:in hält für jede Eingabedatei die korrekte Ausgabedatei bereit.⁴ Mit anderen Worten werden die Trainingsdaten so ausgewählt, dass sie das zu erlernende Wissen und damit die zu erlernenden Regeln enthalten.⁵ Diese Art des Trainings ist vergleichbar mit einem: einer Tennistrainer:in, welche:r neben dem:der Schüler:in steht und dessen:deren Hand bei jedem Schlag führt.⁶ Dies erscheint in der Theorie einfach, da es sich nach einem simplen Frage-Antwort-System anhört. In der Praxis ist dieses Lernverfahren jedoch äußerst aufwendig. Die Dimensionen der Eingabedateien sind enorm⁷ und die Trainingsdaten sind beinahe stets verrauscht.⁸ Die verrauschten Trainingsdaten haben zur Folge,

¹ Statt vieler: ZECH, Risiken, S. 34 ff.

² Siehe dazu weiter unten Teil 5.

³ KI & Recht kompakt-HOPPE, S. 9.

⁴ KI & Recht kompakt-HOPPE, S. 10; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 40; ZECH, Risiken, S. 36.

⁵ ZECH, Risiken, S. 36.

⁶ Beispiel von KI & Recht kompakt-HOPPE, S. 10.

⁷ So rechnet KI & Recht kompakt-HOPPE, S. 11 vor, dass bei einer handelsüblichen Kamera, welche mit 1600 x 1200 Pixeln auflöst, zwecks Bestimmung des Helligkeitswertes eines jeden Pixels eine Reihe von 1'920'000 Zahlen als Eingabe notwendig sind.

⁸ Statt vieler: KI & Recht kompakt-HOPPE, S. 11.

dass nur die Mehrzahl (und nicht alle) der Trainingsdaten näherungsweise (und nicht exakt) die gewünschten Ausgaben erzielt.⁹ Die notwendige Menge an Trainingsdaten und deren Unsauberkeit führt dazu, dass selbst bei den besten Lernprozessen ungenaue, widersprüchliche oder schlicht falsche Ein- und Ausgabe-Paare resultieren. Dies hat wiederum zur Folge, dass die Auswertung der Lernergebnisse durch den:die Trainer:in nur noch statistisch erfolgen kann.¹⁰

Dem überwachten steht das unüberwachte Lernen gegenüber. Es ist die freieste Art des Trainings von KI-Technologien.¹¹ Bei dieser Form werden der untrainierten Software die Trainingsdaten zur Verfügung gestellt, ohne Kennzeichnung dessen, was ein einzelnes Datum für die Aufgabe bedeutet. Die zu trainierende Software identifiziert sodann in den Trainingsdaten Muster und deckt diese auf.¹² Das grundlegende Merkmal des unüberwachten Trainings ist so gleich auch dessen größtes Problem: Da die Muster in den Trainingsdaten unbekannt sind bzw. nicht bekannt ist, welche Muster aufgedeckt werden sollen, ist es auch nicht möglich, zu überprüfen bzw. zu beweisen, dass die von der Software aufgedeckten Muster die Richtigen sind.¹³ Ein weiterer Umstand des unüberwachten Lernens ist der Grad der Abstraktion der Daten. Sie ist derart – für einen Menschen – andersartig bzw. unverständlich¹⁴, dass eine Qualifikation als erfolgreiches oder unerfolgreiches Training nicht möglich ist. Die Bewertung und Überprüfung der Ergebnisse von unüberwachtetem Training einer KI-Technologie erfolgt durch die Anwendung der Trainingsergebnisse.¹⁵

⁹ Statt vieler: KI & Recht kompakt-HOPPE, S. 11.

¹⁰ Statt vieler: KI & Recht kompakt-HOPPE, S. 11 f.

¹¹ KI & Recht kompakt-HOPPE, S. 16; ZECH, Risiken, S. 36; s. auch KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 41.

¹² KI & Recht kompakt-HOPPE, S. 16; ZECH, Risiken, S. 36.

¹³ Statt vieler: KI & Recht kompakt-HOPPE, S. 17.

¹⁴ KI & Recht kompakt-HOPPE, S. 16 f. benutzt folgendes Beispiel: Es wird beim Hören einer Symphonie der Versuch unternommen, die Partitur des Stückes aufzuzeichnen. Wem das gelingt, der wird die Melodien für jedes einzelne Instrument notieren – allerdings in einem komplett neuen, selbst entwickelten Notationssystem. Dies führt dazu, dass auch Personen mit einer hohen musikalischen Ausbildung die Notation nicht nachvollziehen können.

¹⁵ KI & Recht kompakt-HOPPE, S. 17.

Das verstärkende Lernen oder das Lernen durch Verstärkung kann als Mittelweg zwischen dem überwachten und dem unüberwachten Lernen gesehen werden. Hierbei beruht das Trainieren auf Rückmeldung.¹⁶ Die KI-Technologie wird basierend auf ihren Aktionen bewertet. Anhand der Bewertung lernt die Softwareebene, sich stets zu verbessern, um langfristig diejenige Handlungsvariante zu wählen, die der Technologie die beste Note einbringt. Mit anderen Worten sind die zu trainierenden Regeln bekannt (dies als Unterschied zum unüberwachten Lernen), allerdings muss nicht dafür gesorgt werden, dass diese Regeln bereits in den Trainingsdaten enthalten sind.¹⁷ Entscheidendes Programmierungsmerkmal bei dieser Lernmethode ist die Programmierung der Reward-Funktion.¹⁸ Der Technologie werden damit keine Regeln programmiert, sondern viel mehr Ziele, die zu der zu erlernenden Regel führen sollen. Der Technologie soll ermöglicht werden, frei eine Lösung zu finden.¹⁹ Dies wiederum ist dem unüberwachten Lernen ähnlich. Das Lernprogramm hingegen ist wieder dem überwachten Lernen angenähert. Zwar funktioniert dieses nicht anhand der Eingabe-Ausgabe-Beispielen, sondern mit der Reward-Funktion und der Komponente zur Bestimmung der Handlungsmöglichkeiten. Aber da auch hier wieder äußerst große Datenmengen notwendig sind, ist die Nachvollziehbarkeit der Entscheidungen der Technologie wieder nur statistisch, verallgemeinernd möglich.²⁰

B. Daten als *conditio sine qua non*

Das Lernen ist nur durch datengetriebenes Training möglich. Daten sind also die *conditio sine qua non* für die Entwicklung von intelligenten Systemen.²¹

¹⁶ KI & Recht kompakt-HOPPE, S. 13; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 44; ZECH, Risiken, S. 36.

¹⁷ ZECH, Risiken, S. 36.

¹⁸ KI & Recht kompakt-HOPPE, S. 14.

¹⁹ KI & Recht kompakt-HOPPE, S. 14; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 44; ZECH, Risiken, S. 36.

²⁰ KI & Recht kompakt-HOPPE, S. 15.

²¹ KI & Recht kompakt-HOPPE, S. 18; vgl. auch KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 79.

Daten werden deshalb als wichtiger erachtet als die Auswahl der zu programmierenden Programmabfolgen.²²

Wie oben aufgezeigt, werden für das Training von KI-Technologien hunderttausende bis Millionen Datensätze nötig.²³ Diese Daten müssen nicht nur entsprechend dem gewünschten Programmresultat ausgewählt werden, sondern auch kuratiert²⁴ und – bei der Form des überwachten Lernens – auch annotiert werden. Die Qualität der Trainingsdaten ist für das Ergebnis des Trainings und mithin der KI-Technologie schließlich ausschlaggebend. Dies setzt voraus, dass sie das zu lösende Problem repräsentativ und in möglichst allen Varianten enthalten.²⁵ Der Datensammlung und -aufbereitung kommt somit enormer Wert zu, was die Daten wiederum kostbar werden lässt. Die Quellen der Daten könnten zudem unterschiedlicher nicht sein – von Daten aus Sozialen Medien über Textdaten aus Online-Bibliotheken bis hin zu Daten aus Straßenaufnahmen.

C. Funktionsweise intelligenter digitaler Systeme anhand dreier Beispiele

Es gibt verschiedene Arten bzw. Funktionsweisen von intelligenten digitalen Systemen. Dazu zählen Künstliche Neuronale Netze (KNN)²⁶, *Support Vector Machines*²⁷ oder *Genetic Algorithms* (GA) bzw. auf diesen aufbauend: genetische Programme²⁸. Je nach Ansicht werden auch Expertensysteme – korrekter- und konsequenterweise – als KI-Technologie betrachtet.²⁹ Nachfolgend sollen die Funktionsweisen von Expertensystemen, KNN und genetischen Algorithmen erläutert werden. Die unterschiedlichen Funktionsweisen sind entscheidend für die Beurteilung der Schutzfähigkeit der Technologien.

²² So z.B. RUSSEL/NORVIG, 3. Auflage, S. 52.

²³ KI & Recht kompakt-HOPPE, S. 18.

²⁴ Bspw. müssen die Daten mit dem zu trainierenden Programm kompatibel sein, oder Datensätze mit vielen Dimensionen müssen in ihren Dimensionen verringert werden.

²⁵ KI & Recht kompakt-HOPPE, S. 19; KI-Rechtshandbuch-NIEDERÉE/NEJD, § 2 Rn. 95 ff.; ZECH, Risiken, S. 37.

²⁶ Statt vieler: KI-Rechtshandbuch-NIEDERÉE/NEJD, § 2 Rn. 58 ff.

²⁷ Statt vieler: KI-Rechtshandbuch-NIEDERÉE/NEJD, § 2 Rn. 51 f.

²⁸ Statt vieler: PAPASTEFANOU, CR 2019, 209 ff.

²⁹ Siehe dazu sogleich Kap. 2.

I. Expertensysteme

Expertensysteme haben zum Ziel, Spezialwissen und die Entscheidungsfindung von Fachleuten auf einem Aufgabengebiet künstlich darzustellen.³⁰ Dabei wird davon ausgegangen, dass menschliche Experten ihre Schlussfolgerungen aus Einzelkenntnissen ableiten. Neben diesen Einzelkenntnissen sind zwecks Lösungsfindung Strategien notwendig, mit welchen die Probleme überhaupt gelöst werden können. Expertensysteme bestehen deshalb aus einer Wissensbasis und einer Inferenzmaschine (mit Dialogkomponente).³¹ In der Wissensbasis sind die Lösungen zu verschiedenen Problemen hinterlegt – mit anderen Worten ist das Expertenwissen (die Einzelkenntnisse) in der Wissensbasis repräsentiert.³² Es handelt sich konkret bspw. um Diagnosen und Therapiestrategien im Medizinbereich³³ oder Einstellungsoptionen für Transformatorstationen in der Energieversorgung³⁴. Getrennt von der Wissensbasis finden sich die Problemlösungsstrategien in Form von Regeln in der Inferenzmaschine. Die Inferenzmaschine wird über eine Dialogkomponente von den Nutzer:innen bedient.³⁵

Die Wissensbasis wird in Expertensystemen streng von den Problemlösungsstrategien in der Inferenzmaschine getrennt.³⁶ Dies soll einerseits die Weiterentwicklung bzw. das Erforschen von Expertensystem begünstigen. Durch die Trennung von Wissens- und Problemlösungskomponenten können nämlich die Problemlösungsstrategien unabhängig vom spezifischen Anwendungsgebietes weiterentwickelt werden. Andererseits und vor allem unterscheidet die Trennung von Wissens- und Problemlösungskomponenten Expertensysteme von herkömmlichen Computerprogrammen. Bei letzteren werden die Probleme Schritt für Schritt in einer von den Programmierer:innen fest vorgegebenen Reihenfolge abgearbeitet. Die Programmierenden legen fest, „was getan wird und in welcher Reihenfolge es getan wird“³⁷. Bei Expertensystemen ist lediglich mittels Regeln festgelegt, was in welcher Situation geschehen soll. Die Reihenfolge, in

³⁰ PUPPE, S. 2.

³¹ KKI-LINKE, S. 41.

³² PUPPE, S. 2 ff.

³³ PUPPE, S. 161 ff.

³⁴ STYCZYNSKI/RUDION/NAUMANN, S. 243 ff.

³⁵ PUPPE, S. 12 ff.

³⁶ PUPPE, S. 2 ff., 12 ff.

³⁷ PUPPE, S. 3.

welcher die Problemlösungsstrategien angewandt werden, ist nicht vorgegeben und der Maschine überlassen.³⁸ Die Inferenzmaschine fungiert dabei als Experte. Sie stellt auf Grundlage der Wissensbasis und den ihr zur Verfügung stehenden Problemlösungsstrategien Rückfragen an die Nutzer:innen und schlägt diesen schließlich eine Entscheidung vor.³⁹

Von bloßen Datenbanken unterscheiden sich Expertensysteme dadurch, dass ihr Wissen nicht nur abgefragt, sondern auch zur Problemlösung herangezogen werden kann. Mit anderen Worten soll zwecks Lösungsfindung mit dem Wissen bzw. den Wissensdaten interagiert werden.⁴⁰ Die Wissensbasis ist somit von der Datenebene dahingehend abgetrennt, dass sie auch für einen Computer lesbare Anweisungen über die Wissensverwendung enthält und somit anders als Daten konkrete Steuerungsanweisungen an ein digitales System richten. So kann das Expertensystem das Wissen autonom interpretieren.⁴¹ Dies erfordert aber, dass das Wissen in geeigneter Weise repräsentiert wird: mit entsprechenden Steuerungsanweisung bzw. interoperabel. Die Interoperabilität bezieht sich dabei auf das Verhältnis Wissensbasis-Inferenzmaschine sowie die einzelnen Elemente in der Wissensbasis untereinander.⁴²

Weil Expertensysteme in der Lage sind, Wissen autonom zu interpretieren, verfügen sie über die Fähigkeit, durch autonome Interpretation der in der Wissensbasis gespeicherten Einzelkenntnissen auch neues Wissen herzuleiten.⁴³ Sie sind demnach nicht nur betreffend die Informationsverarbeitung autonom. Sie sind auch in der Lage, sich autonom weiterzuentwickeln. Damit sind Expertensysteme konsequenterweise auf dem Gebiet der Künstlichen Intelligenz zu verorten bzw. als intelligente digitale Systeme zu qualifizieren.⁴⁴ Expertensystemen wird nicht die konkrete Lösungsstrategie für jedes Problem vorgegeben bzw.

³⁸ PUPPE, S. 2 ff.

³⁹ PUPPE, S. 12 ff.; vgl. auch KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 15; KKI-LINKE, S. 41.

⁴⁰ PUPPE, S. 4.

⁴¹ PUPPE, S. 5.

⁴² PUPPE, S. 2 ff.

⁴³ PUPPE, S. 123 ff.; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 15.

⁴⁴ Vgl. das Wesensmerkmal der autonomen Verhaltenssteuerung von intelligenten digitalen Systemen oben Kap.1, B., II.; vgl. PUPPE, S.168 ff.

programmiert. Sie sollen vielmehr basierend auf dem ihnen zur Verfügung gestellten Regelset autonom Lösungen zum konkreten Problem finden.⁴⁵

Von Expertensystemen erhofft man sich eine hohe Problemlösungskompetenz in ihrem Anwendungsbereich.⁴⁶ Die Anwendungsbereiche sind aber regelmäßig sehr begrenzt bzw. sehr spezifische Fachbereiche. Das heißt aber nicht, dass es sich dabei um einfache Anwendungsgebiete handelt. Das Gegenteil ist der Fall. Die Anwendungsfelder sind oft komplex. Es sind Gebiete, welche sich kaum oder nur sehr schwer mathematisch beschreiben lassen.⁴⁷ So werden Expertensysteme bspw. in der Medizin eingesetzt, wo sie Fachkräfte im Gesundheitsbereich bei der Diagnose unterstützen.⁴⁸ Auch auf Gebieten der Technik, wie bspw. als Überwachungssysteme bei der Energieversorgung, finden Expertensysteme Anwendung.⁴⁹ Da Expertensysteme im Grunde dennoch „einfache“ Wenn-dann-Systeme sind,⁵⁰ dürften sie eher am „unteren Ende“ des KI-Spektrums anzusiedeln sein – sowohl betreffend die Vielseitigkeit des Einsatzgebietes als auch betreffend die Autonomie. Dies liegt vor allem an der im Vergleich zu anderen KI-Technologien begrenzten Lernfähigkeit. Hauptnachteil von Expertensystemen ist ihr begrenzter Datenumfang und dass ihnen oft nur Daten aus der unmittelbaren Problemumgebung eingespeist werden.⁵¹ Sie finden das Ende ihres Potenziales dort, wo sie Allgemeinwissen simulieren sollen. Dazu sind sie nicht in der Lage.⁵²

II. Künstliche Neuronale Netze

Künstliche neuronale Netze (KNN) sind wohl die derzeit am stärksten untersuchte Technologie auf dem Gebiet der künstlichen Intelligenz.⁵³ Dies liegt mitunter daran, dass sie durch ihren mehrschichtigen Aufbau dazu in der Lage

⁴⁵ PUPPE, S. 3 ff.

⁴⁶ PUPPE, S. 3 f.

⁴⁷ PUPPE, S. 180.

⁴⁸ PUPPE, S. 180.

⁴⁹ Vgl. dazu sehr ausführlich STYCZYNSKI/RUDION/NAUMANN, *passim*.

⁵⁰ PUPPE, S. 2.

⁵¹ Zu den Grenzen von Expertensystemen ausführlich PUPPE, S. 181 ff.

⁵² PUPPE, S. 185 f.

⁵³ Z.B. KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 56; EHINGER/STIEMERLING, CR 2018, 761.

sind, nichtlineare Probleme zu lösen und deshalb mehr- bzw. hochdimensionale Daten verarbeiten können.⁵⁴ Sie sind prägende Technologie auf dem Gebiet des sogenannten *deep learnings*.⁵⁵

1. Von Neuronen über Schichten zur Architektur

KNN basieren auf dem Versuch, das menschliche Gehirn mittels Vernetzung künstlicher Neuronen nachzubilden.⁵⁶ Daher stammt auch ihr Name. Sie bestehen aus miteinander verbundenen künstlichen Neuronen⁵⁷, die wiederum in Schichten angeordnet sind.⁵⁸ Es existieren ein- und mehrschichtige KNN. Während die Lernfähigkeit einschichtiger KNN sehr begrenzt ist,⁵⁹ sind die Möglichkeiten betreffend Lernfähigkeit von mehrschichtigen KNN vielversprechend.⁶⁰ Die verschiedenen Schichten eines mehrschichtigen KNN lassen sich in die Eingangs- oder Eingabeschicht (*input layer*), die Ausgangs- oder Ausgabeschicht (*output layer*) und die Zwischenschichten einteilen. Die Zwischenschichten werden verborgene Schichten (*hidden layers*) genannt, weil ihre Informationsverarbeitung bei einer äußerlichen Betrachtung nicht beobachtet werden kann.⁶¹ Verschiedene KNN können wie ihre jeweiligen Schichten auch gänzlich unterschiedlich aufgebaut bzw. gestaltet werden. Bei der Festlegung der Anzahl und Verknüpfung von Neuronen, Kanten, Schichten und Rückkopplungen sind die entwickelnden Personen gänzlich frei.⁶² Zuständig für die Um-

⁵⁴ RUSSEL/NORVIG, 4. Auflage, S. 801.

⁵⁵ RUSSEL/NORVIG, 4. Auflage, S. 801.

⁵⁶ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 7.

⁵⁷ Passender wäre „Prozessoren“, siehe dazu unten Kap. 2, C., II., 2.

⁵⁸ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 34.

⁵⁹ Vgl. RUSSEL/NORVIG, 3. Auflage, S. 848 ff.

⁶⁰ Vgl. KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 18 ff.

⁶¹ PRIDDY/KELLER, S. 8; KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 34.

⁶² GOODFELLOW/BENGIO/COURVILLE, S.151; PRIDDY/KELLER, S. 9.

setzung des Designs bzw. für die „Herstellung“ der Netzstruktur sind die Programmierer:innen.⁶³ Sind die verschiedenen Parameter⁶⁴ festgelegt und programmiert, liegt die Netzstruktur vor.⁶⁵ Die Netzstruktur kann auch als Architektur bezeichnet werden⁶⁶ und stellt als solche ein Modell dar und wird im Rahmen dieser Arbeit als untrainiertes KNN bezeichnet.

Ist die Architektur eines KNN erstellt, kann sie für verschiedene Zwecke verwendet werden – die endgültige Funktion des KNN wird durch das Training des Modells festgelegt.⁶⁷ Es existieren auch verschiedene vorgefertigte Architekturen – kostenpflichtige wie auch *open source* und *open access* –, die erlangt und individuell trainiert werden können.⁶⁸

2. Funktionsfähigkeit durch Neuronengewichtung

Ebenso wichtig für die Beurteilung der immaterialgüterrechtlichen Schutzfähigkeit wie der Aufbau von KNN ist deren Funktionsweise. Diese wird nachfolgend erläutert, bevor auf das Training von KNN eingegangen wird. Die Ansätze im Training lassen sich einfacher nachvollziehen, wenn das Grundprinzip der Funktionsweise von (trainierten) KNN bekannt ist.

Jede Eingabe in ein KNN durchläuft das Netz und führt zu einer entsprechenden Ausgabe.⁶⁹ Dabei ist zentral zu wissen, dass jedes Neuron einen Aktivierungszustand hat und dass die Verbindungen zwischen zwei Neuronen (Kanten) gewichtet sind (Verbindungsgewichte).⁷⁰ Ein solches Gewicht bestimmt die Stärke des Informationsflusses von Neuron zu Neuron. Es verstärkt oder schwächt das Aktivierungssignal, das von einem Neuron entlang einer Kante

⁶³ Statt vieler: HARTMANN/PRINZ, S. 770 f.; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 56 ff.

⁶⁴ Anzahl und Anordnung der Neuronen, (Rück)kopplungen, Pfade, Kanäle und Ebenen sowie Schichten.

⁶⁵ PRIDDY/KELLER, S. 9.

⁶⁶ GOODFELLOW/BENGIO/COURVILLE, S.193 f.

⁶⁷ AGGARWAL, S. 2; HARTMANN/PRINZ, S. 771.

⁶⁸ Vgl. für *convolutional neural networks* AlexNet, GoogLeNet und ResNet.

⁶⁹ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 36 ff.; PRIDDY/KELLER, S. 8 ff.

⁷⁰ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 3; vgl. auch KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 58 ff.

zum anderen geleitet wird um einen bestimmten Faktor. Dieser Faktor entspricht dem (Verbindungs)gewicht.⁷¹

Die Eingabe steuert, ausgehend von der Eingangsschicht, die verschiedenen Neuronen an. Sofern die Aktivierungsschwelle eines Neurons überschritten ist, aktiviert dieses Neuron ein weiteres Neuron der nachgehenden Schicht. Erreicht der Input wiederum die Aktivierungsschwelle des nachgeschalteten Neurons, leitet es seinen Aktivierungszustand an das nachgeschaltete Neuron. Falls der Input die Schwelle nicht erreicht, hat die Kettenreaktion an dieser Stelle – genauer: an diesem Neuron – ein Ende. Weil aber zu Beginn in der Eingabeschicht mehrere Neuronen gleichzeitig angesteuert werden, laufen verschiedene solcher Kettenreaktionen parallel.⁷² Dies setzt sich so fort, bis die Ausgabebene erreicht ist und eine Ausgabeinformation ausgegeben wird.⁷³ Dabei sind die Aktivierungszustände (Schwellenwerte) an und die Gewichtungen zwischen den Neuronen ausschlaggebend dafür, ob das nachgeschaltete Neuron angesteuert wird. Somit sind die Schwellenwerte, v.a. aber die Gewichtungen für die Kettenreaktion und damit die Funktion des KNN insgesamt entscheidend.⁷⁴ Die Ausgabebene muss so gestaltet sein, dass sie für die Aufgabe auch eine sinnvolle Form der Repräsentation aufweist.⁷⁵

Ein einzelnes Neuron kann als einfacher Prozessor verstanden werden. Es berechnet aus den (summierten) Eingabewerten und je nach dem aus weiteren Parametern eine Ausgabe.⁷⁶ Das Neuron berechnet also anhand der Aktivierungsfunktion aus der Eingabe, eventuellen weiteren Parametern und je nachdem einer Rückführung der aktuellen Aktivierung des Neurons (Rückkopplung) die neue Aktivierung des Neurons. Anhand dieser neuen Aktivierung berechnet das Neuron über die Ausgabefunktion die Ausgabe des Neurons. Diese Ausgabe wird sodann an das nachgeschaltete Neuron geleitet, wo diese Ausgabe als Eingabe wiederum via eigener Aktivierungsfunktion in eine neue Ausgabe dieses

⁷¹ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 35.

⁷² KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 8 und insb. 36 ff.

⁷³ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 36 ff.

⁷⁴ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 36 ff.

⁷⁵ GOODFELLOW/BENGIO/COURVILLE, S. 167, 173, insb. 177 ff.

⁷⁶ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 36.

nachgeschalteten Neurons umgerechnet wird.⁷⁷ Die Argumente der Aktivierungsfunktion innerhalb eines Neurons können für jedes Neuron innerhalb eines KNN unterschiedlich sein. Meistens sind es zwei Argumente: die Eingabe und ein zusätzlicher Parameter, der ein Schwellenwert sein kann. Die Ausgabe-funktion dient lediglich der (meist) linearen Übertragung der Ausgabe in einen bestimmten Wertebereich. Damit ist auch ersichtlich, warum die Schwellenwerte innerhalb der Neuronen sowie die Gewichte zwischen den Neuronen (auf den Kanten) für das Funktionieren des KNN so wichtig sind. Beide haben einen direkten Einfluss auf die Aktivierung oder Nicht-Aktivierung eines Neurons. Ein Gewicht ist somit – vereinfacht gesagt – ein Multiplikator des Signals, das entlang der Kante von einem Neuron zum nächsten geleitet wird. Ein Neuron kann mehrere Eingabekanten haben bzw. können mehrere Kanten zu einem Neuron führen.⁷⁸ In solchen Fällen spricht man von einer Summe der Gewichte, weil auf jeder Kante das Eingangssignal anhand des Gewichts multipliziert und alle Eingabekanten summiert werden, die ein und dasselbe Neuron ansteuern.⁷⁹

3. Einstellen der Gewichte als Training

Vor dem Training sind alle Gewichte willkürlich auf Werten zwischen „0“ und „1“ eingestellt.⁸⁰ Das untrainierte Netz kann noch keine Funktion erfüllen und erzeugt lediglich ein sogenanntes Rauschen.⁸¹ Im Training werden die Gewichte und die Parameter innerhalb eines Neurons so lange eingestellt bis das Ergebnis befriedigt.⁸² Bei typischen Netzwerkgrößen müssen Millionen von Gewichten eingestellt werden.⁸³ Hinzu kommt ein weiterer Umstand: Aufgrund der Tiefschichtigkeit von KNN kennt die trainierende Person lediglich die Ein- und die Ausgabe. Sie kennt in aller Regel nicht den Grund, weshalb die Ausgabe so dargestellt wird, wie sie dargestellt wird. Aus diesen Gründen kann die Einstellung der Gewichte nicht manuell erfolgen. Sie erfolgt automatisiert unter

⁷⁷ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 36.

⁷⁸ Vgl. PRIDDY/KELLER, S. 8.

⁷⁹ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 39.

⁸⁰ KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 69.

⁸¹ Statt vieler: KI-Rechtshandbuch-HEINZE/WENDORF, § 9 Rn. 49.

⁸² KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 40 ff.; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 56 ff.

⁸³ KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 66.

Zuhilfenahme eines sogenannten Optimierungsalgorithmus.⁸⁴ Die Gewichte werden von der Ausgabe her angepasst – also rückwärts, ausgehend von der Ausgabeschicht. Dies erfolgt mittels sogenannter *Backpropagation*.⁸⁵ Dabei werden die Änderungen schrittweise rückwärts in das Netz propagiert, indem anhand der Trainingsdaten die Eingabe mit der Ausgabe verglichen wird und die Fehler minimiert werden.⁸⁶ Diese als Fehler bezeichnete Abweichungen des Ist-vom Soll-Zustand werden mithilfe der sogenannten *loss function* formalisiert.⁸⁷ Das *trial and error* Verfahren in der *Backpropagation* wird dadurch optimiert, dass ein als *Stochastic Gradient Descent* bezeichnetes Verfahren angewandt wird.⁸⁸ Mit anderen Worten erfolgt die Auswahl der in der *Backpropagation* zu treffenden Entscheidungen annäherungsweise (also nicht exakt) unter Zuhilfenahme stochastischer und somit statistischer Regeln.⁸⁹ Diese Regeln sind im Optimierungsalgorithmus implementiert und geben vor, an welcher Stelle im Netz welche Gewichte wie angepasst werden. Der Optimierungsalgorithmus ist für sich gesehen wiederum eine Software bzw. ein Computerprogramm⁹⁰. Die Anpassung der Gewichte erfolgt ausgehend vom Optimierungsalgorithmus anhand der Trainingsdaten und – je nach Trainingsmethode – des Trainingsfeedbacks.⁹¹

Der Optimierungsalgorithmus ist nicht Teil des KNN und ist in der Anwendungsphase nicht für die Funktionsfähigkeit des trainierten KNN notwendig.⁹²

⁸⁴ AGGARWAL, S. 21, S. 107 ff.; ROJAS, S. 149 ff.

⁸⁵ AGGARWAL, S. 21 ff., S. 107 ff.; ROJAS, S. 149 ff.

⁸⁶ AGGARWAL, S. 107 ff.; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 70.

⁸⁷ AGGARWAL, S. 7.

⁸⁸ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 21 ff.; ROJAS, S. 149 ff.; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 70.

⁸⁹ AGGARWAL, S. 107 ff.; KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 21 ff.; ROJAS, S. 227 ff.

⁹⁰ Im Sinne einer Steuerung eines Computers mittels Regeln, welche eine entsprechende Funktion erfüllen, s. auch später Kap. 8, A., III., 1. ff. zum Computerprogrammbegriff im urheberrechtlichen Sinn.

⁹¹ AGGARWAL, S. 107 ff.; KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 21 ff.; ROJAS, S. 149 ff.

⁹² Als Beispiel kann dabei der Vorgänger von gpt3 (<https://openai.com/api/>), gpt2, dienen. Das anwendungsbereite Modell von gpt2 wurde bspw. auf www.huggingface.co veröffentlicht.

Der Optimierungsalgorithmus lässt sich untechnisch gesprochen wie ein Rezept für ein Gericht verstehen. Dem fertigen Gericht ist das Rezept nicht zu entnehmen und das Rezept wird auch nicht mehr benötigt, nachdem das Gericht zubereitet wurde. Natürlich besteht die Möglichkeit, das Rezept beim Servieren des Gerichts ebenfalls zum Gericht dazuzulegen bzw. den Optimierungsalgorithmus in der Anwendungsphase ebenfalls zu veröffentlichen. Notwendig ist das aber nicht.

Das Training kann folglich so verstanden werden, dass entsprechend den Regeln des Optimierungsalgorithmus rückwärts von der Ausgangsschicht Schritt für Schritt bzw. Schicht für Schicht und annäherungsweise die Gewichte entlang der Kanten angepasst werden. Dieses Vorgehen wird iterativ wiederholt, bis das Erlernte befriedigt oder mit anderen Worten: bis das KNN die gewünschte Funktionsfähigkeit zeigt. Ab diesem Zeitpunkt wird das KNN für den Fortgang dieser Arbeit als trainiertes KNN bezeichnet. Es setzt sich zusammen aus der Architektur (untrainiertes KNN) und den eingestellten Schwellenwerten und Verbindungsgewichten. Die Informationen über die Schwellenwerte und die Verbindungsgewichte werden als Gewichtungsinformationen sowie *weights* bezeichnet.

Der kreative menschliche Einfluss auf das Trainingsergebnis und damit die Funktion des trainierten KNN ist also beschränkt. Zwar kann der Mensch einerseits die Trainingsdaten auswählen und – je nach Trainingsform – diese auch annotieren.⁹³ Diese Auswahl ist aber eher von Funktionalitätsüberlegungen als von gestalterischen Motiven getrieben. Die trainierende Person wird die Daten nicht aus kreativen, gestalterischen Überlegungen auswählen, sondern aufgrund ihrer Geeignetheit bzw. anhand dessen, ob sie die zu erlernende Information beinhalten.⁹⁴ Auch das Design des untrainierten KNN bzw. der Architektur ist

(<https://huggingface.co/gpt2>). Details zum Training (wie bspw. der Optimierungsalgorithmus) sowie die Trainingsdaten wurden nicht mitveröffentlicht, <https://huggingface.co/gpt2>. Das Modell kann aber weiterverwendet werden. Bspw. kann es mittels *finetuning* sogar umtrainiert werden (bspw.: <https://towardsdatascience.com/how-to-fine-tune-gpt-2-for-text-generation-ae2ea53bc272>, jeweils zuletzt besucht am 9. Mai 2023).

⁹³ Vgl. oben Kap. 2, B.

⁹⁴ GOODFELLOW/BENGIO/COURVILLE, S. 236 ff.

weniger von gestalterischen als viel eher von funktionalen Überlegungen gezeichnet.⁹⁵ Der menschliche Einfluss erschöpft sich in der Bestimmung der Tiefe des Netzwerkes (Anzahl verborgener Schichten) und der Breite sowie die Ausgestaltung⁹⁶ der jeweiligen Schichten (Anzahl der Neuronen innerhalb einer Schicht).⁹⁷ Dabei reicht schon das Implementieren einer verborgenen Schicht, um das KNN trainierbar und damit lernfähig zu gestalten.⁹⁸

Andererseits kann der Mensch den Optimierungsalgorithmus immerhin auswählen oder selbst programmieren. Aber auch hier handelt es sich weniger um gestalterische als um Zweckmäßigkeitüberlegungen. Die statistischen und stochastischen Regeln geben die Funktionsweise des Optimierungsalgorithmus mehrheitlich vor.⁹⁹ Mit anderen Worten bestimmen die Gesetzmäßigkeiten der Mathematik über die Funktionsweise des Optimierungsalgorithmus. Der Mensch kann dahingehend eingreifen, indem er bestimmt, wie groß die einzelnen Schritte sein sollen, in welchen die Gewichte eingestellt werden oder worauf sich der Optimierungsalgorithmus beziehen soll.¹⁰⁰ Die Schrittgröße hat einen Einfluss auf die Genauigkeit des Trainingsergebnisses. Je kleiner die Trainingschritte, desto länger dauern die Iterationen und desto höher die beanspruchten Rechenkapazitäten.¹⁰¹ Letztlich ist aber entscheidend, dass mittels Optimierungsprozesses jedes Neuron einmal eingestellt wurde.¹⁰² Damit ist auch hier deutlich: die vom Menschen zu entscheidenden Einzelheiten sind nicht von kreativen Möglichkeiten bedingt. So hat der Mensch durch das Einstellen der Größe der Optimierungsschritte keinen direkten Einfluss auf die Funktionsweise bzw. die Programmstruktur des KNN, sondern lediglich auf die Trainingsdauer, -effizienz und die Genauigkeit des KNN.¹⁰³

⁹⁵ Vgl. GOODFELLOW/BENGIO/COURVILLE, S. 416 ff.

⁹⁶ Im Sinne, ob die Schichten noch gefaltet werden wie bspw. bei *convolutional nets*.

⁹⁷ GOODFELLOW/BENGIO/COURVILLE, S. 196 ff., vgl. auch S. 426.

⁹⁸ GOODFELLOW/BENGIO/COURVILLE, S. 194.

⁹⁹ KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 49 ff.

¹⁰⁰ GOODFELLOW/BENGIO/COURVILLE, S. 200 ff., insb. S. 211 f.; KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 49 ff., insb. S. 51 ff.

¹⁰¹ GOODFELLOW/BENGIO/COURVILLE, S. 200 ff., insb. S. 211 f.; KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 49 ff., insb. S. 51 ff.

¹⁰² GOODFELLOW/BENGIO/COURVILLE, S. 206 ff.

¹⁰³ GOODFELLOW/BENGIO/COURVILLE, S. 200 ff.

Schließlich kann der Mensch entscheiden, wann er das Training für beendet erachtet. Dies kann bspw. dann der Fall sein, wenn sich die Ausgaben des KNN nicht mehr verbessern oder aber die vorweg bestimmte Anzahl an Iterationen erreicht ist.¹⁰⁴

4. Einsatzgebiete und weitere Besonderheiten von neuronalen Netzen

Eine weitere Besonderheit von KNN gegenüber „klassischen Computerprogrammen“¹⁰⁵ ist deren Informationsrepräsentation. Im Gegensatz zu den typischerweise symbolisch repräsentierten Informationen bei klassischen Computerprogrammen, erfolgt die Informationsrepräsentation bei KNN implizit.¹⁰⁶ Symbolische Repräsentation bedeutet, dass eine klare Zuordnung von Zeichen zu technischer Funktion vorliegt.¹⁰⁷ Bei KNN ist die Information aber im Gesamtzustand des Netzwerks – implizit – repräsentiert.¹⁰⁸ Daher ist übrigens auch die Funktion des Netzes als Ganzes kein Algorithmus.¹⁰⁹

Ebenfalls erwähnenswert ist die Determiniertheit sowie der Determinismus von KNN. Diese Thematik gestaltet sich zwar nicht nur bei KNN als besonders, sondern auch andere bzw. eine Vielzahl von Softwareebenen intelligenter digitaler Systeme werden als nicht deterministisch bezeichnet.¹¹⁰ Dennoch zeigt sich das Problem des Determinismus sowie der Determiniertheit am Beispiel von KNN besonders deutlich: Ein Algorithmus ist determiniert, wenn er bei einer entsprechenden Eingabe immer die gleiche Ausgabe generiert.¹¹¹ Bei einem deterministischen Algorithmus sind zudem die einzelnen Zwischenschritte auf dem Weg zur Lösung immer dieselben.¹¹² Mit anderen Worten ist ein determi-

¹⁰⁴ GOODFELLOW/BENGIO/COURVILLE, S. 236 ff.; KI-Rechtshandbuch-NIEDERÉE/NEJDL, § 2 Rn. 70.

¹⁰⁵ Im Sinne von explizit von Menschenhand programmierter Wenn-Dann-Regelwerke auf Softwareebene eines digitalen Systems.

¹⁰⁶ Statt vieler: ZECH, Risiken, S. 15.

¹⁰⁷ Statt vieler: ZECH, Risiken, S. 14.

¹⁰⁸ Statt vieler: ZECH, Risiken, S. 15.

¹⁰⁹ Siehe Kap. 1, E. oben; Vgl. ZECH, Risiken, S. 15.

¹¹⁰ KIRN/MÜLLER-HENGSTENBERG, MMR 2014, 228; Zech, Risiken, S. 46.

¹¹¹ KONERTZ/SCHÖNHOF, S. 59; vgl. auch ZECH, Risiken, S. 46.

¹¹² KONERTZ/SCHÖNHOF, S. 59.

nistischer Algorithmus inklusive seiner Zwischenschritte gänzlich vorhersagbar.¹¹³ Ein probabilistischer bzw. stochastischer Algorithmus agiert hingegen mit Zufallszahlen. Er erreicht hinsichtlich seiner Ausgabe nur ein mit einer gewissen Wahrscheinlichkeit gleiches Ergebnis.¹¹⁴ Die Vorhersagbarkeit bezieht sich bei probabilistischen bzw. stochastischen Systemen aber nicht auf die Zwischenschritte.¹¹⁵ Mit unterschiedlichem Komplexitätsgrad eines KNN ändert sich also die Antwort nach der Frage der Determiniertheit.¹¹⁶ Allerdings werden weniger komplexe KNN bei exakt gleicher Eingabe immer die exakt gleiche Ausgabe generieren.¹¹⁷ Komplexe KNN mit Rückkopplung können sich hingegen spontan bzw. unvorhersehbar verhalten. Sie sind damit nicht determiniert und auch nicht deterministisch.¹¹⁸ Dies ist aber auch bei klassischen Computerprogrammen mit Rückkopplungen möglich.¹¹⁹ Schließlich bleibt zu erwähnen, dass jeder deterministische Algorithmus auch determiniert ist.¹²⁰

Zudem existieren KNN, welche noch in der Anwendungsphase neue Funktionen hinzulernen und sich optimieren.¹²¹ Mit anderen Worten ist die Entwicklung des KI-Programms nicht zwingend mit dem Übergang in die Anwendungsphase abgeschlossen. Bei sich selbst anpassenden KNN ist weder der Determinismus noch die Determiniertheit gegeben.

Aufgrund ihrer Komplexität eignen sich KNN besonders für die Lösung komplexer, nicht linearer Probleme. KNN eignen sich vor allem für das Erkennen und Erlernen von Mustern und können bislang unbekannte Daten verarbeiten. Beispielsweise werden für Sprach-, Bild- oder Texterkennung vor allem KNN verwendet.¹²²

¹¹³ KONERTZ/SCHÖNHOF, S. 19; ZECH, Risiken, S. 46.

¹¹⁴ Vgl. ZECH, Risiken, S. 46.

¹¹⁵ Statt vieler: ZECH, Risiken, S. 46.

¹¹⁶ Vgl. ZECH, Risiken, S. 46 f.

¹¹⁷ Weil die Wahrscheinlichkeit dann 100% beträgt, siehe auch ZECH, Risiken, S. 47.

¹¹⁸ Vgl. ZECH, Risiken, S. 47.

¹¹⁹ ZECH, Risiken, S. 47.

¹²⁰ KONERTZ/SCHÖNHOF, S. 59.

¹²¹ Statt vieler: Rechtshandbuch-AI-STIEMERLING, Kap. 2.1 Rn. 64 ff., insb. Rn. 65.

¹²² Bspw. AGGARWAL, S. 363 ff.

Schließlich ist erwähnenswert, dass sich die Gewichtungsinformationen getrennt von der Architektur abspeichern und auch auf Architekturen mit gleicher und ähnlicher Struktur übertragen lassen.¹²³ Dabei lassen sich die Gewichtungsinformationen durchaus symbolisch darstellen, doch ergeben sich für menschliche Betrachter der Gewichtungsinformationen keine logischen Rückschlüsse auf die Zusammenhänge bzw. die logischen Abläufe im KNN selbst.¹²⁴

III. Evolutionäre und genetische Algorithmen sowie genetische Programme

Genetische Algorithmen gehören zu den evolutionären Algorithmen. Auch bei evolutionären Algorithmen dient die Natur als Vorbild. Anders als bei KNN dienen nicht die natürlichen Neuronen in Gehirnen als Vorbild, sondern die Entwicklung und Optimierung von Algorithmen¹²⁵ soll nach Prinzipien der natürlichen Evolution erfolgen.¹²⁶ Wie die Natur nach evolutionären Gesetzen die schwächsten Individuen einer Population über die Generationen aussterben lässt, sollen bei der Entwicklung von evolutionären Algorithmen über die verschiedenen Generationen von generierten Algorithmen nur die jeweils guten Problemlösungsstrategien weiterentwickelt werden – während die schlechten gelöscht werden.¹²⁷

Maschinelles Lernen nach evolutionärem Vorbild ist derzeit weniger populär als das maschinelle Lernen mittels KNN.¹²⁸ Die Nutzung des natürlichen Vorbilds der Evolution zur Entwicklung maschineller Lernfähigkeit gehört aber zu den ältesten Methoden auf dem Gebiet der künstlichen Intelligenz: Bereits in den

¹²³https://pytorch.org/tutorials/beginner/basics/saveloadrun_tutorial.html#saving-and-loading-model-weights, zuletzt besucht am 9. Mai 2023.

¹²⁴Siehe für ein Beispiel einer Gewichtsmatrix KRUSE/BORGELT/BRAUNE/KLAWONN/MOEWES/STEINBRECHER, S. 33 ff. und 43 ff. Bereits der Umstand, der impliziten Informationsrepräsentation und -verarbeitung führt dazu, dass aus der symbolischen Darstellung der Gewichtungsinformationen kein Rückschluss auf die Funktions- und Arbeitsweise des KNN gezogen werden kann – wenn aus der gewichteten Architektur keine Rückschlüsse gezogen werden können, können auch aus den Gewichtungen allein keine Informationen erschossen werden.

¹²⁵ Im Sinne von Problemlösungsstrategien.

¹²⁶ SIVANANDAM/DEEPA, S. V.

¹²⁷ SIVANANDAM/DEEPA, S. V.

¹²⁸ PAPASTEFANOU, CR 2019, 210.

1950er Jahren stellte TURING entsprechende Überlegungen an,¹²⁹ bevor sich HOLLAND in den 1960er Jahren vertieft mit der Entwicklung genetischer Algorithmen befasste.¹³⁰

Genetische Algorithmen sind die bekannteste und am besten erforschte Art evolutionärer Algorithmen.¹³¹ Sie legen den Fokus der Evolution auf genetische Mechanismen: Die einzelnen Populationen bestehen aus sog. *strings*¹³², die wiederum aus einer bestimmten Anzahl *bits*¹³³ bestehen. Jene *strings* sind jeweils einzelne „Algorithmen“, genauer: Problemlösungsstrategien. Sie sollen in der Evolutionssprache die Chromosomen darstellen. Mehrere *bits* innerhalb eines *strings* bilden sodann Segmente. Diese Segmente enthalten jeweils die Entscheidungsvariable für das zu lösende Problem. Diese Variable ist binär codiert und korrespondiert mit einer entsprechenden Variable des zu lösenden Problems.¹³⁴

Die einzelnen *bits* repräsentieren ein bestimmtes Merkmal des jeweiligen Individuums bzw. *strings* – analog den genetischen Markern auf einem Chromosom.¹³⁵ Die *strings* werden nach dem Vorbild der natürlichen genetischen Vorgänge in der Evolution selektioniert, gekreuzt und mutiert.¹³⁶ Die Besonderheit von genetischen Algorithmen besteht darin, dass ihre Informationen als *bits* in binärer Form dargestellt werden. Bei anderen evolutionären Algorithmen erfolgt die Informationsrepräsentation in Form von Vektoren.¹³⁷ Das Grundprinzip ist aber bei allen evolutionären Algorithmen gleich und wird sogleich (Kap. 2, C., III., 1.) erläutert. Die Prinzipien werden darüber hinaus auch bei der genetischen Programmierweise (sog. *genetic programming*) verwendet. Dort sind die Individuen, die gemeinsam Populationen bilden, nicht *strings* oder Vektoren, sondern Computerprogramme in sämtlichen Ausgestaltungen, meist

¹²⁹ FOGEL, S. 59.

¹³⁰ NISSEN, S. 33.

¹³¹ EIBEN/SMITH, S. 6; NISSEN, S. 33; SIVANANDAM/DEEPA, S. V.

¹³² Sie stellen die Individuen der Population dar.

¹³³ Also Zahlenwerten von entweder 1 oder 0.

¹³⁴ NISSEN, S. 34.

¹³⁵ SIVANANDAM/DEEPA, S. 2.

¹³⁶ SIVANANDAM/DEEPA, S. V.

¹³⁷ SIVANANDAM/DEEPA, S. 2 ff.

aber Entscheidungsbäume.¹³⁸ Diese sind in ihrer Größe nicht begrenzt. Die einzelnen Entscheidungsbäume stellen sodann Funktionen dar und können wiederum genetische Algorithmen sein.¹³⁹

1. Evolutionäre und genetische Algorithmen

Das Grundkonzept bei der Entwicklung von evolutionären bzw. genetischen Algorithmen lässt sich wie folgt skizzieren: In einem ersten Schritt – der Initialisierungsphase – wird eine erste Population an Individuen generiert. Im Falle von genetischen Algorithmen sind dies eine Anzahl an *strings*. Dabei soll das genetische Material bzw. die *bits* mit den entsprechenden „genetischen“ Informationen so divers wie möglich sein. Je größer der „Genpool“ bzw. der *bitpool*, desto größer die Wahrscheinlichkeit, dass sich die optimale Lösung in ihm finden lässt.¹⁴⁰ Die einzelnen *bits* verschiedener *strings* werden jeweils mit gleicher Wahrscheinlichkeit auf „0“ oder „1“ gesetzt.¹⁴¹

Nach der initialen Generierung der ersten Population beginnt der eigentliche, iterative Entwicklungsprozess von genetischen und evolutionären Algorithmen. Die einzelnen *strings* der ersten Generation werden anhand der Fitnessfunktion betreffend ihre Geeignetheit zur Problemlösung bewertet.¹⁴² Die Fitnessfunktion wird bei evolutionären bzw. genetischen Algorithmen aus den Zielkriterien abgeleitet.¹⁴³ Nach der Bewertung werden die *strings* selektioniert, die für die Weiterentwicklung in Frage kommen. Diese Selektion erfolgt zufällig und aufgrund einer Wahrscheinlichkeit, die von der Geeignetheit – bzw. Fitness – der einzelnen Individuen abhängt. Je besser die Fitness bewertet ist, desto größer ist die Wahrscheinlichkeit, dass das Individuum für die Reproduktion selektioniert wird.¹⁴⁴

¹³⁸ NISSEN, S. 112.

¹³⁹ SIVANANDAM/DEEPA, S. 3 f.

¹⁴⁰ SIVANANDAM/DEEPA, S. 30.

¹⁴¹ NISSEN, S. 37.

¹⁴² NISSEN, S. 37; SIVANANDAM/DEEPA, S. 30.

¹⁴³ NISSEN, S. 37.

¹⁴⁴ SIVANANDAM/DEEPA, S. 30.

Nach der Bewertung und Selektionierung folgt die Reproduktion. Die Selektionierung erfolgt in Gruppen à zwei. Zwei *strings* bilden zusammen ein Elternpaar. Dieses Elternpaar wird sodann anhand eines Kreuzungsoperators gekreuzt und es werden jeweils zwei Nachkommen gezeugt.¹⁴⁵ Die Kreuzung (*crossover*) erfolgt ebenfalls entsprechend einer Wahrscheinlichkeit. Es ist also auch möglich, dass gar keine Kreuzung geschieht. In diesem Fall ist der jeweilige Nachkomme eine exakte Kopie des Elters.¹⁴⁶

Nach Anwendung des Kreuzungsoperators werden die Nachkommen an den Mutationsoperator (*mutation*) überwiesen.¹⁴⁷ Dieser hat vor allem den Zweck zu verhindern, dass an einzelnen Stringpositionen aller Individuen innerhalb einer Population der gleiche Wert steht.¹⁴⁸ Für das, was technisch tatsächlich erfolgt, ist der Begriff „Mutation“ unter Umständen etwas hoch gegriffen. Bei der Mutation wird jedes bit entsprechend einer Wahrscheinlichkeit invertiert – also von 1 auf 0 gestellt oder umgekehrt.¹⁴⁹

Ist die Mutation (bzw. die Inversion der *bit*-Werte) abgeschlossen, werden die Nachkommen wiederum anhand der Fitnessfunktion bewertet und in die neue Population übertragen.¹⁵⁰ Dies wird mit den restlichen Elternpaaren wiederholt, bis die vordefinierte Anzahl an Individuen in der neuen Population erreicht ist. Ist das der Fall, ersetzt die neue Population die alte. Aus der neuen Population werden ausgehend von der Bewertung wiederum Individuen selektiert, Elternpaare gebildet und Nachwuchs erzeugt, welcher wiederum in eine neue Population übertragen wird. Dieser Vorgang wird so lange wiederholt, bis ein Abbruchkriterium erreicht wird und das beste Individuum bzw. die beste Problemlösungsstrategie eruiert wurde.¹⁵¹ Diese beste Problemlösungsstrategie – das Ergebnis eines Entwicklungszyklus – wird im Rahmen dieser Arbeit als Ziel-Algorithmus bezeichnet. Das Ergebnis der Anwendung dieses Ziel-Algorithmus‘

¹⁴⁵ NISSEN, S. 38; SIVANANDAM/DEEPA, S. 30.

¹⁴⁶ NISSEN, S. 39; SIVANANDAM/DEEPA, S. 30 f.

¹⁴⁷ NISSEN, S. 39.

¹⁴⁸ NISSEN, S. 40 f.

¹⁴⁹ NISSEN, S. 40; vgl. auch SIVANANDAM/DEEPA, S. 30.

¹⁵⁰ NISSEN, S. 40.

¹⁵¹ NISSEN, S. 40; vgl. auch SIVANANDAM/DEEPA, S. 30 f.

ist sodann eine Quantität, wie bspw. die Form einer Antenne für die Weltraumfahrt.¹⁵²

Die Abbruchkriterien können unterschiedlich ausgestaltet sein. So kann der Entwicklungszyklus abgebrochen werden, wenn eine bestimmte Zeit verstrichen ist oder eine bestimmte Anzahl an Generationen erreicht ist. Ebenfalls denkbar ist ein Abbruch, wenn über eine bestimmte Zeit keine Verbesserung mehr beobachtet werden konnte, bzw. die verschiedenen Individuen einer Population an vielen Stellen übereinstimmen.

Die aufgezeigten Entwicklungsschritte bilden nur das Grundkonzept von evolutionären und genetischen Algorithmen. NISSEN bezeichnet einen so entwickelten Algorithmus als „Basis-GA“.¹⁵³ Es gibt zahlreiche Abwandlungen. Diese betreffen nicht nur den Gegenstand der Entwicklung, wie bspw. Vektoren statt *strings* bei evolutionären Algorithmen oder Entscheidungsbäume statt *strings* bei genetischen Programmen. Sondern auch die Einzelheiten in der Entwicklung selbst. So existieren Ansätze, bei welchen die Selektion nicht fitnessproportional (und damit skaliert) sondern rangbasiert (und damit ohne Skalierung) erfolgt. Unterschiede können sich auch in abweichenden Lösungsrepräsentationen zeigen.¹⁵⁴ Aus den Abwandlungen erhofft man sich bessere bzw. geeignetere Lösungen. Für welche Varianten sich die Entwickler:innen schließlich entscheiden, hängt hauptsächlich vom zu lösenden Problem ab.¹⁵⁵

2. Genetische Programme (*genetic programming*)

Beim *genetic programming* geht es darum, anhand von Trainingsdaten ein Computerprogramm automatisch zu generieren, das in der Lage ist, eine gegebene Aufgabenstellung zu lösen.¹⁵⁶ Dazu wird auf die Prinzipien der Entwicklung von genetischen Algorithmen zurückgegriffen. Genetische Programme

¹⁵² Siehe sogleich Kap. 2, C., III., 2. und Kap. 2, C., III., 3.

¹⁵³ NISSEN, S. 41, wobei das „GA“ für „genetischen Algorithmus“ steht.

¹⁵⁴ Siehe für die verschiedene Abwandlungen NISSEN, S. 45 ff.

¹⁵⁵ NISSEN, S. 43 ff.

¹⁵⁶ NISSEN, S. 111; SIVANANDAM/DEEPA, S. 131.

sind als Variante der genetischen Algorithmen zu sehen.¹⁵⁷ Beim *genetic programming* ist das Ergebnis ein Computerprogramm und bei genetischen Algorithmen eine konkrete Lösung, in Form einer Quantität.¹⁵⁸

Die Entwicklung von genetischen Programmen läuft im Wesentlichen gleich ab wie diejenige der genetischen Algorithmen. Ausgangspunkte sind keine binär codierten *strings*, sondern ein *function set* sowie ein *terminal set*. Aus diesen beiden Sets werden automatisch und auf stochastischer Basis Programme generiert, die dann in den iterativen Zyklus über Selektion, Kreuzung und Mutation treten.¹⁵⁹

Allerdings werden in der Grundform von *genetic programming* keine Mutationsoperatoren verwendet. Die Individuen-Komplexität sowie die Populationsgrößen sind komplex bzw. groß genug. So ist die Wahrscheinlichkeit klein, dass Individuen verloren gehen.¹⁶⁰ Dennoch gibt es Abwandlungen bei der Entwicklung von genetischen Programmen, bei denen Mutationsoperatoren eingesetzt werden.¹⁶¹ Solche Abwandlungen sind heute zunehmend häufiger.¹⁶²

Das *function set* beinhaltet eine Menge an problemangemessenen elementaren Funktionen¹⁶³, die Werte verarbeiten, die sich bereits im Programm befinden.¹⁶⁴ Im *terminal set* sind Konstanten und Variablen hinterlegt, die auch stochastisch bestimmt sein können¹⁶⁵ und zusammen mit den Funktionen aus dem *function set* automatisiert zu Computerprogrammen zusammengesetzt werden.¹⁶⁶ Das führt dazu, dass aus den Elementen der beiden *sets* eine Lösung für das Problem

¹⁵⁷ NISSEN, S. 111.

¹⁵⁸ SIVANANDAM/DEEPA, S. 162

¹⁵⁹ NISSEN, S. 117 ff.

¹⁶⁰ Siehe oben Kap. 2, C., III., 1. ff. zur Mutation genetischer Algorithmen.

¹⁶¹ NISSEN, S. 119 f.

¹⁶² SIVANANDAM/DEEPA, S. 136.

¹⁶³ Vgl. NISSEN, S. 113: es kann sich dabei namentlich um folgende Funktionen handeln: (i) arithmetische Funktionen (+, -, *, /), (ii) mathematische Funktionen (bspw. Sin, Cos, etc), (iii) boolsche Operationen (AND, NOT, etc.), Verzweigungen (If-Then-Else); (iv) Iterationen (For, Do-Until, etc.); (v) anwendungsspezifische Funktionen.

¹⁶⁴ SIVANANDAM/DEEPA, S. 135 f.

¹⁶⁵ NISSEN, S. 114.

¹⁶⁶ EIBEN/SMITH, S. 75 f.; NISSEN, S. 111 ff.

bzw. eine Problemlösungsstrategie formulierbar ist.¹⁶⁷ Im Gegensatz zu den Funktionen im *function set*, beziehen sich die Werte im *terminal set* nicht auf dem Programm inhärente Werte, sondern liefern dem Programm Input.¹⁶⁸ Bei der Festlegung der Inhalte der beiden *sets* sind die Entwickler:innen frei. Die Festlegung der Werte in den beiden Sets ist entscheidend für die Qualität des Ziel-Programms – des Programms also, das entwickelt werden soll und am Ende der Iterationen als Ergebnis steht. So ist bei praktischen Anwendungen das anwendungsspezifische Wissen – falls vorhanden – zu berücksichtigen und mittels entsprechender Funktionen im *function set* zu hinterlegen.¹⁶⁹

Bei evolutionären und genetischen Algorithmen wird die Fitnessfunktion anhand von Zielkriterien abgeleitet.¹⁷⁰ Die Fitnessfunktion bewertet die Individuen anschließend direkt.¹⁷¹ Beim *genetic programming* muss die Fitnessfunktion für jedes beliebige Programm, das generiert wird, einen Fitnesswert berechnen können.¹⁷² Diese Programme sind wesentlich komplexer als die *strings* bei den genetischen Algorithmen.¹⁷³ Mitunter deshalb beschränkt sich das Testen der Fitness bei genetischen Programmen darauf, die Ausgabe des Programms (Individuums) mit der korrekten Ausgabe zu vergleichen und eine Differenz zu berechnen.¹⁷⁴ Da die korrekte Ausgabe aber oft nicht im Voraus bekannt ist, erfolgt der Vergleich – ähnlich wie bei den neuronalen Netzen – anhand von Trainingsdaten. Diese fungieren als repräsentative Beispiele und müssen somit so ausgewählt und kuratiert werden, dass sie die Lösung beinhalten.¹⁷⁵ Wenn diese aber nicht bekannt ist, kann die Lösung auch in Ansätzen den Trainingsdaten inhärent sein.¹⁷⁶ Die Fitnessfunktion bewertet nicht nur Komplett- sondern auch Teillösungen.¹⁷⁷

¹⁶⁷ NISSEN, S. 115.

¹⁶⁸ SIVANANDAM/DEEPA, S. 135 f.

¹⁶⁹ NISSEN, S. 114.

¹⁷⁰ NISSEN, S. 37.

¹⁷¹ NISSEN, S. 37, siehe auch oben Kap. 2., C., III., 1.

¹⁷² NISSEN, S. 115.

¹⁷³ Vgl. dazu oben Kap- 2. C., III.

¹⁷⁴ NISSEN, S. 115 f.

¹⁷⁵ NISSEN, S. 116 f.

¹⁷⁶ NISSEN, S. 116 f.

¹⁷⁷ NISSEN, S. 116; siehe für eine ausführliche Beschreibung der vorbereitenden Handlungen generell NISSEN, S. 111 ff.

Die Entwicklungsläufe beim *genetic programming* laufen im Prinzip gleich ab wie diejenigen der evolutionären bzw. genetischen Algorithmen. Es ergeben sich nur kleine Unterschiede, die in der Komplexität der unterschiedlichen Individuen der verschiedenen Technologien begründet liegen: Die Individuen¹⁷⁸ der ersten Generation werden wahrscheinlichkeitsbasiert durch einen Computer generiert.¹⁷⁹ Dazu werden für jedes Individuum mit gleicher Wahrscheinlichkeit Funktionen aus dem *function set* ausgewählt¹⁸⁰ und mit Argumenten zu Programmen verbunden.¹⁸¹ Die Argumente werden mit gleicher Wahrscheinlichkeit aus der Vereinigungsmenge der Elemente von *function set* und *terminal set* bestimmt.¹⁸² Handelt es sich beim bestimmten Argument um ein Element aus dem *terminal set*, endet die Funktion (im Falle von Entscheidungsbäumen der Ast), nicht aber das Programm an der Stelle.¹⁸³ Die so bestimmten Argumente werden sodann wiederum mit einer Funktion aus dem *function set* verbunden. Dieser Vorgang wird für jedes Individuum wiederholt, bis die im Voraus festgelegte maximale Länge des Programmes erreicht ist, oder an jedem Ast Elemente des *terminal sets* an letzter Stelle stehen.¹⁸⁴ Die so generierten Programme werden in die genetisch-evolutionären Iterationen überführt.¹⁸⁵

Genauer betrachtet bedeutet das, dass die Programme anhand der Fitnessfunktion bewertet und anschließend selektiert werden.¹⁸⁶ Auch beim *genetic programming* wird der Nachwuchs anhand zweier Elternteile generiert – nach Regeln der Kopie, Kreuzung und Mutation¹⁸⁷. Es werden ebenfalls immer zwei

¹⁷⁸ Wie in Kap. 2, C., III., 2. gesehen, sind dies beim *genetic programming* Programme, oft aber nicht ausschließlich Entscheidungsbäume.

¹⁷⁹ NISSEN, S. 117 f.; SIVANANDAM/DEEPA, S. 147.

¹⁸⁰ Im Falle von Entscheidungsbäumen ist die Funktion sodann die Wurzel des Entscheidungsbaumes, NISSEN, S. 118.

¹⁸¹ NISSEN, S. 117; SIVANANDAM/DEEPA, S. 147 f.

¹⁸² NISSEN, S. 118.

¹⁸³ NISSEN, S. 118.

¹⁸⁴ NISSEN, S. 118; vgl. auch SIVANANDAM/DEEPA, S. 147 ff.

¹⁸⁵ NISSEN, S. 119; SIVANANDAM/DEEPA, S. 147 ff.

¹⁸⁶ NISSEN, S. 119; SIVANANDAM/DEEPA, S. 146 f.

¹⁸⁷ NISSEN, S. 119 ff.; SIVANANDAM/DEEPA, S. 146 ff.; vgl. aber Kap. 2, C., III., 1. oben zum Vorbehalt betreffend Mutationen.

Nachkommen gezeugt.¹⁸⁸ Bei der Kreuzung werden bei den beiden Elternteilen jeweils ein Punkt in der Programmstruktur bestimmt.¹⁸⁹ Die dem Punkt nachfolgende Programmstruktur wird sodann mit der dem Punkt nachfolgenden Programmstruktur des anderen Elters „getauscht“ und so durch Kreuzung zwei Nachkommen gezeugt.¹⁹⁰ Diese Nachkommen werden bewertet und in die neue Population überführt, wo eine neue Iteration ihren Lauf nimmt.¹⁹¹ Dies wird so lange wiederholt, bis ein Abbruchkriterium eingreift.¹⁹² Am Ende wird das Programm ausgewählt, welches die beste Fitness aufweist.¹⁹³

Für komplexere Probleme wird das zu lösende Problem in Teilprobleme zerlegt, die entsprechend den Regeln der genetischen Programmierweise gelöst werden sollen und in einem anschließenden Schritt zur Lösung des Hauptproblems zusammengeführt werden.¹⁹⁴ Für diese komplexeren Probleme werden auch vermehrt Mutationsoperatoren eingesetzt. Man erhofft sich dadurch eine höhere Effizienz.¹⁹⁵

3. Anwendungsbeispiele

Genetische Algorithmen und Programme werden verschiedentlich eingesetzt, oft aber zu Optimierungszwecken.¹⁹⁶ Die Ergebnisse der Entwicklung genetischer Algorithmen und Programme – sprich die Ziel-Algorithmen und die Ziel-Programme – können entweder eigenständig eingesetzt werden, oder aber sie können in andere KI-Technologien implementiert werden.¹⁹⁷ So können

¹⁸⁸ NISSEN, S. 120 f.; SIVANANDAM/DEEPA, S. 146 f.

¹⁸⁹ NISSEN, S. 117 ff.; insb. 119 f.

¹⁹⁰ NISSEN, S. 120 f.; vgl. SIVANANDAM/DEEPA, S. 151.

¹⁹¹ NISSEN, S. 120 f.

¹⁹² NISSEN, S. 122; SIVANANDAM/DEEPA, S. 146 f.

¹⁹³ NISSEN, S. 126; SIVANANDAM/DEEPA, S. 147.

¹⁹⁴ NISSEN, S. 129 ff.

¹⁹⁵ NISSEN, S. 143 ff.

¹⁹⁶ ALAM/QAMAR/DIXIT/BENAIDA, *ijEP* 2020, Kap. 8. 4 f.; SIVANANDAM/DEEPA, S. 12, 20 ff., 34.

¹⁹⁷ ALAM/QAMAR/DIXIT/BENAIDA, *ijEP* 2020, Kap. 8; SIVANANDAM/DEEPA, S. 35.

bspw. Ziel-Algorithmen und -Programme Bestandteile von KNN sein.¹⁹⁸ Darüber hinaus werden die Ansätze aus der genetischen Programmierweise auch bei der Entwicklung von KNN eingesetzt.¹⁹⁹

Genetische Algorithmen und Programme werden aber nicht nur zwecks Optimierung eingesetzt. Sie können auch zur Modellierung oder Mustererkennung eingesetzt werden.²⁰⁰ Schließlich finden sie auch Anwendung auf dem Gebiet der bildenden und akustischen Kunst.²⁰¹

Während die Informationsverarbeitung in KNN nicht symbolisch repräsentiert werden kann, ist die Informationsverarbeitung bei genetischen Algorithmen und Programmen explizit symbolisch repräsentiert.²⁰² Die meisten symbolischen KI-Technologien sind nur dazu in der Lage, ein spezifisches Problem zu lösen.²⁰³ Technologien, bei welchen genetische Algorithmen oder Programme implementiert wurden, gehören nicht dazu. Sie sind in der Lage, sich anzupassen und eine Mehrzahl verschiedener Probleme zu lösen.²⁰⁴

Die praktischen Anwendungsgebiete reichen von autonomer Robotersteuerung²⁰⁵ über das Design von Abwassernetzwerken²⁰⁶ bis hin zum Entwurf von Flugzeugen²⁰⁷ und Antennen für die Nutzung in der Raumfahrt²⁰⁸.

¹⁹⁸ SIVANANDAM/DEEPA, S. 35.

¹⁹⁹ ALAM/QAMAR/DIXIT/BENAIDA, iJEP 2020, Kap. 8.7; SIVANANDAM/DEEPA, S. 35.

²⁰⁰ SIVANANDAM/DEEPA, S. 156; vgl. auch ALAM/QAMAR/DIXIT/BENAIDA, iJEP 2020, Kap. 8,2.

²⁰¹ SIVANANDAM/DEEPA, S. 156.

²⁰² Siehe oben Kap. 2, C., II., 4.

²⁰³ Vgl. SIVANANDAM/DEEPA, S. 29.

²⁰⁴ SIVANANDAM/DEEPA, S. 29.

²⁰⁵ ALAM/QAMAR/DIXIT/BENAIDA, iJEP 2020, Kap. 8.2, 8.10; SIVANANDAM/DEEPA, S. 320 ff.

²⁰⁶ SIVANANDAM/DEEPA, S. 157.

²⁰⁷ ALAM/QAMAR/DIXIT/BENAIDA, iJEP 2020, Kap. 8.11.

²⁰⁸ <https://www.jpl.nasa.gov/nmp/st5/TECHNOLOGY/antenna.html>, zuletzt besucht am 11. Mai 2023.

4. Genetische Programmierweisen, Autonomie und künstliche Intelligenz

Es wurde aufgezeigt, dass evolutionäre und genetische Problemlösungsstrategien auf einem konstanten *trial- and error*-Prozess fußen. Dieser Prozess ist an ein ständiges Bewerten der gefundenen Lösungen und einen damit zusammenhängenden Verbesserungsprozess gekoppelt. Bei evolutionären und genetischen Algorithmen bestehen die einzelnen Populationen aus relativ simplen Individuen (*strings*). Diese Strings bestehen wiederum aus *bits* – sprich aus Einsen und Nullen. Man könnte also argumentieren, dass die Entwicklung von genetischen und evolutionären Algorithmen nicht sehr bahnbrechend ist. Dabei wird übersehen, dass diese Prinzipien zu Lösungen führen können, die von einem Menschen nicht angedacht worden wären. Insbesondere wenn man sich die Funktionsweise des *genetic programming* vergegenwärtigt, die sich die Prinzipien und Erkenntnisse aus der Entwicklung von genetischen Algorithmen zu Nutze macht, zeigt sich, dass es sich um eine autonome und damit intelligente Technologie handelt: Aus einem gegebenen Set an (Grund-)Regeln, Funktionen, Variablen und Konstanten werden Problemlösungsstrategien entwickelt. Diese Lösungen werden anhand einer Fitnessfunktion und von Trainingsdaten bewertet. Aus den Bewertungen werden sodann Rückschlüsse für die Anpassung und Weiterentwicklung der Lösungsstrategien gezogen.

Der menschliche Einfluss besteht in den folgenden Punkten: Decodierung des zu lösenden Problems und anschließende Codierung dieses Problems in einer für die Maschine verständlichen Form; Auswahl/Entwicklung der Fitnessfunktion; Auswahl bzw. Bestimmung der Kreuzungs- und Mutationsoperatoren; Zusammenstellung und Auswahl der Regeln; Auswahl der Variablen und Konstanten; Festlegen der Abbruchkriterien und vor allem Auswahl und Kuration der Trainingsdaten. Der menschliche Aufwand ist damit zwar hoch. Dennoch basieren die evolutionären Strategien auf dem Konzept, dass sich das System die Regeln der Informationsverarbeitung selbst setzt. Nicht der Mensch entscheidet, an welchem Knoten des Entscheidungsbaums welche Funktion und an welchem Ast welches Argument eingesetzt wird. Der Mensch hat oftmals keine Vorstellung davon, wie die Problemlösungsstrategie am Ende aussehen könnte. Die Festlegung der effektiv eingesetzten Regeln erfolgt autonom – entscheidend sind vor allem das Feedback, welches über die Fitnessfunktion errechnet wird sowie die den Trainingsdaten inhärenten Problemlösungsansätzen. Evolutionäre Strategien und damit genetische Algorithmen sowie Programme sind dem-

entsprechend intelligent und auf dem Gebiet der Künstlichen Intelligenz zu verorten.²⁰⁹ Das Ergebnis von evolutionären Strategien wird sodann auf der Softwareebene intelligenter digitaler Systeme eingesetzt.

IV. Zwischenergebnis

Als Zwischenergebnis zu den dargestellten Beispielen von KI-Technologien kann somit festgehalten werden, dass gewisse Gemeinsamkeiten bestehen. Einerseits bedarf die Entwicklung der Systeme – sowohl bei den Expertensystemen, bei KNN wie auch beim evolutionärem *computing* großer Datenmengen. Aus diesen Datenmengen erlernen KNN und genetische Programme sodann – mehr oder minder – autonom die Regeln, nach welchen sie die Informationen verarbeiten. Expertensysteme ziehen die Daten direkt zur Lösungsfindung heran. Es handelt sich bei Expertensystemen also eher um Wissens- als um Trainingsdaten. Die Trainings- und Wissensdatenmenge allein entscheidet jedoch nicht über die Funktionalität und Qualität des Systems, es ist vielmehr die Qualität der Daten. Wenn sich also KNN selbst Funktionen aneignen oder der Programmierprozess wie bei den genetischen Programmen gänzlich automatisiert bzw. ohne direkten menschlichen Einfluss erfolgt und so der Eindruck erweckt werden könnte, dass sich Computerprogramme selbst entwickeln, ist der Mensch dennoch notwendig. Der menschliche Einfluss bei diesen Technologien unterscheidet sich aber grundlegend von demjenigen bei klassischen Programmierweisen. Während bei den klassischen Programmierweisen die Programmierer:innen direkt die Funktionalität bestimmen, indem sie die Regeln der Informationsverarbeitung vorgeben, liegt der menschliche Einfluss bei KI-Technologien anders gelagert. Er besteht besonders in der Qualitätssicherung der Trainings- und Wissensdaten sowie der Kontrolle über die Trainingsergebnisse bzw. die Kuration der Daten und letztlich der KI-Technologie. Hinzu kommt, dass es nach wie vor der Mensch ist, der eine KI-Technologie überhaupt als lernfähig gestaltet. Der Mensch entwirft und programmiert die Architektur und die „Hilfsprogramme“ wie Optimierungsalgorithmus KNN oder die Fitnessfunktion beim *genetic programming*. Bei Expertensystemen programmiert

²⁰⁹ So auch NISSEN, S. 21; vgl. auch SIVANANDAM/DEEPA, S. 154 f., die auf ALAN TURING verweisen, der bereits 1948 und 1950 die These aufstellte, dass *machine intelligence* durch das Imitieren evolutionärer Prozesse erreicht werden könne.

der Mensch die entsprechende Programmumgebung und die Problemlösungsstrategien. Besonders die Konzeptionierung der Lernfähigkeit sowie das Sammeln der Wissens- und Trainingsdaten, deren Aufbereitung, Erhaltung und Einpflegen in den Entwicklungs- und Trainingsvorgang, macht die Entwicklung trainierter KI-Technologien derart kostenintensiv.

Neben den Gemeinsamkeiten bestehen aber auch erhebliche Unterschiede. Diese lassen sich nicht nur in der Entwicklung, sondern vielmehr auch in der effektiven Funktionsweise der Technologien finden. So handelt es sich beim Ziel-Programm der genetischen Programmierweise nach wie vor um ein (sehr komplexes) Wenn-Dann-Regelwerk, wie es auch klassische Programme sind. Bei KNN kann hingegen nicht von Wenn-Dann-Regelwerken gesprochen werden – vielmehr handelt es sich um eine neuartige Funktionsweise mit Nachschaltungen, Rückkopplungen und Schichten, bei welchen die Informationsrepräsentation und -verarbeitung implizit erfolgt.

Teil 2

Das Immaterialgüterrecht und dessen Rechtfertigung

Kapitel 3

Begriff und Wesen des Immaterialgüterrechts

Das Immaterialgüterrecht bzw. die Rechtsinstitutionen, welche das geistige Eigentum schützen, lassen sich in den gewerblichen Rechtsschutz sowie das Urheberrecht aufteilen.¹ Zum gewerblichen Rechtsschutz gehören die Rechtsgebiete des Patent-, Marken-, Gebrauchsmuster-, Design-, Sortenschutz-, Halbleiterschutz- sowie des Lauterkeitsrechts.² Sie schützen den jeweiligen Schutzgegenstand nur betreffend seine gewerbliche Verwertbarkeit bzw. Verwendung.³ Das Urheberrecht als Schutz von Werken der Kunst, Literatur und Wissenschaft hingegen ist auch im privaten, nicht gewerblichen Bereich anwendbar.⁴ Das Immaterialgüterrecht wird auch als Schutz des geistigen Eigentums bezeichnet.⁵ Diese Gleichsetzung mit dem Sacheigentum wird in der Literatur mehrheitlich (und berechtigterweise) kritisiert. Die Kritik liegt mitunter darin begründet, dass der Begriff des Eigentums die persönlichkeitsrechtliche Seite der immateriellen Güter vernachlässigt.⁶ Dennoch wird der Begriff des geistigen Eigentums aufgrund seiner Etablierung und zwecks Leser:innenfreundlichkeit im Rahmen dieser Arbeit verwendet.

Die Schutzgüter im Immaterialgüterrecht sind unkörperlich und damit zeitlich wie örtlich ungebunden.⁷ Sie sind in ihrer Verwendung also weder rival noch

¹ Statt vieler: PEUKERT, § 3 Rn. 27 ff.; PIERSON/AHRENS/FISCHER, S. 39.

² Statt vieler: PEUKERT, § 3 Rn. 27 ff.; PIERSON/AHRENS/FISCHER, S. 39.

³ Statt vieler: PEUKERT, § 3 Rn. 27 ff.; PIERSON/AHRENS/FISCHER, S. 39.

⁴ Statt vieler: PEUKERT, § 3 Rn. 27 ff.; PIERSON/AHRENS/FISCHER, S. 39; S. 379.

⁵ Statt vieler: PEUKERT, § 3 Rn. 27 ff.; PIERSON/AHRENS/FISCHER, S. 39.

⁶ Vgl. nur: PIERSON/AHRENS/FISCHER, S. 39.

⁷ Statt vieler: PIERSON/AHRENS/FISCHER, S. 40.

exklusiv oder abnutzbar. Das macht sie zu faktisch nicht knappen Gütern.⁸ Immaterielle Güter werden deshalb auch als öffentliche Güter qualifiziert.⁹ Rivalität, Exklusivität und Knappheit müssen bei immateriellen Gütern künstlich geschaffen werden – durch Schaffung von Ausschließlichkeitsrechten.¹⁰ Mit diesen Ausschließlichkeitsrechten wird das Immaterialgut der berechtigten Person zugewiesen. Immaterialgüterrechte sind subjektive Rechte absoluter Natur.¹¹ Es handelt sich bei jedem Immaterialgüterrecht um ein gegen alle wirkendes Bündel von Rechten an der geistigen Leistung.¹² Wichtige Aspekte dieser Rechtszuweisung sind die ausschließliche Befugnis zur Verwertung des Gutes sowie die ausschließliche Befugnis, Dritte von Einwirkungen auszuschließen.¹³ Eine solche Einschränkung von öffentlichen bzw. gemeinfreien Gütern mittels ausschließlicher Rechtszuweisung bedarf der Rechtfertigung¹⁴, welche folgend erläutert wird.

⁸ Vgl. nur ZECH, Information, S. 118 f.

⁹ Vgl. nur ZECH, Information, S. 115, 117 f.

¹⁰ Vgl. ZECH, Information, S. 46, 117 ff., 147; PIERSON/AHRENS/FISCHER, S. 40.

¹¹ Statt vieler: PEUKERT, § 1 Rn. 7; PIERSON/AHRENS/FISCHER, S. 40.

¹² Statt vieler: PIERSON/AHRENS/FISCHER, S. 40.

¹³ Statt vieler: PEUKERT, § 1 Rn. 7; PIERSON/AHRENS/FISCHER, S. 40.

¹⁴ Vgl. ZECH, Information, S. 124.

Kapitel 4

Rechtfertigungsansätze im Immaterialgüterrecht

Die Rechtfertigung von Ausschließlichkeitsrechten an geistigen Leistungen kann nicht anhand einer einzigen Theorie erfolgen. Einerseits greift jede Theorie für sich allein betrachtet zu kurz, um die Facetten von Ausschließlichkeitsrechten umfassend zu rechtfertigen. Andererseits bedingen auch die verschiedenen Arten von geistigen Eigentumsrechten verschiedene Ansätze. So lässt sich im Urheberrecht noch der urheberrechtliche Schutz als Normalzustand (nicht etwa die Gemeinfreiheit) ausmachen, während bspw. im Patentrecht die Zuweisung des Ausschließlichkeitsrecht als „unnatürlich“ aufgefasst werden kann.¹ Damit ist die Immaterialgüterrechtsrechtfertigung umstritten. Im Ergebnis ist die ausschließliche Rechtszuweisung an immateriellen Gütern also nur durch ein Zusammenspiel verschiedener Theorien zu rechtfertigen.

Ein Ansatz in der Lehre unterscheidet zwischen deontologischen und utilitaristischen Rechtfertigungstheorien.² Deontologische Theorien gehen anders als utilitaristische Ansätze von der Legitimität von Ausschließlichkeitsrechten aus, ohne dass ein volkswirtschaftlicher Nutzen durch die Schaffung des Ausschließlichkeitsrechts erreicht werden muss.³ Zu den deontologischen Theorien werden die naturrechtlichen Eigentumstheorien sowie diejenigen mit Persönlichkeitsbezug oder aber auch der patentrechtliche Belohnungsgedanke gezählt.⁴ Da die utilitaristischen Ansätze die ausschließliche Zuordnung von Gütern mit einem volkswirtschaftlichen Nutzen rechtfertigen, erwachsen die utilitaristischen Ansätze aus der ökonomischen Analyse des Immaterialgüterrechts. So sollen

¹ ZECH, Information, S. 149. Es sei aber darauf hingewiesen, dass auch das Urheberrecht mit dem vermehrten Aufkommen von Open-Source bzw. ähnlichen Bewegungen je länger je verstärkter unter einen Legitimationsdruck gerät (Depenheuer/Peifer/SCHACK, S. 124).

² So bspw. Depenheuer/Peifer/OHLY, S. 141 ff.; ZECH, Information, S. 149 ff.

³ So bspw. Depenheuer/Peifer/OHLY, S. 145; ZECH, Information, S. 150.

⁴ Statt vieler: ZECH, Information, S. 150.

Ausschließlichkeitsrechte an immateriellen Gütern ein Marktversagen verhindern. Basierend auf der Theorie der *property rights* sollen nämlich die positiven und negativen Effekte aus dem Umgang mit den Gütern den jeweils Berechtigten zugewiesen werden. Es müssen also die externen Effekte internalisiert werden.⁵ Zu den utilitaristischen Ansätzen gehören die Anreiztheorie sowie die Offenbarungstheorie.⁶

A. Deontologische Theorien

Mit der Naturrechtslehre geht die Eigentumstheorie einher. Nach der Eigentumstheorie steht jedem Menschen an den eigenen Ideen ein entsprechendes Eigentumsrecht zu, welches von jeder Person zu beachten ist.⁷ Entsprechend dem Sacheigentum soll so auch am geistigen Eigentum ein Ausschließlichkeitsrecht bestehen.⁸ Durch die Gleichsetzung von Sach- zu geistigem Eigentum hat dessen Rechtfertigung auch Gleichbehandlungsmotive. Ein Eigentum an Ideen geht aber zu weit.⁹ Dies zeigt sich auch im Urheberrecht, wo die der Werkschöpfung zugrundeliegenden Ideen eben nicht geschützt sind, sondern nur die konkrete Ausdrucksform.¹⁰ Bedeutender Ausfluss der Eigentumstheorie ist die von JOHN LOCKE entwickelte Arbeitstheorie. Nach der Arbeitstheorie besteht durch Bearbeitung ein Bezug von der Persönlichkeit zur Sache, wodurch eine schützenswerte Position entsteht.¹¹ Die Arbeitstheorie schränkt sozusagen die Eigentumstheorie ein, indem sie ein Arbeitsergebnis verlangt – mit anderen Worten müssen die Ideen Ausdruck gefunden haben in Form eines Arbeitsoutputs. Damit

⁵ Siehe zum Ganzen ZECH, Information, S. 153; vgl. auch Depenheuer/Peifer/SCHACK, S. 133 f.

⁶ Vgl. ZECH, Information, S. 152 ff.

⁷ AHRENS, Rn. 8; BEIER, GRUR Int. 1970, 2; STIERLE, S. 191 f.; ZECH, S. 151 f.

⁸ AHRENS, Rn. 8; BEIER, GRUR Int. 1970, 2; STIERLE, S. 191 f.; ZECH, S. 151 f.

⁹ Depenheuer/Peifer/OHLY, S. 145; siehe aber für die Gegenmeinung die Meinung von MERGES, zusammengefasst bei STIERLE, S. 193 f.

¹⁰ Siehe unten Kap. 8, A., I.

¹¹ ZECH, Information, S. 151.

ist die Arbeitstheorie aber auch nahe an den persönlichkeitsrechtlichen Ansätzen (s. sogleich).¹² Legt man den Schwerpunkt der Arbeitstheorie auf den schöpferischen bzw. bearbeitenden Aspekt, lässt sich aber vor allem der Schöpfungsgedanke bei den Immaterialgüterrechten rechtfertigen.¹³

Rückt man den Persönlichkeitsbezug der Arbeitstheorie in den Vordergrund, drängt sich der persönlichkeitsrechtliche Ansatz auf. Dieser hat vor allem im Urheberrecht Bedeutung.¹⁴ Er geht davon aus, dass das zu schützende immaterielle Gut bzw. dessen konkrete Ausdrucksform einen Bezug zur Persönlichkeit der berechtigten Person hat und dieser Bezug genauso wie die Persönlichkeit *per se*¹⁵ Schutz verdient.¹⁶ Vereinfacht gesagt, soll mit dem schöpferischen Akt ein Teil der Persönlichkeit der schöpfenden Person in das geschaffene Gut übergehen und so alsdann geschützt werden.¹⁷

Allein vermögen die Eigentumstheorie bzw. die Arbeitstheorie und die persönlichkeitsrechtlichen Theorien jedoch nicht Ausschließlichkeitsrechte an immateriellen Gütern zu rechtfertigen. Dies zeigt sich im Patentrecht bereits daran, dass ein hoheitlicher Akt zur Einräumung des Rechts notwendig ist.¹⁸ Besonders deutlich aber ist dies an der zeitlichen Begrenzung des Patentrechts auf grundsätzlich 20 Jahre ersichtlich.¹⁹ Dies ist auch der Grund, weshalb diese Ansätze für die Rechtfertigung der gewerblichen Schutzrechte weniger herangezogen werden. Bei den gewerblichen Schutzrechten finden sich nur fragmentarisch persönlichkeitsrechtliche Elemente²⁰ während diese nach der im deutschem

¹² Vgl. auch ZECH, Information, S. 151.

¹³ ZECH, Information, S. 151 mit dem Verweis darauf, dass das BVerfG bis heute den wichtigsten Grund für Art. 14 GG im Schutz des Ergebnisses persönlicher Leistung sieht.

¹⁴ Vgl. ZECH, Information, S. 150.

¹⁵ Vgl. bspw. Art. 2 GG.

¹⁶ Vgl. ZECH, Information, S. 150.

¹⁷ Depenheuer/Peifer/SCHACK, S. 129 f.

¹⁸ BEIER, GRUR Int. 1970, 2.

¹⁹ BEIER, GRUR Int. 1970, 2; siehe zur zeitlichen Begrenzung auch unten Kap. 7, B., III.

²⁰ ZECH, Information, S. 150 nennt den patentrechtlichen Schutz der Erfinderehre als Beispiel. Dieser ist Ausfluss von § 37 Abs. 1 PatG bzw. Art. 81 EPÜ und geht wesentlich weniger weit als bspw. der Schutz des urheberrechtlichen Werkes vor Entstellung nach § 14 UrhG, welcher im Persönlichkeitsschutz seine Rechtfertigung findet.

Recht geltenden monistischen Theorie im Urheberrecht mit den vermögensrechtlichen Elementen zu einer Einheit verbunden sind.²¹

Schließlich lässt sich auch die Belohnungstheorie unter die deontologischen Rechtfertigungsansätze fassen. Sie kann zwar auch unter die utilitaristischen Methoden eingeordnet werden, indem für die Gesellschaft nützliches Schaffen mit Ausschließlichkeitsrechten belohnt wird. Doch lässt sich die Belohnungstheorie ebenso rein deontologisch verstehen: „gerechter Lohn für nützliche Arbeit“ in Form von Ausschließlichkeitsrechten an immateriellen Gütern.²² Mit dem Erfordernis der Nützlichkeit rückt die Belohnungstheorie einerseits die Rechtfertigung dennoch stark in die Nähe des Utilitarismus. Andererseits ist unklar, was alles als nützliche Arbeit angesehen werden soll und was als unnützlich bzw. als nicht nützlich genug gilt.²³ Die Belohnungstheorie wird vor allem – aber nicht nur²⁴ – für die Rechtfertigung des Patentrechts herangezogen.²⁵ Großen Einwand erfährt die Belohnungstheorie – vor allem auf dem Gebiet des Urheberrechts – durch die Argumente, dass einerseits auch die kleine Münze²⁶ geschützt ist²⁷ und andererseits (Kunst)Werke bereits zu Zeiten geschaffen wurden, in welchen noch kein Urheberrecht eingeräumt wurde.²⁸

Gewisse Stimmen in der Lehre gehen sogar so weit, dass auch für das Urheberrecht sämtliche naturrechtliche Rechtfertigung (nicht nur Eigentums- und Arbeitstheorie) versagen.²⁹ Dennoch ist festzustellen, dass die deontologischen Ansätze jeweils Kerninhalte der einzelnen Immaterialgüterrechte betreffen. Zu diesen Kerninhalten gehören bspw. das Recht auf Erfindernennung im Patentrecht gemäß Art. 81 EPÜ bzw. §§ 37 und 63 PatG oder der Schutz vor

²¹ ZECH, Information, S. 150 m.w.N.: ein monistischer Ansatz verbindet gerade die persönlichkeitsrechtlichen und die vermögensrechtlichen Aspekte des Rechtes zu einer untrennbaren Einheit.

²² BEIER, GRUR Int. 1970, 2 f.; STIERLE, S. 195 f.; vgl. ZECH, Information, S. 152.

²³ Vgl. dazu STIERLE, S. 197; ZECH, Information, S. 152.

²⁴ Vgl. bspw. für das Urheberrecht Depenheuer/Peifer/SCHACK, S. 133 f.

²⁵ BEIER, GRUR Int. 1970, 2 f.

²⁶ Siehe dazu weiter unten Kap- 8, A., I.

²⁷ Vgl. Depenheuer/Peifer/OHLY, S. 145 f. für die persönlichkeitsrechtlichen Ansätze.

²⁸ Vgl. Depenheuer/Peifer/SCHACK, S. 134; LANDES/POSNER, S. 22.

²⁹ Depenheuer/Peifer/OHLY, S. 146.

Entstellung des urheberrechtlich geschützten Werkes nach § 14 UrhG. Vor allem sind aber die utilitaristischen Ansätze heranzuziehen, um die Immaterialgüterrechte in ihrem *status quo* rechtfertigen zu können.

B. Utilitaristische Theorien

Nach – mehrheitlich westlichem³⁰ – modernem Verständnis haben Ausschließlichkeitsrechte vor allem der Wohlfahrt dienliche bzw. volkswirtschaftlich erwünschte Effekte zu zeitigen, um Legitimation zu genießen.³¹ Volkswirtschaftlich erwünscht sind die Effizienzziele hohe Produktion, weite Verbreitung und niedrige Kosten im Umgang.³²

Die Anreiztheorie³³ bzw. das Anreizparadigma hat die Erhöhung der Produktion zum Ziel. So soll mit der Monopolstellung in Form des Ausschließlichkeitsrechts ein Anreiz geschaffen werden, neue immaterielle Güter zu schaffen und so den technischen und wirtschaftlichen Fortschritt zu fördern.³⁴ Die (befristete) Monopolstellung ermöglicht die Amortisation der – unter anderem im Patentrecht zum Teil sehr hohen – Fixkosten.³⁵ Vor allem im Hinblick auf die in der Regel wesentlich höheren Fixkosten in der Schaffung der Ausschließlichkeitsrechte im Vergleich zu den tiefen Kosten ihrer Vervielfältigung und Verbreitung und der damit einhergehenden Gefahr von Nachahmer:innen soll nach der Anreiztheorie der Nutzen internalisiert werden.³⁶ Die Ähnlichkeiten der Anreiztheorie mit der Belohnungstheorie sind augenfällig. Die Belohnungstheorie legt ihren Schwerpunkt aber auf die Belohnung im Gegenzug zu sozial-nützlichem Schaffen, anstatt wie die Anreiztheorie auf die Förderung von technischem und wirtschaftlichem Fortschritt.³⁷ Viele Künstler:innen, Autor:innen und auch Wissenschaftler:innen sind jedoch intrinsisch motiviert. Das zeigt sich

³⁰ Siehe für den Anreizgedanken Art. 1 Section 8 der US-Bundesverfassung.

³¹ Depenheuer/Peifer/SCHACK, S. 133 f.; SHAVELL, S. 21; ZECH, Information, S. 152 f.

³² Genauer: ZECH, Information, S. 154.

³³ Auch Anspornungstheorie genannt.

³⁴ BEIER, GRUR Int. 1970, 3 f.; COOTER/ULEN, S. 116 f.; SHAVELL, S. 11 ff.; STIERLE, S. 198 ff.

³⁵ So bspw. auch ZECH, Information, S. 154.

³⁶ STIERLE, S. 200; ZECH, Information, S. 154.

³⁷ BEIER, GRUR Int. 1970, 3; ZECH, Information, S. 152.

bspw. daran, dass v.a. Werke auch bereits in einer Zeit vor den Ausschließlichkeitsrechten geschaffen wurden.³⁸ Da die intrinsische Motivation für das Schaffen von immateriellen Gütern vordergründig für das Urheberrecht gilt, ist die Anreiztheorie in erster Linie im Patentrecht vorherrschend in der Rechtfertigung.³⁹ Damit vermag die Anreiztheorie nicht allein Ausschließlichkeitsrechte ökonomisch zu rechtfertigen.

Die Steigerung der Verbreitung von vorhandener Information in Form von immateriellen Gütern ist das Ziel der Offenbarungstheorie.⁴⁰ Die Offenbarungstheorie soll einen Anreiz schaffen, die Information in Form des immateriellen Gutes (möglichst früh im Schaffungsprozess) mit der Allgemeinheit zu teilen.⁴¹ So soll einerseits erreicht werden, dass geheime Information offenbart wird und diese so auch von anderen Personen als den Geheimnisinhaber:innen genutzt werden kann, ohne dass diese des Wertes Ihres Gutes verlustig gingen.⁴² Das bedingt aber, dass die Einräumung des Rechts die Offenbarung der Information verlangt,⁴³ wie das im Patentrecht der Fall ist.⁴⁴ Zudem hebt der Offenbarungsgedanke das sogenannte Geheimnisparadox auf, indem er den vertraglichen Umgang mit der Information erleichtert.⁴⁵ In der Regel können nicht allgemeinbekannte Informationen nur zum Gegenstand von Rechtsgeschäften werden, wenn sie zumindest teilweise offenbart werden. Dies kann bspw. bei Geschäftsgeheimnissen wirtschaftlich verheerend sein, da der ganze Wert der Information verloren gehen kann. Der Wert der Information geht aber nicht verloren, wenn der Vertragspartei ein Ausschließlichkeitsrecht an der Information eingeräumt wurde und der:die Geheimnisinhaber:in so eine rechtliche Handhabe gegeben wird, die Nutzung der Information durch andere zu verhindern.⁴⁶

³⁸ Siehe dazu bereits oben Kap- 4, A.; Depenheuer/Peifer/SCHACK, S. 134; LANDES/POSNER, S. 22.

³⁹ BEIER, GRUR Int. 1970, 3.

⁴⁰ BEIER, GRUR Int. 1970, 4; STIERLE, S. 206 ff.; ZECH, Information, S. 156.

⁴¹ BEIER, GRUR Int. 1970, 4; STIERLE, S. 206 ff.; ZECH, Information, S. 156, vgl. teilweise auch SHAVELL, S. 18 ff.

⁴² BEIER, GRUR Int. 1970, 4; ZECH, Information, S. 156.

⁴³ ZECH, Information, S. 156.

⁴⁴ Siehe dazu unten Kap- 7, B., III. ff.

⁴⁵ ZECH, Information, S. 156 m.w.N.

⁴⁶ ZECH, Information, S. 156.

Schließlich sollen durch Ausschließlichkeitsrechte die Kosten gesenkt werden, die durch den faktischen Umgang mit vorhandener (geheimer) Information einhergehen. So entstehen bspw. für die Geheimhaltung von Information Kosten. Diese reichen von Kosten für physische Sicherheitsmaßnahmen bis zu immateriellen Kosten wie zum Beispiel dem Aufwand für Geheimhaltungsvereinbarungen. Durch die Einräumung von Ausschließlichkeitsrechten werden die faktischen Kosten für die Geheimhaltung hinfällig. Zwar können auch durch die Einräumung von Ausschließlichkeitsrechten Kosten entstehen, sofern es sich dabei um Registerrechte handelt. Es ist dabei an die Kosten für die Anmeldung von Patenten zu denken oder an die Jahresgebühren. Doch sind solche Kosten für den rechtlichen Schutz niedriger als solche für den Faktischen.⁴⁷

Ausschließlichkeitsrechte stellen Monopole dar. Monopole haben schädliche Auswirkungen auf Gesellschaft und Wirtschaft.⁴⁸ Die mit Monopolen einhergehenden schädlichen Effekte werden im Immaterialgüterrecht durch Schranken und zeitliche Begrenzung verhindert bzw. zumindest abgemildert.⁴⁹ So weichen zum Teil Ausschließlichkeitsrechte bloßen Vergütungsansprüchen oder das Gesetz sieht eine gänzlich vergütungsfreie Nutzung bspw. eines Werkes vor.⁵⁰ Auch die Befristungen der Ausschließlichkeitsrechte betont deutlich, dass die Monopolstellung der Rechteinhaber:innen nicht unbegrenzt gelten soll.

C. Zwischenergebnis

Damit lässt sich zusammenfassen, dass die Begründungsansätze von Immaterialgüterrechten bzw. ausschließlichen Rechten an immateriellen Gütern unterschiedlich sind. Sie reichen von deontologischen Ansätzen, die von einem Naturrecht ausgehen bis hin zu utilitaristischen Ansätzen, die ökonomische Effizienzsteigerung zum Ziel haben. Sie variieren zudem von Immaterialgüterrecht zu Immaterialgüterrecht. So lässt sich beobachten, dass im Urheberrecht die persönlichkeitsrechtlichen Aspekte noch wesentlich ausgeprägter sind als bei den

⁴⁷ ZECH, Information, S. 157.

⁴⁸ Vgl. nur Depenheuer/Peifer/SCHACK, S. 135.

⁴⁹ Depenheuer/Peifer/SCHACK, S. 135 f.; ZECH, Information, S. 155.

⁵⁰ Vgl. bspw. die Privatkopieschranke im Urheberrecht in § 53 UrhG; weitergehend auch Depenheuer/Peifer/SCHACK, S. 135.

gewerblichen Schutzrechten.⁵¹ Während aber die ökonomischen Begründungsansätze bspw. im Patentrecht etabliert sind, wird sich im Urheberrecht noch über die wirtschaftsrechtliche Begründung gestritten.⁵² Auch innerhalb eines Immaterialgüterrechts sind die Stoßrichtungen unterschiedlich: so sind es vor allem wirtschaftliche Überlegungen, die Leistungsschutzrechte (§§ 70 ff. UrhG) rechtfertigen, während die Dauer des urheberrechtlichen Schutzes in § 64 ff. UrhG stark persönlichkeitsrechtlich geprägt ist. Somit ist es ein Zusammenwirken der verschiedenen Ansätze, das zur Rechtfertigung von Ausschließlichkeitsrechten an immateriellen Gütern herangezogen wird.

Dennoch liegt das Übergewicht der geeigneten Rechtfertigungstheorien auf den utilitaristischen, vor allem volkswirtschaftlichen, Ansätzen. Diese Ansätze haben vor allem zum Ziel, durch die Einführung eines Immaterialgüterrechtes ein Marktversagen zu verhindern.⁵³ Die deontologischen Ansätze lassen sich dabei für einzelne Aspekte der Immaterialgüterrechte heranziehen.

⁵¹ Bspw. ist die Befristung des Urheberrechts an die Lebensdauer des Urhebers gebunden, während im Patentrecht eine Begrenzung auf grundsätzlich 20 Jahre vorgesehen ist, siehe unten Kap. 7, B., III., Kap. 8, A, II., 3.

⁵² Vgl. bspw. Depenheuer/Peifer/OHLY, S. 141 ff. als Antwort auf Depenheuer/Peifer/SCHACK, S. 123 ff.

⁵³ Siehe bereits kurz oben Einl., C. und ausführlich sogleich Kap. 5, A. ff.

Teil 3

Ökonomische Analyse und Schutzbedürftigkeit von KI-Technologien

Die verschiedenen Rechtfertigungsansätze für Immaterialgüterrechte wurden im Überblick dargestellt. Es wurde gezeigt, dass utilitaristische Ansätze in einem modernen Verständnis des Immaterialgüterrechts geeigneter sind, Ausschließlichkeitsrechte zu rechtfertigen. Zumal die deontologischen Ansätze nach diesem Verständnis nur noch monetär weniger relevante Teilaspekte der Ausschließlichkeitsrechte zu rechtfertigen vermögen. Vor allem wenn die Rechtsordnung Investitionen schützen (Leistungsschutzrechte) und die Amortisation von Fixkosten ermöglichen (gewerblicher Rechtsschutz) soll, können die entsprechenden Normen nur utilitaristisch bzw. volkswirtschaftlich gerechtfertigt sein.

Deshalb wird für die vorliegende Arbeit als Ganzes ein ökonomischer Maßstab herangezogen.¹ Ohne Beachtung etwaiger Schutzrechte² wird im folgenden Teil der Markt für KI-Technologien nach möglichen Ineffizienzen untersucht, die ein Schutzrecht beheben könnte. Dazu werden in einem ersten Schritt die notwendigen ökonomischen Grundlagen gelegt und die Maßstäbe herausgearbeitet, anhand welcher die Marktanalyse erfolgen soll. Es wird aufgezeigt werden, dass Anzeichen für Ineffizienzen vorliegen, die auch auf ein Marktversagen hindeuten könnten. Damit gehen ineffizienzbedingte Wohlfahrtsverluste einher. Daraus lässt sich schließlich ein Schutzbedürfnis von KI-Technologien ableiten.

¹ Ohne jedoch den ökonomischen Maßstab genauer zu erläutern auch LINKE, S. 134 ff.

² Infrage kommende Schutzrechte sind Teil des vierten Teils der Arbeit.

Kapitel 5

Von der ökonomischen Analyse des Rechts zur Rechtspolitik

Die volkswirtschaftliche Rechtfertigung eines Immaterialgüterrechts hat das Verhindern bzw. das Beheben eines Marktversagens zum Ziel.¹ Was zeichnet einen funktionierenden Markt aus? Was muss vorliegen, damit ein Markt nach ökonomischem Verständnis nicht versagt? Die einfach formulierte Antwort auf diese Fragen lautet: Der Markt muss effizient sein. Genauer formuliert: Ein Markt gilt als effizient, wenn die Güter des Marktes effizient verteilt sind.² Mit einer effizienten Verteilung der Güter soll die Wohlfahrt maximiert werden. Damit ist der Maßstab der ökonomischen Analyse des Rechts die Wohlfahrtsökonomik. Rechtliche Regelungen haben demnach einem „wohlfahrtsökonomischen Effizienzkriterium“³ zu genügen.

Doch was bedeutet Effizienz? Der wohlfahrtsökonomische Effizienzbegriff ist vom juristischen Effizienzbegriff zu unterscheiden. Wenn Jurist:innen von Effizienz sprechen, kann dies oft als Wirtschaftlichkeit aufgefasst werden. Dabei geht es um eine Zweck-Mittel-Relation. Mit anderen Worten ist es vom jeweiligen Ziel abhängig, ob der Einsatz eines Mittels als wirtschaftlich erachtet wird. In der Wohlfahrtsökonomik ist aber die Effizienz Regelungsziel, an welchem andere Ziele und Mittel gemessen werden.⁴

Ob ein sozialer Zustand als effizient gilt, wird in der modernen Wohlfahrtsökonomik anhand einer Kosten-Nutzen-Rechnung beurteilt. Anfänglich wurde das *Pareto*-Kriterium zur Beurteilung der Effizienz eines Zustandes herangezogen: demnach gilt ein Zustand X gegenüber dem Zustand Y als effizient, wenn

¹ Siehe oben Kap. 6.

² TOWFIGH/PETERSEN, Rn. 153.

³ EIDENMÜLLER, S. 41.

⁴ Genauer: EIDENMÜLLER, S. 55 ff., S. 75.

mindestens ein Individuum den Zustand X präferiert und kein Individuum Zustand Y präferiert.⁵ Nach dem *Pareto*-Kriterium resultiert demnach *de facto* ein Veto-Recht eines jeden Individuums. Insbesondere die Rechtspolitik muss aber auch die Entscheidungen des Staates miteinbeziehen. Deshalb ist das *Pareto*-Kriterium für die ökonomische Analyse, welche u.a. rechtspolitischen Entscheidungen und Maßnahmen regelmäßig vorgeht, zu verwerfen: Es ist kein staatliches Eingreifen vorstellbar, mit welchem jedes Individuum einverstanden ist.⁶

Gestützt auf das *Pareto*-Kriterium folgte das *Kaldor/Hicks*-Kriterium. Nach KALDOR/HICKS ist ein Zustand X gegenüber dem Zustand Y auch dann effizient, wenn Individuen in Zustand Y einen Nachteil erleiden, die Vorteile der Individuen in Zustand X diese Nachteile aber aufwiegen.⁷ Wenn also die Nutzen in Zustand X die Kosten in Zustand Y übertreffen.⁸ Das *Kaldor/Hicks*-Kriterium wird ebenfalls in der ökonomischen Analyse des Rechts herangezogen⁹ und scheint diesbezüglich die Problematik des *Pareto*-Kriteriums zu lösen, indem es nicht mehr jedem Individuum ein quasi Veto-Recht einräumt. Allerdings ergeben sich für die Rechtspolitik beim *Kaldor/Hicks*-Kriterium vor allem Probleme betreffend die Wertung und Messung der einzelnen Kosten bzw. Nutzen.¹⁰ Die Bewertung von Kosten und Nutzen in Geldeinheiten ist lediglich in der Theorie einfach zu bewerkstelligen – in der Praxis gestaltet sich diese Bewertung als herausfordernd,¹¹ sodass das *Pareto*- sowie das *Kaldor/Hicks*-Kriterium eher als konzeptionelle Grundlagen für das rechtspolitische Programm gesehen werden können.¹² Sie dienen der Ermittlung und Bewertung der Folgen rechtlicher Regeln.¹³

Die ökonomische Analyse des Rechts befasst sich nur mit dem Status Quo des Rechts – der *lex lata*. Sobald aus der ökonomischen Analyse des Rechts gestützt auf die Ermittlung und Bewertung der *lex lata* aber Änderungen des geltenden

⁵ EIDENMÜLLER, S. 48 m.w.N.

⁶ EIDENMÜLLER, S. 49.

⁷ KALDOR, 550; HICKS, 706.

⁸ COOTER/ULEN, S. 42 f.; EIDENMÜLLER, S. 51 ff.

⁹ EIDENMÜLLER, S. 52.

¹⁰ EIDENMÜLLER, S. 54.

¹¹ EIDENMÜLLER, S. 54.

¹² So bspw. EIDENMÜLLER, §§1 und 2.

¹³ EIDENMÜLLER, S. 57.

Rechts gefordert werden, übertritt die ökonomische Analyse des Rechts die Schwelle zur Rechtspolitik. Diese befasst sich mit der Frage nach der Beschaffenheit von rechtlichen Regeln.¹⁴

Grundlage für eine auf die ökonomische Analyse des Rechts fußende Rechtspolitik ist das *Coase*-Theorem. Das *Coase*-Theorem wurde von POSNER weiterentwickelt.¹⁵ COASE ging davon aus, dass Individuen gestützt auf Verhandlungen immer eine invariante und effiziente Allokation volkswirtschaftlicher Ressourcen erreichen.¹⁶ Bedingung für eine effiziente Ressourcenallokation ist aber die Abwesenheit von (prohibitiv hohen) Transaktionskosten.¹⁷ COASE stellte sich also gegen staatliche Eingriffe und verließ sich auf das Verhandlungsgeschick der Marktteilnehmer.¹⁸

POSNER kommt auf COASE zurück und greift dessen Verhandlungslösung auf, plädiert aber dafür, dieses nur als Denkmodell heranzuziehen.¹⁹ Das soll heißen, dass bei der Absenz von Transaktionskosten und der Möglichkeit von fairen Verhandlungen die Ressource immer demjenigen Marktakteur zukommt, welcher dazu bereit ist, am meisten für sie zu bezahlen bzw. der Ressource am meisten Wert beimisst.²⁰ Damit aber eine solche Verhandlungslösung überhaupt funktionieren kann, muss ein Markt vorliegen, auf welchem die Ressourcen – *in casu* Rechtspositionen – ver- und gehandelt werden. Aus diesem Denkmodell POSNERS können für das rechtspolitische Programm der ökonomischen Analyse des Rechts drei Anforderungen an das Recht abgeleitet werden: In erster Linie muss das Recht einen Markt für Rechtspositionen zulassen. In zweiter Linie soll das Recht die Markttransaktionen erleichtern und drittens soll das Recht die marktmäßige Lösung dort simulieren, wo die Markttransaktionen durch prohibitiv hohe Kosten verhindert werden.²¹

¹⁴ EIDENMÜLLER, S. 58.

¹⁵ POSNER, S. 50 ff.

¹⁶ COOTER/ULEN, S. 81 ff.; EIDENMÜLLER, S. 59 ff., S. 75.

¹⁷ COOTER/ULEN, S. 88 ff.

¹⁸ EIDENMÜLLER, S. 60, welcher COASES Ziel als anti-interventionistisch bezeichnet.

¹⁹ POSNER, S. 50 f.

²⁰ POSNER, S. 50 ff.

²¹ POSNER, S. 54 f.; EIDENMÜLLER, S. 63.

Die erste Anforderung sieht mit anderen Worten lediglich vor, dass Rechtspositionen handelbar sein müssen. Handelbare Rechtspositionen kennen wir typischerweise vom Eigentum. Es gibt aber auch Rechtspositionen, die nicht handelbar sind. Zu denken ist dabei an den Extremfall der Verfügungsgeschäfte über Menschen.²²

Die zweite Anforderung will die Transaktions- und damit die Handelshindernisse weitestgehend minimieren. Transaktionskosten können nämlich prohibitiv wirken und damit verhindern, dass eine Rechtsposition überhaupt gehandelt wird. Aber auch hier gibt es Ausnahmen im Recht: Formvorschriften sind eben solche Transaktionshindernisse, die die Transaktionskosten erhöhen und mithin die Erträge der handelnden Parteien minimieren. Formerfordernisse sind jedoch – wiederum teilweise aus paternalistischen Überlegungen – gewünscht und üblich.²³

Die dritte Anforderung verlangt ein Eingreifen des Staates über rechtliche Regelungen, sobald die Verhandlungslösung ausgeschlossen ist und damit der Markt nicht funktioniert.²⁴ Mit anderen Worten soll also das Recht, sobald der Markt versagt, die Rechtsposition so zuweisen, dass die Zuweisung dem Verhandlungsergebnis entspricht, auf welches sich die Parteien ohne den verhin-dernden Umstand auf einem funktionierenden Markt geeinigt hätten. Im Falle von POSNER ist dieser Umstand die prohibitive Höhe der Transaktionskosten.²⁵ Allerdings gibt es weitere Gründe, weshalb Märkte versagen. Auf diese wird so- gleich eingegangen.

Ausgehend von der ökonomischen Analyse anhand des Effizienzkriteriums geht es also bei der Rechtspolitik darum, Recht „an marktmäßigen Gesichtspunkten zu gestalten.“²⁶ Allerdings wurde auch klar, dass das Recht erst dann und nur so weit gestalterisch in den Markt eingreifen soll, wenn dieser versagt.²⁷ So soll ein

²² Vgl. EIDENMÜLLER, S. 363 ff. Beispiele dafür sind v.a. Versklavung, Menschen- und Organhandel.

²³ Vgl. EIDENMÜLLER, S. 64.

²⁴ EIDENMÜLLER, S. 65 ff.

²⁵ Siehe zum Beispiel POSNER, S. 51.

²⁶ EIDENMÜLLER, S. 66.

²⁷ Vgl. oben Kap- 5: dritte Anforderung.

effizientes Ergebnis sichergestellt werden.²⁸ Das effiziente Ergebnis ist die effiziente Allokation und damit effiziente Zuweisung von volkswirtschaftlichen Ressourcen.

Dabei ist aber zu beachten, dass der staatliche Eingriff nicht lediglich eine Ineffizienzquelle durch eine andere ersetzen darf.²⁹ Mitunter muss also auch der staatliche Eingriff ökonomisch analysiert werden und der *status quo* des Marktes mit dem *status quo post* des Marktes (nach rechtlichem Eingriff) anhand des *Kaldor/Hicks*-Kriteriums abgewogen werden. Der rechtliche Eingriff ist nur dann gerechtfertigt und nach einem ökonomischen Maßstab erwünscht, wenn er eine effizientere Ressourcenallokation ermöglicht als der *status quo*.

Neben dem ökonomischen Ansatz, der das Effizienzziel als vorrangiges Ziel für die Rechtspolitik sieht, existieren noch weitere Maßstäbe für die Rechtspolitik. Unter sie fallen unter anderem soziologische oder ethische Ansätze bzw. Mischformen wie bspw. die Verteilungsgerechtigkeit. Diese sollen aber für die vorliegende Arbeit nicht primär herangezogen werden. Ökonomische Effizienz gilt – wie aufgezeigt und noch weiter aufzuzeigen sein wird – als Teil der utilitaristischen Rechtfertigung des Immaterialgüterrechts im Besonderen. Für die vorliegende Arbeit wird sodann hauptsächlich der ökonomische Maßstab angewendet. Nicht zuletzt auch deshalb, weil das Immaterialgüterrecht ebenfalls die Steigerung von Effizienzen – der statischen und dynamischen – zum Ziel hat.³⁰

In einem nächsten Schritt werden die Marktversagensgründe genauer vorgestellt, auf welche es den KI-Markt zu untersuchen gilt, um ein etwaiges Schutzbedürfnis bzw. die Notwendigkeit eines rechtlichen Eingreifens des Staates bestimmen zu können.

²⁸ EIDENMÜLLER, S. 66 drückt es so aus, dass die Logik des Marktes das Recht beherrsche.

²⁹ Vgl. EIDENMÜLLER, S. 67.

³⁰ Vgl. oben Kap. 4, B. ff. und sogleich Kap. 5, B., I. ff.

A. Marktversagensgründe

Es wurde aufgezeigt, dass ein Markt dann versagt, wenn er die Ressourcen nicht effizient zuzuteilen vermag.³¹ Die Gründe für ein solches Versagen können unterschiedliche sein, doch können Sie unter die vier Fallgruppen von Marktmacht, asymmetrischer Information, externen Effekten und öffentliche Güter zusammengefasst werden

I. *Marktmacht*

Es existieren verschiedene Formen von Marktmacht: Monopole, Kartelle und Oligopole.³² Gemein ist ihnen, dass auf Märkten mit Marktmacht die anbietenden Marktakteure den Preis nicht als gegeben akzeptieren müssen, sondern diesen beliebig festsetzen können. Damit können sie den Preis auch (langfristig) anheben.³³ Der Preis für das Gut ist in diesem Fall nicht mehr effizient. Die Nachfrage hängt allerdings vom Preis ab und damit wird das Gut in der falschen – ineffizienten – Menge nachgefragt *und* angeboten. Mit anderen Worten werden potentielle Nachfrager des Gutes ausgeschlossen, obwohl sie dazu bereit wären, die Herstellungskosten zzgl. einer gewissen – der effizienten – Gewinnmarge zu bezahlen. Damit sinkt allerdings auch die Produktionsrente³⁴ und nicht nur die Konsumentenrente. So verliert also auch der Anbieter mit Marktmacht im Vergleich zum Markt ohne Marktmacht – nicht nur die Konsument:innen. Daher sinkt auf Märkten mit Marktmacht die Gesamtrente im Vergleich zum Markt derselben Güter ohne Marktmacht: Der Markt versagt.

Positionen mit Marktmacht – seien diese monopolistisch, oligopolistisch oder kartellistisch – können sowohl stabil als auch instabil sein. Sie sind instabil,

³¹ Oben Kap.5, statt vieler: COOTER/ULEN, S. 38; TOWFIGH/PETERSEN, Rn. 153.

³² Bspw. COOTER/ULEN, S. 39.

³³ COOTER/ULEN, S. 38; SCHÄFER/OTT, S. 86.

³⁴ Weil mit einer falschen Produktionsmenge auch die Produktionsrente aufgrund der ineffizienten Produktionsstruktur sinkt, SCHÄFER/OTT, S. 86.

wenn die Markteintrittsschwelle niedrig ist und man davon ausgeht, dass die preisbestimmende Position Anreize für weitere Wettbewerber setzt.³⁵

Stabil sind solche Strukturen, wenn der Marktzutritt erschwert oder gar unmöglich gemacht wird. So kann der Marktzutritt gesetzlich versagt sein, wie das bspw. beim Notarberuf in Deutschland und in der Schweiz der Fall ist.³⁶ Andererseits kann der Marktzutritt auch *de facto* versagt sein. Dies ist bspw. der Fall, wenn nur eine bestimmte Kostenstruktur eines Unternehmens den Marktzutritt ermöglicht. Das kann entweder darin begründet liegen, dass nur das Unternehmen über die erforderliche Infrastruktur verfügt, das Gut herzustellen bzw. anzubieten.³⁷ Oder dies liegt in Skaleneffekten begründet: die Durchschnittskosten pro hergestelltes Gut sinken bei Erhöhung der Produktion, während aber die Herstellungskosten in einem ersten Schritt (prohibitiv) hoch waren.³⁸

II. Externe Effekte

Die Markttheorie besagt, dass alle Kosten und der gesamte Nutzen bei Herstellung und Konsum eines Gutes bei denjenigen anfallen, die die Markttransaktion vornahmen.³⁹ Von externen Effekten wird gesprochen, wenn dies nicht der Fall ist. Wenn also Kosten und/oder Nutzen bei anderen Akteur:innen anfallen als bei denjenigen, die die Markttransaktion tätigten.⁴⁰ Typisches Beispiel ist die Umweltverschmutzung bei der Herstellung eines Gutes. Dabei handelt es sich um einen (Wohlfahrts)kostenpunkt, der sich ohne staatlichen Eingriff nicht in der Kosten-Nutzen-Rechnung der Anbieter:innen niederschlägt.⁴¹ Es resultieren wiederum falsche Preise, die nicht die wirklichen Kosten widerspiegeln. Die angebotene Menge ist demnach für den Marktpreis zu hoch.⁴² Die Gesamtrente des Marktes sinkt.⁴³

³⁵ TOWFIGH/PETERSEN, Rn. 157.

³⁶ TOWFIGH/PETERSEN, Rn. 157.

³⁷ Im digitalen Kontext ist hierbei vor allem an Serverinfrastrukturen und Daten zu denken.

³⁸ TOWFIGH/PETERSEN, Rn. 157.

³⁹ COOTER/ULEN, S. 39; SCHÄFER/OTT, S. 88; SHAVELL, S. 77 ff.; TOWFIGH/PETERSEN; Rn. 161.

⁴⁰ COOTER/ULEN, S. 39 f.; SCHÄFER/OTT, S. 88; SHAVELL, S. 77 ff.

⁴¹ COOTER/ULEN, S. 39; SCHÄFER/OTT, S. 88; TOWFIGH/PETERSEN, Rn. 161.

⁴² COOTER/ULEN, S. 40; SCHÄFER/OTT, S. 88; TOWFIGH/PETERSEN, Rn. 161.

⁴³ SCHÄFER/OTT, S. 88; TOWFIGH/PETERSEN, Rn. 161.

In solchen Fällen soll rechtliches Eingreifen diese externen Effekte bei denjenigen Marktakteur:innen internalisieren, die an der Markttransaktion beteiligt sind.⁴⁴

III. Informationsasymmetrie

Zum Teil wird auch das Vorliegen von asymmetrischen Informationen als Form des Marktversagens gesehen. Es geht bei der Informationsasymmetrie darum, dass bei Marktakteur:innen nicht dieselben Informationen vorhanden sind.⁴⁵ Eines der Beispiele ist der Gebrauchtwagenkauf: Wenn sich die Käuferin nicht sicher ist, wie stark der Wagen gebraucht wurde bzw. wie hoch dessen Qualität ist, wird sie keinen hohen Preis für den Wagen bezahlen. Außer sie sucht eine andere Werkstatt oder eine:n Gutachter:in auf und lässt den Wert schätzen. Aber auch das ist wiederum mit Kosten verbunden. Abermals wird kein effizienter Preis erreicht, den die Käuferin in Kenntnis der Qualität aber zu bezahlen gewillt wäre. Ein anderes Beispiel ist das Arbeitsverhältnis: der Arbeitgeber will gute Arbeit entsprechend entlohnen. Doch es ist ihr nicht möglich, die Arbeitnehmerin ständig zu überwachen und ihre Arbeit zu bewerten. Entsprechend wird ein tieferer Lohn bezahlt und die Arbeitnehmerin wird nicht so gut arbeiten, wie sie dies bei einem besseren Lohn täte.⁴⁶

In beiden Beispielen kann keiner der Marktakteure sämtliche wertsteigernden Transaktionen verwirklichen und die Gesamtrente des Marktes bleibt hinter ihrem Potenzial zurück.⁴⁷

⁴⁴ Es sei kurz darauf hingewiesen, dass *Coase* davon ausging, dass auch bei Vorliegen externer Effekte Markteffizienz erreicht werden kann. Dies sei nämlich dann der Fall, wenn das Recht, externe Effekte zu erzeugen oder zu unterbinden, handelbar wäre. Auf diese Art und Weise können die Externalitäten nämlich internalisiert werden. Allerdings gilt das auch nur insofern und solange, als dass die Transaktionskosten vernachlässigbar tief sind. Vgl. dazu genauer auch TOWFIGH/Petersen, Rn. 162; vgl. auch SHAVELL, S. 80 ff., insb. S. 92 ff.

⁴⁵ COOTER/ULEN, S. 41; SPIECKER GEN. DÖHMANN, S. 40; TOWFIGH/PETERSEN, Rn. 160.

⁴⁶ Beispiele entnommen bei TOWFIGH/PETERSEN, Rn. 160; vgl. aber auch SPIECKER GEN. DÖHMANN, S. 40.

⁴⁷ COOTER/ULEN, S. 41 f.; TOWFIGH/PETERSEN, Rn. 160.

IV. *Nicht private Güter/öffentliche Güter*

Ein weiterer und für die Rechtfertigung des Immaterialgüterrechts wesentlicher⁴⁸ Marktversagensgrund liegt vor, wenn die auf dem Markt gehandelten Güter nicht privat bzw. wenn sie öffentlich sind.⁴⁹ Öffentliche Güter sind im Verbrauch nicht exklusiv und nicht rival.⁵⁰ Das heißt, die einzelnen Marktteilnehmer:innen können andere Marktteilnehmer:innen nicht vom Gebrauch des Gutes ausschließen und, öffentliche Güter können von mehreren Akteur:innen gleichzeitig gebraucht werden, ohne dass der Nutzungswert des Gutes abnimmt.⁵¹ Die Ökonomik der Informationsgüter geht davon aus, dass Information – zumindest semantische Information – ein öffentliches Gut darstellt.⁵²

Der Markt versagt bei öffentlichen Gütern, weil es für die Anbieter:innen keine Möglichkeit gibt, Nachahmer:innen und Trittbrettfahrer:innen von der Nutzung auszuschließen.⁵³ Handelt es sich bei den auf dem Markt gehandelten Gütern um öffentliche Güter oder weisen die Güter zumindest Merkmale von öffentlichen Gütern auf, werden aufgrund des Nachahmungsrisikos zu wenig Güter produziert.⁵⁴ Gleichzeitig wird von den Gütern weniger nachgefragt als wenn sie rival wären. Da die Nachfrager:innen hoffen, umsonst an das Gut zu kommen. Damit verheimlichen sie ihre Nachfrage. Im Endeffekt werden für die Nachfrage zu wenig Güter angeboten, was dazu führt, dass der Preis für das Gut zu hoch ist.⁵⁵

Ein anderer kostentreibender Punkt besteht darin, dass die Anbieter die Rivalität oder zumindest die Exklusivität bei Gütern mit Merkmalen von öffentlichen Gütern faktisch herstellen müssen – bspw. mit technischen Schutzmaßnahmen. Offensichtlich gehen mit solchen technischen Schutzmaßnahmen zusätzliche

⁴⁸ Vgl. bspw. SPIECKER GEN. DÖHMANN, S. 39.

⁴⁹ COOTER/ULEN, S. 40 f.; SCHÄFER/OTT, S. 86 f.; TOWFIGH/PETERSEN, Rn. 166.

⁵⁰ SCHÄFER/OTT, S. 86; TOWFIGH/PETERSEN, Rn. 166; vgl. SHAVELL, S. 111 f.

⁵¹ COOTER/ULEN, S. 40; SHAVELL, S. 110 ff.

⁵² Siehe dazu ausführlich ZECH, Information, S. 153 ff. m.w.N.

⁵³ COOTER/ULEN, S. 41 und S. 103 f.; SCHÄFER/OTT, S. 86 f.; TOWFIGH/PETERSEN, Rn. 166; d.h. es liegt ein externer Effekt vor.

⁵⁴ COOTER/ULEN, S. 41; SPIECKER GEN. DÖHMANN, S. 39; SCHÄFER/OTT, S. 86 f.; TOWFIGH/PETERSEN, Rn. 166.

⁵⁵ SCHÄFER/OTT, S. 87; SHAVELL, S. 112 f.; TOWFIGH/PETERSEN, Rn. 166.

Kosten einher, die ein Anbieter durch einen höheren Preis umzulegen versucht – wieder ist der Marktpreis zu hoch und wohlfahrtsökonomisch ineffizient.⁵⁶

B. Volkswirtschaftliche Ziele

Um eine umfassende Analyse des Marktes für KI-Technologien durchführen zu können und daraus dann eventuelle Marktversagensgründe abzuleiten, wären ökonomische empirische Erhebungen über den Markt notwendig. Vor dem Hintergrund, dass es sich hierbei um eine juristische Arbeit handelt, können ökonomische empirische Erhebungen im Rahmen dieser Arbeit nicht geleistet werden.

Die Fähigkeiten von Jurist:innen liegen aber darin, einen Sachverhalt normativ einzuordnen. Soll also die Frage nach einer ökonomisch begründeten Schutzbedürftigkeit von KI-Technologien aus einer juristischen Perspektive beantwortet werden, so muss ein normativer Maßstab gefunden werden. Dieser lässt sich erörtern, wenn die Marktversagensgründe positiv formuliert werden – in Form von volkswirtschaftlichen Zielen

Im Rahmen der ökonomischen Grundlagen konnte gezeigt werden, dass Effizienz das Ziel von rechtlichen Regelungsvorhaben ist. Ob ein Zustand effizient ist, wird anhand einer Kosten-Nutzen-Analyse beurteilt. Angewandt auf den Markt für KI-Technologien ist also zu beurteilen, ob der Markt im Status ohne Schutzrecht effizient ist. Anders formuliert: ergibt die Kosten-Nutzen-Analyse des Zustands ohne Schutzrecht einen größeren Wohlfahrtsgewinn als die Kosten-Nutzen-Analyse des Zustands mit einem entsprechenden Schutzrecht?

Schutzrechte sollen die Information schützen, die die KI-Technologie verkörpert. Bei Information als Marktgut wurde aber auch schon ersichtlich, dass sie öffentliche Güter darstellen oder zumindest Charakteristika von öffentlichen Gütern aufweisen.⁵⁷ Damit befinden wir uns bereits im Teilbereich des Marktversagensgrundes der öffentlichen Güter und der damit einhergehenden Gefahr der Unterproduktion bzw. Produktionsineffizienz. Wenn also die Marktanalyse

⁵⁶ SCHÄFER/OTT, S. 8.

⁵⁷ Vgl. oben Kap. 5, A., IV.

zeigen würde, dass zu wenig KI-Technologien entwickelt würden, müsste das Recht über Schutzrechte entsprechende Anreize zur Produktion setzen.

Produktionseffizienz allein ist aber noch nicht wohlfahrtsfördernd. Die (produzierte) Information soll auch verbreitet werden. So wird nicht nur die Schaffung neuer Information gestützt auf die bereits vorhandene ermöglicht. Es ist auch sichergestellt, dass die Information demjenigen Marktakteur zugeteilt wird, der die Information am höchsten bewertet. Das bedeutet, dass Anreize durch rechtliche Eingriffe gesetzt werden müssen, sollten die Informationen von KI-Technologien nicht effizient verbreitet werden.

Wenn das Vorliegen von Marktversagensgründen auf dem Markt für KI-Technologien aufgrund fehlender ökonomisch-empirischer Untersuchungsmöglichkeiten nicht festgestellt werden kann, kann ein etwaiges Schutzbedürfnis für KI-Technologien auch anhand der Frage nach Zielerreichung beantwortet werden. Die Marktversagensgründe treten nicht auf, wenn der Markt folgende volkswirtschaftliche Ziele erreicht: (i) hohe Produktion von Gütern, (ii) weite Verbreitung der Güter und (iii) niedrige Kosten im Umgang mit den Gütern.⁵⁸ Der Markt für KI-Technologien ist also darauf zu untersuchen, ob er die genannten Ziele erreicht. Als Marktgut wird die KI-Technologie als immaterielles Gut und damit als Information betrachtet.⁵⁹

I. Ziel der hohen Produktion – dynamische Effizienz

Ein Ziel eines effizienten Marktes ist dasjenige der hohen Produktion neuer Information. Information gilt als einer der wichtigsten Wohlfahrtsfaktoren für eine Gesellschaft. Neue Information bedeutet neues Wissen. Wissen bedeutet Wohlfahrtsgewinne.⁶⁰ Aus dem markttheoretischen Ziel der hohen Produktion von Information leitet sich auch das Anreizparadigma in der utilitaristischen Rechtfertigung von Immaterialgüterrechten ab.⁶¹

⁵⁸ ZECH, Information, S. 154; vgl. auch SCHÄFER/OTT, S. 745; SIEBER, NJW 1989, 2575.

⁵⁹ Bislang waren die markttheoretischen Ausführungen allgemeiner Natur – unabhängig der Natur des Marktgutes.

⁶⁰ COOTER/ULEN, S. 113; SCHÄFER/OTT, S. 745; SHAVELL, S. 139; vgl. ZECH, Information, S. 154.

⁶¹ Vgl. oben Kap. 4, B.

Immateriellen Gütern und damit auch Informationen ist gemein, dass ihre variablen Kosten sehr tief sind.⁶² Das heißt die Grenzkosten für die Vervielfältigung sind sehr niedrig. Grenzkosten beschreiben die Kosten, die für die Herstellung einer zusätzlichen Einheit anfallen.⁶³ Damit sind immaterielle Güter und Informationen günstig zu vermarkten.⁶⁴ Allerdings verursachen immaterielle Güter bzw. ihre Schaffung oft sehr hohe Fixkosten.⁶⁵ Fixkosten beschreiben die Kosten, die es zur Schaffung eines Gutes bedarf – unabhängig der Nachfrage und anderer Faktoren.⁶⁶ Beispiele für immaterielle Güter mit hohen Fixkosten sind u.a. Erfindungen – vor allem im pharmazeutischen Bereich.⁶⁷

Die tiefen Grenzkosten führen dazu, dass es Trittbrettfahrer:innen bzw. Nachahmer:innen vergleichsweise günstig möglich ist, das Gut zu kopieren und eigenständig zu vermarkten – und zwar zu Grenzkostenpreisen. Wenn es aber den ursprünglichen Produzenten nicht möglich ist, ihre Fixkosten durch einen über den Grenzkosten liegenden Preis zu amortisieren, wird niemand produzieren und neues Wissen generieren wollen.⁶⁸ Schutzrechte können hier eingreifen, indem sie durch ihren Schutz, der damit „künstlich“ erzeugten Rivalität sowie Exklusivität und der damit einhergehenden ausschließlichen Vertriebsbefugnis eine entsprechende Amortisation ermöglichen.⁶⁹ Wenn also die Analyse des KI-Technologien-Marktes eine Produktionsineffizienz zeigen würde, könnte daraus ein Schutzbedürfnis abgeleitet werden.

Allerdings ist es den Produzent:innen auch ohne Schutzrecht möglich, Trittbrettfahrer:innen und Nachahmer:innen von der Verbreitung ihrer Information abzuhalten. Mit faktischen Schutzmaßnahmen, namentlich durch Geheimhaltung, können sie Trittbrettfahrer:innen und Nachahmer:innen die

⁶² COOTER/ULEN, S. 114; LANDES/POSNER, S. 24; SHAVELL, S. 138.

⁶³ Springer Gabler (Hrsg.), *Kompakt-Lexikon Wirtschaft*, S. 187.

⁶⁴ COOTER/ULEN, S. 114; LANDES/POSNER, S. 16 f., S. 24; SHAVELL, S. 138; ZECH, *Information*, S. 154.

⁶⁵ COOTER/ULEN, S. 114; LANDES/POSNER, S. 16 f.; S. 24; SHAVELL, S. 138.

⁶⁶ Springer Gabler (Hrsg.), *Kompakt-Lexikon Wirtschaft*, S. 154.

⁶⁷ ZECH, *Information*, S. 154.

⁶⁸ SHAVELL, S. 138, S. 140.

⁶⁹ Statt vieler: COOTER/ULEN, S. 116 ff.; SCHÄFER/OTT, S. 745 f.; SHAVELL, S. 142; vgl. auch LANDES/POSNER, S. 13, S. 20.

Möglichkeit nehmen, an ihre Information zu gelangen und diese zu Grenzkosten auf den Markt zu bringen.⁷⁰ Bei KI-Technologien ist dabei insbesondere an technische Schutzmaßnahmen wie Verschlüsselungen zu denken.⁷¹ Wenn die Information nicht offenkundig ist und potenzielle Nachahmer:innen aufgrund der Schutzmaßnahmen nicht an die Information gelangen können, können die Produzent:innen ihre Fixkosten über den Preis amortisieren.

Selbstredend sind solche faktischen Schutzmaßnahmen mit zusätzlichen Kosten verbunden.⁷² Diese Zusatzkosten sind aber wiederum effizienzmindernd.⁷³

II. Ziel der weiten Verbreitung – statische Effizienz

Die Generierung von neuem Wissen allein erzeugt noch wenig wohlfahrtseffiziente Wirkungen. Erst wenn das Wissen auch verbreitet und dadurch Wert erzeugt wird, entstehen die wohlfahrtsökonomisch gewünschten Effekte.⁷⁴ Durch die Verbreitung des Wissens kann neues, auf dem bereits bestehenden Wissen beruhendes Wissen generiert werden.⁷⁵ Zudem wird durch die Verbreitung von Wissen sichergestellt, dass es an den Ort der „nützlichsten Verwendung“⁷⁶ gelangt.⁷⁷

Ein freier Markt mit uneingeschränkten Nutzungsmöglichkeiten wäre dazu am besten geeignet, bestehende Information möglichst weit zu verbreiten und gestützt darauf, neues Wissen zu generieren.⁷⁸ Gegen die Einführung einer solchen Marktstruktur spricht aber der soeben in Kapitel 5, B., I. genannte Einwand der Produktionsineffizienz aufgrund von Trittbrettfahrerproblematiken.⁷⁹

⁷⁰ Vgl. auch COOTER/ULEN, S. 115; SHAVELL, S. 140 f, S: 149.

⁷¹ Siehe dazu genauer unten Kap. 9, B., I. ff.; vgl. auch COOTER/ULEN, S.114.

⁷² Siehe dazu sogleich das dritte volkswirtschaftliche Ziel, Kap. 5, B., III. ff.; so auch SHAVELL, S. 149.

⁷³ Oben unter Kap. 5, A. ff. wurde gezeigt, dass sich Effizienz mittels Kosten-Nutzen-Vergleichs berechnen und bewerten lässt.

⁷⁴ SHAVELL, S. 18 ff., S. 139.

⁷⁵ Statt vieler: SCHÄFER/OTT, S. 745; vgl. auch SHAVELL, S. 148.

⁷⁶ SCHÄFER/OTT, S. 745.

⁷⁷ Statt vieler: SCHÄFER/OTT, S. 745; SHAVELL, S. 138.

⁷⁸ SCHÄFER/OTT, S. 745; SHAVELL, S. 139; vgl. zur Bedeutung eines Nachahmungswettbewerbs auch LANDES/POSNER, S. 22 f.

⁷⁹ Oben Kap. 5, B. I. ff.; SCHÄFER/OTT, S. 745 f.

Der Zielkonflikt zwischen Anreizen zur Generierung von neuem Wissen und Anreizen zur Verbreitung bestehenden Wissens wird offenkundig.⁸⁰ Der Zielkonflikt ist dahingehend aufzulösen, dass die Situation – Schutzrecht oder kein Schutzrecht – Vorzug erhält, welche die höheren Wohlfahrtsgewinne mit sich bringt.⁸¹ Die Einführung eines Schutzrechts führt zu Wohlfahrtsverlusten, weil der freie Nachahmungswettbewerb beeinträchtigt oder unmöglich gemacht wird.⁸² Allerdings kann eine Situation ohne Schutzrecht zum gleichen Ergebnis führen: Wenn der Nachahmungswettbewerb durch Geheimhaltung der Produzenten faktisch verunmöglicht wird.⁸³ Geheimhaltung verursacht damit nicht nur Kosten auf Seiten der Geheimnisinhaber:innen⁸⁴ sondern auch auf Seiten der Gesellschaft.

Dabei ist einerseits an die Wohlfahrtsverluste aufgrund der faktischen Verhinderung des Nachahmungswettbewerbs zu denken.⁸⁵ Andererseits kann Geheimhaltung von Information zum Verlust der Information führen. Als Beispiel dafür werden die Werke von WILLIAM SHAKESPEARE genannt. Alle seine Werke wurden sicher im Globe Theater weggesperrt und jeweils nur den Schauspieler:innen und nur zwecks Erlernens der Texte übergeben. Während SHAKESPEARES Leben wurden nur fünf seiner 39 Werke veröffentlicht – gegen seinen Willen. Die restlichen Werke blieben unveröffentlicht und wären bis zum heutigen Tage wohl verschollen, wie das mit mehreren Werken von JEAN-PHILIPPE RAMEAU passierte, hätten nicht Kolleg:innen SHAKESPEARES die Werke nach dessen Tod veröffentlicht und so für den Erhalt der Information in Form der Werke durch Verbreitung gesorgt.⁸⁶ Es liegt auf der Hand, dass der Verlust von Information wohlfahrtsmindernd oder gar -schädigend ist. Aus verlorener Information lässt sich kein Nutzen generieren.

⁸⁰ SCHÄFER/OTT, S. 746.

⁸¹ SHAVELL, S. 144.

⁸² SCHÄFER/OTT, S. 746; SHAVELL, S. 138.

⁸³ Vgl. auch ZECH, Information, S. 156.

⁸⁴ Es sei dabei an die Kosten für die faktischen Schutzmaßnahmen zu erinnern.

⁸⁵ Analog den Gesellschaftskosten, die bei monopolistischen Situationen anfallen.

⁸⁶ Siehe dazu ausführlicher SCHÄFER/OTT, S. 746.

Zwar stellt ein Schutzrecht ein Hindernis für den freien Nachahmungswettbewerb dar.⁸⁷ Ein Schutzrecht kann aber auch zur statischen Effizienz beitragen. Durch Schutzrechte wird ein Markt für Wissen in Form von Information ermöglicht.⁸⁸ Es stellt die Produktion von neuer Information sicher und befreit die Anbieter:innen davon, auf Geheimhaltung (und damit zusätzliche Kosten) zurückgreifen zu müssen. Ohne Geheimhaltung kann die Information als solche überhaupt auf dem Markt zirkulieren. Dadurch wird wiederum Wissen verbreitet, was dann Folgewissen generieren kann.⁸⁹ Ein freier Nachahmungsmarkt würde allerdings diese Menge an Folgewissen übertreffen und diesbezüglich wohlfahrtseffizienter sein, aber eben auch zu Produktionsineffizienzen führen.

Im Hinblick auf die Verbreitung von KI-Technologien und der damit zusammenhängenden Informationen ist darauf hinzuweisen, dass ein Schutzregime auch Bewegungen wie Copyleft und Open-source- bzw. Opensoftware überhaupt erst sinnvoll ermöglichen kann. Nur mittels eines wirksamen Ausschließlichkeitsrechts können die Rechtsinhaber:innen erst die *community*-Regeln durchsetzen.

Es ist also bei der Analyse des Marktes für KI-Technologien darauf zu achten, ob die Informationen im Zusammenhang mit KI-Technologien (effizient) verbreitet werden. Ergibt die Analyse des Marktes, dass KI-Technologien nicht verbreitet werden, würde dies ebenfalls ein Schutzbedürfnis begründen können. Allerdings müsste das Schutzrecht mehr Wohlfahrtsgewinne ermöglichen, als das Schutzrecht an Wohlfahrtsverlusten verursacht.⁹⁰

III. Niedrige Kosten im Umgang

Hohe Produktion und weite Verbreitung von Information allein sind nicht gleichzusetzen mit Effizienz. Es wurde gezeigt, dass Effizienz erst durch die Relation von Kosten und Nutzen beurteilt werden kann.⁹¹ Deshalb sind hohe Pro-

⁸⁷ Vgl. COOTER/ULEN, S. 116 f.

⁸⁸ Siehe soeben oben Kap. 5, B., II.; vgl. auch SCHÄFER/OTT, S. 746; SHAVELL, S. 143.

⁸⁹ ZECH, Information, S. 156.

⁹⁰ Vgl. SCHÄFER/OTT, S. 746.

⁹¹ Oben Kap. 5.

duktion und weite Verbreitung erst dann und soweit effizient und damit wohlfahrtsfördernd, wenn die Kosten tief sind, die mit dem Umgang mit den Informationen einhergehen. Eine hohe Produktion ist nicht effizient, wenn die Aneignung der Information durch Nachahmer:innen nur durch teure Geheimhaltungsmaßnahmen abzuwenden ist.⁹² Gleiches gilt für die Übertragung von Information im Sinne der Verbreitung. Wenn die Verbreitung nur mit hohen Zusatzkosten – auch hier ist an Kosten für Geheimhaltungsmaßnahmen zu denken – möglich ist, liegen (möglicherweise prohibitiv)⁹³ hohe Transaktionskosten vor, die ebenfalls effizienzmindernd sind.⁹⁴

Im Hinblick auf die Beantwortung der Frage der Schutzbedürftigkeit von KI-Technologien ist also einerseits darauf zu achten, ob durch ein Schutzrecht die Kosten im Umgang gesenkt werden können oder ob die Kosten im Umgang auch ohne Schutzrecht effizient tief sind. Auch unter diesem Titel muss die Kostensenkung gegen die Kosten aufgewogen werden, die mit einem Schutzrecht einhergehen.

C. Zusammenfassung

Die Frage nach der Schutzbedürftigkeit von KI-Technologien soll in dieser Arbeit nach ökonomischen Gesichtspunkten beantwortet werden. Es soll die Frage beantwortet werden, ob der Markt für KI-Technologien wohlfahrtsökonomisch effizient funktioniert oder ob sich Effizienzpotenziale ergeben, die durch Schutzrechte ausgefüllt werden könnten. Effizienz wird dabei entsprechend KALDOR/HICKS als positiver Kosten-Nutzen-Vergleich zweier Situationen⁹⁵ aufgefasst.

Methodisch soll die Frage nicht anhand des Aufzeigens von möglichen Marktversagensgründen beantwortet werden. Der Markt für KI-Technologien wird viel eher darauf untersucht, ob er die Effizienzziele der hohen Produktion von

⁹² Vgl. LANDES/POSNER, S. 12 f.; ZECH, Information, S. 156.

⁹³ Siehe dazu im Speziellen oben Kap. 5.

⁹⁴ ZECH, Information, S. 157 m.w.N.

⁹⁵ Situation A: ohne Schutzrecht; Situation B: mit Schutzrecht.

KI-Technologien sowie deren weite Verbreitung erreicht und ob dabei die Kosten im Umgang mit den KI-Technologien tief sind. Unter der Prämisse der Schutzfreiheit sollen Überlegungen angestellt werden, wo ein Schutzrecht produktionserhöhend, güterverbreitend oder kostensenkend eingreifen kann. Die genannten Effizienzziele sind klassische Ausflüsse der Innovations- und damit der Wohlfahrtsökonomik.

Die drei genannten Ziele vereinen die negativen Marktversagensgründe als positive, normativ eher greifbare bzw. beschreibbare Ziele als die Marktversagensgründe selbst:

Durch die Produktion von (handelbaren) Gütern wird ein Markt bei vorhandener Nachfrage überhaupt ermöglicht. Wenn bei einem Vergleich zweier Situationen eine Situation eine höhere Produktionsrate aufweist, ist diese prinzipiell wohlfahrtsökonomisch vorzuziehen. Die Verbreitung der produzierten Güter entspricht der Verteilung der Güter über den Markt. Werden in einer Situation die Güter weiter verbreitet als in einer anderen, ist die erste Situation wohlfahrtsökonomisch vorzuziehen. Die tiefen Kosten im Umgang sollen dabei als „Kontrollinstrument“ dienen – keine maximale Produktion und Güterverbreitung um jeden Preis. Die Verringerung der Kosten bzw. tiefe Kosten in der (höheren) Produktion sowie in der (weiteren) Verbreitung der Güter macht die ersten beiden Ziele überhaupt erst nach vorliegendem Verständnis effizient.

Dementsprechend werden nun in einem ersten Schritt die Charakteristika des Marktes für KI-Technologien untersucht und anhand der dadurch gewonnenen Erkenntnisse beurteilt, ob die drei erörterten Ziele erreicht werden. Dabei wird stets der Vergleich gezogen mit der (hypothetischen) Situation mit Schutzrechten für die KI-Technologie. Diese Analyse wird Anhaltspunkte ergeben, die darauf schließen lassen, dass der Markt für KI-Technologien mit einem Schutzrecht wohlfahrtsökonomisch effizienter ist als der Markt für KI-Technologien ohne Schutzrecht. Daraus wird ein Schutzbedürfnis für KI-Technologien abgeleitet.

Kapitel 6

Markt für KI-Technologien

Der Markt für KI-Technologien zeigt sich als Markt mit schnellen Entwicklungszyklen, damit einhergehend als Markt konstanter Verbesserung und einer hohen Marktdynamik.¹ KI-Technologien werden demnach in großem Umfang und in einem schnellen Tempo (weiter)entwickelt. Die sinkenden Kosten für die Entwicklung von KI-Technologien, während diese dabei leistungsfähiger werden, fördern das Entwicklungs- und Produktionsniveau zusätzlich.²

A. Marktdynamik und potenzielle Marktzutrittsschranken

Betreffend die hohe Marktdynamik ist ein Vorbehalt zu machen – zumindest wenn die Marktdynamik als Fluktuation von Marktteilnehmer:innen verstanden wird. Der Markt für KI-Technologien könnte Zutrittsschranken aufweisen. Die Zutrittsschranken würden diesfalls in Form der für die Entwicklung der Technologien notwendigen Datenmengen bestehen.³ Die Datenmengen, die für die Entwicklung von KI-Technologien notwendig werden, variieren zwar von Industriesektor zu Industriesektor.⁴ Generell kann aber festgehalten wer-

¹ Stanford University, Annual Report 2022, S. 3, 11, 16, 16 ff.; SEITZ/RITZMANN, S. 8; WIPO, Technology Trends 2019, Artificial Intelligence, S. 30 ff., 31 f.; siehe dazu auch HILTY/HOFFMANN/SCHEUERER, Max Planck Institute for Innovation and Competition Research Paper 20-02, 20.

² Stanford University, Annual Report 2022, S. 11.

³ Siehe oben Einl. und sogleich genauer: Kap.6 A.; MAAMAR, S. 117 m.w.N.; BESSEN, S. 25; BESSEN/IMPINK/REICHENSBERGER/SEAMANS, Research Policy 51, 2, vgl. auch COBBE/SINGH, Computer Law & Security Review 2021, 2 ff.

⁴ BESSEN, S. 25; BESSEN/IMPINK/REICHENSBERGER/SEAMANS, Research Policy 51, 2.

den, dass die benötigte Menge an Daten groß ist und die Kosten für die Sammlung und Aufbereitung der Trainingsdaten hoch sind.⁵ In diesem Zusammenhang wird sodann mehrheitlich vorgebracht, dass diese notwendigen Datenmengen eine Zutrittsschranke für neue Marktteilnehmer darstellen können.⁶

Neben der Datenmenge spielt auch die Datenqualität eine Rolle. Eine große Datenmenge kann unter Umständen wenig Nutzen bringen, wenn die Datenqualität schlecht ist. Dies dürfte vor allem für Formen des unüberwachten Trainings gelten, bei welchem die Daten nicht bzw. weniger aufbereitet werden (müssen) als bei anderen Formen des Trainings.⁷ Unabhängig der Trainingsform kann festgehalten werden, dass die erforderliche Datenmenge in der Tendenz eine Marktzutrittsschranke darstellen könnte.

Sinnvoller ist es jedoch, die Frage nach dem Zutrittsschrankencharakter von Daten industriespezifisch zu beantworten. So muss unterschieden werden, woher die Trainingsdaten stammen, auf welche die Entwickler:innen angewiesen sind.⁸ Es existieren Ansätze, Daten von Kund:innen oder von Drittparteien zu verwenden. Selten werden Daten aus eigenen Quellen⁹ verwendet.¹⁰ Industriespezifisch können diesbezüglich Unterschiede feststellbar sein. In Bereichen, in welchen es schwierig ist, mit eigenen Daten ein sinnvolles KI-Produkt herzustellen, stellen Daten eher eine Marktzutrittsschranke dar, als wenn sich die Entwickler:innen auf eigene Daten stützen können.¹¹

Eine weitere Zutrittsschranke wird auch in der notwendigen Hardware für die Entwicklung, Bereitstellung und Unterhaltung von KI-Technologien gesehen.¹² Dem wird entgegengehalten, dass die Zutrittsschwelle durch die immer weitere Verbreitung von *cloud-computing* sinken würde. Die Entwickler:innen

⁵ BESSEN, S. 25; BESSEN/IMPINK/REICHENSPERGER/SEAMANS, Research Policy 51, 2; HACKER, GRUR 2020, 1026.

⁶ BESSEN, S. 11 ff.; MAAMAR, S. 117 m.w.N.; WIPO, Technology Trends 2019, Artificial Intelligence, S. 106.

⁷ Siehe zu den Einzelheiten der verschiedenen Trainingsarten oben Kap. 2, A.

⁸ Siehe dazu die Studie bei BESSEN, S. 18 f.

⁹ Im Sinne von Daten der Entwickler:innen.

¹⁰ BESSEN, S. 18 f.

¹¹ BESSEN, S. 18 f., 25; BESSEN/IMPINK/REICHENSPERGER/SEAMANS, Research Policy 51, 2.

¹² BESSEN, S. 25.

seien dadurch nicht mehr darauf angewiesen, die notwendige Hardware selbst anzuschaffen.¹³ Diesem Argument ist entgegenzuhalten, dass auch beim *cloud-computing* reale, physische Komponenten gebraucht werden. *Cloud-computing* kann mit anderen Worten als „IT-outsourcing“ gesehen und verstanden werden.¹⁴ Damit sind Entwickler:innen auch beim Einsatz von *cloud-computing* auf die notwendige, leistungsstarke Hardware angewiesen – nur ist sie nicht in der unmittelbaren Herrschaftsgewalt der Entwickler:innen selbst. *Amazon Web Services (AWS)* sind ein Beispiel für ein *cloud-computing*-Angebot. Dabei stellt *Amazon* die Hardware zur Verfügung und verfügt dabei über die unmittelbare Herrschaftsmacht über diese und bietet *cloud-computing*-Dienste an, über welche Entwickler:innen¹⁵ unter anderem auf die Hardware von *Amazon* zugreifen können. Durch das *cloud-computing* können also neue Marktteilnehmer:innen ihre Ressourcen effizienter einsetzen.¹⁶

Allerdings begeben sie sich dadurch auch in Abhängigkeiten von größeren, bereits etablierten Marktteilnehmer:innen, die auch Konkurrenz darstellen können. Zudem gewinnen diese weiter an Bedeutung und die Marktmacht konzentriert sich weiter auf bereits etablierten Marktteilnehmer:innen.¹⁷

B. Treiber des Marktes

Um einen Markt erfassen zu können, ist es wichtig, dessen treibende Kräfte zu kennen. Nur so ist es möglich, die Marktentwicklung auf dem Markt für KI-Technologien auch nachzuvollziehen. Zudem können die Treiber eines Marktes Anhaltspunkte für mögliche Schutzgegenstände in der Diskussion um potentielle neue Schutzrechte bieten

¹³ BESSEN, S. 25.

¹⁴ Vgl. zum Beispiel JIN/MCELHERAN, S. 7.

¹⁵ In diesem Fall als Nutzer:innen.

¹⁶ Vgl. zum Ganzen auch COBBE/SINGH, *Computer Law & Security Review* 2021, 2 ff.; GULL/SCHRADE-GRYTSENKO/LUNDBORG, WIK Diskussionsbeitrag Nr. 469, 12 ff.

¹⁷ Vgl. GULL/SCHRADE-GRYTSENKO/LUNDBORG, WIK Diskussionsbeitrag Nr. 469, 13.

Der Markt für KI-Technologien blüht erst seit den letzten fünf bis zehn Jahren auf.¹⁸ KI-Technologien bzw. Forschung auf dem Gebiet der Künstlichen Intelligenz existiert aber bereits seit den 1950er-Jahren.¹⁹ Das Wachstum des Marktes für KI-Technologien kann damit nicht im Forschungsgebiet der Künstlichen Intelligenz selbst begründet liegen. Was also ist der Auslöser dafür, dass der Markt für KI-Technologien in den vergangenen Jahren derart gewachsen ist? Das Wachstum lässt sich auf vornehmlich drei Gründe zurückführen: Fortschritte in der Entwicklung von Hardware, größere, bessere und leichter verfügbare Datenmengen und schließlich neue Heuristiken der mit der Entwicklung von KI-Technologien betrauten Personen.²⁰

Verschiedene sogenannte KI-Winter²¹ bremsten die Forschung und Weiterentwicklung auf dem Gebiet der Künstlichen Intelligenz. Der Beginn einer dieser Winter wird in den frühen 1980er-Jahren festgemacht.²² Grund für den KI-Winter war, dass die Fortschritte in den KI-Anwendungen nicht den Erwartungen entsprechen konnten. Dies lag mitunter daran, dass die damaligen Hardwareressourcen nicht das Rechenvermögen aufbringen konnten, die notwendig waren. So brauchen vor allem Ansätze im maschinellen Lernen ein hohes Maß an Rechenkraft, um überhaupt die entsprechenden Technologien zu entwickeln.²³

Die Fortschritte in der Hardwareleistung hängen u.a. mit dem *Moore'schen Gesetz* zusammen.²⁴ Vereinfacht lässt sich das *Moore'sche* Gesetz zusammenfassen

¹⁸ Statt vieler: AGRAWAL/GANS/GOLDFARB, in: *The Economics of Artificial Intelligence*, S. 1; vgl. auch Stanford University, Annual Report 2022, S. 11; TANG/LI/DING/SONG/BU, *Journal of Informetrics*, 2020, Vol. 14, 1 ff.

¹⁹ Vgl. oben Kap. 1, B. ff.

²⁰ HILTY/HOFFMANN/SCHEUERER, Max Planck Institute for Innovation and Competition Research Paper 20-02, 20; TANG/LI/DING/SONG/BU, *Journal of Informetrics*, 2020, Vol. 14, 1 ff.

²¹ Siehe dazu bspw. NILSSON, S. 327 ff.; vgl. auch TANG/LI/DING/SONG/BU, *Journal of Informetrics*, 2020, Vol. 14, 1 ff.

²² NILSSON, S. 327.

²³ HILTY/HOFFMANN/SCHEUERER, Max Planck Institute for Innovation and Competition Research Paper 20-02, 20.

²⁴ Dieses besagt, dass sich die Anzahl Transistoren, die auf die festgelegte Größe eines Schaltkreises passt, ungefähr alle zwei Jahre verdoppelt; MOORE, *Electronics* 1965, Bd. 38, Nr. 8.

als zweijährliche Verdoppelung der Rechenkapazität von Computerchips. Damit geht nicht nur eine rapide Entwicklung der Rechenleistung einher, sondern auch eine entsprechende Senkung der Kosten für solch leistungsfähige Hardware.

So sind erst in der heutigen Zeit die Hardwareressourcen ausreichend, um die Entwicklungen in der KI-Forschung auch faktisch umzusetzen. Damit lässt sich wiederum verstehen, warum die Hardware als solche als Marktzutrittsschranke aufgefasst wird.²⁵

In den technischen Grundlagen wurde aufgezeigt, dass die Entwicklung von KI-Technologien im Vergleich zu herkömmlichen Programmierweisen einer wesentlich größeren Datenmenge bedarf. Die Verfügbarkeit der notwendigen Datenmengen ist ein weiterer Treiber des Marktes für KI-Technologien. Die *Datafizierung*²⁶ der Gesellschaft führte dazu, dass seit der Erfindung des Internets und v.a. mit der Manifestation von Social Media und Smartphones die Datenmenge sprunghaft anstieg und weiter wächst, die von der Gesellschaft und Industrie generiert wird.²⁷ Es ist aber nicht nur die größere Datenmenge, die das Wachstum des Marktes für KI-Technologien ermöglicht und antreibt, sondern es ist auch die damit einhergehende kostengünstigere Datenverfügbarkeit. Diese ist wiederum an Speicherkapazitäten geknüpft, welche sich ebenfalls nach *Mooreschem* Gesetz in allzweijährlichen Verdopplungsschritten verbessern.²⁸ Die größeren Datenmengen sind bei KI-Technologien mit einem weiten Einsatzgebiet wichtiger als bei KI-Technologien, die auf engen Spezialgebieten²⁹ zum Einsatz kommen sollen. Bei Letzteren entscheidet vor allem die Datenqualität. Auch hier lässt sich nun nachvollziehen, warum die erforderlichen Datenmengen als Marktzutrittshindernis aufgefasst werden können.³⁰

²⁵ Siehe soeben Kap. 6, A.

²⁶ Siehe zum Begriff CUKIER/MAYER-SCHOENBERGER.

²⁷ So stieg das Volumen der jährlich generierten/replizierten digitalen Datenmenge weltweit von 6,5 Zetabyte im Jahre 2012 auf 64,2 Zetabyte im Jahre 2020, <https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/>, zuletzt besucht am 9. Mai 2023.

²⁸ Siehe oben Kap. 6, B.

²⁹ Wie bspw. bei der Tumorerkennung in der Radiologie.

³⁰ Siehe oben Kap. 6, A.

Schließlich gilt es auch einen menschlichen Faktor als Treiber des Marktes zu nennen: (neue) Heuristiken der Entwickler:innen in Form von neuen Herangehensweisen und Lösungsansätzen haben auch einen Einfluss darauf, dass der Markt für KI-Technologien in den vergangenen Jahren wuchs.³¹ Allerdings sind die Heuristiken der Entwickler:innen nicht ein derart starker Treiber wie die zuvor genannte Hardware und die verfügbare Datenmenge. Dies liegt mitunter daran, dass die verschiedenen Technologien in ihrer Entwicklung auf unterschiedlich starke Inputs der Entwickler:innen angewiesen sind.³²

Verbesserung in der Rechenleistung (Hardware), bessere, größere und einfacher verfügbare Datenmengen sowie schließlich neue Heuristiken der Entwickler:innen konnten als die drei hauptsächlichen Treiber des KI-Marktes eruiert werden. Sie sind überdies die Hauptkostenpunkte in der Entwicklung von KI-Technologien – allen voran jedoch die erforderliche Datenmenge.³³ Die Investitionen in die Beschaffung, Aufarbeitung und Anwendung der Trainingsdaten können nicht bzw. nur sehr schwer umgangen werden. Die Kosten für die erforderliche Hardware können etwa über IT-Outsourcing tief gehalten werden.³⁴ Neue Heuristiken sind einerseits nicht für jede KI-Technologie Voraussetzung und andererseits existieren vor allem bei KNN vorgefertigte Architekturen, die sich weiterentwickeln lassen und teilweise bereits die notwendigen Heuristiken verkörpern.³⁵

Diese kostenverursachenden Treiber sind Anhaltspunkte bei der Erwägung der Schutzbedürftigkeit von KI-Technologien. Der Investitionsschutz ist Ausfluss des volkswirtschaftlichen Zieles der hohen Produktionseffizienz.³⁶ Im Sinne des

³¹ HILTY/HOFFMANN/SCHEUERER, Max Planck Institute for Innovation and Competition Research Paper 20-02, 20.

³² HILTY/HOFFMANN/SCHEUERER, Max Planck Institute for Innovation and Competition Research Paper 20-02, 20; vgl. auch oben Kapitel 2.

³³ Siehe oben Kap. 6, A f.

³⁴ Siehe dazu soeben Kap. 6, A.

³⁵ Siehe dazu oben Kap. 2, C., II, 3.; vgl. auch mit Betonung darauf, dass der Wert bei KNN weniger im Modell selbst als in den Gewichtungsinformationen liegt HILTY/HOFFMANN/SCHEUERER, Max Planck Institute for Innovation and Competition Research Paper 20-02, 21.

³⁶ Vgl. oben Kap. 5, B., I.

Investitionsschutzes drängt sich dort ein Schutz auf, wo (hohe) Investitionskosten anfallen. Ohne entsprechenden Schutz für die Investition werden keine weiteren Investitionen sowie Innovationen getätigt – ansonsten gingen die Entwickler:innen und insbesondere die Investor:innen ihrer Leistung verlustig.³⁷ Von den drei genannten Treibern dürften bessere, größere und einfacher verfügbare Datenmengen der wichtigste Markttreiber sein. Dies geht nicht nur aus dem Investitionsvolumen in Datensammlungen hervor, sondern auch durch die Bedeutung der Trainingsdaten für den Entwicklungsprozess der KI-Technologien. Wie unter Kapitel 2 gesehen, entscheiden in einem großen Maße die Trainingsdaten über Funktionsfähigkeit bzw. die Qualität der KI-Technologie.³⁸

C. Produkte des Marktes

Hohe Entwicklungs- bzw. Fixkosten bei tiefen Grenzkosten indizieren vor dem Hintergrund des Investitionsschutzes Schutzbedürftigkeit.³⁹ Dieser Schutz kann sodann rechtlicher oder faktischer bzw. technischer Natur sein. Um ein abschließendes Urteil über eine rechtliche Schutzbedürftigkeit fällen zu können, müssen auch die Produkte des KI-Marktes betrachtet werden. Anhand der Produkte lässt sich zeigen, ob die volkswirtschaftlichen Ziele erreicht werden, oder ob Anzeichen für das Nichterreichen dieser Ziele oder für andere Ineffizienzen bestehen, die für eine Schutzbedürftigkeit sprechen.

Bei der Betrachtung der Produkte des Marktes für KI-Technologien fällt auf, dass die KI-Technologien vermehrt als Dienstleistung in Form von cloudbasierten Anwendungen (*AI-as-a-service*) und nicht als eigentliche Produkte in Form von lokalen KI-Anwendungen angeboten werden.⁴⁰ Der Studie BESSENS zufolge

³⁷ Vgl. auch HILTY/HOFFMANN/SCHUEERER, Max Planck Institute for Innovation and Competition Research Paper 20-02, 19 ff.

³⁸ Zusammenfassend dazu BESSEN/IMPINK/REICHENSPERGER/SEAMANS, Research Policy 51, 2.

³⁹ Siehe dazu Kap. 6, D., I. unten.

⁴⁰ Vgl. dazu COBBE/SINGH, Computer Law & Security Review 2021, 2 ff. m.w.N.; siehe auch eingehend zur Marktstruktur des Marktes für *cloudcomputing* GULL/SCHRADE-GRYTSSENKO/LUNDBORG, WIK Diskussionsbeitrag Nr. 469, 12 ff.

böten gerade mal 3% der befragten Startups ihre KI-Technologien noch ausschließlich als Produkt an – während die restlichen 97% ihre Technologie als *service* anbieten. 33% der Startups würden sowohl *service* als auch ein Produkt anbieten.⁴¹

Bei KI-Technologien als Dienstleistungen wird den Nutzer:innen (im Sinne von Endverbraucher:innen) die KI-Technologie nicht als Software überlassen. Die Nutzer:innen können in solchen Fällen über ein Interface Anfragen an ein Serviceportal stellen. Auf dieses Serviceportal haben nur die Anbieter:innen unmittelbaren Zugriff. Das Serviceportal verarbeitet die Anfrage und leitet sie an die Hardwarestruktur weiter, auf welcher die KI-Technologie implementiert ist. Je nach Dienstleistung verarbeitet die KI-Technologie eigene Daten der Anbieter:innen oder diejenige der Nutzer:innen und generiert einen entsprechenden Output, der sodann den Nutzer:innen präsentiert wird. Der Maschinencode der KI-Technologie läuft in solchen Fällen nicht auf den Endgeräten der Nutzer:innen ab. Auf den Endgeräten läuft lediglich der Maschinencode des Interfaces ab.⁴² Vereinfacht gesagt, geben die Anbieter:innen ihr Produkt nicht preis bzw. nicht aus der Hand.⁴³

Die Nutzer:innen wissen in solchen Fällen nicht, welche Technologie hinter der Anwendung steht. Sie haben keine bzw. nur sehr begrenzte Möglichkeiten⁴⁴, die Angaben der Anbieter:innen über die Technologie zu verifizieren

Es lassen sich mehrere Gründe aufführen, warum auf dem Markt Dienstleistungen die eigentlichen Produkte überwiegen. Auf diese Gründe wird nachfolgend vertieft eingegangen

⁴¹ BESSEN, S. 25; vgl. auch HILTY/HOFFMANN/SCHUEYERER, Max Planck Institute for Innovation and Competition Research Paper 20-02, 20 f.

⁴² Dies hat auch für das sogenannte *reverse engineering* bedeutende Folgen, siehe zum *reverse engineering* weiter unten Kap. 9, C. II. ff. Als Beispiele für solche Anwendungen lassen sich diejenigen von OpenAI (DALL E, DALL E 2, ChatGPT), dataguard und Luminovo nennen.

⁴³ Siehe für die Funktionsweise von *AI-as-a-service* COBBE/SINGH, Computer Law & Security Review 2021, 5 ff.

⁴⁴ Siehe zum *reverse engineering* von Cloudangeboten weiter unten Kap. 9, C., II. 2. ff.

Einerseits wurde in den vorherigen Abschnitten aufgezeigt, dass die technologischen Fortschritte bei KI-Technologien eher gering sind. Nicht der technologische Fortschritt auf dem Gebiet der KI ist Grund dafür, warum der Markt für KI-Technologien von Dynamik, ständiger Verbesserung und schnellen Entwicklungszyklen geprägt ist.⁴⁵

Wo die Fortschritte in der Technologie relativ gering sind, ist auch der Aufwand gering, dessen es bedarf, eine Technologie basierend auf deren Vorgängertechnologie nachzubauen bzw. nachzuzahlen. Dies kann ein Grund dafür sein, warum KI-Technologien eher in Form von Dienstleistungen als in Form von Produkten angeboten werden. Anbieter:innen halten ihre trainierte Technologie geheim, indem sie nur eine cloudbasierte Anwendung anbieten.

Insbesondere bei KNN dürften Anbieter:innen ein großes Interesse daran haben, die Gewichtungsinformationen nicht preiszugeben.⁴⁶ Zumal diese das Ergebnis des aufwändigen Trainingsprozesses sind und deren Übertragung auf eine bloß funktional ähnliche Architektur genügt, um die Funktionalität zu imitieren.⁴⁷ So ist es den Anbieter:innen möglich, ihre Investitionen zu amortisieren, ohne dabei der Gefahr von Trittbrettfahrer:innen ausgesetzt zu sein.⁴⁸

Damit können also Geheimhaltungs- und Investitionsschutzüberlegungen generell zum Entschluss von Anbieter:innen führen, ihre Technologie nur cloudbasiert anzubieten.⁴⁹ Ein weiterer Grund kann auch die notwendige Rechenleistung sein. Einige trainierte KI-Technologien bedürfen je nach Komplexität⁵⁰ für

⁴⁵ Siehe dazu oben Kap. 6, B. ff.

⁴⁶ Vgl. auch MUHR, S. 110.

⁴⁷ Vgl. dazu oben Kap. 2, C, II., 4.

⁴⁸ Die Gefahr rührt eben aus dem Umstand, dass die Fixkosten die Grenzkosten stark überwiegen, vgl. dazu oben Kap. 6, D., I., 1. Siehe aber Kap. 9, C., II. ff. unten zum *reverse engineering* und dem damit zusammenhängenden Erlangen der Technologie durch Konkurrent:innen.

⁴⁹ So auch MUHR, S. 110 f.

⁵⁰ So erfordert der Betrieb von neuronalen Netzen etwa mehr Rechenleistung als derjenige eines genetischen Programms oder eines Expertensystems. Zudem unterscheiden sich auch unter den neuronalen Netzen die Anforderungen an die Rechenkapazität. So benötigen Sprachmodelle deutlich mehr Rechenleistung als neuronale Netze, die für andere Zwecke eingesetzt werden. Vgl. zum Ganzen VILLALOBOS/SEVILLA/BESIROGLU/HEIM/HO/MARIUS, 1 ff.

ihre Funktionsfähigkeit einer starken Rechenleistung, die nicht in jedes Endgerät implementiert werden kann bzw. über welche nicht die Mehrheit der Nutzer:innen verfügt. In solchen Fällen ist es einfacher, die Rechenleistung über Cloudlösungen und damit zusammenhängend über ausgelagerte Serverinfrastrukturen zu erreichen.⁵¹ Allerdings entwickeln sich die Rechenleistung wie in Kapitel 6, B. beschrieben nach dem *Moore'schen* Gesetz weiter. Es ist also nicht auszuschließen, dass die Endgeräte der Nutzer:innen in naher Zukunft auch bei großen Modellen die notwendige Rechenleistung aufweisen könnten.

Weiter erleichtern Cloudanwendungen die Implementierung von Updates. Es ist auch bei nicht intelligenten Softwareebenen ein Trend in Richtung Dienstleistungslösungen zu beobachten.⁵²

Der Aspekt der Geheimhaltung wurde bereits aufgegriffen. Mit dem Anbieten von Software als Cloudanwendung geht der Umstand einher, dass die Technologie – genauer: der Maschinencode – nicht offengelegt werden muss. Es lässt sich damit sagen, dass Cloudlösungen im Hinblick auf die Funktionsweise der KI-Technologie, deren Maschinencode, inkl. deren Trainingsergebnisse, eine faktische Schutzmaßnahme vor Nachahmer:innen darstellen. Solche Nachahmer:innen können bei Schutzfreiheit die nachgeahmte Technologie zu Grenzkosten verkaufen. Den ursprünglichen Entwickler:innen wird die Möglichkeit genommen, die (hohen) Fixkosten auf den Preis umzulegen. Die Bereitschaft, Technologien kommerziell zu entwickeln würde schwinden und damit würde das marktwirtschaftliche Ziel der hohen Produktion(seffizienz) verfehlt.⁵³

Wie gesehen, dürften faktische Schutzüberlegungen aber nicht die einzigen Gründe dafür sein, eine KI-Technologie lediglich über eine Cloudanwendung anzubieten.⁵⁴

⁵¹ COBBE/SINGH, Computer Law & Security Review 2021, 2 ff.

⁵² Vgl. GULL/SCHRADE-GRYTSSENKO/LUNDBORG, WIK Diskussionsbeitrag Nr. 469, 1 ff.

⁵³ Siehe zu diesem Ziel oben Kap. 5, B., I ff.

⁵⁴ Vgl. soeben Kap. 6, C.

D. Ineffizienzen des Marktes?

Anhand der Betrachtung der Markttreiber und -produkte werden nun Aspekte des Marktes aufgezeigt, die auf Ineffizienzen schließen lassen. Diese Ineffizienzen beziehen sich vor allem auf die Kostenstruktur bei der Entwicklung und Inverkehrbringung von KI-Technologien sowie auf die statische Effizienz.

Die folgenden Ausführungen erfolgen unter der Prämisse der rechtlichen Schutzfreiheit von KI-Technologien, um die rechtlichen Schutzbedürfnisse aufzuzeigen.

I. *Ineffizient hohe Kosten*

1. *Fixkosten*

Die Entwicklung von KI-Technologien kann sehr kostenintensiv sein.⁵⁵ Neben der erforderlichen Hardware bedarf der Trainingsschritt höhere Investitionen als die Herstellung herkömmlicher Software im Rahmen der klassischen Programmierweisen. Der Trainingsschritt ist im Vergleich zur herkömmlichen Programmierung ein neuer Schritt.⁵⁶ Dieser bedarf nicht nur der Vergütung der mit dem Training betreuten Personen. Viel eher stellt die Datenakquise, -aufbereitung und -anwendung einen der hauptsächlichen Kostenfaktoren in der Entwicklung und Herstellung von KI-Technologien dar.⁵⁷

Hohe Fixkosten bedeuten jedoch nicht *eo ipso*, dass ein Markt ineffizient ist bzw. dass eine Unterproduktion vorliegt. Entscheidend ist die Höhe der Grenzkosten. Sind die Grenzkosten auch entsprechend hoch, besteht kein oder ein geringerer Anreiz für Trittbrettfahrer:innen, das Gut nachzuzahlen und selbst zu vertreiben, da die Marge zwischen Fix- und Grenzkosten nicht groß genug ist. Je größer die Differenz zwischen Fix- und Grenzkosten, desto lukrativer ist es bei

⁵⁵ Siehe oben Einl.

⁵⁶ Siehe oben Kap. 2, A.

⁵⁷ Siehe dazu oben Kap. 2. B. f., Kap. 6, A. ff.

Schutzfreiheit eines Gutes, dieses nachzuzahlen und zu Grenzkosten zu verkaufen.⁵⁸ Bei KI-Technologien liegt ein großes Gefälle zwischen Fix- und Grenzkosten vor.⁵⁹ Bei Schutzfreiheit besteht demnach ein großer Anreiz für Trittbrettfahrer:innen. Damit geht jedoch mit der Zeit eine Unterproduktion einher, da die Bereitschaft abnimmt, neue Technologien zu entwickeln, da keine Möglichkeit besteht, die Fixkosten zu amortisieren.⁶⁰

Dieser Umstand wurde oben in Kap. 6, C. ff. als möglicher Grund dafür gesehen, dass auf dem Markt für KI-Technologien die Anwendungen vermehrt und fast ausschließlich cloudbasiert in Form von Dienstleistungen angeboten werden.⁶¹ Bei Fehlen einer rechtlichen Schutzmöglichkeit sind die Anbieter:innen also auf einen faktischen Schutz angewiesen. Dieser faktische Schutz hat aber Zusatzkosten als Folge. Diese erhöhten Fixkosten finden ihr Maximum aber nicht mit dem Ende der Entwicklung und auch nicht spätestens mit dem Inverkehrbringen. Die Schutzmaßnahmen müssen über diesen Zeitpunkt hinaus aufrechterhalten und damit auch die Kosten aufgewendet werden.⁶²

Um welche zusätzlichen Kosten handelt es sich bei diesen faktischen Schutzmaßnahmen? Es sind die Kosten für die Bereitstellung der Hardware, auf der die KI-Technologie implementiert ist und abläuft. Zudem muss diese Hardware über die Interfaces und das Serviceportal erreichbar sein. Die notwendige Software im Zusammenhang mit der Cloudanwendung muss programmiert werden und die Hardware bedarf der Unterhaltungskosten. Dies sind Kosten, die Anbieter:innen zusätzlich aufwenden im Vergleich zu wenn sie ihre Technologie lokal anbieten würden. Kosten, die aus Investitionsschutzgedanken nicht aufgewendet werden müssten, wenn ein rechtliches Schutzrecht bestehen würde, welche die Nachahmung zu Grenzkosten rechtlich unzulässig machen würde.

Hohe Fixkosten bei tiefen Grenzkosten sind beispielsweise aus dem Patentrecht und dort insbesondere aus dem pharmazeutischen Bereich bereits bekannt.⁶³

⁵⁸ Vgl. so auch EMMERICH, S. 26 ff.

⁵⁹ Vgl. oben Kap. 5, B., I.; siehe im Ergebnis wohl gleich MUHR, S. 116.

⁶⁰ Vgl. auch EMMERICH, S. 34 und MUHR, S. 110 f.

⁶¹ Ähnlich, wenn auch nur summarisch MUHR, S. 111.

⁶² Vgl. auch MUHR, S. 138.

⁶³ Vgl. oben Kap. 5, B., I.

Unterschied zu den hohen Fixkosten bei cloudbasierten KI-Technologien ist allerdings, dass bei KI-Technologien diese zusätzlichen Kosten auch noch in der Anwendungsphase anfallen. Im Patentrecht sind diese Kosten aus Geheimnis-schutzüberlegungen nach Inverkehrbringen nicht mehr nötig aufzuwenden. Aufgrund des absolutrechtlichen Patentschutzes ist es den Anbieter:innen möglich, potenziellen Nachahmer:innen die Nutzung des Gutes zu untersagen.⁶⁴ Rechtliche Schutzfreiheit führt also bei KI-Technologien auch noch in der Anwendungsphase zu höheren Fixkosten.

Bedarf es für die Produktion und das Inverkehrbringen eines Gutes hoher Fixkosten, die eigentlich nicht in der Natur dieses Gutes liegen, können diese zusätzlichen Kosten eine abschreckende Wirkung auf potenzielle Markteinsteiger:innen haben.⁶⁵ Eine solche Abschreckung ist wiederum im Hinblick auf die Produktionseffizienz zu bemängeln.

Eine ineffiziente Erhöhung der Fixkosten aufgrund der Ergreifung von faktischen Schutzmaßnahmen wirkt sich auf die Effizienz des gesamten Marktes aus. So führen diese hohen Fixkosten zu einem höheren Marktpreis. Ein Preis, der nicht notwendigerweise so hoch sein würde, wäre das Gut rechtlich geschützt. In diesem Fall könnte auf die faktischen Schutzmaßnahmen und damit auf die zusätzlichen Kosten verzichtet werden. Zu hohe Preise wirken sich gesamtwohlfahrtsschädigend aus – ein Schutzrecht könnte hier gesamtwohlfahrtsfördernd eingreifen.⁶⁶

2. Transaktionskosten

Mangelnder rechtlicher Schutz kann auch zu ineffizient bzw. prohibitiv hohen Transaktionskosten führen.⁶⁷ Transaktionskosten sind die Kosten für die Übertragung eines Gutes unabhängig vom Preis des Gutes an und für sich.⁶⁸ Aus dem oben erläuterten *coase*-Theorem lässt sich ableiten, dass je tiefer die Transaktionskosten sind, desto effizienter ist die Güterverteilung.⁶⁹ Somit können

⁶⁴ Siehe zum Patentrecht unten Kap. 7.

⁶⁵ Vgl. so auch EMMERICH, S. 34.

⁶⁶ Siehe dazu genau oben Kap. 5. A. I., Kap. 5, B., III. f.

⁶⁷ ARORA/FOSFURI/GAMBARDELLA, S. 115 ff.; vgl. auch MAAMAR, S. 128.

⁶⁸ SCHÄFER/OTT, S. 80.

⁶⁹ Siehe oben Kap. 5.

ineffizient hohe Transaktionskosten dazu führen, dass Güter nicht effizient verteilt werden.

Es wird sogleich dargelegt, dass auch bei KI-Technologien ohne rechtlichen Schutz ineffizient hohe Transaktionskosten vorliegen. Ein rechtlicher Schutz für KI-Technologien kann an dieser Stelle effizienzerhöhend eingreifen.

Grundsätzlich ließen sich KI-Technologien zu sehr tiefen Kosten übertragen, weil es sich bei den Technologien um immaterielle Güter und damit um Informationen handelt. Diese weisen in der Übertragung im Unterschied zu materiellen Gütern geringe Kosten auf. KI-Technologien würden also nach dem *coase*-Theorem effizient verteilt werden, wenn sie frei handelbar sind.⁷⁰ In Ermangelung eines rechtlichen Schutzes müssen die Anbieter:innen von KI-Technologien aber auf einen faktischen Schutz zurückgreifen, um ihrer Innovation bzw. Investition nicht verlustig zu gehen. Der faktische Schutz und dessen Aufrechterhaltung verursachen Kosten und wirken sich damit auch erhöhend auf die Transaktionskosten aus. Zumal die Schutzmaßnahmen auch während der Transaktion aufrechterhalten werden müssen.⁷¹

Solche faktischen Schutzmaßnahmen – technischer⁷² oder zwischenparteilicher⁷³ Natur – machen mit anderen Worten die KI-Technologien ohne rechtlichen Schutz in einem ersten Schritt überhaupt handelbar.⁷⁴ Diese Handelbarkeit von Gütern ist im Sinne des zweiten oben genannten volkswirtschaftlichen Zieles besonders wichtig. Durch die Handelbarkeit ist eine effiziente Verbreitung von Gütern erst möglich.⁷⁵ Ein Schutzrecht kann hier besonders effizienz erhöhend eingreifen. Durch die absolutrechtliche Absicherung der rechtsin-

⁷⁰ So für KI-Erzeugnisse auch MAAMAR, S. 128.

⁷¹ Vgl. auch ARORA/FOSFURI/GAMBARDELLA, S. 115 ff.

⁷² Bspw. durch Verschlüsselungen oder durch das Anbieten der Technologie über eine Cloud.

⁷³ Bspw. durch Geheimhaltungsmaßnahmen.

⁷⁴ So ausführlich für den Handel mit Know-How ARORA/FOSFURI/GAMBARDELLA, S. 115 ff.; in Kap. 5 wurde aufgezeigt, dass die Handelbarkeit eines Gutes erste Voraussetzung für das Funktionieren eines Marktes ist; vgl. auch MAAMAR, S. 128.

⁷⁵ SCHÄFER/OTT, S. 78 ff.

benden Anbieter:innen brauchen diese nicht auf einen faktischen Schutz zurückgreifen, um Handelbarkeit ihres Gutes zu erreichen. Der rechtliche Schutz ermöglicht damit auch die Handelbarkeit eines Gutes.⁷⁶

Es handelt sich um kein neuartiges Phänomen, dass bei Transaktionen mit Geheimhaltungsvereinbarungen operiert wird. So muss auch im Bereich von Erfindungen in der Phase vor der Patentierung die Geheimniswahrung bei Transaktionen mit Geheimhaltungsvereinbarungen erfolgen.⁷⁷ Entscheidender Unterschied zu schutzfreien KI-Technologien ist aber auch hier, dass bei diesen die Geheimhaltungsvorkehrungen auch in der Anwendungsphase bzw. nach Inverkehrbringen getroffen werden müssen. Die Geheimhaltungsmaßnahmen müssen darüber hinaus auch für jede einzelne vermarktete Einheit getroffen werden, die das immaterielle Gut⁷⁸ verkörpert. Solche Geheimhaltungsmaßnahmen sind ineffizient. Sie erhöhen die Transaktionskosten und wirken demnach gemäß *Coase* einer effizienten Güterverbreitung entgegen.⁷⁹

Ein Schutzrecht kann hier korrigierend eingreifen, indem es durch die Schaffung eines rechtlichen Schutzes erstens das Gut überhaupt handelbar macht. Zweitens macht es faktische Schutzmaßnahmen in der Anwendungsphase bzw. nach Inverkehrbringen obsolet. So können Kosten gesenkt werden.

Mangelnder rechtlicher Schutz kann die Transaktionskosten auch in Form von Informationskosten erhöhen. So bestehen bei rechtlicher Schutzfreiheit Unsicherheiten über die Verfügungsrechte. Besonders bei der Entwicklung von KI-Technologien sind verschiedene Akteur:innen beteiligt. Diese reichen von den Investor:innen über die Softwareentwickler:innen, Datenwissenschaftler:innen, Programmierer:innen, Trainer:innen bis hin zu den Betreiber:innen und Anbieter:innen. Fehlt ein rechtliches Schutzrecht, ist es bei vielen an der Wertschöpfung beteiligten Akteur:innen umso anspruchsvoller, die Verfügungsberechtigung festzustellen. Der damit einhergehende Aufwand führt zu höheren Informationskosten und damit zu höheren Transaktionskosten.

⁷⁶ARORA/FOSFURI/GAMBARDELLA, S. 116 f.; vgl. auch COOTER/ULEN, S. 116 f.; SCHÄFER/OTT, S. 78 ff.

⁷⁷ ARORA/FOSFURI/GAMBARDELLA, S. 116 f.

⁷⁸ Hier die KI-Technologie.

⁷⁹ Siehe oben Kap.5.

Ein Schutzrecht kann auch hier kostenmindernd eingreifen. Es stellt die Berechtigung sicher und weist die Information in Form der KI-Technologie ausschließlich zu. Damit kann spätestens in der Phase nach Inverkehrbringen auf die faktischen Schutzmaßnahmen verzichtet werden und bereits davor ist klar, wem das Recht zuzuordnen ist, sodass auch die zusätzlichen Informationskosten entfallen.

3. Zwischenergebnis

Es wurde aufgezeigt, dass bei Schutzfreiheit von KI-Technologien Kosten aufgewendet werden müssen, um sie geheim zu halten bzw. faktisch zu schützen. Dieser Schutz ist notwendig, damit die KI-Technologien aus Sicht der Anbieter:innen gewinnbringend angeboten werden können und um sie überhaupt handelbar zu machen.

Es fällt auf, dass die aufgeführte Argumentation an diejenige von öffentlichen Gütern erinnert.⁸⁰ KI-Technologien sind als Informationen weder rival noch exklusiv. Darüber hinaus weisen sie in der Entwicklung mehrheitlich wesentlich höhere Fixkosten auf – dies bei relativ geringen Grenzkosten. Dies zieht bei gewinnorientierten Anbieter:innen zwingend nach sich, dass der Schutz faktisch erfolgen muss – wo ein rechtlicher Schutz fehlt bzw. ein solcher versagt oder aufhört. Diese Schutzmaßnahmen führen dazu, dass die Fix- und Transaktionskosten im Vergleich zu ihrem Effizienzpotenzial ineffizient hoch sind. Mit anderen Worten weisen KI-Technologien als Informationen Charaktereigenschaften von öffentlichen Gütern auf.⁸¹ Damit indizieren die Charaktereigenschaften von KI-Technologien einen Marktversagensgrund und so auch ein Schutzbedürfnis. Es ergeben sich allerdings aufgrund der Marktstrukturen noch weitere Ineffizienzen, die für ein Schutzbedürfnis sprechen. Diese werden sogleich dargelegt.

⁸⁰ Siehe dazu oben Kap. 5, A., IV. ff.

⁸¹ Vgl. so auch EMMERICH, S. 23.

II. *Unterbleibende Güterverbreitung – statische Ineffizienz*

Als zweites volkswirtschaftliche Ziel unter dem Titel der Effizienz wurde die (effiziente) Güterverbreitung aufgeführt.⁸² Die effiziente Güterverbreitung soll sicherstellen, dass ein handelbares Gut mittels Rechtsgeschäfts demjenigen zuteilwird, der dem Gut den höchsten Wert beimisst.⁸³

Es wurde aufgezeigt, dass die KI-Technologien auf dem Markt überwiegend nicht als eigentliche Güter angeboten werden, sondern als Dienstleistungen. Anbieter:innen halten ihre Technologien geheim und bringen diese nicht als solche in Verkehr.⁸⁴ Wie aufgezeigt, kann ein Grund dafür sein, dass bei Schutzfreiheit die Anbieter:innen ihr Gut durch Geheimhaltung faktisch schützen wollen. Damit ist der fehlende rechtliche Schutz unter anderem ein Grund, warum der Markt für KI-Technologien statisch ineffizient ist. Oben wurde erläutert, dass Geheimhaltung nicht nur statisch ineffizient wirkt, sondern gar zum Informationsverlust führen kann.⁸⁵

Ein Schutzrecht kann dieser statischen Ineffizienz entgegenwirken. Dies bedeutet jedoch, dass die Güter in einem ersten Schritt in einer solchen Form handelbar sein müssen, dass eine Geheimhaltung nicht mehr zwingend notwendig ist. Hierfür kann ebenfalls ein Schutzrecht behilflich sein. So sind die Anbieter:innen bspw. durch ein absolutes Ausschließlichkeitsrecht nicht darauf angewiesen, Geheimhaltungsmaßnahmen zu ergreifen, wenn es ihnen um die Abwehr von Aneignung Ihres Gutes durch Nachahmung geht. Damit kann ein Schutzrecht genügend Schutz vor Trittbrettfahrer:innen bieten, sodass das Gut handelbar wird.⁸⁶ Mit der Handelbarkeit des Gutes wird dieses dann auch vermehrt als solches in Umlauf gesetzt – und nicht bloß als Dienstleistung.⁸⁷

Die Geheimhaltungsmaßnahmen sind mit einem Schutzrecht obsolet, sofern sie die Aneignung des Gutes durch Nachahmer:innen verhindern sollen. Damit sind auch die Kosten für die Geheimhaltung aus dieser Perspektive obsolet. Auf

⁸² Siehe oben Kap. 5, B., II.

⁸³ Vgl. oben Kap. 5, B. II. ff.

⁸⁴ Vgl. oben Kap. 6, C.

⁸⁵ Vgl. oben Kap. 5, B., II.

⁸⁶ Vgl. oben Kap. 5, B., II. ff. zur Handelbarkeit unter dem Titel der hohen Transaktionskosten.

⁸⁷ Vgl. dazu oben Kap. 5, B., II. ff.

die Geheimhaltungsmaßnahmen kann sodann aus Kostengründen verzichtet werden – ohne der Innovation verlustig zu gehen. Ein Schutzrecht ermöglicht damit nicht nur einen effizienteren Preis, indem es transaktionskostensenkend und damit positiv auf die dynamische Effizienz wirkt, sondern ermöglicht auch den Handel mit dem Gut. Damit kann sich das Schutzrecht auch positiv auf die statische Effizienz auswirken.

Sollte die Erfassung von KI-Technologien mittels Ausschließlichkeitsrechts nicht die aufgezeigten Wirkungen auf die statische Effizienz haben, kann eine zwingende Offenbarung die Verbreitung des Gutes zusätzlich begünstigen. Knüpft das Schutzrecht wie im Patentrecht an eine Offenbarung des Gutes bzw. der Information an⁸⁸, kann die statische Effizienz maximiert werden. Das Gut – in diesem Falle die KI-Technologie – wird im Gegenzug zur Einräumung eines absoluten Schutzrechtes veröffentlicht. So wird die damit einhergehende Information verbreitet und kann von anderen Marktakteur:innen – unter Beachtung des Schutzrechtes – verwendet und weiterentwickelt werden. Eine solche Offenbarung ermöglicht so auch Folgeinnovationen.

Mit der Thematik von Folgeinnovationen ist auf dem Gebiet von KI-Technologien und damit von Software auch auf Bewegungen wie *copyleft* oder *opensource* hinzuweisen, die durch ein wirksames Schutzrecht überhaupt erst ermöglicht werden.⁸⁹

III. Fehlende Transparenz

Als dritten Nachteil bringen die Marktstrukturen mangelnde Transparenz mit sich. Dadurch, dass KI-Technologien mehrheitlich nur als Dienstleistung angeboten werden, haben die Kund:innen keinen Zugriff auf die Technologie. Sie können daher die Angaben der Anbieter:innen nicht verifizieren. Sie haben keine Möglichkeit zu überprüfen, ob es sich bei der angebotenen Technologie tatsächlich um eine KI-Technologie handelt. Das bedeutet, dass sich Anbieter:innen hinter dem Begriff der Künstlichen Intelligenz⁹⁰ verstecken können

⁸⁸ Siehe zum Patentrecht unten Kap. 7.

⁸⁹ Siehe oben Kap. 5, B., II.

⁹⁰ Oder damit assoziierten Schlagworten wie bspw. Algorithmus.

und dabei jedoch herkömmliche bzw. gewöhnliche Computerprogramme anbieten.⁹¹

Dies bringt nicht nur Marketingvorteile mit sich sondern auch hohe bzw. überhöhte Preise und damit wiederum Wohlfahrtsverluste.⁹² Durch die Geheimhaltung ist es sodann auch Konkurrent:innen nicht möglich, auf den Missstand hinzuweisen. Auf dem Markt übliche Preiskontrollmechanismen funktionieren durch die Geheimhaltungsmaßnahmen auf dem Markt für KI-Technologien nicht.

Die Geheimhaltung führt also nicht nur zu einer Verringerung der dynamischen und statischen Effizienz, sondern ist auch aus Preiskontrollargumenten zu bemängeln. Mit einem entsprechenden Schutzrecht können Anreize gesetzt werden, auf Geheimhaltung zu verzichten und so die Technologien offenzulegen.⁹³ Damit ließen sich die Angaben betreffend künstliche Intelligenz von Softwareprodukten auch entsprechend überprüfen und effizientere Preise erzielen. Zudem können Anbieter:innen die Offenlegung der Technologie auch zur Abhebung gegenüber der Konkurrenz verwenden.

E. Schlussfolgerung: Indizien für Schutzbedürfnis

Der Markt für KI-Technologien ist ein sehr dynamischer, sich rasch entwickelnder Markt, welcher besonders in den vergangenen fünf bis zehn Jahren gewachsen ist. Es werden laufend neue KI-Anwendungen auf dem Markt positioniert und diese finden Verwendung in beinahe sämtlichen Sektoren. Die KI-Anwendungen werden laufend weiterentwickelt und ständig verbesserte Technologien werden präsentiert. Das wohlfahrts- und innovationsökonomisch gewünschte Ziel der hohen Produktion von Gütern auf einem Markt – die dynamische Effizienz – scheint erreicht zu werden.

⁹¹ So zeigte die vielfach zitierte Studie des Londoner *venture capital*-Unternehmens MMC Ventures, *The State of AI: Divergence 2019*, S. 99, dass nur bei 60% der KI-Startups auch entsprechende Belege hätten gefunden werden konnten, dass tatsächlich eine KI-Technologie angeboten würden.

⁹² Siehe oben Kap. 5. A., I., Kap. 5, B., III. f. wie zu hohe Preise zu Wohlfahrtsverlusten führen.

⁹³ Siehe dazu Kap. 5, B., II. und soeben Kap. 6, D., III. ff.

Der Grund für das rapide Wachstum des Marktes liegt aber nicht in den KI-Technologien selbst begründet. Verbesserungen in der Rechenleistung, neue Heuristiken der Entwickler:innen und vor allem eine größere, bessere und einfacher verfügbare Datenmenge sind der Grund für das Marktwachstum. Vor allem in die Datenbeschaffung, -aufbereitung und -anwendung fließen Investitionen. Bei der Betrachtung der Marktstruktur fällt auf, dass KI-Technologien hauptsächlich und in der Tendenz gar steigend, als cloudbasierte und nicht als lokale Anwendungen angeboten werden.

Das Anbieten von KI-Technologien über eine Cloud ermöglicht es Anbieter:innen, ihre Technologie bzw. ihr Produkt geheim zu halten und damit ihre Investitionen in die Entwicklung der Technologien zu amortisieren. Sind KI-Technologien rechtlich schutzfrei, bietet diese Geheimhaltung den notwendigen Schutz vor Trittbrettfahrer:innen und Nachahmer:innen, die ohne Schutzmaßnahmen die Technologie kopieren oder nachahmen könnten und dann zu Grenzkosten vertreiben.

Selbstredend sind diese Schutzmaßnahmen mit Zusatzkosten verbunden, die bei einem rechtlichen Schutz (zu einem großen Teil) entfallen dürften. Die Kosten für die faktischen Schutz- und Geheimhaltungsmaßnahmen sind aus einer wohlfahrtsökonomischen Perspektive ineffizient. Sie wirken sich kosten- und damit ineffizienzerhöhend sowohl auf die Fix- als auch die Transaktionskosten aus. Bei Schutzfreiheit wird das wohlfahrts- und innovationsökonomisch erwünschte Ziel der niedrigen Kosten im Umgang mit den Gütern also nicht bzw. nicht effizient erreicht. Ein rechtlicher Schutz kann hier effizienzfördernd eingreifen, da er die Kosten für den faktischen Schutz obsolet werden lässt.

Die Geheimhaltung hat zum Zweck, das Gut – die KI-Technologie – nicht offenlegen zu müssen. Die in der KI-Technologie enthaltene Information wird damit nicht freigegeben. Die Anbieter:innen behalten diese Informationen für sich, weil sie bei Schutzfreiheit dieser Information verlustig gingen. Nachahmer:innen und Trittbrettfahrer:innen können sich bei Schutzfreiheit die Information aneignen und so diese unter Fixkosten zu Grenzkosten vertreiben. Es wäre ein Zustand maximaler statischer Effizienz. Doch führte dieser Zustand zu einer unterbleibenden Produktion und damit zu dynamischer Ineffizienz – ein

wohlfahrtsökonomisch unerwünschter Zustand. Die auf dem Markt vorherrschende Situation suggeriert das Fehlen eines rechtlichen Schutzes – die Anbieter:innen scheinen auf einen faktischen Schutz auszuweichen. Dieser Umstand führt dazu, dass die Güter – und damit die Information – nicht verbreitet werden. Der auf dem Markt zu beobachtende Zustand ist ein Zustand statischer Ineffizienz. Ein rechtlicher Schutz könnte Anreize dazu setzen, auf diese Geheimhaltung zu verzichten und damit die statische Effizienz zu erhöhen. Knüpft das Schutzrecht an eine Offenbarung an, würde die statische Effizienz gar maximiert.

Würde die nachfolgende Untersuchung die Schutzfähigkeit von KI-Technologien ergeben, müsste in einem nächsten Schritt untersucht werden, warum die Technologien dennoch geheimgehalten werden. Mitunter wäre zu ergründen, ob es eines Offenbarungsanreizes bedarf.⁹⁴

Auch für die dynamische Effizienz böte ein Schutzrecht Effizienzpotenziale – auch wenn das Ziel der hohen Produktion aktuell auf dem Markt erreicht zu werden scheint.⁹⁵ Ein Schutzrecht wirkt sich im Fall der KI-Technologien wie aufgezeigt auch senkend auf die Fixkosten aus. Damit werden die Zutrittschwellen für neue Marktakteur:innen gesenkt, was sich auch positiv auf die dynamische Effizienz auswirken kann. Ein Schutzrecht könnte also mehr Anbieter:innen einen Marktzutritt ermöglichen.

Doch nicht nur Effizienzüberlegungen sprechen für ein Schutzbedürfnis. Auch Transparenz- und vor allem Preiskontrollüberlegungen sprechen für eine Schutznotwendigkeit. Mit einem Schutzrecht sind KI-Anbieter:innen nicht mehr auf Geheimhaltung angewiesen. Diese Geheimhaltung ermöglicht es aber auch Anbieter:innen herkömmlicher Softwareanwendungen, sich hinter dem Schlagwort der Künstlichen Intelligenz zu verstecken und „KI-Preise“ für herkömmliche Software zu verlangen. Überhöhte Preise für ein Gut sind wohlfahrtsökonomisch ineffizient. Es handelt sich auch hier um einen Zustand, bei welchem ein Schutzrecht korrigierend eingreifen kann.

⁹⁴ Siehe dazu unten Kap- 11.

⁹⁵ Siehe soeben Kap. 6, E.

Zusammenfassend werden also zwei von drei im Kapitel 5 genannten Ziele bei Schutzfreiheit nicht erreicht: Die Ziele der weiten Verbreitung⁹⁶ und der niedrigen Kosten im Umgang.⁹⁷ Ein rechtlicher Schutz für KI-Technologien könnte dazu beitragen, diese beiden Ziele zu erreichen. Darüber hinaus könnte er auch das Ziel der hohen Produktion⁹⁸ unter Umständen positiv beeinflussen. Aus diesen dargelegten Umständen werden Indizien für den Fortgang der Untersuchung abgeleitet, die für ein rechtliches Schutzbedürfnis sprechen. Ein Schutzbedürfnis, welches im folgenden Teil mit der tatsächlichen Schutzfähigkeit *de lege lata* abgeglichen wird. Die rechtliche Analyse des *status quo* soll anhand der eben unter dem Titel der Wohlfahrts- und Innovationsökonomie aufgezeigten Maßstäbe erfolgen. Mit anderen Worten wird die rechtliche Schutzfähigkeit kritisch hinterfragt und dahingehend untersucht, ob sie zur Effizienzsteigerung auf dem Markt für KI-Technologien beitragen kann.

⁹⁶ Siehe oben Kap. 5, B., II. ff.

⁹⁷ Siehe oben Kap. 6, D., I., 1. ff.

⁹⁸ Siehe oben Kap. 5, B., I. ff.

Teil 4

Schutzrecht an KI-Technologien *de lege lata*

Die Analyse des Marktes für KI-Technologien ergab, dass sich bei Schutzfreiheit der Technologien Ineffizienzen ergeben, denen mit einem entsprechenden Schutzrecht entgegengewirkt werden kann. Deshalb soll in einem nächsten Schritt die immaterialgüterrechtliche Schutzfähigkeit von KI-Technologien am Beispiel von KNN, genetischen Algorithmen bzw. Programmen und Expertensystemen untersucht werden. Zum immaterialgüterrechtlichen Schutz gesellt sich in diesem Teil auch die Untersuchung der Schutzfähigkeit nach dem GeschGehG. Der Schutz nach GeschGehG wird teilweise in die Nähe des Immaterialgüterrechts gerückt.¹ Zudem hat das GeschGehG ebenfalls Information zum Schutzgegenstand,² weshalb sich eine Untersuchung der Schutzfähigkeit auch nach dem GeschGehG anbietet. Die Untersuchung soll insbesondere die Frage beantworten, ob die Schutzmöglichkeiten *de lege lata* das Schutzbedürfnis entsprechend dem aufgezeigten Effizienzkriterium zu befriedigen vermögen.

Demnach wird nach Aufzeigen der patent-, urheber- und geheimnisschutzrechtlichen Schutzmöglichkeiten ein Vergleich mit dem eben aufgezeigten Schutzbedürfnis gemacht. Dabei offenbaren sich diverse Schutzlücken, die für einen Schutz *de lege ferenda* sprechen.

¹ Siehe zur Verortung des Know-How-Schutzes im deutschen Recht ausführlich HOHENDORF, S. 63 ff.

² Siehe unten Kap. 9, A.

Kapitel 7

Patentrechtlicher Schutz von KI-Technologien

Die Prüfung eines patentrechtlichen Schutzes drängt sich auf, da das Patentrecht technische Erfindungen schützt und KI-Technologien als Teilgebiet der Informationstechnik zumindest im weitesten Sinne Technizität zukommen könnte.¹

A. Grundlagen des Patentrechts

I. Materielle Voraussetzungen des Patentschutzes

Durch das Patentrecht sollen neue technische Erfindungen geschützt werden. Anders als das Urheberrecht, wo das absolute Recht im Zeitpunkt der Schöpfung entsteht², ist das Patentrecht ein Registerrecht.³ Zur Entstehung der absolutrechtlichen Stellung ist eine Anmeldung beim zuständigen Patentamt notwendig.⁴

Geregelt wird das Patentrecht auf nationaler Ebene durch das PatG und auf europäischer Ebene durch das EPÜ. Das vom Territorialitätsprinzip beherrschte Patentrecht machte zusammen mit der europäischen Zusammenarbeit sowie der Globalisierung allgemein eine europäische Vereinheitlichung notwendig. Aus diesem Grund wurde das EPÜ erlassen – es regelt ein einheitliches Patenterteilungsverfahren sowie ein gemeinsames materielles Recht für den europäischen Binnenraum. Es handelt sich dabei aber mitnichten um ein europäisches

¹ Vgl. aber zu den hohen Technizitätsanforderungen im Patentrecht ausführlich unten Kap. 7, A. III., 1.

² Siehe dazu unten Kap. 8, A.

³ Vgl. § 30 PatG.

⁴ Vgl. § 16 PatG.

Patent. Vielmehr kommt die Erteilung des Patents durch das Europäische Patentamt der Erteilung eines Bündels nationaler Patentrechte der Vertragsstaaten gleich.⁵ Am 1. Juni 2023 wurde das europäische Patent mit einheitlicher Wirkung eingeführt.⁶ Es führt ein Einheitspatent in allen Unterzeichnerstaaten mit einheitlichem Patentgericht ein. Dabei hat ein und dasselbe Patent in allen Vertragsstaaten dieselbe einheitliche Wirkung. Ausgangspunkt ist aber auch für dieses Einheitspatent das EPÜ: Im neunten Teil des EPÜ findet sich die Grundlage zur Schaffung eines solchen Einheitspatentes.⁷

Patentschutz wird erteilt für „Erfindungen auf allen Gebieten der Technik [...], sofern sie neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind.“⁸

Die Erfindung ist dem Patent zeitlich vorgelagert. Eine Erfindung ist eine technische Lehre und somit eine „Anweisung zum planmäßigen Handeln unter Einsatz beherrschbarer Naturkräfte zur Erreichung eines kausal überschaubaren Erfolgs.“⁹ Dabei muss die Anweisung mehr als eine bloße Entdeckung sein. Die Anweisung muss aufzeigen, wie die Idee zur Einsetzung der Naturbeherrschung umzusetzen ist.¹⁰ Nicht entscheidend ist dabei, ob sich der Erfinder über die Wirkung geirrt hat.¹¹ Das Erfordernis des Einsatzes von Naturkräften soll lediglich sicherstellen, dass naturwissenschaftliche Erkenntnisse für einen bestimmten Zweck auch tatsächlich verwendet werden und nicht bloße menschliche Logik- bzw. Verstandestätigkeit.¹² Mit „kausal überschaubarem Erfolg“ wird eine

⁵ Statt vieler: LETTL, S. 21 ff.

⁶ Vgl. dazu ausführlich ABl. EPA 2013, 111 ff. und 132 ff.

⁷ Materiell- und formellrechtliche Grundlagen dafür sind einerseits die Verordnung (EU) Nr. 1257/2012 des Europäischen Parlaments und des Rates über die Umsetzung der Verstärkten Zusammenarbeit im Bereich der Schaffung eines einheitlichen Patentschutzes und andererseits die Verordnung Nr. 1260/2012 des Rates über die Umsetzung der verstärkten Zusammenarbeit im Bereich der Schaffung eines einheitlichen Patentschutzes im Hinblick auf die anzuwendenden Übersetzungsregelungen.

⁸ Art. 52 Abs. 1 EPÜ; vgl. auch § 1 Abs. 1 PatG.

⁹ Zitat gem. LETTL S. 23 f.; für die Rechtsprechung statt vieler: BGH GRUR 1958, 602 – Wett-schein.

¹⁰ Statt vieler: LETTL, S. 24.

¹¹ BGH GRUR 1994, 357 – Muffelofen.

¹² Statt vieler: BPatG GRUR 2004, 851 – Kapazitätsberechnung.

technische Lösung verlangt. Dabei muss der Erfolg nicht auf einem technischen Gebiet liegen. Es genügt der Einsatz technischer Mittel.¹³ Die Erfindung muss dabei zu einem gewissen Grad fertig bzw. abgeschlossen sein. Mit anderen Worten muss sie ausführbar¹⁴, wiederholbar¹⁵ und funktionsfähig¹⁶ sein. Das Erfordernis der Funktionsfähigkeit soll die technische Brauchbarkeit sicherstellen. Es ist aber lediglich notwendig, dass die Anweisung beschreibt, wie der kausale Erfolg erzielt wird und nicht weshalb.¹⁷

Die Erfindung muss weiter neu sein. Sie darf mit anderen Worten nicht zum Stand der Technik gehören.¹⁸ Als Stand der Technik gelten alle Kenntnisse, die vor dem für den Altersrang der Patentanmeldung maßgeblichen Tag durch schriftliche oder mündliche Beschreibung, durch Benutzung oder in sonstiger Weise der Öffentlichkeit zugänglich gemacht worden sind.¹⁹ Als öffentlich zugänglich gemacht gilt eine Lehre dann, wenn die Möglichkeit besteht, dass beliebige Dritte zuverlässig und ausreichend von ihr Kenntnis erhalten.²⁰ Zugänglich ist die Lehre, wenn sie eine Fachperson unter Anwendung ihres Fachwissens anwenden kann.²¹ Art. 55 EPÜ bzw. § 5 PatG enthalten zwei Beispiele von Situationen, wo die Bekanntmachung nicht neuheitsschädlich ist. Neuheit bedeutet also, dass die Erfindung nicht bereits bekannt sein darf. Diese Bekanntheit kann sich auch aus bereits bestehenden Patentansprüchen ableiten.²²

Eine Tätigkeit gilt als erfinderisch, wenn sie sich für einen Fachmann nicht in naheliegender Weise aus dem Stand der Technik ergibt.²³

¹³ Statt vieler: BGH GRUR 1967, 591 - Garagentor

¹⁴ Ausschluss bspw. des *perpetuum mobile*; BGH GRUR 1993, 653 f. – Tetraploide.

¹⁵ Ausschluss des Zufalls; BGH GRUR 1987, 232 – Tollwutvirus.

¹⁶ Technische Brauchbarkeit; BGH GRUR 1992, 430 – Tauchcomputer.

¹⁷ Statt vieler: BGH GRUR 1994, 358 - Muffelofen.

¹⁸ Art. 54 Abs. 1 EPÜ bzw. § 3 Abs. 1 PatG.

¹⁹ Art. 54 Abs. 2 EPÜ bzw. § 3 Abs. 1 PatG.

²⁰ BGH GRUR 1993, 468 – Preprint-Versendung.

²¹ Statt vieler: BPatG GRUR 1994, 109 – Tauchcomputer II.

²² Art. 54 Abs. 3 EPÜ bzw. § 3 Abs. 2 PatG.

²³ Art. 56 EPÜ bzw. § 4 PatG.

Die gewerbliche Anwendbarkeit setzt voraus, dass die Erfindung auf irgendeinem gewerblichen Gebiet benutz- oder herstellbar ist. Es muss mithin eine praktische Verwertbarkeit außerhalb des rein privaten Raums vorliegen.²⁴

Sobald die Erfindung im Sinne von Art. 52 EPÜ bzw. § 1 PatG fertiggestellt ist, entsteht das Erfinderrecht bzw. das Recht an der Erfindung. Sind auch die anderen Voraussetzungen der Patentierung gegeben, so erlangt der Erfinder das „Recht auf das Patent“.²⁵ Es handelt sich dabei um ein absolutes subjektives Ausschließlichkeitsrecht.²⁶ Es stellt darüber hinaus ein übertragbares Vermögensrecht dar.²⁷

II. Formelle Voraussetzungen des Patentschutzes

Auf formeller Seite setzt der Patentschutz eine Anmeldung beim zuständigen Patentamt voraus. Das Recht am Patent entsteht mithin nicht *eo ipso*.²⁸ Auf die Formalia soll lediglich summarisch eingegangen werden. Das Anmeldeverfahren wird in Art. 75 ff. EPÜ bzw. § 34 ff. PatG geregelt.

Das Recht zur Anmeldung der Erfindung steht nach Art. 60 EPÜ bzw. § 6 PatG dem Erfinder zu – mithin dem Inhaber des Rechts auf das Patent bzw. dessen Rechtsnachfolger. Zwecks Anmeldung muss die Erfindung beschrieben werden – im sogenannten Patentanspruch.²⁹ Der Patentanspruch definiert sodann auch den Schutzbereich des Patents.³⁰ Denn nur was ausreichend offenbart wurde, kann auch geschützt werden. Auf diesem Grundsatz fußt auch die Rechtfertigung des Patentrechts gemäß der Offenbarungstheorie.³¹

²⁴ Vgl. Art. 57 EPÜ bzw. § 5 PatG.

²⁵ Art. 60 EPÜ bzw. § 6 PatG.

²⁶ Benkard/MELULLIS, PatG, § 6 Rn. 16 m.w.N.

²⁷ Art. 14 Abs. 1 GG.

²⁸ Vgl. oben Kap. 7, A., II.; Wie erwähnt, kann die Anmeldung beim Europäischen Patentamt erfolgen, worauf der Erfinder ein Bündel an nationalen Patentrechten erhält.

²⁹ Vgl. Art. 78 Abs. 1 lit. c EPÜ bzw. § 34 Abs. 3 Nr. 3 PatG.

³⁰ Art. 69 EPÜ bzw. § 14 PatG.

³¹ Siehe dazu oben Kap. 4, B.: Der Erfinder soll im Gegenzug zu seinem absoluten Schutzrecht an der Erfindung, aus welchem er Kapital schlagen kann, die Erfindung auch offenbaren. Damit

Der Rechtsinhaber soll nach erfolgter Patentanmeldung und -erteilung den kompletten wirtschaftlichen Nutzen aus der Erfindung ziehen können. § 9 PatG umschreibt die dem Patentinhaber vorbehaltenen Rechte. Art. 64 EPÜ beschreibt, dass mit der Erteilung des Patents durch das Europäische Patentamt dem Patentinhaber das Bündel an Patentrechten für jeden Vertragsstaat zukommt, für welchen das Patent angemeldet wurde. Gemäß Art. 64 Abs. 1 und Abs. 2 EPÜ richtet sich dabei die Berechtigung des Patentinhabers betreffend den einzelnen Staat nach dem jeweiligen nationalen Recht.

Schließlich existiert die Möglichkeit, die Anmeldung auch gestützt auf die Pariser Verbandsübereinkunft weltweit vorzunehmen. Dabei erfüllt die WIPO eine Art „Briefkastenfunktion“. Sie nimmt die Patentanmeldung entgegen und leitet diese an die Patentämter der in der Anmeldung genannten Staaten weiter. Dabei handelt es sich bei weitem nicht um eine Art Weltpatent. Vielmehr bearbeiten die einzelnen Patentämter die jeweilige Anmeldung selbständig und unabhängig von anderen Ämtern und der WIPO.³²

III. Ausschluss von mathematischen Methoden und Computerprogrammen vom Patentschutz

Bei der Betrachtung der Patentfähigkeit von KI-Technologien interessieren vor allem die Patentierungsausschlüsse in § 1 Abs. 3 PatG sowie Art. 52 Abs. 2 EPÜ. Beide Absätze schließen einerseits mathematische Methoden und andererseits Programme für Datenverarbeitungsanlagen von der Patentierung aus. Sie stellen damit die erste Hürde hinsichtlich eines patentrechtlichen Schutzes von KI-Technologien dar. Wie vorstehend ausgeführt wurde, sind KI-Technologien die Softwareebene intelligenter digitaler Systeme.³³ So betrachtet sind sie auch Programme für Datenverarbeitungsanlagen und damit Computerprogramme im patentrechtlichen Sinne. Programme – ob intelligent oder nicht – können auf

soll die Erfindung der Allgemeinheit bekannt gemacht werden und so untersucht und weiterentwickelt.

³² Vgl. PVÜ.

³³ Vgl. oben Einl.

ihrer einfachsten Ebene als mathematische Methoden aufgefasst werden, die beliebig komplex zu einem Computerprogramm³⁴ kombiniert werden können.³⁵ KI-Technologien fallen also *prima vista* in den Anwendungsbereich der Patentierungsausschlüsse in § 1 Abs. 3 PatG sowie Art. 52 Abs. 2 EPÜ. Dies nicht nur unter dem Titel der Programme für Datenverarbeitungsanlagen, sondern in ihrer simpelsten Betrachtung auch unter demjenigen Titel der mathematischen Methoden.

Der Ausschluss von mathematischen Methoden liegt in deren Abstraktheit begründet. Die Anwendung von mathematischen Methoden führt in der Regel nicht zu einem Ergebnis technischer Art, da sie sich nicht irgendwelcher Naturkräfte bedienen, sondern der Logik.³⁶ Dies bedeutet jedoch nicht, dass eine mathematische Methode doch als Grundlage für eine technische Handlungsanweisung herangezogen werden kann.³⁷ Gleiches gilt für Softwareebenen von digitalen Systemen. Auch sie bedienen sich somit keiner Naturkraft, sondern wie mathematische Methoden der Regeln der Logik.³⁸

Der Ausschluss von Computerprogrammen ist ähnlich begründet. Computerprogramme im Sinne von Softwareebenen digitaler Systeme an sich sind nichts weiter als abstrakte Rechenregeln, die Anweisungen an den menschlichen Geist darstellen.³⁹

1. (Zweistufiger) Prüfungsansatz des EPA

Dies bedeutet aber nicht, dass Erfindungen auf dem Gebiet von Datenverarbeitungsprogrammen gänzlich von der Patentierbarkeit ausgenommen wären. Der Ausschluss betrifft gemäß Art. 52 Abs. 3 EPÜ bzw. § 1 Abs. 4 PatG nur die Patentierung des Computerprogrammes als solches. Sie sind als Bestandteil computerimplementierter Erfindungen dennoch patentfähig. Wann dies der

³⁴ Möglich ist auch eine Übersetzung in die menschliche Sprache.

³⁵ Vgl. oben Kap. 1, A. ff.

³⁶ Statt vieler: Benkard/BACHER, PatG, § 1 Rn. 98.

³⁷ Statt vieler: Benkard/BACHER, PatG, § 1 Rn. 98; vgl. Mes/MES, PatG § 1 Rn. 109 f.

³⁸ Statt vieler: Benkard/BACHER, PatG, § 1 Rn. 98; MELULLIS GRUR 1998, 852; a.M. KRASSER/ANN, § 12 Rn. 146.

³⁹ HAEDICKE, Kap. 10 Rn. 10 ff.; REDEKER, Rn. 144; vgl. Benkard/BACHER, PatG, § 1 Rn. 98 f.

Fall ist, wird sogleich aufgezeigt – sowohl für das PatG als auch für das EPÜ. Vorweg ist festzuhalten, dass sich die Prüfung in der Rechtsprechung des BGH von derjenigen in der Entscheidungspraxis des EPA betreffend computerimplementierte Erfindungen unterscheidet. Dennoch führen beide Prüfungsarten zu demselben Ergebnis. Dies liegt darin begründet, dass sich die Praxis des BGH derjenigen des EPA angenähert hat.⁴⁰

Es sei darauf hingewiesen, dass es sich beim EPA nicht um ein Gericht handelt. Es handelt sich um ein Amt, das über die Erteilung von Patenten entscheidet. Das EPÜ sieht dabei gewisse interne Beschwerdemechanismen gegen (Nicht)Erteilungen von Patenten vor.⁴¹ Über die Gültigkeit eines Patentes entscheiden die nationalen Gerichte.

Das EPA geht davon aus, dass Computerprogramme nur dann ausgeschlossen sein sollen, wenn der Patentanspruch auf eine rein abstrakte Befehlsfolge gerichtet ist. Sobald der Anspruch mindestens ein technisches Element umfasst, ist das Computerprogramm der Patentierung zugänglich.⁴² Das EPA verfolgt dabei einen zweistufigen Prüfungsansatz. In einem ersten Schritt wird – noch ohne Bezug zum Stand der Technik – geprüft, ob die Erfindung grundsätzlich dem Patentschutz zugänglich ist. Mithin wird geprüft, ob die Erfindung technischen Charakter aufweist.⁴³ Dabei muss die Erfindung einen „weiteren technischen Effekt“ als die bloße Programmabfolge auf der Hardware aufweisen.⁴⁴ Ist dies nicht der Fall, gilt die Erfindung als vom Patentschutz ausgeschlossen.⁴⁵ Dieser „weitere technische Effekt“ muss nicht neu sein und auch nicht auf einer erfinderischen Tätigkeit beruhen.⁴⁶ Es reicht ein einziges technisches Merkmal im Anspruch und dieses kann auch durch „die Funktionsweise des Computers, auf dem das Programm läuft, also durch die Funktionsweise der Hardware dieses

⁴⁰ HAEDICKE, Kap. 10 Rn. 17; siehe auch Benkard/BACHER, PatG, § 1 Rn. 116.

⁴¹ Art. 99 ff. EPÜ und Art. 109 ff. EPÜ.

⁴² Statt vieler: Benkard/BACHER, PatG, § 1 Rn. 111.

⁴³ SCHWARZ/KRUSPIG, Rn. 336; EPA GRUR Int 2008, 340 – T 0154/04, E. 5.

⁴⁴ Da alle Computerprogramme zwecks Ablaufs auf einer Hardwarekomponente physikalische Veränderungen bei der Hardware verursachen, würde der Patentierungsausschluss sonst gegenstandslos, vgl. auch GRUR Int. 1999, 1055 - T 1173/97, E. 6.4.

⁴⁵ Vgl. SCHWARZ/KRUSPIG, Rn. 341.

⁴⁶ GRUR Int 1999, 1056 - T 1173/97, E. 8.

Computers bewirkt werden.⁴⁷ Kann die Technizität bejaht werden bzw. ist die Erfindung nicht vom Ausschluss in Art. 52 Abs. 2 EPÜ erfasst, liegt eine Erfindung vor. Es sind aber nach wie vor die weiteren Voraussetzungen zu prüfen:

In einem zweiten Schritt werden die Neuheit und erfinderische Tätigkeit (sowie die gewerbliche Anwendbarkeit) geprüft.⁴⁸ Das EPA erachtet in Art. 52 Abs. 2 EPÜ eine nicht abschließende Negativ-Aufzählung von Beispielen für das Technizitätserfordernis in Art. 52 Abs. 1 EPÜ.⁴⁹ Für die Beurteilung der Neuheit und der erfinderischen Tätigkeit werden nur die technischen Merkmale berücksichtigt. Es ist allerdings nicht schädlich (für den Erfindungscharakter), wenn die nichttechnischen Merkmale den bestimmenden Teil des Anspruchs bilden.⁵⁰ Unter dem Titel der Neuheit und der erfinderischen Tätigkeit verfolgt das EPA den sogenannten Aufgabe-Lösungs-Ansatz. Dieser besagt, dass die von der Erfindung zu lösende „Aufgabe eine technische sein muss, dass sie durch die beanspruchte Erfindung auch tatsächlich gelöst werden muss, dass alle Merkmale des Anspruchs zur Lösung beitragen sollen und dass es sich um eine Aufgabe handeln muss, die einem Fachmann des betreffenden technischen Gebiets am Prioritätstag zur Lösung angetragen werden könnte.“⁵¹ Dabei dürfen aber nur die technischen Merkmale (und nicht die nicht-technischen Merkmale) berücksichtigt werden.⁵² Mit anderen Worten wird im zweiten Schritt geprüft, ob sich die Erfindung aufgrund der technischen Mittel vom Stand der Technik abhebt.

2. Prüfungsansatz des BGH

Der BGH verfolgt einen leicht unterschiedlichen Prüfungsansatz. Dies rührt daher, dass der BGH in § 1 Abs. 3 PatG nicht wie das EPA eine Negativ-Aufzählung für die Technizität sieht, sondern eine zusätzliche Voraussetzung für das Vorliegen einer Erfindung zusätzlich zur Technizität.⁵³

⁴⁷ GRUR Int 1999, 1055 - T 1173/97, E. 6.6; vgl. auch SCHWARZ/KRUSPIG, Rn. 347.

⁴⁸ EPA GRUR Int. 2008, 340 - T 0154/04, E. 5.

⁴⁹ Anders als der BGH, dazu sogleich.

⁵⁰ EPA GRUR Int 2008, 340 - T 0154/04, E. 5.

⁵¹ EPA BeckRS 2002 30618032 - T0641/00, E. 5.

⁵² EPA BeckRS 2002 30618032 - T0641/00, E. 6.

⁵³ Vgl. HAEDICKE, Kap. 10 Rn. 18; SCHWARZ/KRUSPIG, Rn. 339.

Der BGH prüft, ob der Ausschlussatbestand von § 1 Abs. 3 i.V.m. § 1 Abs. 4 PatG erfüllt ist. Um den Tatbestand nicht zu erfüllen, muss das Computerprogramm ein *konkretes* technisches Problem lösen.⁵⁴ Dabei reicht es aus, wenn nur ein Teilaspekt des zu schützenden Computerprogramms ein technisches Problem löst.⁵⁵

Diese zusätzliche Anforderung ist bspw. bereits bei der Modifizierung von Gerätekomponenten erfüllt, wie das bei einer bestimmten Anordnung der Speicherbelegung der Fall ist⁵⁶, oder wenn der Ablauf des Programms durch technische Gegebenheiten bestimmt wird. Dies ist bspw. dann der Fall, wenn die Auflösung des Computertomographen anhand von medizinischen Informationen automatisch eingestellt wird, nachdem auch die Patientendaten eingegeben wurden.⁵⁷ Es reicht dabei aus, wenn das Programm Rücksicht auf die technischen Gegebenheiten der Datenverarbeitungsanlage selbst nimmt.⁵⁸ Eine Einflussnahme auf technische Gegebenheiten außerhalb der Datenverarbeitungsanlage ist nicht Voraussetzung.⁵⁹

Danach prüft der BGH das Vorliegen der Technizität und die weiteren Voraussetzungen wie Neuheit und erfinderische Tätigkeit. Die vorgelagerte Frage nach dem Nicht-Vorliegen des Ausschlussgrundes ist also eine Hürde.⁶⁰ Diese ist, wie soeben gezeigt,⁶¹ jedoch leicht überwunden. Sodass sich die Handhabungen des EPA sowie des BGH seit dessen Angleichung an die europäische Behörde nicht wesentlich unterscheiden.⁶²

3. Zwischenergebnis

Es kann somit festgehalten werden, dass mathematische Methoden wie auch Computerprogramme durchaus patentierungsfähig sind. Eine mathematische

⁵⁴ BGH MMR 2002, 106 – Suche fehlerhafter Zeichenketten.

⁵⁵ BGH GRUR 2011, 127 – Verfahren zur visuellen Darstellung für die Navigation *e contrario*.

⁵⁶ Statt vieler: BGH MMR 2010, 553 – Dynamische Dokumentengenerierung.

⁵⁷ Statt vieler: BGH GRUR 2009, 480 – Kopierläden II.

⁵⁸ Statt vieler: BGH MMR 2010, 551 – Dynamische Dokumentengenerierung.

⁵⁹ Statt vieler: BGH MMR 2010, 551 – Dynamische Dokumentengenerierung.

⁶⁰ Oder von Benkard/BACHER, PatG, § 1 Rn. 113 als „Filterwirkung“ bezeichnet.

⁶¹ Soeben Kap. 7, A., III., 2.

⁶² Benkard/BACHER, PatG, § 1 Rn. 116; KRASSER/ANN, § 12 Rn. 115.

Methode, wenn sie zum technischen Charakter der Erfindung beiträgt,⁶³ und ein Computerprogramm, wenn es zur Lösung eines technischen Problems mit technischen Mitteln dient bzw. selbst technischen Charakter aufweist.⁶⁴ Mit anderen Worten muss das Computerprogramm das Vorhandensein von technischen Mitteln (wie bspw. ein Computernetzwerk) voraussetzen oder von einem anderen technischen Gerät mit technischer Wirkung ausgeführt werden und dabei technischen Charakter besitzen. Dabei genügt allerdings der alleinige Umstand nicht, dass ein Verfahren den Einsatz eines Computers erfordert. Das Computerprogramm muss beim Ablauf auf einem Computer eine weitere technische Wirkung erzeugen, bspw. die Steuerung eines technischen Verfahrens.⁶⁵

B. Prüfung der patentrechtlichen Schutzfähigkeit von KI-Technologien

Es sollen nachfolgend die Problempunkte aufgezeigt werden, die sich beim patentrechtlichen Schutz von KI-Technologien ergeben. Vorweg sollte aber bereits aufgrund des Erfindungsbegriffs deutlich werden, dass eine KI-Technologie, die noch nicht trainiert wurde, dem Patentrechtsschutz unzugänglich ist.⁶⁶ Dies liegt in der Voraussetzung der Funktionsfähigkeit einer Erfindung⁶⁷ begründet. Untrainierte KI-Technologien nach dem dargelegten Verständnis – seien dies Expertensysteme, genetische Programme oder KNN – sind mithin funktionsunfähig. Sie sind daher nicht in der Lage, ein technisches Problem zu lösen, weshalb sie bereits an dieser Stelle als patentfähige Erfindungen ausscheiden.

⁶³ Vgl. EPA, Richtlinien für die Prüfung, Teil G Kap. II 3.3.

⁶⁴ Kap. 7, A., III., 1. f. hiervor.

⁶⁵ EPA, Richtlinien für die Prüfung, Teil G Kap. II 3.6.

⁶⁶ „Untrainiert“ ist hierbei gleichzusetzen mit dem Stand im Entwicklungsprozess, der die Konzeptualisierung mit erster programmatischer Umsetzung nicht übersteigt. Bei Expertensystemen die Phase also, in der die Wissensbasis nicht erstellt wurde. Dabei kann das Regelset aber durchaus bereits programmiert sein. Bei Neuronalen Netzen, wenn die Architektur erstellt wurde und bei genetischen Programmen das Stadium, bevor die *fitness* der Individuen anhand der Trainingsdaten bewertet wird. Diesfalls wären die einzelnen Individuen als Gegenstand der computerimplementierten Erfindung.

⁶⁷ Siehe oben Kap. 7, A., III., 1.

I. Die erforderliche Technizität und erfinderische Tätigkeit

Die soeben besprochenen Ausnahmen betreffend mathematische Methoden wie auch Computerprogramme bedürfen hinsichtlich der Patentierung von KI-Technologien⁶⁸ einer genaueren Betrachtung der Technizität sowie der erfinderischen Tätigkeit.

Zwecks Subsumtion von KI-Technologien unter die patentrechtlichen Schutzvoraussetzungen drängt sich zudem die Konsultation der EPA-Prüfungsrichtlinie auf. Diese widmet sich in Teil G, Kapitel II 3.3.1 künstlicher Intelligenz sowie dem maschinellen Lernen.⁶⁹ In der Richtlinie wird in einem ersten Schritt darauf hingewiesen, dass KI und maschinelles Lernen auf Rechenmodellen und Algorithmen zur Klassifizierung fußen. Dies deckt sich mit dem unter Kapitel 1 aufgeführten Wesensmerkmal digitaler Systeme. Das EPA verortet demnach KI-Technologien nicht erst bei den Computerprogrammen, sondern noch grundlegender als Rechenmodelle und damit als mathematische Methode, die für sich allein grundsätzlich nicht patentierbar ist.⁷⁰

Es ist also davon auszugehen, dass KI-Technologien analog der mathematischen Methoden oder Computerprogramme dann nicht von den Patentierungsausschlüssen in § 1 Abs. 3 PatG bzw. Art. 52 Abs. 2 EPÜ erfasst sind, wenn sie (i) Grundlage einer technischen Erfindung bilden; (ii) im Kontext der Erfindung einem technischen Zweck⁷¹ dienen; oder (iii) wenn der Anspruch unabhängig einer technischen Anwendung auf eine spezifische technische Umsetzung der der Technologie zugrunde liegenden Rechenmodelle und Rechenregeln gerichtet ist und das System, in welches die Technologie implementiert ist, für diese Umsetzung besonders angepasst ist. Mit anderen Worten ist für eine KI-Technologie Technizität gegeben, wenn sie eine Anweisung zum technischen Handeln, mithin die Lösung eines technischen Problems mittels technischer Mittel darstellt.⁷²

⁶⁸ KI-Systeme primär im Sinne der Kern-KI auf Programmebene.

⁶⁹ EPA, Richtlinien für die Prüfung, Teil G Kap. II 3.3.1.

⁷⁰ Vgl. oben Kap. 7, A., III.

⁷¹ Siehe Kap. 7, A., III., 3. hiervor; EPA, Richtlinien für die Prüfung, Teil G Kap. II 3.3. Dabei genügt die Steuerung eines technischen Systems jedoch nicht.

⁷² HAEDICKE, Kap. 10 Rn. 42; KRAUSEN, S. 68 f.; Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3. Rn. 9; BGH MMR 2010, 551 – Dynamische Dokumentengenerierung; vgl. auch HAUCK/CEVC, ZGE 2019, 148 ff.

Als Beispiel führt das EPA die Verwendung eines KNN zwecks Erkennung der Herzschlagfrequenz in einem Herzüberwachungsgerät an.⁷³ Die Hürde der Technizität ist demnach gut zu überwinden,⁷⁴ was das EPA mit seinem Entscheid „Computerprogramme“ besonders deutlich machte. In diesem Fall genügte es, dass die Lehre, für welche Schutz begehrt wurde, den Einsatz technischer Vorrichtungen umfasste. Sei es auch nur eine Datenverarbeitungsanlage.⁷⁵ Dies bedeutet jedoch nicht, dass auch automatisch eine erfinderische Tätigkeit im Sinne des EPA vorliegt.⁷⁶ Vielmehr bedarf es der eingehenden Auseinandersetzung mit dem technischen Charakter unter dem Titel der erfinderischen Tätigkeit.⁷⁷ Denn das bloße Implementieren einer Kern-KI in einen Computer dürfte regelmäßig am Erfordernis des Nichtnaheliegens scheitern.

Sowohl KNN wie auch genetische Programme und Expertensysteme dürften somit die Voraussetzungen der Technizität bzw. erfinderischen Tätigkeit erfüllen, sofern sie einen genügenden technischen Bezug aufweisen.⁷⁸ Während dies bei einer bereits (technisch) implementierten KI-Vorrichtung relativ niederschwellig erreicht werden kann, bedarf es zwecks Patentierung der Technologie als solcher im Sinne der reinen Softwareebene in Form von Code mehr zur Überwindung der Technizitätshürde.⁷⁹ Es ist dabei vor allem an die Patentierung einer KI-implementierten Erfindung zu denken.⁸⁰ Entscheidend könnte beispielsweise sein, ob die KI-Technologie über die „bloße“ Erfassung, Verarbeitung, Speicherung, Auswertung, Übermittlung von Daten und/oder Bereitstellung von Informationen hinausgeht und tatsächlich ein technisches Problem gelöst wird oder sich auch mit dem „Wie“ der Ermittlung des zu analysierenden

⁷³ EPA, Richtlinien für die Prüfung, Teil G Kap. II 3.3.1.

⁷⁴ So auch DELTORN/LEMÉNAGER, *Réalités industrielles* Nov. 2020, 35.

⁷⁵ EPA GRUR Int 2010, 614 – G 3/08.

⁷⁶ So auch das EPA GRUR Int 2010, 614 – G 3/08; oder auf nationaler Ebene der BGH unter dem Titel der Technizität, siehe dazu oben Kap. 7, A., III., 1.

⁷⁷ Siehe dazu oben Kap. 7, A., III., 1. ff.; vgl. auch KRAUSEN, S. 69 f.; KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 43; MUHR, S. 78 ff.

⁷⁸ So auch DELTORN/LEMÉNAGER, *Réalités industrielles* Nov. 2020, 35 f.; ähnlich KRAUSEN, S. 331 ff.

⁷⁹ DELTORN/LEMÉNAGER, *Réalités industrielles* Nov. 2020, 36; Rechtsprechung in KI-Rechtshandbuch-HEINZE/ENGEL, §10 Rn.24 ff und Rn. 35 f.

⁸⁰ KRAUSEN, S. 67 ff.; MUHR, S. 78 ff.; vgl. Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3. Rn. 10 ff.

Dateninputs befasst.⁸¹ Ebenfalls kann entscheidend sein, ob die KI-Technologie auf einem nichttechnischen oder technischen Gebiet eingesetzt wird.⁸²

Das Aufarbeiten und Bereitstellen der Trainingsdaten wie auch das Training des Systems kann gemäß EPA den technischen Charakter eines KI-Systems (mit)prägen.⁸³ Dasselbe muss folgerichtig auch für die im System eingesetzte Technologie gelten. Voraussetzung dazu ist aber, dass das KI-System bzw. die KI-Technologie⁸⁴ selbst einem technischen Zweck dient und das Training diesen technischen Zweck unterstützt.⁸⁵

Die Ausformulierung des Patentanspruchs hinsichtlich dieser Voraussetzungen bedingt eine eingehende Auseinandersetzung mit den Ausschlusskriterien der mathematischen Methoden und Computerprogramme. Das EPA weist in seinen Richtlinien darauf hin, dass Begriffe wie „neuronales Netz“, „*Support Vector Machine*“ oder „*reasoning engine*“ auf abstrakte Modelle oder Algorithmen hindeuten können und nicht *per se* einen technischen Charakter implizieren.⁸⁶ Es ist folglich bei der Ausformulierung des Patentanspruches mit der Verwendung dieser Begriffe Vorsicht geboten. Das wiederum zeigt auf, dass betreffend die erforderliche Technizität von KI-Technologien stets eine Einzelbetrachtung notwendig ist.⁸⁷ Insofern gilt für KI-Technologien als Objekt des Patentrechts nichts anderes als bereits für mathematische Methoden und (herkömmliche) Computerprogramme galt.⁸⁸

⁸¹ HAEDICKE, Kap. 10 Rn. 30; KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 27; vgl. auch KRAUSEN, S. 68 f.

⁸² KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 25, 27.

⁸³ EPA, Richtlinien für die Prüfung, Teil G Kap. II 3.3.1.

⁸⁴ Je nach Patentanspruch.

⁸⁵ EPA, Richtlinien für die Prüfung, Teil G Kap. II 3.3.1.

⁸⁶ EPA, Richtlinien für die Prüfung, Teil G Kap. II 3.3.1.

⁸⁷ KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 18; Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3. Rn. 15; SÖBBING, MMR 2021, 113; vgl. auch APEL/KAULARTZ, RD 2020, 29 und GRÄFE/KAHL, MMR 2021, 123.

⁸⁸ Vgl. sehr detailliert die Dissertation von KRAUSEN.

Im Hinblick auf die Patentierung von KI-Technologien gilt dagegen viel eher für die patentrechtlichen Begriffe des menschlichen Erfinders und der hinreichenden Offenbarung Neues. Diese Themenaspekte sind Gegenstand der kommenden Abschnitte.

II. *Erfinderbegriff*

Wie auch das Urheberrecht⁸⁹ ist das Patentrecht vom Anthropozentrismus geprägt und geht damit vom menschlichen Erfinder aus.⁹⁰ Die Erfindung kann nach allgemeinem Verständnis in der Lehre und Rechtsprechung nur einem menschlich geistigen Gedanken entsprungen sein.⁹¹ Dabei kann durchaus ein Computer eingesetzt werden. Wesentlich ist dabei, dass der Mensch anhand der Ergebnisse des Computers eine Lösung für ein technisches Problem erkennt bzw. die Computerergebnisse zur technischen Problemlösung heranzieht.⁹²

Der Umstand des menschlichen Erfinders ist bei der Patentierung von anwendungsbereiten KI-Technologien nicht unproblematisch. Wie aufgezeigt wurde, werden bei der genetischen Programmierweise die Individuen automatisch durch einen Computer generiert und danach auch automatisch weiterentwickelt, bis das Ziel-Programm vorliegt.⁹³ Es handelt sich also nicht um einen Menschen, welcher das Ziel-Programm und damit die KI-Technologie programmiert.

Auch bei der Entwicklung von KNN ist es letztlich der Optimierungsalgorithmus, welcher dem untrainierten Netz die eigentliche Funktion verleiht. Der Op-

⁸⁹ Siehe unten Kap. 8, A., I.

⁹⁰ Siehe zur Thematik ausführlich KRAUSEN, S. 113 ff.; zum allgemeinen statt vieler: KRASSER/ANN, § 19 Rn. 7; für die ständige Rechtsprechung vgl. BGH GRUR 1971, 212 – Wildverbißverhinderung; vgl. auch MENIERE/PIHLAJAMAA, GRUR 2019, 335 mit dem Hinweis, dass es sich dabei um einen dem Patentsystem sowie EPÜ zugrunde liegenden und auf internationalen Verträgen (Art. 4^{ter} PVÜ; Regel 4.6 und 4.17 i) PCT; Regel 51^{bis} 1 a) i) und 51^{bis} 2 i) PCT) beruhenden weltweiten Konsens.

⁹¹ Siehe stellvertretend Benkard/MELULLIS, PatG, § 6 Rn. 30 ff.

⁹² Siehe stellvertretend Benkard/MELULLIS, PatG, § 6 Rn. 31 f. m.w.N.

⁹³ Oben Kap. 2, C., III., 4. f.

timierungsalgorithmus und nicht etwa ein Mensch stellt die einzelnen Gewichtungsinformationen der jeweiligen Neuronen ein – der entscheidende Schritt im Hinblick auf die Funktionsfähigkeit des KNN.⁹⁴

Wie oben unter Kapitel 2, C., IV. aufgezeigt wurde, ist es bei KI-Technologien nicht unüblich, dass das Programm die für die Frage nach dem „Wie“ der Problemlösung notwendigen Zusammenhänge selbst erlernt.⁹⁵ Zudem existieren bereits KI-Technologien, welche das zu lösende Problem in einem ersten Schritt auch erst entdecken (sollen) und dieses danach mittels Trainings autonom lösen.⁹⁶ Schließlich sei auch an solche Systeme erinnert, die noch in der Anwendungsphase losgelöst von einem menschlichen Input neue Funktionen hinzulernen.⁹⁷

Setzt man auch im Patentrecht eine geistige Schöpfung voraus, stellt sich auch sogleich die nächste Herausforderung: Je nach Ausgestaltung der KI-Technologie ist die erfinderische Leistung der schöpfenden Person im Hinblick auf die Formulierung des Codes verschwindend klein oder gegen Null.⁹⁸

Bedarf es demnach im Patentrecht einer Anpassung des Verständnisses des Erfinderbegriffs, wenn man die Patentierung von KI-Systemen, insb. der zugrundeliegenden KI-Technologie, zulassen will? Eine Anpassung in die Richtung, dass auch ein geringer Beitrag der programmierenden Person zu Beginn des Prozesses ausreicht?⁹⁹

Sofern es sich um KI-Technologien handelt, welche das technische Problem nicht autonom erkennen und die technische Lösung dazu auch nicht selbstständig lösen, bereitet der anthropozentrische Gedanke im Patentrecht weniger

⁹⁴ Siehe oben Kap. 2, C., II., 3. ff.

⁹⁵ Siehe oben Kap. 2, C. IV. f. Dieses Problem wird insbesondere dann pointiert, wenn die erforderliche Technizität gerade erst durch diese Fähigkeit des KI-Systems begründet wird.

⁹⁶ NÄGERL/NEUBURGER/STEINBACH GRUR 2019, 340 mit Verweis auf US Patent Nr. 5,852,815 (Creativity Machine) und US Patent Nr. 6,847,851 (Invention Machine); skeptisch hierzu Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3. Rn. 38.

⁹⁷ Siehe oben Kap. 2, C., II., 4.

⁹⁸ Selbstredend darf es geistiger Leistung bei der Entwicklung von KI-Technologien, doch erschöpfen sich diese in der Vorbereitung sowie in der Verwertung des KI-Erzeugnisses.

⁹⁹ Siehe nur: MENIERE/PIHLAJAMAA, GRUR 2019, 335 f.

Probleme als im Urheberrecht¹⁰⁰: Einerseits ist die Erfindung nicht an die Persönlichkeit des Erfinders geknüpft, wie das bei der geistigen Schöpfung im Urheberrecht der Fall ist.¹⁰¹ Andererseits besteht die erfinderische Leistung im Auffinden des technischen Problems oder im Finden des Einsatzgebietes für die Lösung eines solchen Problems.¹⁰² Solange diese Leistung von einem Menschen erbracht wird, sollte der Erfinderbegriff hinsichtlich der Patentierung von KI-Technologien keine Probleme bereiten.¹⁰³

Betreffend die KI-Technologien, die dazu in der Lage sind, ein Problem selbst zu eruieren, bedarf es einer genaueren Betrachtung. Es stellt sich die Frage, wie gering der menschliche Beitrag sein kann, um das erforderliche Maß an Menschlichkeit im Erfindungsprozess zu erreichen.¹⁰⁴ So steht am Ursprung jeder KI-Technologie ein Mensch bzw. sind Menschen an der Entwicklung jeder KI-Technologie sowie jedes KI-Systems beteiligt. Es ist dabei nicht nur an Programmierer:innen und Trainer:innen (zusammen als Entwickler:innen) zu denken, sondern insbesondere bei solchen Technologien, die auch zur Selbstoptimierung in der Lage sind, auch an die Benutzer:innen in der Anwendungsphase. Diese trainieren und damit entwickeln – wenn auch unter Umständen unbewusst – die KI-Technologie weiter. Daneben kommen auch die Eigentümer:innen des KI-Systems als Rechtsinhaber:innen in Frage. Sie leisten zwar keinen schöpferischen, dafür aber einen wirtschaftlichen Beitrag. Unter Umständen ermöglichen sie damit erst das erfinderische Schaffen.¹⁰⁵

Das Programmieren der Grundstruktur sowie des Optimierungsalgorithmus (oder die Auswahl eines Optimierungsalgorithmus) bei KNN, wie auch eines Expertensystems,¹⁰⁶ dürfte bereits eine ausreichende geistige Schöpfung im patentrechtlichen Sinne darstellen. Auch bei der genetischen Programmierweise

¹⁰⁰ Siehe dazu weiter unten Kap. 8, A., I. ff.

¹⁰¹ KKI-PAPASTEFANOU, S. 20, welcher dabei auf die freie Übertragbarkeit des Patents im Gegensatz zur mangelnden Übertragbarkeit des Urheberrechts hinweist.

¹⁰² HARTMANN/PRINZ, S. 787; KKI-PAPASTEFANOU, S. 24.

¹⁰³ So auch KRAUSEN, S. 125; HARTMANN/PRINZ, S. 787; KKI-PAPASTEFANOU, S. 24; vgl. aber BECKER, S. 209 f.

¹⁰⁴ Vgl. KI & Recht kompakt-HARTMANN/OHST, S. 162.

¹⁰⁵ NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 340; Rechtshandbuch-AI-TOCHTMANN, Kap. 7.3. Rn. 43.

¹⁰⁶ Damit ist das Regelset sowie die Inferenzmaschine gemeint.

dürfte das Programmieren der Struktur, die die Individuen generiert sowie die Auswahl und Programmierung der Fitnessfunktion ausreichend geistig herausfordernd sein.

Selbst wenn man die menschliche Erfindungstätigkeit betreffend das Programmieren der Grundstrukturen (bei allen besprochenen Technologien) im Sinne des Patentrechts ablehnen würde oder wenn bei der zu patentierenden Technologie vorprogrammierte Strukturen verwendet wurden, stellt die Auswahl, Zusammenstellung und Aufbereitung, mithin die Kuration der Trainingsdaten, einen entscheidenden menschlich geistigen Beitrag dar: Wie aufgezeigt wurde, ist es zu einem erheblichen Anteil die Qualität der Trainingsdaten, die über den Erfolg bzw. die Qualität der KI-Technologie entscheidet.¹⁰⁷ Wenn auch das Training mit Trainingsdaten allein nicht die Technizität begründen kann,¹⁰⁸ dürfte es das Erfordernis der notwendigen Menschlichkeit im Erfindungsprozess erfüllen.¹⁰⁹

Es ergeben sich somit wohl genügend menschliche Beiträge, sodass diesbezüglich keine Änderung des Patentrechts notwendig wird.¹¹⁰ Es besteht kein Anlass, den Anthropozentrismus im Patentrecht aufzugeben oder aufzuweichen. Es existieren wie gesehen verschiedene Möglichkeiten, dem anthropozentrischen Verständnis des Patentrechts gerecht zu werden.¹¹¹ Allerdings stellt sich aufgrund der Mehrheit von an der Entwicklung beteiligten Personen die Frage, wem die Erfindung zugerechnet werden soll.

¹⁰⁷ Siehe oben Kap. 2, B.

¹⁰⁸ Siehe oben Kap. 7, B., I.

¹⁰⁹ Vgl. Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 20 f., welche aus dem Training mit Trainingsdaten bereits Technizität ableiten will oder KI & Recht kompakt-HARTMANN/OHST, S. 161 f., die bereits die Programmierleistung – möge sie auch noch so klein sein – *de lege ferenda* als ausreichende menschlich geistige Leistung erachten.

¹¹⁰ So auch LAUBER-RÖNSBERG/HETMANK, GRUR Int. 2019, 642; MENIERE/PIHLAJAMAA, GRUR 2019, 336; Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 48; vgl. auch SCHAUB, JZ 2017, 348 f.; a.M. wohl KI & Recht kompakt-HARTMANN/OHST, S. 161 f.

¹¹¹ Dies im Unterschied zum Urheberrecht, wo der Anthropozentrismus ausgeprägter ist bzw. eine größere Hürde darstellt. Siehe dazu unten Kap. 8, A., I. ff.

Kann die KI-Technologie selbst als Inhaberin der Erfindung gelten? Eine solche Lösung ist abzulehnen.¹¹² Einerseits ist unklar, welcher Teil der KI nun als Erfinder gelten soll. Das ablaufende Programm? Oder ist es die gesamte KI-Vorrichtung im Sinne des fertigen KI-Systems? Für welche Lösung man sich auch entscheidet, entscheidender ist die Frage nach der Rechtsfähigkeit von KI-Systemen.¹¹³ Solange solche Systeme über keine Rechtsfähigkeit besitzen bzw. solange die E-Person nur Gegenstand von unter anderem juristischen Diskursen ist, entfällt auch die Möglichkeit, sie als Inhaberin der Erfindung zu qualifizieren.¹¹⁴

Zudem steht eine Zuweisung der Erfindung an die KI-Technologie bzw. deren Bestandteile diametral gegen die Belohnungs- sowie Anspornungstheorie als Teil der Patentrechtsrechtfertigung.¹¹⁵ Zumindest zum jetzigen Stand der Technik dürften KI-Systeme und deren Bestandteile den finanziellen Anreiz nicht als tatsächlichen Anreiz empfinden. In Anbetracht einer rein utilitaristischen Betrachtung der Patentrechtsrechtfertigung steht dem Gedanken eines KI-Systems oder von dessen Bestandteile als Erfinder jedoch nichts entgegen.¹¹⁶ Steht doch bei dieser Rechtfertigungstheorie der technische und wirtschaftliche Fortschritt im Vordergrund.¹¹⁷

Wenn also das KI-System und damit auch die KI-Technologie nicht als Inhaber der Erfindung in Frage kommt, drängt sich auf, diejenige Person als Erfinder zu betrachten, auf die die Entwicklung der KI-Technologie zurückgeht. Damit

¹¹² BPatG GRUR 2022, 1213 ff. – FOOD CONTAINER; EPA 21.12.2021 – J 8/20 und J 9/20; vgl. HARTMANN/PRINZ, S. 787; KRAUSEN, S. 118 f.; SCHAUB, JZ 2017, 347; i.E. wohl ebenfalls: MENIERE/PIHLAJAMAA, GRUR 2019, 335 f.; nicht gänzlich ablehnend: NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 340.

¹¹³ Vgl. dazu Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3. Rn. 38 ff.

¹¹⁴ MENIERE/PIHLAJAMAA, GRUR 2019, 336; Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3. Rn. 39 ff.; vgl. auch DELTORN/LEMÉNAGER, *Réalités industrielles* Nov. 2020, 37; HARTMANN/PRINZ, S. 787; SCHAUB, JZ 2017, 347.

¹¹⁵ So auch KI & Recht kompakt-HARTMANN/OHST, S. 161 f.; Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3. Rn. 41; differenzierend, aber i.E. wohl gleich KRAUSEN, S. 116 f., 190 ff.

¹¹⁶ Vgl. NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 340.

¹¹⁷ Vgl. oben Kap. 4, B.

könnte bspw. die Person als Erfinder gelten, die die Daten zur Verfügung stellt.¹¹⁸

Eine Lehrmeinung schlägt vor, dass das Ergebnis der Erfindungszuweisung von der jeweiligen Patentrechtsrechtfertigung abhängig gemacht werden soll.¹¹⁹ Eine solche Lösung erschließt sich nach der hier vertretenen Ansicht nicht, da sich die Rechtfertigung des Patentrechts nicht mit einer abschließenden Theorie erklären lässt.¹²⁰ Die Beantwortung der Frage nach der Erfinderschaft muss darüber hinaus nur schon aus Rechtssicherheit- und Praktikabilitätsüberlegungen auf eindeutige Weise erfolgen.

Wem schließlich die Erfindung zugeordnet wird, wird sich zeigen müssen.¹²¹ Dabei könnte ausschlaggebend sein, wie substantiell der Beitrag an die Erfindung ist.¹²² Zwar dürfte die Erfindung in der Mehrheit der Fälle und nach einer traditionellen Auffassung des Patentrechts am ehesten der trainierenden oder der programmierenden Person zugerechnet werden, da erstere mit der Auswahl der Trainingsdaten und dem Überwachen des Trainings und zweite mit der Bereitstellung und Modulation der Architektur wohl am entscheidendsten beitragen.¹²³ Auch eine Miterfinderschaft nach Art. 59 EPÜ bzw. § 6 PatG ist möglich und denkbar.¹²⁴ Allerdings können sich angesichts der Mannigfaltigkeit der KI-Technologien und deren Entwicklungsprozesse¹²⁵ die Einzelheiten und Verhält-

¹¹⁸ Vgl. Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 44; siehe oben Kap. 7, B., II.

¹¹⁹ NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 340.

¹²⁰ Vgl. bspw. Kap. 4, A. und Kap. 7, B., II. hiervor.

¹²¹ Vgl. z.B. KKI-PAPASTEFANOU, S. 24.

¹²² Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 44; vgl. auch KKI-PAPASTEFANOU, S. 19; GODDAR, GRUR 2021, 197.

¹²³ So auch Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 45, 47.

¹²⁴ Vgl. KRAUSEN, S. 246 ff.; LAUBER-RÖNSBERG/HETMANK, GRUR Int. 2019, 642; Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 45.

¹²⁵ So dürfte bspw. bei der Verwendung von vorgefertigten KI-Architekturen der Beitrag der programmierenden Person weniger bedeutend sein.

nisse der verschiedenen Beiträge von Fall zu Fall unterscheiden, sodass keine generalisierte Antwort auf die Frage nach der Zuweisung des Erfinderrechts möglich ist, sondern viel eher eine Einzelbetrachtung notwendig sein wird.¹²⁶

Schließlich ist darauf hinzuweisen, dass dem Patentrecht ein Ausgleich von verschiedenen Interessen an der Erfindungsentwicklung nicht fremd ist. Bereits mit dem Arbeitnehmererfindungsgesetz erfolgt ein solcher Interessensausgleich.¹²⁷

III. *Hinreichende Offenbarung*

Gemäß § 34 Abs. 4 PatG bzw. Art. 83 EPÜ ist die Erfindung so deutlich und vollständig zu offenbaren, dass sie ein Fachmann ausführen kann. Dies spiegelt einen Grundgedanken der Rechtfertigung des Patentrechts wider. Die erfindende Person erhält ein grundsätzlich 20 Jahre dauerndes Monopol, die Erfindung unter anderem wirtschaftlich zu verwerten. Im Gegenzug ist die Erfindung im Patentanspruch hinreichend zu offenbaren.¹²⁸ Dies soll sicherstellen, dass die Allgemeinheit an der Erfindung teilhaben kann.¹²⁹ Die Offenbarung der Erfindung ermöglicht so bspw. deren Weiterentwicklung oder Forschungen betreffend andere Einsatzgebiete als ursprünglich vom Erfinder angedacht.¹³⁰ Es muss der Fachperson anhand des Patentanspruchs und den darin enthaltenen Unterlagen, den vorhandenen wissenschaftlichen Hilfsmitteln und anhand der am Anmeldetag vorhandenen Fachkenntnissen möglich sein, den angestrebten Erfolg zu erreichen und die Erfindung auszuführen.¹³¹

Dabei reicht eine detaillierte Strukturbeschreibung nicht zwingend aus. Es muss auch die Funktion beschrieben werden, sofern sich diese nicht ohne Weiteres

¹²⁶ Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 44; i.E. wohl auch für eine Einzelbetrachtung, wobei aber für die Zurechnung der Erfindung an die Nutzer:in bzw. Eigentümer:in plädiert wird: NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 340.

¹²⁷ So auch KKI-PAPASTEFANOU, S. 20.

¹²⁸ Vgl. statt vieler: PIERSON/AHRENS/FISCHER, S. 89.

¹²⁹ Statt vieler: KRASSER/ANN, § 24 Rn. 64.

¹³⁰ Vgl. statt vieler: PIERSON/AHRENS/FISCHER, S. 89 oder Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3 Rn. 22.

¹³¹ Statt vieler: Benkard/SCHÄFERS, PatG, § 34 Rn. 34 ff. mit Hinweis auf die Rechtsprechung.

aus der Strukturbeschreibung ergibt.¹³² Das EPA weist ausdrücklich darauf hin, dass bei Datenverarbeitungsanlagen eine klare, detaillierte Funktionsbeschreibung viel zweckmäßiger sein kann als eine „übergenaue“ Strukturbeschreibung.¹³³ Ist eine Erfindung ungenau beschrieben und kann sie nicht anhand der Patentanmeldungsunterlagen nachgebildet werden, läuft ihre Patentierung dem Patentgedanken zuwider und wird demnach widerrufen oder für nichtig erklärt.¹³⁴

Eine Offenlegung der Programmstruktur sowie der Trainingsdaten kann ausreichen.¹³⁵ Dabei muss aber maßgeblich sein, dass das KI-Modell anhand der Offenbarung nachgebildet werden kann. Eine unzureichende Offenbarung darf nie Grundlage einer Patentierung sein.¹³⁶

KI-Technologien lassen sich zwar in Form von Code darstellen. Allerdings kann bei KI-Technologien oftmals deren Funktionsweise bzw. gar ihre Struktur nicht nachvollzogen bzw. dargestellt, geschweige denn erklärt werden. Einerseits ist da an sogenannte „*Black Box*“ – KI zu denken.¹³⁷ Andererseits dürfte auch bei verschiedenen Arten von „*White Box*“ – KI die Struktur bereits äußerst komplex nachzuvollziehen bzw. zu erklären sein.¹³⁸

Bei Expertensystemen lässt sich die Struktur der Inferenzmaschine inklusive Regelset sowie der Dialogkomponente wie auch der Datensatz vergleichsweise einfach erklären.

Bei der genetischen Programmierweise ist zwar die Funktionsweise des Ziel-Programms schwer zu beschreiben, da diese in der Regel weitaus komplexer ist als bei herkömmlichen Programmierweisen.¹³⁹ Dennoch handelt es sich um „wenn-

¹³² EPA, Richtlinien für die Prüfung, Teil F Kap. III 1.

¹³³ EPA, Richtlinien für die Prüfung, Teil F Kap. III 1.

¹³⁴ Art. 100 lit. b EPÜ, Art. 138 Abs. 1 lit. b EPÜ bzw. Art. § 21 Abs. 1 Bst. 2. PatG, § 22 PatG.

¹³⁵ KI-Rechtshandbuch-HEINZE/ENGEL § 10 Rn. 66; MENIERE/PIHLAJAMAA, GRUR 2019, 335; a.A. Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3 Rn. 23.

¹³⁶ MENIERE/PIHLAJAMAA, GRUR 2019, 335; Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3 Rn. 23.

¹³⁷ KKI-PAPASTEFANOU, S. 25 f.; vgl. auch MENIERE/PIHLAJAMAA, GRUR 2019, 335.

¹³⁸ KKI-PAPASTEFANOU, S. 25 f.

¹³⁹ Siehe dazu oben Kap. 2, C., III., 2.

dann“-Regelwerke, die Informationen *explizit* verarbeiten.¹⁴⁰ Damit kann zwecks Offenbarung im Rahmen der Patentanmeldung der Quellcode offengelegt werden. Auch wenn die Funktionsweise von genetisch entwickelten Programmen schwer erklärbar ist, so lässt sich deren Entwicklungsverfahren sowie die Funktionsweise nicht schwieriger als andere Patentanmeldungen beschreiben. So kann offengelegt werden, wie und wie viele Individuen pro Generation generiert wurden, wie sich das Trainingsdatenset zusammenstellt, wie sich die Fitnessfunktion berechnet, was die Abbruchkriterien sind und wie hoch die Anzahl der Iterationen war.

Bei KNN hingegen dürfte insbesondere die Struktur des trainierten Netzes mit- samt den verschiedenen Parametereinstellungen schwer erklärbar sein.¹⁴¹ In diesem Zusammenhang spricht man auch vom Problem der Erklärbarkeit von KI.¹⁴² Möchte man die Patentierbarkeit von KNN nicht an der mangelnden Offenbarung scheitern lassen, stellt sich die Frage nach einem neuen Begriffsverständnis betreffend die Offenbarung der Erfindung.¹⁴³ Eine Herabsetzung der Anforderungen an die genügende Offenbarung ist dabei aber abzulehnen.¹⁴⁴ Es darf nicht angehen, dass die Neuartigkeit einer Technologie dazu führt, dass das Patentrecht entgegen seiner Grundidee angepasst wird.¹⁴⁵

Nur weil ein Mensch nicht dazu in der Lage ist, die Funktionsweise einer „*Black-Box*“ – KI zu verstehen, darf dies nicht zu deren leichteren Patentierung führen, während auf anderen Gebieten der Technik wie bspw. der Neurobiologie oder bei pharmazeutischen Erfindungen ebenfalls sehr komplexe Vorgänge Teil der Erfindung sind und sich die Erfinder:innen bzw. Patentanwält:innen auf diesen Gebieten vertiefter mit der –ebenfalls schwer verständlichen – Struktur und Funktionsweise auseinandersetzen müssen als die mit einer KI-Patentierung be- traute Person.

¹⁴⁰ Siehe dazu oben Kap. 2, C., III., 3.

¹⁴¹ KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 66; KKI-PAPASTEFANOU, S. 25 f.; vgl. auch Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 22 f.

¹⁴² Siehe nur: KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 66.

¹⁴³ Vgl. auch Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 23.

¹⁴⁴ KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 66.

¹⁴⁵ So auch Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 23.

Muss also der Begriff der Offenbarung neu verstanden werden? Die Offenbarung von KI-Technologie bedingt deren Beschreibung. Bereits die Darstellung der Beschreibung in einer für Menschen verständlichen Form dürfte herausfordernd sein. Das EPA fordert hinsichtlich KNN spezifische Informationen zur Topologie, den Gewichtungen und die Art des Trainings zwecks Problemlösung der Erfindung.¹⁴⁶

Bei KNN müssen also die Schichten¹⁴⁷, die Anpassungen der Gewichtungen bzw. die genauen Gewichtungseinstellungen sowie die Aktivierungs- und Optimierungsfunktionen detailliert dargestellt werden. Anhand dieser Darstellung muss sodann beschrieben werden, wie das (technische) Problem von der KI-Technologie gelöst wird.¹⁴⁸ Ein Fachmann muss anhand dieser Information die KI-Technologie entwickeln können, damit hinreichende Offenbarung vorliegt. Soll eine KNN-Architektur für verschiedene Anwendungsbereiche eingesetzt werden können, und wird auch der Patentschutz für diese Anwendungsbereiche begehrt, sind entsprechend alle Trainingsarten und damit Datensätze zu offenbaren.¹⁴⁹ Es ist bei einem KNN äußerst herausfordernd, mehrere Millionen Gewichtungen, die auf hunderte oder tausende Schichten verteilt sind, verständlich darzustellen. Wenn es auch stimmen mag, dass die Entwickler:innen einer „*Black-Box*“ – KI die Funktionsweise nicht erklären können, so werden sie das KNN aber regelmäßig selbst reproduzieren und das Problem benennen können, welches das Netz löst bzw. die Funktion benennen können, die das KNN besitzt.¹⁵⁰ Schließlich lassen sich auch die Architektur, die Gewichtungseinstellungen, der Optimierungsalgorithmus, die *loss function* sowie die Trainingsdaten und andere Parameter in Code und anderer wahrnehmbaren Form darstellen.

Fachpersonen werden generell dazu in der Lage sein, ein KNN bzw. dessen Funktionsweise anhand der Modellstruktur sowie der Trainingsdaten mitsamt

¹⁴⁶ EPA BeckRS 2000 30598818 – T 521/95.

¹⁴⁷ Inklusive deren Anzahl, Verbindungen, Neuronenanzahl.

¹⁴⁸ KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 65.

¹⁴⁹ KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 65; vgl. als Beispiel für eine mangelnde Offenbarung GRUR-RS 2020, 13002 – T 0161/18.

¹⁵⁰ KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 66; MENIERE/PIHLAJAMAA, GRUR 2019, 335.

Optimierungsalgorithmus oder anhand der Struktur und der Gewichtungsinformationen nachzubilden.¹⁵¹ Dies dürfte sodann das bei einer Erfindung zu verlangende Offenbarungsniveau darstellen. Sofern die Formulierungen auch eindeutig, klar und vollständig sind, sind auch die Offenbarungsvoraussetzungen des Patentrechts in der Regel erfüllt.¹⁵²

IV. *Mangelnde Schutzfähigkeit von Trainingsdatensätzen*

Die Trainingsdaten als solche sind einem patentrechtlichen Schutz nicht zugänglich. Sie sind keine technischen Lehren, sondern Informationen in Form von Bild, Text oder Sprache. Sie können höchstens Teil einer technischen Lehre darstellen.

V. *Exkurs: selbständige Weiterentwicklungen intelligenter digitaler Systeme*

KI-Technologien sind teilweise dazu in der Lage, sich autonom zu verbessern und weiterzuentwickeln.¹⁵³ Diese Fähigkeit bringt die Frage nach der patentrechtlichen Schutzfähigkeit dieser Weiterentwicklungen auf. Der Schutzzumfang eines Patents ergibt sich gemäß §§ 14 und 9 PatG aus den Patentansprüchen. Sofern eine Weiterentwicklung bereits im Patentanspruch beschrieben ist, dürften sich keine Besonderheiten ergeben.¹⁵⁴ Gleich verhält es sich mit der Fähigkeit zur autonomen Weiterentwicklung überhaupt als Teil des Patentanspruchs und somit des Patenumfanges.¹⁵⁵

Eine unvorhergesehene bzw. nicht im Patentanspruch beschriebene Weiterentwicklung kann nicht vom Patentschutz umfasst sein. Eine solche Ausweitung des Schutzzumfanges würde einer Überdehnung des Patentrechts gleichkommen

¹⁵¹ MENIERE/PIHLAJAMAA, GRUR 2019, 335; i.E. wohl auch KI & Recht kompakt-HARTMANN/OHST, S. 161; a.A. KKI-PAPASTEFANOU, S. 26 und wohl auch NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 339; siehe zudem oben Kap. 2, C., II.; Kap. 2, C., II., 4. *in fine*.

¹⁵² Vgl. bspw. NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 339.

¹⁵³ Vgl. Kap. 1, B., II. oben, SCHAUB, JZ 2017, 346.

¹⁵⁴ SCHAUB, JZ 2017, 346.

¹⁵⁵ SCHAUB, JZ 2017, 346.

und ist bereits aus Rechtssicherheitsüberlegungen strikt abzulehnen.¹⁵⁶ Unvorhergesehene Weiterentwicklungen können somit nur Teil einer eigenständigen Patentierung sein.¹⁵⁷ Da es sich dabei aber um eine gänzlich maschinell programmierte Programmstruktur handelt, besteht die Problematik viel eher im Erfordernis des menschlichen Erfinders.¹⁵⁸ Es wird hierzu auf die einschlägige Literatur zu KI-generierten Schutzgütern verwiesen, was nicht vertiefter Gegenstand vorliegender Untersuchung sein soll.¹⁵⁹

VI. Zwischenergebnis

Als Zwischenergebnis kann somit festgehalten werden, dass KI-Technologien einem Patentrechtsschutz grundsätzlich zugänglich sind. Dies gilt vor allem für computerimplementierte KI-Technologien, wenn diese in einer technischen Vorrichtung technische Funktionen erfüllen oder Teil eines technischen Verfahrens sind. KI-Technologien im Sinne der bloßen Programmstruktur können in Ausnahmefällen auch einem Patentschutz zugänglich sein. Sie müssen sich jedoch von bloß abstrakten, mathematischen Methoden oder abstrakten Computerprogrammen unterscheiden.¹⁶⁰

Die Begriffe im Patentrecht sind zudem ausreichend und bedürfen lediglich in ihrem Verständnis gewisser Anpassung, um der „neuen“ Herausforderung der intelligenten digitalen Systeme gerecht zu werden.¹⁶¹

¹⁵⁶ SCHAUB, JZ 2017, 346.

¹⁵⁷ SCHAUB, JZ 2017, 346; gänzlich ablehnend Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3 Rn. 49.

¹⁵⁸ Vgl. Kap. 7, B., II. oben.

¹⁵⁹ Vgl. Literaturhinweise hierzu bei KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 86 ff. und KRAUSEN, S. 107 ff., insb. S. 113 ff.

¹⁶⁰ Vgl. Kap. 7, A., III. ff. oben; so auch APEL/Kaulartz, RD 2020, 29; DELTORN/LEMÉNAGER, *Réalités industrielles* Nov. 2020, 38; HARTMANN/PRINZ, S. 786 f.; HAUCK/CEVC, ZGE 2019, 148 ff.; zustimmend, aber skeptisch KKI-PAPASTEFANOU, S. 25 f und PAPASTEFANOU, CR 2019, 215; KI-Rechtshandbuch-HEINZE/ENGEL, § 10 Rn. 9 ff.; Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3 Rn. 48 f.; i.E. wohl auch KI & Recht kompakt-HARTMANN/OHST, S. 162; siehe auch HETMANK/LAUBER-RÖNSBERG, GRUR 2018, 575 oder NÄGERL/NEUBURGER/STEINBACH, GRUR 2019, 340.

¹⁶¹ KRAUSEN, S. 342 plädiert für eine Rückbesinnung auf die grundsätzliche Funktionsweise des Patentrechts; vgl. auch Rechtshandbuch-AI-TOCHTERMANN, Kap. 7.3 Rn. 48.

Die erforderliche Technizität grenzt den Anwendungsbereich von KI-Technologien ein, die einem patentrechtlichen Schutz zugänglich sind. Mit dem Patentrecht können (zurecht) lediglich Technologien geschützt werden, die auf einem Gebiet der Technik eingesetzt werden. Technologien namentlich aus dem kreativen oder linguistischen Bereich lösen kein technisches Problem und sind somit nicht patentierbar.¹⁶² Zudem müssen selbst technische Anwendungsfelder ausreichend technisch im patentrechtlichen Sinne sein. Damit bleibt ein sehr enger Anwendungsbereich für den Patentschutz von KI-Technologien bestehen. Es bedarf dabei stets eines „menschlichen Anknüpfungsverhaltens“¹⁶³. Gänzlich durch KI-Technologie eigenständig entwickelte Erfindungen dürften aktuell nicht nur Zukunftsmusik sein, sondern sind auch einem Patentschutz unzugänglich.¹⁶⁴

Das Patentrecht schließt hingegen keine der betrachteten KI-Technologien aus. Sowohl KNN wie auch genetisch entwickelte Programme oder Expertensysteme dürften dem patentrechtlichen Schutz prinzipiell zugänglich sein.

¹⁶² Vgl. bspw. GRÄFE/KAHL, MMR 2021, 122; MUHR, S. 90 ff.

¹⁶³ KRAUSEN, S. 342.

¹⁶⁴ KRAUSEN, S. 331, insb. S. 342.

Kapitel 8

Urheberrechtlicher Schutz von KI-Technologien

Die Prüfung eines urheberrechtlichen Schutzes drängt sich auf, weil das Urheberrecht in § 69a ff. UrhG den urheberrechtlichen Schutz von Computerprogrammen vorsieht. Das Urheberrecht bietet damit eine Grundlage für den Schutz der Softwareebenen von digitalen Systemen.

Nach einer Einführung in die Grundlagen des Urheberrechts soll untersucht werden, ob das Urheberrecht auch Raum für den Schutz von Softwareebenen *intelligenter* digitaler Systeme bietet. Dabei wird sowohl untersucht, ob die KI-Technologien unter den Computerprogrammschutz nach §§ 69a UrhG als auch unter den sonstigen Werkschutz nach §§ 2 ff. UrhG fallen. Es wird sich zeigen, dass der urheberrechtliche Schutz nur bedingt bzw. nur für Einzelteile der betrachteten Technologien tauglich ist.

A. Grundlagen des Urheberrechts

I. Voraussetzungen des urheberrechtlichen Schutzes nach UrhG¹

Das Urheberrechtsgesetz schützt gemäß § 1 UrhG Werke der Literatur, Wissenschaft und Kunst. Ein Werk ist eine persönliche geistige Schöpfung, welche eigentümlich sein muss. Ein Werk genießt urheberrechtlichen Schutz, wenn es (i) dem Bereich der Literatur, Wissenschaft und Kunst zugehört, (ii) das Ergebnis persönlichen Schöpfens ist, (iii) einen geistigen Gehalt zum Ausdruck bringt, (iv) in eine konkrete, sinnlich wahrnehmbare Form überführt wurde und (v) individuell ist.²

¹ Die Darlegung der allgemeinen urheberrechtlichen Schutzvoraussetzungen orientieren sich an den Ausführungen im Lehrbuch SCHACK.

² Statt vieler: SCHACK, Rn. 184 ff.

Die Voraussetzung der persönlichen Schöpfung soll sicherstellen, dass das Werk Ergebnis einer menschlich-gestalterischen Leistung ist.³ Somit ist auch das Urheberrecht von einem anthropozentrischen Gedanken geprägt. Werke, die ausschließlich mithilfe von Maschinen oder Apparaten hergestellt wurden – wie bspw. Übersetzungen mittels Übersetzungscomputers – sind grundsätzlich nicht vom Schutz erfasst.⁴ Durch das Erfordernis der geistigen Schöpfung soll sich der menschliche Geist im Werk konkretisieren und zum Ausdruck kommen. Darin liegt auch die immaterielle Natur des Urheberrechts. Die Formung der geistigen Idee ist der immaterielle Aspekt des Urheberrechts.⁵

Individualität liegt vor, wenn der Urheber die schöpferischen Fähigkeiten in eigenständiger Weise zum Ausdruck bringt. Es muss also Formgebung vorliegen, die aber nicht vollendet sein muss – auch der Entwurf oder Skizzen können Werke im urheberrechtlichen Sinne sein. Das Erfordernis der Formgebung schließt Ideen, Erkenntnisse und Informationen als solche vom Schutz aus.⁶ Es ist somit die konkrete Ausdrucksform geschützt und nicht der Inhalt.⁷ Nur das konkrete, individuell gestaltete Werk kann urheberrechtlich geschützt sein.⁸ Damit sind unter anderem Methoden und Konzepte nicht schutzfähig. Individualität schließt nicht nur alle geistigen Schöpfungen aus, die lediglich banal und alltäglich sind. Das Erfordernis, dass die Schöpfung in eigenständiger Art und Weise zu erfolgen hat, schließt auch alle Schaffensergebnisse aus, die lediglich auf handwerklicher Leistung oder auf Routine fußen – auch bei Achtung und Befolgung sämtlichen fachmännischen Wissens.⁹ Allerdings sind keine hohen Forderungen an die Schöpfung zu stellen, solange Individualität gegeben ist und

³ SCHACK, Rn. 189.

⁴ SCHACK, Rn. 189.

⁵ SCHACK, Rn. 199 f.

⁶ SCHACK, Rn. 199.

⁷ Es ist aber nicht auf eine Fixierung des Werkes abzustellen. So kann der Inhalt eben die Individualität begründen, was bspw. bei Fabelerzählungen besonders einleuchtend ist. Eine solche Fabelerzählung ist dennoch ein urheberrechtlich geschütztes Werk. Vereinfacht gesagt ist die impressionistische Darstellung eines Bergzuges geschützt, nicht aber impressionistische Darstellungen des Bergzuges generell oder etwa gar der Bergzug an und für sich; siehe dazu genauer SCHACK, Rn. 192 f.

⁸ SCHACK, Rn. 199.

⁹ SCHACK, Rn. 198.

damit ein gewisser schöpferischer Gestaltungsraum genutzt wurde.¹⁰ Auch die sogenannte kleine Münze ist geschützt. Bei Werken, die der kleinen Münzen zuzuordnen sind, ist der Individualitätsgrad besonders tief. Als Beispiele gelten Kataloge, Adressbücher und Formulare. Die notwendige Gestaltungshöhe erfordert kein Schaffen bestimmter Qualität, sondern gibt lediglich ein Maß an Individualität des Werkes wieder. Das Maß an Individualität ist zugleich auch maßgeblich für den Schutzzumfang, denn nur soweit die individuelle Prägung reicht, rechtfertigt sich auch die ausschließliche Rechtszuweisung an den Urheber. Individualität bedeutet auch nicht Einmaligkeit oder Neuheit.¹¹

Das Urheberrecht ist kein Registerrecht. Zur Entstehung des immaterialgüterrechtlichen Schutzes bedarf es somit nicht einer Anmeldung zur Aufnahme in ein Register, sondern sobald das Werk im Sinne des Urheberrechts geschöpft ist, entsteht auch die Berechtigung.¹² Dies macht es erforderlich, dass das Werk über eine sinnlich wahrnehmbare Form verfügt.¹³ Der Schutz beginnt, sobald das Werk erkennbar ist. Somit sind bereits Entwürfe geschützt, sofern sie eine persönliche geistige Schöpfung darstellen. Die sinnliche Wahrnehmbarkeit kann auch mittels technischer Hilfsmittel erfolgen.¹⁴

Gemäß § 3 S. 1 UrhG kann auch die Bearbeitung eines urheberrechtlich geschützten Werkes urheberrechtlichen Schutz erlangen, sofern der Bearbeitungsakt die Voraussetzungen einer persönlichen geistigen Schöpfung erfüllt.

Im Urheberrecht gilt das Schutzlandprinzip. Das heißt, dass das Urheberrecht mit dem Schöpfungsakt weltweit bei der schöpfenden Person entsteht, die zwingend eine natürliche Person sein muss. Es ist also nicht wie beim Patentrecht für jedes Land eine Registeranmeldung erforderlich, für welches der Schutz gelten soll. Allerdings ist der jeweilige Schutz auf das jeweilige Staatsgebiet begrenzt

¹⁰ SCHACK, Rn. 197.

¹¹ SCHACK, Rn. 194 ff.

¹² SCHACK, Rn. 261.

¹³ SCHACK, Rn. 192.

¹⁴ So reicht bei einem mittels Textverarbeitungsprogramms verfassten Literaturwerk die Wiedergabe auf einem Bildschirm, bei einem digitalen Foto die Speicherung auf dem Chip der Kamera, vgl. dazu weiter m.w.N. Schricker/Loewenheim/LOEWENHEIM/LEISTNER, UrhG, § 2 Rn. 48.

(Territorialitätsprinzip). Somit erhält der Urheber mit Schöpfung ein Bündel an Rechten des jeweiligen Staates.¹⁵ Zur Angleichung der Schutzniveaus im internationalen Verhältnis existieren darüber hinaus Staatsverträge wie bspw. die revidierte Berner Übereinkunft oder das TRIPS-Abkommen.

II. Inhalt des Urheberrechts

Gemäß § 11 UrhG schützt das Urheberrecht den Urheber in seinen geistigen und persönlichen Beziehungen zum Werk und der Nutzung des Werkes. Das Urheberrecht lässt sich somit in die Urheberpersönlichkeits- und die Verwertungsrechte unterteilen.

1. Urheberpersönlichkeitsrechte

Die Urheberpersönlichkeitsrechte umfassen unter anderem das Veröffentlichungsrecht nach § 12 UrhG, die Anerkennung der Urheberschaft gemäß § 13 UrhG sowie den Schutz vor der Entstellung des Werks in § 14 UrhG. Die Urheberpersönlichkeitsrechte zeichnen sich durch ein Band zwischen der Persönlichkeit des Urhebers und dem Werk aus.¹⁶ Während die vorgenannten Rechte auch Urheberpersönlichkeitsrechte im engeren Sinne genannt werden, dürften auch den weiteren Urheberrechten persönlichkeitsrechtlicher Charakter zukommen. Dabei ist etwa an die Unübertragbarkeit des Urheberrechts als solches gemäß § 29 UrhG oder das Änderungsverbot in § 62 UrhG zu denken. Das Veröffentlichungsrecht schreibt dem Urheber das Recht zu, darüber zu entscheiden, ob und wie sein Werk zu veröffentlichen ist. Voraussetzung dabei ist, dass das Recht noch nicht veröffentlicht ist. Genauer wäre somit „Erstveröffentlichungsrecht“, welches sich mit erster mit des Urhebers Zustimmung erfolgter Veröffentlichung erschöpft.¹⁷ Das Recht auf Anerkennung der Urheberschaft gewährt dem Urheber das Recht zu bestimmen, ob das Werk mit einer Urheberbezeichnung zu versehen und welche Bezeichnung zu verwenden ist.¹⁸ Dies ist aufgrund der gesetzlichen Vermutung in § 10 UrhG von Relevanz. § 14 UrhG

¹⁵ SCHACK, Rn. 1152 ff.

¹⁶ SCHACK, Rn. 368.

¹⁷ SCHACK, Rn. 378 ff.

¹⁸ SCHACK, Rn. 385 ff.

gewährt dem Urheber das Recht, jegliche Entstellung oder andere Beeinträchtigung des Werkes zu verbieten, sofern damit seine berechtigten geistigen oder persönlichen Interessen am Werk gefährdet werden könnten.¹⁹

2. Verwertungsrechte

Die Verwertungsrechte sollen dem Urheber den wirtschaftlichen Nutzen zuschreiben. Es soll sichergestellt werden, dass die Früchte geistigen Schaffens dem Urheber zustehen. Die Verwertungsrechte knüpfen anders als bspw. das Patentrecht nicht an die Benutzung, Anwendung oder Gebrauch des Schutzguts an, sondern an die möglichen Formen der Mitteilung des Werkes an die menschlichen Sinne. Das Gesetz geht in § 15 Abs. 1 UrhG von einem allgemeinen körperlichen Verwertungsrecht aus, und nennt namentlich das Vervielfältigungs-, Verbreitungs- und Ausstellungsrecht sowie das Wiedergaberecht.²⁰ In § 15 Abs. 2 sind die unkörperlichen Verwertungsrechte wie das Vortrags-, Aufführungs- und Vorführungsrecht, das Senderecht, etc. aufgezählt.²¹ Die gesetzliche Aufzählung der Verwertungsrechte ist nicht abschließend – es sollen auch solche Verwertungshandlungen abgedeckt sein und dem Urheber zustehen, welche sich erst noch ergeben werden.²²

3. Schranken, Nutzungsrechte und Dauer

Die Schranken in §§ 44a ff. UrhG beschneiden die Rechte des Urhebers. Sie relativieren mit anderen Worten die urheberrechtliche Monopolstellung. Aus der Sicht der Nutzer:innen kann also in Bezug auf die Schrankenregelungen von Befugnissen oder Nutzungsrechten gesprochen werden. Mit den Schrankenregelungen soll ein fairer Ausgleich zwischen den Urheberinteressen und der Interessen der Allgemeinheit betreffend die Werknutzung geschaffen werden.²³

Unter dem Titel der Schranken existieren zum einen die zustimmungsfreien, aber vergütungspflichtigen (sog. gesetzliche Lizenz²⁴) sowie die zustimmungs-

¹⁹ SCHACK, Rn. 395 ff.

²⁰ SCHACK, Rn. 434 ff.

²¹ SCHACK, Rn. 461 ff.

²² SCHACK, Rn. 428.

²³ SCHACK, Rn. 539 ff.

²⁴ SCHACK, Rn. 508 ff.

und vergütungsfreien (sog. Freistellung²⁵) Nutzungen.²⁶ Im Zusammenhang mit digitalen Systemen nennenswerte Schranken sind mitunter die Freistellung in Form der vorübergehenden Vervielfältigungshandlungen in § 44a UrhG, die Zitierfreiheit in § 51 UrhG sowie die Privatkopieschranke in § 53 UrhG und die erlaubten Nutzungen für Unterricht, Wissenschaft und Institutionen in den §§ 60a ff. UrhG. Die Privatkopieschranke erlaubt die Herstellung von Vervielfältigungsstücken (Kopien) von geschützten Werken zum privaten Gebrauch. Dabei kann die Privatperson auch eine:n Dritte:n mit der Vervielfältigungshandlung beauftragen.²⁷ Die Privatkopieschranke ist gemäß § 53 Abs. 5 UrhG bei Datenbankwerken nicht anwendbar. Nach § 87c Abs. 1 Nr. 1 UrhG gilt im Rahmen des Leistungsschutzrechts des Datenbankherstellers die Privatkopieschranke nicht bei elektronischen Datenbanken, deren einzelne Elemente elektronisch zugänglich sind.²⁸

Besonders hervorzuheben ist die Schranke zum Text und Data Mining in § 44b UrhG sowie § 60d UrhG. Wie oben unter Kap. 1, B., I. erläutert, ist das Text und Data Mining im Entwicklungsprozess von KI-Technologien enorm wichtig. Anhand der via Text and Data Mining erlangten und aufbereiteten Text – und Datenmengen erfolgt das Training zahlreicher Technologien. Die Schranke nach § 44b gilt auch außerhalb der wissenschaftlichen Forschungszwecke. Sie erlaubt das Text and Data Mining, sofern (i) die vervielfältigende Person rechtmäßigen Zugang zu den Daten hat und (ii) sofern und solange der Rechteinhaber keinen Nutzungsvorbehalt äußerte. Nach § 66d UrhG ist es zu nicht kommerziellen wissenschaftlichen Forschungszwecken erlaubt, Werke im Rahmen des Text and Data Minings (teilweise) zu vervielfältigen, zu verbreiten und öffentlich zugänglich zu machen.

Nach § 64 UrhG läuft der urheberrechtliche Schutz grundsätzlich 70 Jahre nach dem Tod des Urhebers ab. Ausnahmen gelten diesbezüglich für Leistungsschutzrechte, die kürzere Schutzdauern aufweisen.²⁹

²⁵ Zum Beispiel SCHACK, Rn. 596 ff.

²⁶ Siehe zu den Schranken ausführlich SCHACK, Rn. 557 ff.

²⁷ SCHACK, Rn. 596 ff., insb. Rn. 598.

²⁸ Allerdings gilt die Schranke wiederum zu Zwecken der wissenschaftlichen Forschung sowie zu Zwecken der Lehr- und Unterrichtsveranschaulichung.

²⁹ SCHACK, Rn. 542 ff.

III. Voraussetzungen für den Computerprogrammschutz insbesondere

Da KI-Technologien auf informationstechnischer Grundlage erschaffen sind, muss der urhebergesetzlich speziell verankerte Computerprogrammschutz näher betrachtet werden.³⁰ Computerprogramme sind in § 2 Abs. 1 Nr. 1 UrhG als Sprachwerke aufgeführt.

1. Schutz als Computerprogramm gemäß §§ 69a ff. UrhG

Gemäß § 69a Abs. 1 UrhG gilt der Schutz für Computerprogramme einschließlich ihres Entwurfsmaterials. § 69a Abs. 2 UrhG konkretisiert sodann, dass der gewährte Schutz für alle Ausdrucksformen des Computerprogramms gilt, während die Ideen und Grundsätze, die einem Element oder den Schnittstellen eines Computerprogramms zugrunde liegen, nicht vom Schutz erfasst sind. § 96a Abs. 3 UrhG präzisiert, dass auch Computerprogramme ein individuelles Werk im Sinne einer eigenen geistigen Schöpfung des Urhebers darstellen müssen. Qualitative oder ästhetische Kriterien sind nicht anzuwenden.³¹ Das Erfordernis einer geistigen Schöpfung stellt klar, dass auch betreffend Computerprogramme der menschliche Geist zum Ausdruck kommen muss.³² Auch bei Computerprogrammen ist bereits die kleine Münze geschützt – es bedarf keiner statistischen Einmaligkeit.³³ Damit ist die Schutzunfähigkeit Ausnahme.³⁴ Das Entwurfsmaterial sowie die Vorstufen müssen für sich bereits die notwendige Individualität aufweisen.³⁵

Als Rechtfertigungsgrund für den urheberrechtlichen Schutz von Computerprogrammen erachtete die WIPO, dass „die schöpferische Geistestätigkeit bei der Schaffung von Computersoftware [...] zumeist in dem Geschick und der Anstrengung [liegt], die darauf verwendet werden, diese Ideen einem Computer so wirtschaftlich und effizient wie möglich „verständlich“ zu machen.“³⁶ Mit anderen Worten soll eine Übersetzungsleistung belohnt werden.³⁷

³⁰ Vgl. auch LINKE, S. 133 f.

³¹ Dreier/Schulze/DREIER, UrhG, § 69a Rn. 28.

³² Dreier/Schulze/DREIER, UrhG, § 69a Rn. 25, SCHACK, Rn. 214.

³³ Dreier/Schulze/DREIER, UrhG, § 69a Rn. 25 f.

³⁴ Dreier/Schulze/DREIER, UrhG, § 69a Rn. 26.

³⁵ Dreier/Schulze/DREIER, UrhG, § 69a Rn. 27.

³⁶ WIPO GRUR Int 1978, 287 f.

³⁷ WIPO GRUR Int 1978, 287 f.

Eine Definition des Computerprogrammbegriffs findet sich nicht im Gesetz. Die Mustervorschriften der WIPO definieren ein Computerprogramm als „eine Folge von Befehlen, die nach Aufnahme in einen maschinenlesbaren Träger fähig sind zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt.“³⁸ Der BGH geht mit seinem Begriffsverständnis in dieselbe Richtung und definiert ein Computerprogramm auch „als eine Folge von Befehlen [...], die nach Aufnahme in einen maschinenlesbaren Träger fähig sind zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt“.³⁹ Auch der EuGH verlangt hinsichtlich des Computerprogrammbegriffs in der Computerprogrammrichtlinie, dass das Programm einen Computer zur Ausführung einer Funktion veranlassen kann.⁴⁰ Der Begriff ist weit zu verstehen.⁴¹ So ist sowohl der Quell- als auch der Objektcode geschützt.⁴² Die Programmiersprache ist unerheblich. Sofern einzelne Programmteile die Schutzvoraussetzungen erfüllen, sind sie auch vom Schutz erfasst.⁴³ Bloße Datensammlungen, die keine Steuerungsanweisungen an einen Computer enthalten, erfüllen den Computerprogrammbegriff nicht, sondern können als Datenbankwerke geschützt sein oder werden vom Datenbankherstellerschutz erfasst.⁴⁴

Schließlich ist wesentlich, zu verstehen, dass der urheberrechtliche Computerprogrammschutz nur die konkrete Ausdrucksform eines Computerprogrammes schützt. Die Funktionalität des Programmes ist nicht vom urheberrechtlichen Computerprogrammschutz erfasst⁴⁵ – dies im Gegensatz zum Patentrecht.⁴⁶

³⁸ WIPO GRUR Int 1978, 290.

³⁹ BGH GRUR 1985, 1047 – Inkasso-Programm.

⁴⁰ EuGH GRUR 2011, 222 – BSA.

⁴¹ Siehe LINKE, S. 138 ff. für eine ausführliche historische Herleitung.

⁴² Statt vieler: Dreier/Schulze/DREIER, UrhG, § 69a Rn. 12.

⁴³ Dreier/Schulze/DREIER, UrhG, § 69a Rn. 19 ff.

⁴⁴ Dreier/Schulze/DREIER, UrhG, § 69a Rn. 12.

⁴⁵ Dreier/Schulze/DREIER, UrhG, § 69a Rn. 2; SCHACK, Rn. 215.

⁴⁶ Siehe oben Kap. 7, A., I. ff., Kap. 7, A., III. ff.

Zusammenfassend kann also festgehalten werden, dass ein Computerprogramm im urheberrechtlichen Sinne zwei Merkmale aufweisen muss: Einerseits muss es über ein Steuerungselement verfügen. Andererseits muss die Steuerung dazu führen, dass der Computer eine bestimmte Funktion ausführt. Mithin wird ein Funktionselement verlangt.⁴⁷ Die Funktion muss bestimmt sein. Mit anderen Worten: das Computerprogramm muss determiniert sein. Ein Computerprogramm ist dann determiniert, wenn es bei der gleichen Eingabe stets die gleiche Ausgabe generiert.⁴⁸ Das Erfüllen der Merkmale eines Computerprogrammes verleiht der Softwareebene nicht automatisch urheberrechtlichen Schutz. Das Computerprogramm muss darüber hinaus Ergebnis einer geistigen Schöpfung sein.⁴⁹

2. Schutz als sonstiges Werk nach § 2 UrhG

Erfüllt eine Softwareebene nicht die Voraussetzungen an ein Computerprogramm, ist es zwar nicht als Computerprogramm nach §§ 69a UrhG geschützt. Es kann allerdings als sonstiges Werk nach § 2 UrhG geschützt sein, sofern es Werkcharakter besitzt und Ergebnis einer geistigen Schöpfung ist.⁵⁰

Werkcharakter besitzt die Softwareebene dann, wenn sie eine für den Menschen sinnlich wahrnehmbare Ausdrucksform aufweist und in dieser ein geistiger Gehalt zum Ausdruck kommt.⁵¹ Der urheberrechtliche Schutz knüpft also an ein Kommunikationselement an.⁵² Das zeigt sich besonders an der Werkkategorie von Sprachwerken, in die Softwareebenen regelmäßig fallen dürften.⁵³ Sprachwerke transportieren einen geistigen Inhalt.⁵⁴ Die Sprache ist demnach Träger dieses Kommunikationselementes. Das Urheberrecht setzt damit eine „Aussage

⁴⁷ So auch LINKE, S. 145 f.

⁴⁸ Siehe bereits oben Kap. 2, C., II., 4.

⁴⁹ Siehe oben Kap. 8, A., I.

⁵⁰ Siehe oben Kap. 8, A., I. f.; sofern es aber bereits urheberrechtlichen Computerprogrammenschutz genießt, geht dieser Computerprogrammenschutz als *lex specialis* dem sonstigen Werkchutz vor. Vgl. dazu Schrickler/Loewenheim/SPINDLER, UrhG, Vorb. Zu §§ 69a-69g UrhG Rn. 7. Ein Schutz als sonstiges Werk kommt in einem solchen Fall nicht infrage.

⁵¹ Siehe oben Kap. 8, A., I.

⁵² BECKER, S. 210 ff., insb. S. 212 ff. und S. 216 f.; Schrickler/Loewenheim/LOEWENHEIM/LEISTNER, UrhG, § 2 Rn. 45.

⁵³ Neben oder anstelle derjenigen von Computerprogrammen.

⁵⁴ BECKER, S. 217 ff.; siehe auch SCHACK, Rn. 207.

oder Botschaft“⁵⁵ voraus, die vom Werk transportiert und vom Menschen wahrgenommen⁵⁶ sowie verstanden werden kann.⁵⁷ Bedarf es zum Verständnis oder zur Verwendung dieses Gedankens besonderer Fähigkeiten, die außerhalb des Werkes liegen, so ist das Werk trotzdem schutzfähig. Entscheidend ist, dass ein Mensch mit entsprechenden Fähigkeiten das Kommunikationselement wahrnehmen und verstehen kann.⁵⁸

Softwareebenen können also auch außerhalb des Computerprogrammsschutzes nach §§ 69a UrhG urheberrechtlichen Schutz genießen, wenn sie die allgemeinen Werkvoraussetzungen nach § 2 UrhG erfüllen und dabei insbesondere über ein sinnlich wahrnehmbares Kommunikationselement verfügen. Die §§ 69a ff. UrhG gehen als *leges speciales* § 2 UrhG vor

IV. Leistungsschutzrechte

Leistungsschutzrechte werden auch verwandte Schutzrechte genannt und sind in Teil 2 des UrhG (§ 70 – 87h UrhG) geregelt. Es handelt sich um verschiedene Rechte, die bestimmte Leistungen schützen sollen, die zwar keine urheberrechtliche Schöpfung im Sinne des urheberrechtlichen Werkbegriffs darstellen, aber einer solchen Schöpfung ähnlich sind oder im Zusammenhang mit einer Werkschöpfung entstehen.⁵⁹ Der gesetzliche Katalog an Leistungsschutzrechten ist abschließend.⁶⁰ Leistungsschutzrechte gewähren der rechtsinhabenden Person ausschließliche Verwertungsrechte, die teilweise durch gesetzliche Vergütungsansprüche ergänzt werden. Der Lichtbildschutz, der Schutz der ausübenden Künstler, der Schutz des Tonträgerherstellers oder der Schutz der Datenbankhersteller zählen unter anderem zu den Leistungsschutzrechten.

⁵⁵ Schrickler/Loewenheim/LOEWENHEIM/LEISTNER, UrhG, § 2 Rn. 45.

⁵⁶ BECKER, S. 217 ff. spricht von „Qualia“ als Abgrenzungskriterium; Schrickler/Loewenheim/LOEWENHEIM/LEISTNER, UrhG, § 2 Rn. 45; Nordemann § 2 Rn 25; Dreier/Schulze/SCHULZE, UrhG, § 2 Rn. 12 spricht davon, dass ein Werk auf die betrachtende Person „unterhaltend, belehrend, veranschaulichend, erbauend oder sonstwie anregend“ wirken muss.

⁵⁷ REHBINDER/PEUKERT, 18. Auflage, Rn. 189.

⁵⁸ Siehe REHBINDER/PEUKERT, 18. Auflage, Rn. 189.

⁵⁹ SCHACK, Rn. 722 ff.

⁶⁰ PEUKERT, §32 Rn. 1.

Das Leistungsschutzrecht des Datenbankherstellers ist in § 87a ff. UrhG geregelt und ist vom Schutz des Urhebers eines Datenbankwerks zu unterscheiden. Das Datenbankwerk nach § 4 Abs. 2 UrhG ist ein Werk im urheberrechtlichen Sinne und genießt somit urheberrechtlichen Schutz. Schutzgegenstand beim Datenbankwerk ist die Struktur der Datenbank, nicht aber deren Inhalt. Schutzgegenstand von § 87a UrhG ist eine „Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert.“ Es sind nicht die einzelnen in die Datenbank aufgenommenen Informationen geschützt, sondern nur die unter wesentlichem Investitionsaufwand erstellte Datenbank als Ganzes bzw. ein wesentlicher Teil davon.⁶¹ Mit anderen Worten ist also „die in der Datenbank verkörperte wesentliche Investition bei der Beschaffung, Überprüfung oder Darstellung der Daten“⁶² der Schutzgegenstand der §§ 87a ff. UrhG. Berechtigte Person ist der Datenbankhersteller. Als Datenbankhersteller gilt diejenige Person, die die Investitionen tätigte.⁶³ Die Investition muss nicht finanzieller Art sein. Auch Investitionen in Form von Zeit, Arbeit oder Energie sind vom Datenbankherstellerrecht umfasst.⁶⁴ Die Schutzdauer beträgt gemäß § 87d UrhG 15 Jahre ab Herstellung der Datenbank.

B. Prüfung der urheberrechtlichen Schutzfähigkeit von KI-Technologien

Primär kommt für KI-Technologien bei der Prüfung der urheberrechtlichen Schutzfähigkeit der Computerprogrammenschutz in Frage. Wie gesehen, verlangt der Computerprogrammbegriff der WIPO, des BGH wie auch des EuGH neben dem Steuerungselement von Befehlen die Erfüllung einer bestimmten Funktion bzw. Aufgabe oder das Erreichen eines bestimmten Ergebnisses. Sind diese Voraussetzungen erfüllt, liegt ein Computerprogramm im urheberrechtli-

⁶¹ SCHACK, Rn. 820.

⁶² SCHACK, Rn. 820.

⁶³ SCHACK, Rn. 822.

⁶⁴ Dreier/Schulze/DREIER, UrhG, § 87a Rn. 12.

chen Sinne vor. Damit das Computerprogramm aber darüber hinaus auch urheberrechtlich geschützt ist, muss es Ergebnis einer menschlich-geistigen Schöpfung sein.

Daneben ist für KI-Technologien auch der (sonstige) Werkschutz als solcher zu untersuchen – außerhalb des Computerprogrammschutzes, wo dieser nicht greift.⁶⁵ Entscheidend ist hier neben dem Schöpfungserfordernis auch das oben erwähnte Kommunikationselement.⁶⁶

Bei der Betrachtung der urheberrechtlichen Schutzfähigkeit von KI-Technologien eröffnen sowohl die Begriffsdefinition des Computerprogrammes als auch das Erfordernis der menschlich-geistigen Schöpfung und das Kommunikationselement diverse Problemfelder. Die Probleme ergeben sich sowohl bei untrainierten wie auch bei trainierten Technologien.

Anders als im Patentrecht, wo die bestimmte Funktion der Technologie im Sinne einer konkreten Lösung für ein technisches Problem entscheidend ist, kann im Urheberrecht die bestimmte Funktionsweise für eine Schutzfähigkeit entscheidend sein, während die Funktionalität als solche schutzfrei bleibt.⁶⁷ Wie gesehen, unterscheiden sich diese Funktionsweisen von KI-Technologie zu KI-Technologie – teilweise grundlegend. Daher werden im Nachgang Expertensysteme, genetische Programme und KNN getrennt voneinander betrachtet.

I. Expertensysteme

Betreffend die urheberrechtliche Schutzfähigkeit von Expertensystemen ist sich die Lehre soweit ersichtlich einig. Bei der Betrachtung sind Wissensbasis und Inferenzebene mit Dialogkomponente zu trennen.⁶⁸

⁶⁵ Siehe oben Kap. 8, A., III., 2. ff.

⁶⁶ Siehe soeben Kap. 8, A., III., 2.

⁶⁷ Siehe dazu oben Kap. 8, A., III., 2.

⁶⁸ Unter Kap. 2, C., I. wurde aufgezeigt, dass diese strikte Trennung auch auf technischer Ebene Expertensysteme von gewöhnlichen Programmen unterscheidet.

Die Wissensbasis ist auch technisch von der Inferenzebene getrennt.⁶⁹ Es handelt sich bei ihr um eine Sammlung verschiedener, meist voneinander unabhängigen Daten.⁷⁰ Allerdings wurde unter Kap. 2, C., I. gezeigt, dass die Wissensbasis über eine gewisse Steuerungsfähigkeit verfügt. Diese soll aber lediglich die Interoperabilität innerhalb der Wissensbasis und im Verhältnis Wissensbasis-Inferenzmaschine sicherstellen bzw. dafür sorgen, dass Hardwarekomponenten die Daten abrufen und mit den Regeln in der Inferenzmaschine verbinden können, um das Wissen abzuleiten. Sie richten insofern keine Steuerungsanweisungen an einen Computer, der sodann gestützt auf diese Anweisung eine bestimmte Funktion ausführt. So gesehen ist die Stoßrichtung der Wissensbasis eine andere: Die Steuerungsanweisungen stellen lediglich die Verbindung zwischen Inferenzmaschine und Wissensbasis dar. Deshalb besteht soweit ersichtlich in der Lehre auch Einigkeit, dass die Wissensbasis kein Computerprogramm im urheberrechtlichen Sinne darstellt.⁷¹

Dies bedeutet aber nicht, dass die Wissensbasis gänzlich schutzlos bleibt. Betreffend die Wissensbasis kommt für den Hersteller das Leistungsschutzrecht des Datenbankherstellers von § 87a ff.⁷² UrhG in Betracht. Ebenso kann die Datenbasis als Datenbankwerk nach § 4 Abs. 2 UrhG geschützt sein.⁷³ Das Wesen der Wissensbasis besteht regelmäßig gerade darin, dass sie eine Ansammlung verschiedener, voneinander unabhängiger Daten ist.⁷⁴ Dieses Wesensmerkmal entspricht der urheberrechtlichen Datenbankdefinition.⁷⁵

Bei der Inferenzmaschine (mit Dialogkomponente) hingegen handelt es sich um ein Computerprogramm im „gewöhnlichen“ Sinne, weshalb sie vom urheberrechtlichen Computerprogrammenschutz erfasst ist. Die Inferenzmaschine enthält nämlich die Regeln, nach welchen auf die Wissensbasis zugegriffen werden

⁶⁹ Siehe oben Kap. 2, C., I.

⁷⁰ Siehe oben Kap. 2, C., I. ff.

⁷¹ Siehe dazu Dreier/Schulze/DREIER, UrhG, § 69a Rn. 12; Wandtke/Bullinger/GRÜTZMACHER, UrhG, § 69a Rn. 21; LINKE, S. 163 f., jeweils m.w.N.

⁷² So auch LINKE, S. 163 f.

⁷³ So auch LINKE, S. 163 f.

⁷⁴ Siehe oben Kap. 2, C., I. ff.

⁷⁵ Siehe oben Kap. 8, A., IV.

soll, während die Dialogkomponente dem Benutzer ermöglicht, mit dem System zu interagieren.⁷⁶ Es ist sowohl in Lehre wie auch Rechtsprechung umstritten, ob die bloße Benutzeroberfläche ebenfalls vom urheberrechtlichen Schutz erfasst ist bzw. ein Computerprogramm im rechtlichen Sinne darstellt. Die herrschende Lehre verneint dies.⁷⁷ Offen bleibt der Schutz der Benutzeroberfläche als sonstiges Werk nach § 2 UrhG. Die Benutzeroberfläche kann als kreative Gestaltung durchaus Schutz nach § 2 UrhG erlangen, sofern sie von einem Menschen gestaltet wurde. Die Darstellung einer Benutzeroberfläche könnte bspw. unter § 2 Abs. 1 Nr. 7 UrhG fallen oder als Werk der bildenden Kunst nach § 2 Abs. 2 Nr. 4 UrhG. Es bleibt jedoch zu bedenken, dass dann jeweils nur die entsprechende Ausdrucksform geschützt ist und nicht etwa die Funktionsweise hinter der Benutzeroberfläche.

II. Genetische Programme

Die urheberrechtliche Diskussion betreffend die Schutzfähigkeit von genetischen Programmen ist noch nicht weit fortgeschritten. Dies zeigt sich bereits anhand der geringen Literatur zum Thema. Darüber hinaus hat die Diskussion noch nicht genügend an Tiefe gewonnen. Dies zeigt sich an den in der Diskussion verwendeten Begriffen „Builder-, Test-/Teacher- und Ziel-Algorithmus“ sowie daran, dass die Untersuchung des urheberrechtlichen Computerprogrammenschutzes am Beispiel der genetischen Algorithmen erfolgt.⁷⁸ Ergebnis bei der Entwicklung von genetischen Algorithmen ist aber wie aufgezeigt eine Quantität – in vielen Fällen eine reelle Zahl – und kein Computerprogramm.⁷⁹

Möchte man die Technologie untersuchen, die auch dazu in der Lage ist, (intelligente) digitale Systeme zu steuern, mithin der Untersuchungsgegenstand im Rahmen der vorliegenden Arbeit, muss man sich jedoch den genetisch entwickelten *Programmen* widmen – dem *genetic programming*. Ergebnis des *genetic*

⁷⁶ Statt vieler: Dreier/Schulze/DREIER, UrhG, § 69a Rn. 12; Wandtke/Bullinger/GRÜTZMACHER, UrhG, § 69a Rn. 21.

⁷⁷ Siehe zum Lehrstreit sowie zum Verweis auf herrschende Lehre bei Wandtke/Bullinger/GRÜTZMACHER, UrhG, § 69a Rn. 21.

⁷⁸ So bspw. Wandtke/Bullinger/GRÜTZMACHER, UrhG, § 69a Rn. 21; LINKE, S. 116, 158 ff.; PAPASTEFANOU, CR 2019, 209.

⁷⁹ Siehe oben Kap. 2, C., III., 2.

programmings ist keine Quantität, sondern eine Folge von Anweisungen an einen Computer.⁸⁰

Die Begrifflichkeiten „*Builder-, Test- und Ziel-Algorithmus*“ sind im Zusammenhang mit dem *genetic programming* zu verwerfen. Nicht zuletzt aufgrund der Unbestimmtheit des Algorithmusbegriffs.⁸¹ Beim *genetic programming* handelt es sich stark vereinfacht um eine herkömmlich programmierte Programmumgebung, die die einzelnen Individuen generiert.⁸² Der *Testalgorithmus* wird in der Informatik als Fitnessfunktion bezeichnet.⁸³ Mit der Bezeichnung als Fitnessfunktion geht dem *Testalgorithmus* auch einiges an Zauber verloren. Als Ergebnis steht beim *genetic programming* das Ziel-Programm.⁸⁴ Die Programmumgebung, die die Individuen generiert, die Fitnessfunktion und das Ziel-Programm sind sodann die urheberrechtlich zu untersuchenden Elemente des *genetic programmings*.

Alle diese drei Elemente sind in ihrer Struktur wenn-dann-Regelwerke, bei denen die Informationsverarbeitung explizit erfolgt.⁸⁵

1. Programmumgebung und Fitnessfunktion

Die Programmumgebung, die die Individuen generieren soll, weist eine Hardwarekomponente an, diese Individuen zu erstellen. Zuerst ohne weitere Angaben, danach einerseits entsprechend der mittels Fitnessfunktion berechneten Wahrscheinlichkeiten zur Selektion und andererseits anhand der Wahrscheinlichkeiten für Kreuzung und Mutation.⁸⁶ Sowohl das Steuerungs- als auch das Funktionserfordernis sind damit erfüllt. Wenn auch die ersten Individuen „zufällig“ aus dem *function-* und *terminal set* generiert wurden und noch nicht zur eigentlichen Problemlösung geeignet sind, so stellt das Generieren von Individuen anhand von bestimmten Vorgaben für sich betrachtet eine bestimmte, definierte Funktion dar, die von der Hardwarekomponente ausgeführt wird. Die

⁸⁰ Siehe oben Kap.2, C., III., 2.

⁸¹ Siehe dazu oben Kap. 1, E. f.

⁸² Siehe oben Kap. 2, C., III., 2.

⁸³ Siehe oben Kap. 2, C., III. 1.

⁸⁴ Siehe oben Kap. 2, C., III., 2, Kap. 2, C., III., 2.

⁸⁵ Vgl. bspw. oben Kap. 2, C., IV.; demnach unzutreffend LINKE, S. 119.

⁸⁶ Siehe oben Kap. 2, C., III., 2. ff.

Programmumgebung stellt damit ein Computerprogramm im urheberrechtlichen Sinne dar.⁸⁷

Die Fitnessfunktion enthält Regeln, anhand welcher die Individuen bewertet werden. Die Bewertung hat sodann Einfluss auf die Selektionswahrscheinlichkeit.⁸⁸ Diese Bewertung erfolgt mittels Vergleichs der Trainingsdaten mit der jeweiligen Ausgabe des Individuums. Mit anderen Worten enthält die Fitnessfunktion die Regeln, anhand welcher ein Computer die Selektionswahrscheinlichkeit eines Individuums berechnen soll. Mithin erfüllt auch die Fitnessfunktion die Voraussetzungen des Steuerungs- und Funktionselementes und stellt damit ein Computerprogramm im urheberrechtlichen Sinn dar.⁸⁹

Sowohl die Programmierumgebung als auch die Fitnessfunktion werden von Menschen programmiert. Damit ist auch das Erfordernis einer menschlich-geistigen Schöpfung erfüllt. Die Bereitstellung beider Elemente erfordert auch Kreativität. So ist es den Entwickler:innen überlassen, welche Funktionen und welche Variablen zur Generierung der Individuen im *function* und *terminal set* bereitgestellt werden oder wie die Fitnessfunktion hergeleitet wird. Besonders das Herleiten der Fitnessfunktion erfordert die Repräsentation des Problems in einer für einen Computer verständlichen Form. Eine Herausforderung, die das Programmieren aufgrund bloßer Funktionalitätsüberlegungen bei weitem übersteigen dürfte. Damit ist in aller Regel auch die erforderliche Schöpfungshöhe erreicht.

Sowohl die Programmierumgebung zur Generierung von Individuen als auch die in eine für einen Computer verständliche Sprache übersetzte Fitnessfunktion sind demnach einem urheberrechtlichen Computerprogrammenschutz zu-

⁸⁷ Im Ergebnis wohl gleich – wenn auch ungenau im Bereich der genetischen Algorithmen – LINKE, S. 160 f.; PAPAŞTEFANOU, CR 2019, 212; Wandtke/Bullinger/GRÜTZMACHER, UrhG, § 69a Rn. 21.

⁸⁸ Siehe oben Kap. 2, C., III., 1. und Kap. 2, C., III., 2. ff.

⁸⁹ Im Ergebnis wohl gleich – wenn auch ungenau im Bereich der genetischen Algorithmen – LINKE, S. 160 f.; PAPAŞTEFANOU, CR 2019, 212; Wandtke/Bullinger/GRÜTZMACHER, UrhG, § 69a Rn. 21.

gänglich. . Dieser Schutz bezieht sich jedoch nur auf die konkrete Ausdrucksform in Form des Programms, nicht auf die logischen Rechenregeln, die dahinterstehen.⁹⁰

2. „Ziel-Programm“

Das Ergebnis des *genetic programmings* – das Ziel-Programm – ist eine komplexe Abfolge von Befehlen an einen Computer.⁹¹ Das Ziel-Programm als KI-Technologie, implementiert in ein digitales System, versetzt das digitale System in die Lage, eine bestimmte Funktion zu erfüllen.⁹² Dies sind die typischen Eigenschaften eines Computerprogrammes im Sinne von §§ 69a ff. UrhG.⁹³

Anders verhält es sich mit dem Merkmal der menschlich-geistigen Schöpfung. Das Ziel-Programm ist gänzlich maschinengeneriert. Die Programmierumgebung zur Generierung der Individuen generiert im Zusammenspiel mit der Fitnessfunktion und den Trainingsdaten die Programme, aus denen schließlich das Ziel-Programm resultiert. Das Ziel-Programm entsteht – wie seine Vorgänger – durch einen künstlichen „Evolutionsprozess“, auf welchen der Mensch keinen direkten Einfluss hat. Der Mensch kann nur indirekt über die Trainingsdaten sowie die Festlegung des *function sets* und der Abbruchkriterien Einfluss auf Entwicklung der Individuen nehmen.

Zwar ist die Schaffung von Werken unter Zuhilfenahme von Maschinen und Zufallsmomenten nichts, was dem Urheberrecht unbekannt ist. Entscheidend für den Schutz solcher Werke ist aber, dass der Mensch die Zufallselemente festlegt und vor allem in einem zweiten Schritt eine Auswahl trifft.⁹⁴

⁹⁰ Vgl. oben Kap. 7, B., I.; auch LINKE, S. 158 ff.

⁹¹ Siehe oben Kap. 2, C., III., 2. ff.

⁹² Siehe oben Kap. 2, C., III., 2. ff.

⁹³ Vgl. dazu oben Kap. 8, A., III., 1. ff.

⁹⁴ Dreier/Schulze/SCHULZE, UrhG, § 2 Rn. 8; Schrickler/Loewenheim/LOEWENHEIM/LEISTNER, UrhG, § 2 Rn. 41; Wandtke/Bullinger/BULLINGER, UrhG, § 2 Rn. 17, jeweils m.w.N.

Beim *genetic programming* kann das (menschliche) Festlegen der Zufallselemente durch die Festlegung des *function* und *terminal sets* sowie der Bestimmung und Programmierung der Fitnessfunktion wohl bejaht werden.⁹⁵ Entscheidend ist aber, dass der Mensch beim *genetic programming* eben keine Auswahl trifft. Die Auswahl erfolgt gänzlich maschinengesteuert und ohne Einfluss durch einen Menschen. Der Entwicklungsprozess eines genetischen Programmes erinnert viel mehr an das Schaffen von Werken mittels KI-Technologien bzw. die damit zusammenhängende Diskussion.⁹⁶ Es herrscht mittlerweile wohl Konsens darüber, dass ein rein maschinengeneriertes Werk schutzfrei bleibt, weil es ihm an menschlichem Einfluss mangelt. Der menschliche Geist hat sich in diesem Fall nicht in der Werkformung manifestiert.⁹⁷ Ein mittels Maschine erzeugtes Werk weist erst dann genügend menschlichen schöpferischen Einfluss auf, wenn der menschliche Einfluss auch noch nach der Konzeptionierungsphase ersichtlich ist.⁹⁸

Doch beim *genetic programming* erschöpft sich der menschliche Einfluss in eben dieser Konzeptionierung: Es werden Funktionen und Variablen im *function* oder *terminal set* festgelegt, die Trainingsdaten werden aufbereitet und zur Verfügung gestellt und die Fitnessfunktion wird bestimmt. Welche Funktionen und Variablen schließlich den Weg in ein Individuum finden, liegt nicht im Einflussbereich des Menschen. Wie die Lösungswege weiterentwickelt bzw. kombiniert werden, liegt ebenfalls außerhalb menschlichen Einflusses.

Untechnisch gesprochen, bereitet der Mensch der Maschine lediglich eine Auswahl von Werkzeugen vor, anhand welcher die Maschine (autonom) eine Lösung entwickelt. Oftmals haben die Entwickler:innen beim *genetic program-*

⁹⁵ Sofern in der Informationstechnik überhaupt von Zufall gesprochen werden kann. In der Informationstechnik handelt es sich um sogenannte Pseudozufälle. Der Ausgang eines Ereignisses ist nicht gänzlich „dem Zufall überlassen“, denn der Algorithmus ist in jedem Falle noch determiniert. Allerdings genügt die Wahrscheinlichkeit der Algorithmusausgaben den Anforderungen an Zufall. (vgl. dazu ausführlicher KONERTZ/SCHÖNHOF, S. 54 f.)

⁹⁶ Vgl. ausführlich dazu bspw. GRÄTZ, *passim*; MAAMAR, *passim*; MUHR, *passim*.

⁹⁷ GRÄTZ, S. 116; MAAMAR, S. 164, S. 80 f.; MUHR, S. 50 ff., insb. S. 55 f.; siehe auch oben Kap. 8, A., I.

⁹⁸ Stellvertretend: GRÄTZ, S. 115 m.w.N.

ming auch gar keine Vorstellung davon, wie die Problemlösungsstrategie letztlich aussehen könnte.⁹⁹ Wie die Problemlösungsstrategie schließlich aussieht, wird in keiner Weise von menschlichem Einfluss bestimmt. Entscheidend ist viel eher das Feedback, was aufgrund der Fitnessfunktion unter Bezugnahme auf die Trainingsdaten errechnet wird.¹⁰⁰ Somit ist das Erfordernis der menschlich geistigen Schöpfung für das Ziel-Programm wie auch dessen Vorgänger abzulehnen. Damit ist das Ergebnis beim *genetic programming* nicht urheberrechtlich geschützt – ebenso wenig wie die einzelnen Individuen im Entwicklungsprozess.¹⁰¹

Aus dem gleichen Grund ist auch ein Schutz des Ziel-Programmes und dessen Vorgängers als andere Werkart nach § 2 UrhG ausgeschlossen. Wenn das Ziel-Programm niedergeschrieben wird, weist es zwar in aller Regel eine sinnlich wahrnehmbare Form auf. Da es sich bei den Individuen um – wenn auch sehr komplexe – wenn-dann-Regelwerke handelt, erschließen sie sich dem menschlichen Verstand. Sie verfügen also über das vorausgesetzte Kommunikationselement. Allerdings sind sie auch bei einer Niederschrift¹⁰² maschinengeneriert und nicht das Ergebnis menschlichen Schaffens.¹⁰³

3. Schutz der Trainingsergebnisse

Beim *genetic programming* sind die Trainingsergebnisse nicht vom Gesamtergebnis des Entwicklungsprogrammes – dem Ziel-Programm – zu trennen. Viel eher ist das Ziel-Programm das Trainingsergebnis und verkörpert den Trainingsvorgang, indem die Trainingsdaten zwecks *trial and error* – Verfahren herangezogen wurden und das Trainingsfeedback auch via Bewertungen von Individuen Eingang in die Weiterentwicklung dieser Individuen hatte.¹⁰⁴ Aus

⁹⁹ Siehe oben Kap. 2, C., IV.

¹⁰⁰ Siehe oben Kap. 2, C., IV.

¹⁰¹ Im Ergebnis wohl gleich – wenn auch ungenau im Bereich der genetischen Algorithmen – LINKE, S. 160 f.; PAPASTEFANO, CR 2019, 213; BOMHARD/GAJECK, RDi 2021, 475 f.

¹⁰² Oder bei jeder anderen sinnlich wahrnehmbaren Formgebung.

¹⁰³ Siehe soeben Kap. 8, B., II., 2. ff.

¹⁰⁴ Anders etwa bei KNN, wo sich die Gewichtungsinformationen als Trainingsergebnis separat abspeichern lassen.

diesem Grund entfällt auch eine urheberrechtliche Betrachtung der Trainingsergebnisse – sie sind nicht unabhängig, sondern vielmehr im Gesamttrainingsergebnis inkorporiert.¹⁰⁵

III. *Künstliche Neuronale Netze als Computerprogramme nach §§ 69a ff. UrbG*

Die Frage nach dem urheberrechtlichen Computerprogrammenschutz ist bei KNN umstritten. Dreh- und Angelpunkt sind einerseits die Auffassung der Computerprogrammdefinition und andererseits das Erfordernis der menschlich-geistigen Schöpfung. Wie sich zeigen wird, sind KNN nicht vom urheberrechtlichen Computerprogrammenschutz erfasst – aus verschiedenen Gründen. Um dies aufgrund der Programmstruktur und der Funktionsweise von KNN verständlich darzulegen, bietet es sich an, untrainierte von trainierten KNN getrennt zu betrachten. Die Schutzfähigkeit von KNN als sonstige Werke nach § 2 UrbG wird aufgrund des Umfangs und der getrennten Prüfung von untrainierten und trainierten KNN in einem eigenen Abschnitt geprüft.¹⁰⁶

1. *Untrainierte neuronale Netze*

Wie oben unter Kapitel 2, C., II., 1. beschrieben, sind untrainierte KNN eine Verbindung aus künstlichen Neuronen, die zu Schichten angeordnet sind und gemeinsam das gesamte Netz bilden. Untrainierte neuronale Netze richten Befehle an eine Hardwarekomponente,¹⁰⁷ womit sie das Steuerungserfordernis des Computerprogrammbegriffs erfüllen. Allerdings haben wir gesehen, dass untrainierte KNN nicht dazu in der Lage sind, brauchbare Ergebnisse zu generieren. Ohne Einstellung der Gewichte – zu Beginn des Trainings – produzieren untrainierte KNN lediglich ein sogenanntes Rauschen.¹⁰⁸ Die Ausgabe des Netzes ist dann bei einer entsprechenden Eingabe zufällig. Das Netz generiert „wahllos“ – bzw. zusammenhangslos – Ausgabe A, B oder C. Bei wiederholter gleicher Eingabe generiert das Netz sodann wiederum probabilistisch bzw. wahrscheinlichkeitsbasiert A, B oder C.¹⁰⁹ Das untrainierte Netz hat bis auf den

¹⁰⁵ Vgl. auch PAPAŞTEFANOU, CR 2019, 213.

¹⁰⁶ Siehe unten Kap. 8, B., IV.

¹⁰⁷ Siehe oben Kap. 2, C., II., 3.

¹⁰⁸ Siehe oben Kap. 2, C., II., 3.

¹⁰⁹ Siehe oben Kap. 2, C., II., 3. ff.

Ablauf des Programms keinen zuweisbaren Zweck. Es verfügt somit über keine sinnvolle Funktion. Es ist nicht determiniert.

Der Computerprogrammbegriff des BGH und der WIPO verlangt allerdings, dass die Funktion eines Computerprogramms abschließend definiert und mit einem klaren Sinngehalt versehen sein muss.¹¹⁰ Nach diesem Verständnis des Funktionsbegriffs, scheidet die Subsumtion von untrainierten KNN unter den Computerprogrammbegriff bereits an dieser Stelle.¹¹¹

HARTMANN/PRINZ kritisieren dieses Begriffsverständnis als zu veraltet und plädieren für eine neue, flexiblere Auffassung des Funktionsbegriffs.¹¹² Sie weisen darauf hin, dass sich KNN von der absoluten Beherrschbarkeit des Programmablaufs emanzipieren würden. Die WIPO-Richtlinie gehe aber von herkömmlichen Programmen mit beherrschbarem Programmablauf aus, welche stets nur vorgegebene Lösungswege abarbeiten würden. Wie aufgezeigt, arbeiten KNN aber komplett anders. Sie sind weder determiniert, noch lassen sich ihre Lösungswege in einem Flussdiagramm darstellen (fehlender Determinismus). Deshalb habe der Gedanke, der den KNN zugrunde liegt, nichts mehr mit dem Grund der WIPO zu tun, Computerprogrammen urheberrechtlichen Schutz zu gewähren. Nach HARTMANN/PRINZ reiche es aus, dass einem Computerprogramm die menschliche Idee zur Lösungsfindung „inkorporiert“ sei – auch wenn unklar sei, wie das Problem zu lösen sei. Sie vergleichen dies mit dem Fischen-Lehren, welches ebenso schützenswert sei, wie das Fischen selbst.¹¹³

Eine solche Auffassung ist aus mehreren Gründen abzulehnen. KNN können zweifelsohne dazu in der Lage sein, sehr komplexe Probleme zu lösen, die von herkömmlichen Computerprogrammen nicht bewältigt werden können. Nur bereits daher ist es nachvollziehbar, dieser Technologie Schutz gewähren zu wollen bzw. sie gleich zu behandeln wie herkömmliche Computerprogramme.¹¹⁴ Allerdings müssen die Begriffe des Computerprogramms im urheberrechtlichen Sinne und derjenige der geistigen Schöpfung auseinandergehalten werden. Erst

¹¹⁰ Siehe oben Kap. 8, A., III., 1. ff, insb. 0; vgl. HARTMANN/PRINZ, S. 778.

¹¹¹ A.A. wohl MUHR, S. 73 f.

¹¹² HARTMANN/PRINZ, S. 779 ff.

¹¹³ HARTMANN/PRINZ, S. 776 ff, insb. S. 781.

¹¹⁴ Vgl. zum Schutzbedürfnis ausführlich oben Kap. 6, E.

die geistige Schöpfung macht das Computerprogramm schütbar.¹¹⁵ Der Werkbegriff ist zwar bereits urheberrechtlich aufgeladen.¹¹⁶ Allerdings werden im Rahmen einer urheberrechtlichen Prüfung Überlegungen zur inkorporierten Idee bereits unter dem Titel der geistigen Schöpfung angestellt. Ansonsten wäre § 69a Abs. 3 UrhG überflüssig. Deshalb dürfen Überlegungen zur inkorporierten Idee nicht bereits zur Bejahung des Werkcharakters – in Form eines Computerprogrammes – herangezogen werden. Dies stellt eine (unzulässige) Doppelverwertung dar. So ist beispielsweise eine Melodie auch erst dann urheberrechtlich geschützt, wenn sie eine geistige Schöpfung ist. Die Melodie, die eine Katze beim Lauf über die Klaviertastatur erzeugt, ist keine menschlich-geistige Schöpfung und damit auch kein geschütztes Werk im Sinne des Urheberrechts. Dies ändert jedoch nichts daran, dass die Tonabfolge als solche eine Melodie ist. Es ist somit ein Zirkelschluss, die im KNN inkorporierte Idee als genügendes Funktionserfordernis zu betrachten und damit untrainierte KNN als Computerprogramm im urheberrechtlichen Sinne zu qualifizieren. Die Argumentationslinie von HARTMANN/PRINZ hat zur Folge, dass jede:r Künstler- bzw. Malermeister:in an den Werken und dem Werkschaffen der Schüler:innen urheberrechtlich berechtigt wäre. Das ginge zweifelsfrei zu weit.

Schließlich würde die Meinung von HARTMANN/PRINZ dazu führen, dass nicht mehr die konkrete Ausdrucksform des Computerprogramms geschützt wäre, sondern die dem Computerprogramm zugrundeliegende Idee. Dies wiederum wäre ein Bruch mit dem urheberrechtlichen Prinzip, dass nur die konkrete Ausdrucksform eines Werkes geschützt sein soll – und eben nicht die Idee, die schutzfrei bleiben soll.¹¹⁷

LINKE schließt sich der Auffassung von HARTMANN/PRINZ soweit ersichtlich an.¹¹⁸ Zwar weist er darauf hin, dass die Abgrenzung zur schutzfreien, dem untrainierten KNN zugrundeliegenden Idee zu beachten sei. Allerdings lässt er die

¹¹⁵ Siehe oben Kap. 8, A., III., 1.; a.A. HARTMANN/PRINZ, S. 778.

¹¹⁶ So HARTMANN/PRINZ, S. 778.

¹¹⁷ Explizit im Hinblick auf die Entwicklung von Computerprogrammen das OLG Köln GRUR-RR 2005, 304 – *Entwurfsmaterial*; vgl. ferner auch LINKE, S. 152 ff., welcher aufzeigt, dass nur die konkrete „formgewordene“ Rechenregel („Algorithmus“) in Form des „Gewebes“ unter Umständen Schutz erfahren kann, nicht aber die abstrakte Rechenregel.

¹¹⁸ LINKE, S. 168 ff.

konkrete Abgrenzung offen und argumentiert mit dem gesetzgeberischen Willen, einen umfassenden Schutz zu ermöglichen.¹¹⁹ Diese Abgrenzung ist aber gerade die zentral zu beantwortende Frage. Der angeblich vom Gesetzgeber gewollte Schutz kann nämlich nur so umfassend sein, dass grundlegendere Absichten des Gesetzgebers – wie bspw. der Ausschluss von Ideenmonopolisierungen – nicht tangiert sind.¹²⁰

In eine ähnliche Richtung wie HARTMANN/PRINZ gehen auch die Ansichten von EHINGER/STIEMERLING sowie GRÄTZ. Sie wollen alle auf das Funktionserfordernis „verzichten“ bzw. prüfen dieses Erfordernis nicht und behelfen sich zwecks Korrektur mit dem Schöpfungserfordernis.¹²¹ Gemäß GRÄTZ würde dabei das gestalterische Schöpfungserfordernis verhindern, dass bei dieser Ansicht jede Anweisung an einen Computer vom Computerprogrammschutz erfasst ist.¹²²

Diese Ansichten gehen jedoch alle – auch mit einer Korrektur durch das gestalterische Schöpfungserfordernis – zu weit. Sie qualifizieren jede von einem Menschen geschaffene Anweisung an einen Computer als Computerprogramm. Ließe man dies genügen, wird die Abgrenzung zu einzelnen Informationen bzw. Daten und den grundlegenden mathematischen Rechenregeln unmöglich. Sowohl einfache Informationen als auch mathematische Regeln liegen jedem informationstechnischen System zugrunde, müssen aber schutzfrei bleiben.¹²³ Daran vermag das Erfordernis der gestalterischen Schöpfung als Korrektur¹²⁴ nichts zu ändern. Erstens unterscheidet GRÄTZ nicht zwischen Werk und urheberrechtlich geschütztem Werk. Zweitens ist das Korrektiv sehr schwach, wenn auch die „kleine Münze“ geschützt sein soll. Vor dem Hintergrund, dass bspw. auch Bedienungsanleitungen urheberrechtlichen Schutz genießen können,

¹¹⁹ LINKE, S. 169 f. Allerdings kann der Schutz nur so umfassend sein, dass grundlegendere Absichten des Gesetzgebers – wie bspw. der Ausschluss von Ideenmonopolisierungen – nicht tangiert sind.

¹²⁰ Siehe dazu oben Kap. 8, A., I.

¹²¹ EHINGER/STIEMERLING, CR 2018, 765.

¹²² GRÄTZ, S. 48 f.

¹²³ Vgl. oben bereits im Patentrecht Kap. 7, A., III.

¹²⁴ Wie bei GRÄTZ vorgeschlagen.

würden nach GRÄTZ' Argumentation auch bloße Datensammlungen als Computerprogramme im urheberrechtlichen Sinne gelten. Dies ist wiederum weit entfernt von der ursprünglichen Motivation, Computerprogramme zu schützen: Belohnt werden sollte die Übersetzung einer Aufgabe in eine für eine Maschine verständliche Form.¹²⁵ Bei Zusammenstellung und elektronischer Abspeicherung von Daten wird keine Aufgabe übersetzt, sondern lediglich die strukturelle Ebene von Information gewechselt.

EHINGER/STIEMERLING stellen sich alternativ auf den Standpunkt, dass ein untrainiertes KNN in jedem Falle als Entwurfsmaterial im Sinne von § 69a Abs. 1 UrhG geschützt sei.¹²⁶ Auch eine solche Ansicht vermag nicht zu überzeugen. Ganz allgemein würde sich in diesem Fall immer die Frage stellen als Entwurfsmaterial von welchem *finalen* Computerprogramm das jeweilige untrainierte KNN geschützt sein soll. Ein und dasselbe untrainierte KNN kann nämlich vielseitig eingesetzt werden und mittels verschiedener Trainingsdaten auch zu unterschiedlich funktionierenden finalen (trainierten) KNN trainiert werden. Ein untrainiertes KNN kann bspw. Grundlage bilden für die Erkennung von Katzen auf Bildern. Das gleiche untrainierte KNN kann aber auch zur Verkehrsschilderkennung trainiert werden. Nach der WIPO-Musterdefinition liegt Computerprogrammmentwurfsmaterial aber erst dann vor, wenn eine Programmbeschreibung vorliegt, die ausreicht, das (finale) Computerprogramm darzustellen.¹²⁷ Eine Qualifikation von untrainierten KNN als Entwurfsmate-

¹²⁵ Vgl. oben Kap. 8, A., III., 1.

¹²⁶ EHINGER/STIEMERLING, CR 2018, 765; in eine ähnliche Richtung geht wohl MUHR, S. 73 f., welche aber bereits das untrainierte KNN als schutzfähig erachtet.

¹²⁷ WIPO § 1, (ii) GRUR Int 1978, 290; vgl. SÖBBING, CR 2020, 227; HARTMANN/PRINZ, S. 780.

rial würde daher einerseits die Schutzfähigkeit auch abstrakter Überlegungen ermöglichen, was aber vom Urheberrecht ausgeschlossen bleiben soll.¹²⁸ Andererseits wäre der Schutz zu weit, weil die Entwickler:innen untrainierter KNN ein zu weites Einsatzgebiet des untrainierten KNN monopolisieren könnten.¹²⁹

Als Zwischenergebnis ist also festzustellen, dass untrainierte KNN nicht vom urheberrechtlichen Computerprogrammenschutz erfasst sind. Sie stellen keine Computerprogramme im gesetzlichen Sinne dar. Eine Anpassung des Begriffsverständnisses bzw. Teile des urheberrechtlichen Verständnisses als Ganzes darf nicht erfolgen, weil eine neuartige Technologie auf den Plan tritt, welche Bedürfnisse nach immaterialgüterrechtlichem Schutz erwecken.¹³⁰ Zudem sind sie in aller Regel auch nicht Ergebnis sonstiger persönlich geistiger Schöpfungen.¹³¹

2. *Trainierte neuronale Netze*

Auch die urheberrechtliche Schutzfähigkeit von trainierten KNN ist umstritten. Trainierte KNN können komplexe Aufgaben lösen, dabei weiter lernen und auch ab der Anwendungsphase die Gewichtungsinformationen selbst anpassen, um das Ergebnis bzw. ihre Funktionsfähigkeit zu verbessern. Das Steuerungserfordernis zur Funktionserfüllung aus der Computerprogrammdefinition ist erfüllt.

Die Probleme der Subsumtion von trainierten KNN unter den urheberrechtlichen Computerprogrammenschutz sind anders gelagert. Als Probleme sind die

¹²⁸ Siehe oben Kap. 8, A., I. ff.; so auch LINKE, S. 176 f.; KI & Recht kompakt-HARTMANN/OHST, S. 147. Bei der Qualifikation von untrainierten KNN als urheberrechtlich geschütztes Entwurfsmaterial stellt sich vor allem auch die Frage, wovon genau oder von welchem trainierten KNN bzw. welcher endgültigen Anwendung des trainierten KNN das untrainierte KNN als Entwurf gelten soll. A.A. ANTOINE, CR 2019, 3 f.; KI-Rechtshandbuch-HEINZE/WENDORF, § 9 Rn. 49; EHINGER/STIEMERLING, CR 2018, 765; SÖBBING, MMR 2021, 114 mit Verweis auf SÖBBING, CR 2020, 227 ff.

¹²⁹ Siehe oben Kap. 2, C., II., 1. zu den verschiedenen Funktionen, zu welchen ein untrainiertes KNN trainiert werden kann; A.A. ANTOINE, CR 2019, 3 f.; KI-Rechtshandbuch-HEINZE/WENDORF, § 9 Rn. 49; EHINGER/STIEMERLING, CR 2018, 765.

¹³⁰ Zu der Problematik der erforderlichen menschlichen geistigen Schöpfung bei untrainierten KNN unten Kap. 8, B., III., 1.

¹³¹ Siehe dazu genauer unten Kap. 8, B., III., 1. ff.

fehlende abschließende Determiniertheit eines trainierten KNN sowie der (fehlende) geistig-menschliche Schöpfungsgehalt zu nennen.

a) Abschließende Determiniertheit

Das trainierte KNN kann sich je nach Ausgestaltung auch noch während der Anwendung verändern und seine Funktionen anpassen oder gar neue Funktionen dazulernen. In einem solchen Fall ist das trainierte KNN nicht abschließend determiniert.¹³² Eine weitere Spezialität bei trainierten KNN ist, dass sich der Quell- stark vom Maschinencode unterscheidet. Der Quellcode – sprich das untrainierte Netz – enthält noch keine Grundlagen für die Funktionsbestimmung des (finalen) Programms.¹³³ Damit kann die Determiniertheit auch nicht im untrainierten KNN festgesetzt bzw. „abgelesen“ werden. So fehlt es KNN an der verlangten Determiniertheit, wenn sie sich in der Anwendungsphase autonom optimieren. Aber auch bei einem abgeschlossenem KNN, welches sich in der Anwendungsphase nicht weiterentwickelt, kann die Determiniertheit nicht leichthin bejaht werden. Da trainierte KNN probabilistisch bzw. stochastisch arbeiten, erzeugen auch fertig trainierte KNN bei Eingabe A nicht immer auch Eingabe B. Vielmehr ist es so, dass sie bei Eingabe A nur mit einer gewissen – wenn auch oft sehr hohen – Wahrscheinlichkeit Eingabe B generieren. Sie weisen im Unterschied zu determinierten Programmen keine klaren wenn-dann-Beziehungen auf.¹³⁴

Die Determiniertheit dürfte dennoch unproblematisch sein, wenn sich das KNN weiterentwickelt, diese Änderungen sich aber in einem kleinen, überschaubaren Rahmen bewegen – wenn die neuen Funktionen immer noch von der ursprünglichen Funktion abgedeckt sind.¹³⁵ Dies ist etwa bei neuen Filmvorschlägen eines Online-Streamingdienstes der Fall oder beim Staubsaugroboter, der die neue Position eines Möbels hinzulernt, nicht aber wenn das KNN gänzlich neue Funktionen hinzulernt. Diesfalls lässt sich ein trainiertes KNN auch nicht als Computerprogramm im Sinne der WIPO-Definition einstufen.

¹³² Im Ergebnis wohl gleich, wenn auch unklar LINKE, S. 173.

¹³³ Vgl. Kap. 2, C., II., 3. oben.

¹³⁴ Siehe Kap. 2, C., II., 3., Kap. 2, C., II., 4. oben, vgl. auch soeben Kap. 8, B., III., 1.

¹³⁵ So wohl auch EHINGER, Beilage 1 zu Heft 7/8 K & R 2019, 13, a.A. wohl LINKE, S. 173.

HARTMANN/PRINZ¹³⁶ möchten auch das Problem der fehlenden Determiniertheit damit lösen, den urheberrechtlichen Computerprogrammbegriff auszuweiten. Anstelle eine bestimmte bzw. bestimmbare Funktion zu verlangen, genügt ihnen wiederum die Idee, die der Programmierung sowie dem Training des KNN zugrunde liegt. Sie möchten zwecks Identifikation des Programmes nicht auf eine determinierte Funktion, sondern auf die inkorporierte Idee des Programms abstellen. Diese Begriffsausweitung ist auch an dieser Stelle zu verwerfen. Zwar ermöglicht dieser Ansatz angewendet auf trainierte KNN nicht zwingend eine Ausweitung des Schutzes auf (zu) abstrakte Programme. Dennoch führt er dazu, dass die zugrundeliegende Idee urheberrechtlich geschützt wird anstelle des Werkes in seiner konkreten Ausdrucksform. Dies führt aber, wie bereits aufgezeigt, zu einem Bruch mit einem Grundgedanken des Urheberrechts.¹³⁷

LINKE geht in eine ähnliche Richtung wie HARTMANN/PRINZ und kritisiert die strenge Rechtsprechung des BGH – vor allem Aufgrund des Bestimmtheitserfordernisses (Erfordernis der Determiniertheit). Er schlägt vor, auf dieses Erfordernis zu verzichten.¹³⁸ Alternativ schlägt er vor, anstatt einer strengen Bestimmtheit eine bloße Bestimmbarkeit der Funktion zu verlangen.¹³⁹ Die Ansätze von LINKE gehen wie derjenige von HARTMANN/PRINZ zu weit. Die Abgrenzung zu (zu) abstrakten Programmen bzw. schlichten Anweisungen an

¹³⁶ HARTMANN/PRINZ, S. 784.

¹³⁷ Vgl. zu dieser Problematik auch LINKE, S. 157.

¹³⁸ LINKE, S. 181, S. 185 ff.

¹³⁹ LINKE, S. 182 f., S. 186 f. LINKE möchte dann Überlegungen zur Bestimmtheit bzw. Bestimmbarkeit unter dem Titel der menschlich-geistigen Schöpfung heranziehen – zwecks Zuordnung einer KI-Technologie zu der entwickelnden Person. Diesem Ansatz kann hier nur schon deshalb nicht gefolgt werden, da nach dem hier vertretenen Verständnis das Erfordernis des menschlichen Schöpfungsgehaltes bei trainierten KNN nie erfüllt sein dürfte (vgl. dazu unten Kap. 8, B., III., 2., a. ff.). Darüber hinaus handelt es sich bei LINKES Ansatz wiederum um eine unzulässige Doppelverwertung bzw. um eine zirkuläre Argumentation: Die Bestimmbarkeit ist Voraussetzung für die Qualifikation als Werk und ist mithin Werkcharakter. Das Erfordernis der menschlich-geistigen Schöpfung ist zusätzlich zum Werkcharakter zu prüfen – um mitunter maschinengenerierte Erzeugnisse (Werke) von menschlichen Werken unterscheiden zu können bzw. letztere zu schützen während erstere schutzfrei bleiben sollen (vgl. oben Kap. 8, B., III., 1.).

einen Computer würde schwer bis unmöglich.¹⁴⁰ Wie aufgezeigt lassen sich trainierte KNN unter Umständen¹⁴¹ bereits unter den Computerprogrammbegriff subsumieren.¹⁴² Eine Abkehr vom Bestimmtheitserfordernis ist nicht notwendig.¹⁴³ Die Schutzfähigkeit scheitert nämlich in jedem Fall spätestens mit dem Erfordernis der menschlich-geistigen Schöpfung.

b) Menschlich-geistiger Schöpfungsgehalt

Der Umstand, dass ein trainiertes KNN auch nach Abschluss der Programmierleistung die Funktionen ändert, liegt in der Lernfähigkeit von trainierten KNN begründet. Dabei handelt es sich um eines der Merkmale, welches uns KNN als intelligente Technologie einstufen lässt.¹⁴⁴ Vereinfacht gesagt, programmiert sich das trainierte KNN selbst (um). Damit ist auch das Problem des Erfordernisses einer menschlich-geistigen Schöpfung offensichtlich: Ab einem gewissen Zeitpunkt im Entwicklungsprozess programmiert sich das KNN selbst, losgelöst von einem menschlichen Einfluss. Zwar trifft es zu, dass durch das Training Einfluss auf die Funktion genommen werden kann. Allerdings ist dieser Einfluss einerseits konzeptioneller Natur und andererseits je nach Ausgestaltung des KNN unterschiedlich stark.¹⁴⁵

Dies kommt dem Fischen-Lehren von HARTMANN/PRINZ¹⁴⁶ ziemlich nahe. Doch das darf nicht dazu führen, dass das Urheberrecht die Idee schützt und nicht deren konkrete Ausgestaltung. Der Schutz derartiger trainierter KNN würde dazu führen, dass eine Leistung geschützt wird, die mit dem eigentlichen Programmieren (der Übersetzung von Handlungsanweisungen in eine für die

¹⁴⁰ LINKE, S. 182 argumentiert u.a., dass aus der Möglichkeit aus drei Lernmethoden zu wählen (*supervised, unsupervised und reinforcement learning*), zu einer genügenden Bestimmbarkeit auf Seiten der entwickelnden Person führt. Diese Argumentation ist fragwürdig. Ein und dieselbe Funktion kann auf verschiedene Trainingsarten dem KNN beigebracht werden (Kap. 2, A.) – entscheidend ist die Geeignetheit im konkreten Fall. Es ist also fraglich, wie genau LINKE subjektiv anhand der Trainingsmethode betreffend die Bestimmbarkeit anknüpfen möchte.

¹⁴¹ Dort wo eine Subsumtion mit urheberrechtlichen Prinzipien vereinbar ist.

¹⁴² So eigentlich auch – wenn auch kurz darauf verneinend LINKE, S. 173.

¹⁴³ Siehe für einen weiteren Vorschlag für die Umgehung des Bestimmtheitserfordernisses EHINGER/STIEMERLING, CR 2018, 766 f.

¹⁴⁴ Vgl. oben Kap. 1, B., I. ff.

¹⁴⁵ Siehe oben Kap. 2, C., II., 3. ff.

¹⁴⁶ Siehe oben Kap. 8, B., III., 1.

Maschine verständliche Form)¹⁴⁷ nichts mehr zu tun hat. Sollen also KNN, deren Anpassungen nicht mehr überschaubar sind, als Computerprogramm aufgefasst werden bzw. deren Determiniertheit im urheberrechtlichen Sinne entgegen der hier vertretenen Position bejaht werden, so scheidet deren Schutzfähigkeit an der mangelnden menschlich-geistigen Schöpfung.¹⁴⁸

Gleiches gilt auch für trainierte KNN im Zeitpunkt des Abschlusses des Trainingsvorgangs – unmittelbar vor der Anwendungsphase. Auch dort fehlt die individuelle persönlich-geistige Schöpfung. Der menschliche Schöpfungsgehalt erschöpft sich bei der Entwicklung von KNN im Sammeln und Aufbereiten der Trainingsdaten, je nach Fall dem Grad der Überwachung des Trainingsprozesses, der Auswahl des Optimierungsalgorithmus sowie schließlich in der Konzeptionierung und Programmierung der (lernfähigen) Architektur.¹⁴⁹

Unter Kap. 2, C., II., 3. wurde bereits darauf hingewiesen, dass sich in diesen Aufgaben die entwickelnden Personen aber eher von technischen, experimentellen als von kreativen, gestalterischen Überlegungen leiten lassen.¹⁵⁰ Diese sind darüber hinaus typischerweise Tätigkeiten, die die Schwelle der bloßen Konzeptionierung nicht überschreiten. Die Schwelle der Konzeptionierung ist im Fall der KNN dort überschritten, wo das Netz eine Funktion erlernt. Dies geschieht mittels Einstellung der Verbindungsgewichte.¹⁵¹ Das erfolgt aber durch den Optimierungsalgorithmus – eine Software. Es ist dem Menschen nicht möglich, die Informationsverarbeitung in neuronalen Netzen nachzuvollziehen¹⁵², deshalb und aufgrund der schieren Menge an einzustellenden Gewichten, bedient er sich (gezwungenermaßen) des Optimierungsalgorithmus. Dieser stellt die Gewichtungen unabhängig vom Menschen ein – durch Verarbeitung der Trainingsdaten und dem gleichzeitigen Abgleich mit den jeweiligen Ausgaben. Dazu wendet der Optimierungsalgorithmus mathematische – genauer: stochastische – Regeln an.¹⁵³

¹⁴⁷ Siehe oben Kap. 8, B., III., 1.

¹⁴⁸ MUHR, S. 82 f.; SCHAUB, JZ 2017, 347; im Ergebnis wohl gleich LINKE, S. 198.

¹⁴⁹ Siehe oben Kap. 2, C., II., 3. ff.

¹⁵⁰ Siehe oben Kap. 2, C., II., 3. ff.

¹⁵¹ Siehe oben Kap. 2, C., II., 3. ff.

¹⁵² Weil die Informationsverarbeitung implizit erfolgt.

¹⁵³ Siehe oben Kap. 2., C., II., 3.

Mit anderen Worten macht der Optimierungsalgorithmus das neuronale Netz funktionsfähig, indem er Rechenregeln anwendet. Die Gewichtungseinstellung ist der entscheidende Schritt im Training von KNN. Damit fehlt es dem Entwicklungsschritt, welcher dem Programm seinen entscheidenden Charakter verleiht, an der menschlich geistigen Schöpfung. Dies spricht gegen die Schutzfähigkeit eines trainierten KNN, auch wenn es sich nicht weiterentwickelt.¹⁵⁴

Es ließe sich nun einwenden, dass mit den Möglichkeiten, auf welche die trainierende oder programmierende Person Einfluss nehmen kann, ein erheblicher menschlicher Input vorläge, der auch die Schöpfungshöhe überschreiten dürfte.¹⁵⁵ Dieser menschliche Input ist aber, besonders was die Auswahl und Programmierung des Optimierungsalgorithmus anbelangt, beschränkt und nicht kreativ. Unter Kap. 2, C., II., 3. wurde aufgezeigt, dass die Auswahl und Programmierung des Optimierungsalgorithmus weniger von kreativen und viel eher von Zweckmäßigkeitsüberlegungen getrieben ist. Der Optimierungsalgorithmus arbeitet mit statistischen Regeln und fußt auf dem Prinzip *trial and error*. Die trainierende Person kann lediglich die Trainingseffizienz bestimmen, indem sie die Trainingsdauer bestimmt oder dem Optimierungsalgorithmus die Schrittgröße vorgibt, in welcher er die Neuronen annäherungsweise anpassen soll.¹⁵⁶ Auch was das Sammeln und Kurieren der Trainingsdaten betrifft, liegt die menschliche Schöpfung dabei in einem Aufzeigen von Lösungswegen anstatt des Aufzeigens von Lösungen. Damit würde aber wiederum das Fischen-Lehren geschützt und nicht das Fischen selbst.¹⁵⁷

Ließe man insbesondere die Auswahl und Programmierung von Optimierungsalgorithmen als menschlichen, kreativen bzw. schöpferischen Einfluss genügen, wäre das Ergebnis ein Absurdes: Oft wird ein und derselbe Optimierungsalgorithmus für verschiedene Architekturen eingesetzt. Ein und derselbe Optimie-

¹⁵⁴ Dies würde auch gelten, wenn der Mensch die Gewichte „von Hand“ einstellen würde. Denn auch dieser würde die Gewichte anhand von Rechenregeln und nicht anhand kreativer bzw. gestalterischer Überlegungen einstellen.

¹⁵⁵ Siehe so GRÄTZ, S. 53 m.w.N., S. 86 implizit.

¹⁵⁶ Siehe oben Kap. 2, C., II., 3.

¹⁵⁷ Siehe oben Kap. 8, B., III., 1.; im Ergebnis gleich wie hier MUHR, S. 82 f.

rungsalgorithmus kann also verschiedenen Architekturen verschiedene Funktionen beibringen. Ließe man nun den Einsatz des Optimierungsalgorithmus als menschlich-geistige Schöpfung genügen, würde die Person, die den Optimierungsalgorithmus programmierte, schließlich Urheberin aller trainierter KNN sein, die mit ihrem Optimierungsalgorithmus trainiert wurden. Ihr käme eine unvertretbare Monopolstellung zu.

Die Argumente derer, die in solchen Fällen dennoch eine geistige Schöpfung bejahen wollen, sind auf Aufwands- und Komplexitätsüberlegungen der entwickelnden Personen zurückzuführen. Diese verlieren jedoch wieder an Bedeutung, wenn vorgefertigte Netze verwendet und anschließend trainiert werden. Argumente aus Aufwands- und Komplexitätsüberlegungen dürfen das Urheberrecht nicht überstrapazieren. Solche Überlegungen können viel eher als Argumente für die Einführung eines Leistungsschutzrechtes herangezogen werden.¹⁵⁸

c) Zwischenergebnis

Nach der hier vertretenen Auffassung ist die urheberrechtliche Schutzfähigkeit von trainierten KNN spätestens aufgrund der mangelnden geistigen Schöpfung im Sinne des Urheberrechts zu verneinen. Die geistige Schöpfung muss sich in der Individualität des Werkes widerspiegeln. Nach dem UrhG ist das Werk geschützt und nicht die dem Werk zugrundeliegende Idee. Die Gewichtungseinstellung und damit die Funktionsaneignung des Programms erfolgen gänzlich automatisiert, bei welcher der menschliche Einfluss die Konzeptionierungsphase nicht überschreitet. Damit erfolgt die Individualisierung automatisch – anhand von Regeln der Statistik und Mathematik sowie der den Trainingsdaten inhärenten Informationen und Zusammenhänge. Genau diese Individualisierung muss aber im urheberrechtlichen Sinne das Ergebnis einer geistigen Schöpfung sein, damit ein Computerprogramm urheberrechtlich geschützt ist.

Trainierte KNN erfüllen somit je nach Ausgestaltung bereits den Computerprogramm-begriff nicht und andererseits mangelt es ihnen in jedem Fall an der

¹⁵⁸ Siehe dazu oben generell zu Leistungsschutzrechten, Kap. 8, A., IV. ff. und unten zum Leistungsschutzrecht *de lege ferenda* Kap. 12.

menschlich-geistigen Schöpfung. Sie sind damit nicht vom urheberrechtlichen Computerprogrammschutz erfasst.

3. Schutz der Gewichtungsinformationen (Trainingsergebnisse)

Die Gewichtungsinformationen sind im Grunde nichts weiter als einzelne Daten, die sich auf die einzelnen Neuronen des KNN beziehen. Sie beinhalten die Information, bei welchem Input an das Neuron welcher Output erfolgt.¹⁵⁹ Sie lassen sich isolieren und separat abspeichern. Sie sind jedoch nicht unabhängig voneinander – schließlich ergibt das KNN erst Sinn bzw. kann das KNN sinnvoll funktionieren, wenn das richtige Neuron bei entsprechender Stimulierung auch das entsprechende nächste Neuron ansteuert.

Bis auf ihre Verortung auf der Architektur und die Berechnung des Outputs für das einzelne Neuron, verfügen sie über keine Steuerungsanweisungen an einen Computer, weshalb der Computerprogrammschutz außer Betracht fällt. Das Leistungsschutzrecht des Datenbankherstellers entfällt ebenfalls, weil die Gewichtungsinformationen nicht unabhängig voneinander sind.¹⁶⁰ Unabhängigkeit ist dann gegeben, wenn sich die einzelnen Daten voneinander trennen ließen, ohne dass der Wert ihres informativen Inhalts beeinträchtigt würde. Dadurch entfällt nicht nur das Leistungsschutzrecht des Datenbankherstellers nach §§ 87a ff. UrhG, sondern auch der Schutz als Datenbankwerk nach § 4 UrhG an und für sich. Da auch bei Datenbankwerken die Unabhängigkeit der einzelnen Bestandteile vorausgesetzt wird.

Darüber hinaus fehlt bei den Gewichtungseinstellungen das sinnlich wahrnehmbare Kommunikationselement, weshalb sie bereits deshalb als urheberrechtliches Werk außer Betracht fallen.¹⁶¹ Die Darstellung der Gewichtungsinformationen in Code oder einer anderen sinnlich wahrnehmbaren Form ist zwar möglich, allerdings erschließt sich der Sinn bzw. die Funktionalität der Neuronen dem Menschen nicht.¹⁶²

¹⁵⁹ Siehe oben Kap. 2, C., II., 2.

¹⁶⁰ Siehe zu den Voraussetzungen des Datenbankwerk- und Datenbankherstellerschutzes oben Kap. 8, A., IV.; vgl. auch MUHR, S. 85 ff.

¹⁶¹ Vgl. oben Kap. 8, A., III., 2. und unten Kap. 8, B., III., 1. ff. zur sinnlichen Wahrnehmbarkeit.

¹⁶² Vgl. oben Kap. 2, C., II., 4.; siehe zum erforderlichen Kommunikationselement oben Kap. 8, A., III., 2. und weiter unten Kap. 8, B., IV., 1. ff.

4. Optimierungsalgorithmus

Der Optimierungsalgorithmus ist eine für einen Computer verständliche Folge von Befehlen, anhand welcher die Gewichte von Neuronen eines KNN eingestellt werden.¹⁶³ Damit erfüllt der Optimierungsalgorithmus die Voraussetzungen des Computerbegriffs von § 69a UrhG. Mit anderen Worten ist der Optimierungsalgorithmus ein Computerprogramm im herkömmlichen Programmierverständnis und damit klassische Software. Dies hat zur Folge, dass die Programmierer:in eines Optimierungsalgorithmus auch Urheber des Optimierungsalgorithmus ist.

5. Bestandteile neuronaler Netze

Einzelne Bestandteile von KNN – trainiert und untrainiert – können jedoch einzelne Steuerungsanweisungen sein, die den urheberrechtlichen Computerprogramm-begriff durchaus erfüllen können. Bei diesen Bestandteilen kann es sich um einzelne Verbindungen zwischen Neuronen handeln oder andere Bestandteile wie bspw. Regeln zur Rückkopplung. Diese können für sich betrachtet Schutz genießen, sofern sie ein Steuerungs- und ein Funktionselement aufweisen und Ergebnis einer menschlich-geistigen Schöpfung sind und nicht bloß von Funktionalitätsüberlegungen bzw. technisch bedingt sind und es sich nicht lediglich um mathematische Regeln handelt.¹⁶⁴

6. Zwischenergebnis

Zusammenfassend kann also festgehalten werden, dass nach hier vertretener Ansicht weder das trainierte noch das untrainierte KNN unter den Computerprogramm-schutz des Urheberrechts subsumierbar sind. Gleiches gilt für die Gewichtungsinformationen. Sofern andere Bestandteile wie Verbindungen oder Aktivierungsfunktionen die Voraussetzungen von § 69a UrhG erfüllen, kommt für einzelne Bestandteile unter Umständen ein Computerprogramm-schutz in Frage.¹⁶⁵ Ebenso kann für den Optimierungsalgorithmus ein urheberrechtlicher Schutz vorliegen. Die Funktionalität als solche bleibt aber in jedem Fall ungeschützt.¹⁶⁶

¹⁶³ Siehe oben Kap. 2, C., II., 3. ff.

¹⁶⁴ Vgl. dazu oben Kap. 7, A., III.

¹⁶⁵ Vgl. KRAUSEN, S. 52, welcher von einem fragmentarischen Urberschutz spricht.

¹⁶⁶ Vgl. oben Kap. 8, B.

IV. Künstliche neuronale Netze als sonstige Werke nach § 2 UrhG

KNN fallen nicht unter den urheberrechtlichen Computerprogramm-schutz. Dies bedeutet aber nicht *eo ipso*, dass sie gänzlich keinem urheberrechtli-chen Werkschutz zugänglich sein können. Im Folgenden wird die Frage beant-wortet, ob eine konkrete Ausdrucksform eines KNN urheberrechtlichen Schutz als sonstiges Werk nach § 2 UrhG erfahren kann. Die Darstellung wird aber zei-gen, dass vor allem das Kommunikationselement Schutzhindernis ist.

1. Untrainierte neuronale Netze

Auch unter diesem Titel sollen untrainierte KNN in einem ersten Schritt und getrennt von trainierten KNN betrachtet werden: Es geht also um die Frage, ob die Darstellung der Topologie in einer sinnlich wahrnehmbaren Art – meist Schriftform – als Werk im Sinne von § 2 UrhG geschützt sein kann. Erstes Problem hinsichtlich eines Schutzes stellt das Erfordernis des Kommunikations-elementes – mitunter der geistige Gehalt eines untrainierten KNN – dar.¹⁶⁷ Fä-hige Betrachter:innen der (niedergeschriebenen) Topologie müssten also die Funktionsweise der Topologie verstehen bzw. nachvollziehen können, damit das erforderliche Kommunikationselement bejaht werden könnte. Allerdings verarbeiten KNN – egal ob untrainiert oder trainiert – Informationen implizit im Gesamtzustand des KNN.¹⁶⁸ Deshalb wird bei KNN auch von *black boxes* bzw. fehlender Erklär- und Nachvollziehbarkeit gesprochen.¹⁶⁹ Während bei ein- bzw. geringschichtigen KNN noch dafür argumentiert werden könnte, dass sich für fähige Betrachter:innen noch ein Sinngehalt aus der Darstellung der To-pologie ergibt, ist das bei mehrschichtigen Netzen – demnach der überwiegen- den Mehrzahl der KNN¹⁷⁰ – zu verneinen. Die implizite Informationsverarbei-tung im Netzgesamtzustand macht es Menschen unmöglich, durch bloße Be-trachtung die Funktionsweise nachzuvollziehen.¹⁷¹ Entsprechend ergibt sich auch kein Sinngehalt bzw. Kommunikationsgehalt aus der Betrachtung des

¹⁶⁷ Vgl. dazu oben Kap. 8, A., III., 2.

¹⁶⁸ Siehe dazu oben Kap. 2, C., I., 4.

¹⁶⁹ Siehe dazu ausführlich oben Kap. 7, B., III.

¹⁷⁰ Oben unter Kap. 2, C. II. wurde gezeigt, dass die mehrschichtigen KNN diejenigen sind, die dazu in der Lage sind, sehr komplexe Aufgaben zu lösen.

¹⁷¹ Vgl. oben Kap. 2., C., IV., aufgrund dessen befasst sich ein gesamter Forschungszweig der KI-Forschung mit der Erklärbarkeit von Künstlicher Intelligenz, v.a. von KNN. Man spricht dabei von *explainable AI*.

KNN. Das Kommunikationselement bei untrainierten KNN ist dementsprechend zu verneinen.¹⁷² Ein solches Kommunikationselement ist aber für einen Schutz als sonstiges Werk nach § 2 UrhG Voraussetzung.

Wird das Vorliegen des Kommunikationselementes entgegen der hier vertretenen Ansicht bejaht, stellt auch bei untrainierten KNN die erforderliche geistige Schöpfung – genauer: das Ausnutzen eines Gestaltungsspielraumes – ein weiteres Schutzhindernis dar. Die konkrete Ausdrucksform eines untrainierten KNN ist nur insofern geschützt, als dass sich die entwickelnde Person nicht von reinen Funktionalitätsüberlegungen hat leiten lassen und mithin einen individuellen Gestaltungsspielraum bei der Entwicklung ausnutzte.¹⁷³ Diese kreative Gestaltung von Topologien darf jedoch nicht leichthin bejaht werden. Topologien von KNN werden oft experimentell und anhand von Funktionalitätsüberlegungen entworfen.¹⁷⁴ Dieser Umstand wäre auch vertieft zu betrachten und als problematisch zu erachten, wenn die Computerprogrammeigenschaft von untrainierten KNN nach § 69a ff. UrhG entgegen der hier vertretenen Ansicht bejaht würde. Selbstverständlich weist aber die besonders kreative Darstellungsweise des Codes die notwendige Gestaltungshöhe auf. In einem solchen Fall ist jedoch auch nur eben diese kreative Ausdrucksform Gegenstand des urheberrechtlichen Schutzes.

Die konkrete Ausdrucksform eines untrainierten KNN ist also einem Schutz nach § 2 UrhG nur dann zugänglich; (i) wenn es sich um eine Formgebung handelt, die es fähigen Betrachter:innen ermöglicht, die Funktionsweise der Topologie nachzuvollziehen, und (ii) die Topologie nicht anhand reiner Funktionalitäts- bzw. technischen Überlegungen entworfen wurde. Kann beides bejaht werden, gilt es immer noch zu beachten, dass nur die konkrete Ausdrucksform der Topologie geschützt ist und nicht die zugrundeliegende Funktion bzw. Funktionalität.

¹⁷² A.A. wohl LINKE, S. 192.

¹⁷³ Siehe Kap. 2., C., II. 3 oben.

¹⁷⁴ Siehe oben Kap. 2., C., II. 3.; a.A. MUHR, S. 74 ff., welche davon ausgeht, dass genügend gestalterische Möglichkeiten vorhanden sind.

2. Trainierte neuronale Netze

Die oben unter Kap. 8, B., III., 2, b) aufgeführte Problematik der notwendigen menschlich-geistigen Schöpfung zur Qualifizierung trainierter KNN als Computerprogramme nach UrhG ist auch bei der Qualifikation von trainierten KNN als Werke im Sinne von § 2 UrhG aufzuführen. Während das untrainierte Netz noch überwiegend direkt von Programmierer:innen entwickelt ist¹⁷⁵, ist das trainierte KNN durch den Optimierungsalgorithmus gestaltet. Wird dann das trainierte KNN so übernommen und wahrnehmbar dargestellt, dürfte die Schöpfungshöhe in aller Regel nicht erreicht sein. Wenn jedoch die Darstellung als solche kreativ ist – mithin bei der Darstellung ein bestimmter Gestaltungsspielraum ausgenutzt wurde – kann eine geistige Schöpfung vorliegen.

Das Kommunikationselement wurde bereits unter dem Titel der untrainierten KNN als Schutzhürde eruiert. Es wurde dargelegt, dass sich menschlichen Betrachter:innen aufgrund der Art und Weise der Funktionsweise von KNN – genauer: die Art der Informationsverarbeitung – kein Sinngehalt erschließt. Auch bei trainierten KNN können menschliche Betrachter:innen des Codes die Funktionsweise des KNN nicht ohne Weiteres nachvollziehen. Weil trainierte KNN Informationen implizit im Gesamtzustand des Netzes verarbeiten und darstellen, können Menschen die Funktionsweise von KNN nicht nachvollziehen geschweige denn erklären. Es bedarf der Methoden aus der Forschung zu *explainable AI*, um die Funktionsweise von KNN nachvollziehen zu können.

Wird aber eine Form gefunden, in der (trainierte) KNN wahrnehmbar dargestellt werden können und ergibt sich den menschlichen Betrachter:innen aus der Darstellung auch ein entsprechender Sinngehalt, dürfte einem urheberrechtlichen Schutz nach § 2 UrhG grundsätzlich nichts im Wege stehen. Voraussetzung ist dabei aber stets, dass die Darstellungsform als solche kreativ ist. Nur dann liegt eine menschlich-geistige Schöpfung vor. Es ist jedoch stets nur diese konkrete Ausdrucksform geschützt und keineswegs die dem KNN zugrundeliegende Funktion als Softwareebene.

¹⁷⁵ Es ist noch „*man-made*“.

V. Schutz der Trainingsdaten

Die Trainingsdaten stellen lediglich eine Sammlung von Informationen dar. Sie verfügen über keine Steuerungsanweisung und fallen somit als Computerprogramm außer Betracht.¹⁷⁶ Denkbar wäre ein Schutz gemäß § 2 Abs. 1 Nr. 7 UrhG: als Darstellungen wissenschaftlicher oder technischer Art. Entscheidend dürfte aber auch dort die Individualität der persönlichen geistigen Schöpfung sein. Gemäß Rechtsprechung erreicht das bloße Zusammentragen einzelner Fakten nicht das notwendige Schutzniveau, wenn es sich lediglich um eine Zusammenstellung handelt – auch wenn sie nur mit großer Mühe und erheblichem Zeitaufwand erfolgen konnte.¹⁷⁷ Selbstverständlich kann eine eigenständig kreative Darstellung der Trainingsinformationen Schöpfungshöhe erreichen. Allerdings ist diesfalls nur eben diese konkrete Darstellung in Form der Auf- und Einteilung, Anordnung und Auswahl geschützt. Der Inhalt der Trainingsdaten bleibt in einem solchen Fall frei.¹⁷⁸ Der Schutz von Trainingsdaten nach § 2 Abs. 1 Nr. 7 UrhG ist also eine Frage des Einzelfalles.¹⁷⁹

Es drängt sich die Diskussion nach einem Schutz von Trainingsdaten als Datenbankwerk nach § 4 UrhG sowie im Rahmen des Datenbankherstellerrechts nach §§ 87a ff. UrhG auf. Voraussetzung ist bei beiden Normen das Vorliegen einer Datenbank im urheberrechtlichen Sinne. Dazu müssen die einzelnen Elemente einer Datenbank unabhängig voneinander sein.¹⁸⁰ Unabhängigkeit liegt vor, wenn die einzelnen Elemente nach dem Heraustrennen aus der Datenbank einen selbstständigen semantischen Informationswert aufweisen.¹⁸¹ HACKER formuliert diese Voraussetzung so, dass die einzelnen „Elemente [...] auch nach der

¹⁷⁶ So auch HACKER, GRUR 2020, 1031.

¹⁷⁷ BGH GRUR 1980, 231 – *Monumenta Germaniae Historica*; siehe dazu m.w.N. auch HACKER, GRUR 2020, 1027 f.

¹⁷⁸ HACKER, GRUR 2020, 1028.

¹⁷⁹ So auch HACKER, GRUR 2020, 1028 m.w.N.

¹⁸⁰ Siehe oben Kap. 8, A., IV.

¹⁸¹ EuGH GRUR 2005, 254 Rn. 34 – *Fixtures Marketing*; EuGH GRUR 2015, 1187 Rn. 22 f. – *Verlag Esterbauer*; Rechtsprechungsübersicht entnommen bei HACKER, GRUR 2020, 1029; siehe auch die detaillierte Rechtssprechungszusammenfassung bei Dreier/Schulze/DREIER, UrhG, § 87a Rn. 6: damit Unabhängigkeit vorliegt, müssen die einzelnen Termine „voneinander getrennt werden können, ohne dass der Wert ihres informativen, literarischen, künstlerischen, musikalischen oder sonstigen Inhalts dadurch beeinträchtigt wird“; vgl. bereits Kap. 8., B., III., 3.

Herauslösung [...] für interessierte Dritte noch sachdienliche Informationen liefern [...]“ müssen. Angewandt auf einen Datenkorpus für das Training von KI-Technologien kann diese Unabhängigkeit nicht generell bejaht werden. So geben bspw. Trainingsdaten für das Training von Bilderkennungstechnologien die Kodierung eines Pixels an.¹⁸² Es ist stark zweifelhaft, ob dieser Inhalt semantisch oder wirtschaftlich von Wert ist, ohne dass Informationen über die umliegenden Pixel vorliegen.¹⁸³ Bei einer Zusammenstellung von Hochwasserdaten zwecks Trainings von Flut-/Dürrevorhersagen sieht die Situation anders aus: die einzelnen Informationen dürften diesfalls in der Regel einen eigenen semantischen Wert aufweisen bzw. lassen sich die einzelnen Daten einzeln vermarkten.¹⁸⁴ Das heißt, das Unabhängigkeitserfordernis ist bei einem Trainingsdatenkorpus für die einzelnen Elemente immer im Einzelfall zu entscheiden.¹⁸⁵ Für das Vorliegen eines Datenbankwerkes nach § 4 UrhG ist zusätzlich zur Datenbankerschaft auch eine persönliche geistige Schöpfung erforderlich. Diese ist bei Trainingsdaten ebenfalls nicht leichthin anzunehmen. Analoges zu eben unter Kap. 8, B., V. Ausgeführten lässt sich auch hier sagen: Handelt es sich um eine bloße Zusammenstellung von Daten, ist die Schöpfungshöhe noch nicht erreicht. Auch wenn die Zusammenstellung viel Mühe, Zeit und Fleiß bedeutete. Rein funktionale Überlegungen in der Auswahl, Zusammenstellung und Anordnung reichen ebenfalls nicht aus.¹⁸⁶ Es müssen kreative, eigenständige Entscheidungen getroffen werden.¹⁸⁷

Eine persönliche geistige Schöpfung ist beim Datenbankherstellerrecht nach §§ 87a ff. UrhG nicht vorausgesetzt. Das Datenbankherstellerrecht erfordert jedoch die Aufwendung einer erheblichen Investition, die in der Datenbank verkörpert ist. Regelmäßig ist diese Voraussetzung beim Sammeln und vor allem

¹⁸² HACKER, GRUR 2020, 1029 m.w.N.

¹⁸³ So auch HACKER, GRUR 2020, 1029; siehe auch Dreier/Schulze/DREIER, UrhG, § 87a Rn. 6.

¹⁸⁴ Siehe HACKER, GRUR 2020, 1029 mit dem Beispiel von Wetter- und Verkehrsdaten. Vgl. auch die Rechtsprechung des EuGH in EuGH GRUR 2015, 1187 Rn. 25 ff. – *Verlag Esterbauer*. Hierbei ging es um geografische Daten von Landkarten, die von einem Dritten aus der Landkarte extrahiert wurden, um eine eigene Karte herzustellen.

¹⁸⁵ Siehe HACKER, GRUR 2020, 1029; Rechtshandbuch Industrie 4.0-KUSS/SASSENBERG, § 13 Rn 49.

¹⁸⁶ HACKER, GRUR 2020, 1028 m.w.N.

¹⁸⁷ HACKER, GRUR 2020, 1029 m.w.N.

Aufarbeiten von KI-Trainingsdaten erfüllt. Sodass – sofern die Unabhängigkeit der Daten bejaht werden kann – diese Voraussetzung überwiegend erfüllt sein dürfte.¹⁸⁸ Dabei ist jedoch die Rechtsprechung des EuGH zu beachten. Diese besagt, dass nur die Aufwendungen bei der Suche nach und der Sammlung bereits vorhandener, nicht aber bei der Erzeugung neuer Daten berücksichtigt werden dürfen.¹⁸⁹ Bei der Auf- und Bearbeitung bestehender Daten kann dies zu beträchtlichen Schwierigkeiten führen.¹⁹⁰

Der Schutz von Trainingsdaten im Urheberrecht ist also im Einzelfall zu entscheiden und nicht leichthin anzunehmen.

VI. *Zwischenergebnis zum urheberrechtlichen Schutz von KI-Technologien*

Der urheberrechtliche Schutz ist anders als der patentrechtliche technologie-spezifisch zu betrachten. Obwohl das Urheberrecht grundsätzlich technologie-neutral gestaltet ist,¹⁹¹ führt das urheberrechtliche Verständnis des Computerprogrammbegriffes einerseits und die verschiedenen Entwicklungs- und Funktionsweisen der betrachteten Technologien andererseits zur Notwendigkeit, die Technologien urheberrechtlich separat zu beurteilen

Bei Expertensystemen genießt die Inferenzmaschine urheberrechtlichen Computerprogrammenschutz nach § 69a ff. UrhG. Die Wissensbasis ist von diesem Schutz nicht erfasst. In aller Regel ist die Wissensbasis aber dem Schutz des Datenbankherstellers nach § 87b UrhG zugänglich. Die Wissensbasis kann darüber hinaus auch als Datenbankwerk nach § 4 Abs. 2 UrhG Schutz genießen. Die Benutzeroberfläche ist nicht vom Computerprogrammenschutz erfasst. Die konkrete Ausdrucksform der Benutzeroberfläche kann jedoch als Werk nach § 2 UrhG Schutz genießen.¹⁹²

¹⁸⁸ Vgl. HACKER, GRUR 2020, 1030.

¹⁸⁹ EuGH GRUR 2005, 244 Rn. 31, 42 – *British Horseracing Board*.

¹⁹⁰ Siehe dazu ausführlich HACKER, GRUR 2020, 1030 f.

¹⁹¹ Vgl. oben Kap. 8, A., I., 1.

¹⁹² Vgl. oben Kap. 8, B., I.

Bei der Entwicklung von genetischen Programmen bleiben das Ziel-Programm sowie sämtliche Vorgänger des Ziel-Programmes gänzlich schutzfrei. Grund dafür ist der mangelnde menschliche Schöpfungsgehalt. Die Programmierung, welche die einzelnen Programmindividuen generiert sowie die Fitnessfunktion können einem Computerprogrammenschutz nach § 69a ff. UrhG zugänglich sein. Allerdings nur sofern und soweit ihre Entwicklung nicht von reinen Funktionalitätsüberlegungen geprägt ist.¹⁹³

KNN sind dem urheberrechtlichen Computerprogrammenschutz nach der hier vertretenen Ansicht nicht zugänglich. Das gilt sowohl für untrainierte als auch für trainierte KNN. Dies liegt an der Entwicklungs- und Funktionsweise der KNN. Sie passen nicht in den urheberrechtlichen Rechtsrahmen sowie dessen Verständnis. Sowohl untrainierte als auch in den meisten Fällen trainierte KNN erfüllen bereits den Computerprogrammbegriff des Urheberrechts nicht. Selbst wenn man diese KNN noch unter diesen Begriff subsumieren möchte, scheitert ein Schutz am erforderlichen menschlichen Schöpfungsgehalt.¹⁹⁴ Ein untrainiertes KNN kann in der konkreten Ausdrucksform unter Umständen als sonstiges Werk nach § 2 UrhG geschützt sein.¹⁹⁵ Gleiches gilt für trainierte KNN, wobei bei diesen die Schutzvoraussetzungen noch strenger sind als bei untrainierten KNN.¹⁹⁶ Die Gewichtungsinformationen sind weder nach dem urheberrechtlichen Computerprogrammenschutz noch im Rahmen des Datenbankherstellerrechtes geschützt.¹⁹⁷ Die Trainingsdaten können einzeln bereits geschützte Werke darstellen. In ihrer Gesamtheit können sie unter Umständen als Datenbankwerk oder im Rahmen des Datenbankherstellerrechtes Schutz genießen.¹⁹⁸

¹⁹³ Vgl. bei KNN oben Kap. 2, C., II., 3.; Kap. 8, A., III., 1.; Kap. 8, B., III., 2., b).

¹⁹⁴ Siehe oben Kap. 8, B., III., 2., b).

¹⁹⁵ Siehe zu den einzelnen Voraussetzungen oben Kap. 8, B., IV.

¹⁹⁶ Siehe zu den einzelnen Voraussetzungen oben Kap. 8, B., IV., 2.

¹⁹⁷ Siehe oben Kap. 8, B., III., 3.

¹⁹⁸ Vgl. oben Kap. 8, B., III., V.

Kapitel 9

Schutz von KI-Technologien als Geschäftsgeheimnisse

Der Geschäftsgeheimnisschutz (auch Know-How-Schutz) als Schutzinstrument für KI-Technologie liegt nahe, weil viele Unternehmen ihre KI-Technologien, insbesondere aber die ihnen zugrundeliegenden Daten als Geschäftsgeheimnisse behandeln¹ und sich die KI-Technologien wie gesehen weder durch das Patent- noch das Urheberrecht umfassend schützen lassen.

A. Grundlagen des Know-How- bzw. Geschäftsgeheimnisschutzes

Der Geschäftsgeheimnisschutz ist in Deutschland durch das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) geregelt. Es entspricht der Umsetzung der Geschäftsgeheimnisrichtlinie des Europäischen Parlaments und des Rates² und trat am 26. April 2019 in Kraft. Das Gesetz soll Geschäftsgeheimnisse vor unerlaubter Erlangung, Nutzung und Offenlegung schützen. Als Geschäftsgeheimnis kommt jede Art von Information in Frage, sofern sie

- weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist (§ 2 Nr. 1 lit. a GeschGehG);

¹ Siehe dazu auch oben Kap. 6, C.

² Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (ABl. L 157 vom 15.6.2016, S. 1).

- Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch den rechtmäßigen Inhaber ist (§ 2 Nr. 1 lit. b GeschGehG) und
- bei der ein berechtigtes Interesse an der Geheimhaltung besteht (§ 2 Nr. 1 lit. c GeschGehG)³.

Damit ist eine Information mitunter nur dann als Geschäftsgeheimnis geschützt, wenn und solange sie geheim gehalten wird.

Im Hinblick auf den Geheimnischarakter und im Gegensatz zum Patentrecht ist hier erwähnenswert, dass die Information nicht im patentrechtlichen Sinne absolut neu sein muss. Da lediglich „Personen, die üblicherweise mit dieser Art von Information umgehen“ für den Geheimnischarakter entscheidend sind, geht das GeschGehG von einem relativen Geheimnisbegriff aus.⁴

Das Erfordernis der angemessenen Geheimhaltungsmaßnahme ist entscheidend dafür, ob der Schutz nach GeschGehG greift oder nicht. Mit anderen Worten trifft den Geheimnisinhaber die Obliegenheit der angemessenen Geheimhaltungsmaßnahmen. Die Frage nach der Angemessenheit der Schutzmaßnahme lässt sich nicht allgemein beantworten. Viel eher handelt es sich auch hier um einen relativen Begriff. Somit variiert die Angemessenheit von Information zu Information. Es lässt sich anhand des Wortlautes lediglich eindeutig festhalten, dass keine *optimale* Geheimhaltungsmaßnahme vorausgesetzt ist. Die Angemessenheit der Maßnahme hängt von der Art der Information und den konkreten Nutzungsumständen ab.⁵ Entscheidende Umstände sind im Einzelnen der Wert des Geheimnisses, dessen Entwicklungskosten, die Natur der Information, die Bedeutung für das Unternehmen, die Größe des Unternehmens, die üblichen Geheimhaltungsmaßnahmen im Unternehmen, die Art der Kennzeichnung der

³ Diese zusätzliche Voraussetzung findet sich nicht in der Richtlinie und wurde vom deutschen Gesetzgeber eingefügt.

⁴ Statt vieler: OHLY, GRUR 2019, 443.

⁵ BT-Drs. 19/4724, 24.

Informationen und die vereinbarten vertraglichen Regelungen mit Arbeitnehmer:innen und Geschäftspartner:innen.⁶ Wie aber eine solche Maßnahme zu gestalten ist, lässt sich weder dem Gesetz, dessen Entwurfsgrundlagen noch der Richtlinie entnehmen.⁷

Klar scheint diesbezüglich einerseits, dass nicht jede geheime Information als solche gekennzeichnet werden muss. Vielmehr kann sich bereits aus der Art der Information deren Nicht-Offenkundigkeit ergeben. Es genügt daher, die Informationen zu kategorisieren und anschließend Maßnahmen für die einzelnen Kategorien zu treffen.⁸

OHLY arbeitet mit Verweis auf MASSEN aus rechtsvergleichenden Überlegungen sowie Analogien aus der für Bundesbehörden geltenden Verschlusssachenanweisung fünf verschiedene Maßnahmenarten aus. Diese reichen von Kennzeichnung der Information als geheim⁹ über vertragliche Vertraulichkeitsabreden bis hin zu technischen Schutzmaßnahmen.¹⁰ Dabei sollte auch klar sein, dass die Maßnahmen in verschiedene Dimensionen gerichtet sein müssen. Mit anderen Worten müssen die Maßnahmen genauso angemessenen Schutz vor missbräuchlichem Verhalten der Arbeitnehmer:innen und Geschäftspartner:innen bieten wie vor unbefugten Zugriffen Dritter.¹¹ Nach der Kategorisierung der Geschäftsgeheimnisse¹² sind die Risiken zu eruieren. Anders ausgedrückt müssen die potenziellen Bedrohungen ausgemacht werden und die verschiedenen Informationen entsprechend vor den eruierten Bedrohungen geschützt werden.¹³

⁶ BT-Drs. 19/4724, 24 f.

⁷ Nur MAASSEN, GRUR 2019, 353.

⁸ BT-Drs. 19/4724, 24.

⁹ Sofern sich der Geheimnischarakter eben nicht aus den Umständen ergibt.

¹⁰ Ausführlich OHLY, GRUR 2019, 444 mit Verweis auf MASSEN, GRUR 2019, 356 ff.

¹¹ MASSEN, GRUR 2019, 357 ff.

¹² MASSEN unterteilt in durch ihr Bekanntwerden existenzbedrohende oder dauerhaften sowie nur kurzfristigen wirtschaftlichen Schaden verursachende Informationen (GRUR 2019, 356).

¹³ MASSEN, GRUR 2019, 356 f.

B. Anwendung des GeschGehG auf KI-Technologien

Das GeschGehG sieht keine Anforderungen an den Informationsbegriff als solchen vor.¹⁴ Im Hinblick auf KI-Technologien kommen damit grundsätzlich sämtliche Informationen¹⁵ als mögliche Schutzgegenstände in Frage – unabhängig des Entwicklungsschrittes – sofern sie Gegenstand von Geheimhaltungsmaßnahmen sein können. Wie diese Geheimhaltungsmaßnahmen auszusehen haben, ist, wie eben dargelegt, im Einzelfall zu entscheiden. Da das GeschGehG nur belanglose Informationen nicht schützen möchte¹⁶, dürfte KI-Technologien durch den Geheimnischarakter stets wirtschaftlicher Wert zukommen und es besteht auch durchwegs ein berechtigtes Geheimhaltungsinteresse. Demnach erübrigt sich auch eine technologiespezifische Beantwortung dieser Frage.

I. KI-Technologien als Geheimnis

Im Hinblick auf KI-Technologien als Geschäftsgeheimnisse ist einerseits entscheidend, ob die KI-Anwendung lokal oder cloudbasiert angeboten wird. Läuft die Anwendung lokal ab, bedeutet dies, dass das Programm auf der Hardware der Nutzer:innen abläuft. Geschieht dies unverschlüsselt, ist der Maschinencode offen einsehbar. Beim Maschinencode handelt es sich zwar um einen binären Code und er ist damit für den Menschen nur sehr schwer bis gar nicht verständlich. Mittels Anwendung eines Dekompilierers lässt sich dieser Binär-code aber einfach in einen für den Menschen verständlichen Code umwandeln. Es ist deshalb fraglich, ob der Geheimnischarakter überhaupt vorliegt, wenn der Maschinencode offen einsehbar ist – wenn auch schwer bzw. nicht verständlich.¹⁷

¹⁴ BeckOK GeschGehG FUHLROTT/HIERAMENTE, § 2 Rn. 2 ff. m.w.N.

¹⁵ Technologieunabhängig: die Algorithmen iSv abstrakten Regeln, der Quell- sowie Maschinencodes der verschiedenen Programme, die Trainingsdaten(sätze); bei KNN: die Architekturen, die Gewichtungsinformationen, der Optimierungsalgorithmus, das untrainierte wie auch das trainierte Netz; bei GBA: der Builder-, Test- und der Zielalgorithmus (ebenso wie dessen Vorgänger); bei Expertenmaschinen: die Wissensbasis; vgl. auch MUHR, S. 92 ff.

¹⁶ Erwägungsgrund 13 der Know-How-Schutz-Richtlinie.

¹⁷ Siehe zum Begriff Decompiler (dt. Dekompilierer): MESSIER, S. 252 f. und GUSAROV, Applied Computer Systems 2018 (2), 109 ff.; Siehe für den umgekehrten Vorgang (Übersetzung Quell- in Zielprogramm) VDI-Informatiklexikon, S. 148 f.

Allgemein bekannt dürften die im Code enthaltenen Informationen bei KI-Technologien in der Regel nicht sein. Sodass die in KI-Technologien enthaltenen Geheimnisse gemäß § 2 Abs. 1 lit. a) GeschGehG dann nicht als Geheimnisse im Sinne des GeschGehG gelten, wenn sie „ohne Weiteres“ zugänglich sind. Mit anderen Worten ist also zu beurteilen, ob die Anwendung eines Dekompilierers noch als Handlung „ohne Weiteres“ gilt.

Der deutsche Gesetzestext ist wortgleich mit der deutschen Fassung von Art. 2 Abs. 1 lit. a) der Know-How-Schutz-Richtlinie. Der englische Richtlinienentwurf spricht von „*readily accessible*“, der französische von „*aisément accessibles*“. Daraus lässt sich ableiten, dass die Informationen nur dann nicht als Geheimnisse gelten, wenn sie (für eine Fachperson)¹⁸ leicht zugänglich sind.¹⁹ Dekompilierer sind auf dem Feld von Softwareentwickler:innen bekannt und im regen Gebrauch.²⁰ Dies spricht dafür, dass im Maschinencode enthaltene Information als leicht zugänglich gelten und somit über keinen Geheimnischarakter verfügen. Allerdings löst ein Dekompilierer nicht in jedem Fall den Maschinencode fehlerfrei auf.²¹ Verzerrte oder fehlerhafte Aufschlüsselungen können die Folge sein, welche dann wiederum aufgelöst werden müssen. Hinzu kommt, dass ein Dekompilierer zuerst programmiert bzw. erworben werden muss. Auch dies bedeutet Aufwand und spricht gegen eine leichte Zugänglichkeit. Schließlich ist darauf hinzuweisen, dass der dekompierte Programmcode nur funktional gleich ist wie der Quellcode und nicht identisch.²² Demnach gelten in Maschinencodeform codierte Informationen auch dann als Geheimnisse, wenn sie lokal auf der Hardware der Nutzer:innen vorliegen und mittels Dekompilierens in eine für Menschen lesbare Form übersetzt werden können

Dies gilt besonders für KI-Technologien wie KNN, bei welchen die Informationsverarbeitung implizit in Modellform erfolgt und nicht wie bspw. bei Exper-

¹⁸ Vgl. Art. 2 Abs. 1 lit. a): „[...] Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen“ oder im englischen Text „[...] persons within the circles that normally deal with the kind of information in question“.

¹⁹ Köhler/Bornkamm/Fedderson/ALEXANDER, GeschGehG, § 2 Rn. 36.

²⁰ Vgl. GUSAROVs, Applied Computer Systems 2018 (2), 109 ff.

²¹ MESSIER, S. 252 f.; GUSAROVs, Applied Computer Systems 2018 (2), 109 ff.

²² MESSIER, S. 252 f.; GUSAROVs, Applied Computer Systems 2018 (2), 109 ff.

tensystemen oder genetischen Programmen explizit. Bei einer modellhaften, impliziten Informationsverarbeitung stellt sich nämlich im ersten Schritt die Frage, was überhaupt als geheime Information gelten soll sowie wo und in welcher Form sie repräsentiert ist. Dieses Thema soll im Rahmen dieser Arbeit jedoch nicht vertieft werden.²³ Für das Verständnis reicht es, dass bei KNN die einzelnen Bestandteile als (geheime) Informationen gelten können, die im Kapitel 8 B.III. entsprechend einzeln untersucht wurden: die Trainingsdaten, das untrainierte Netz bzw. die Architektur, der Optimierungsalgorithmus, die Gewichtungsinformationen und das trainierte Modell. Bei genetischen Programmen und den Expertensystemen sind die (geheimen) Informationen weniger schwer zu lokalisieren, da beide KI-Technologien explizit, in Form von wenn-dann-Regelwerken repräsentiert sind

Werden KI-Technologien demgegenüber cloudbasiert angeboten, laufen sie nicht auf Endgeräten der Nutzer:innen ab. Diese haben demnach keinen Zugriff auf den Maschinencode und das Thema der Offenkundigkeit ergibt sich gar nicht erst.

Neben der grundsätzlichen Frage, ob KI-Technologien lokal oder cloudbasiert betrieben werden, bieten sich den Entwickler:innen noch weitere technische Schutzmaßnahmen zwecks Geheimniswahrung. Diese reichen von Kopierschutz über Verschlüsselungen bis zum Passwortschutz. Sie sind weitgehend technologieunabhängig und gelten sowohl für KNN wie auch für GBA und Expertensysteme.

II. Trainingsdaten als Geheimnis

Trainingsdaten und deren Qualität sind die Grundlage für gut funktionierende KNN oder für ein gut funktionierendes genetisches Programm. Bei Expertensystemen ist es technisch gesehen ungenau, von Trainingsdaten zu sprechen. Bei ihnen handelt es sich eher um „Wissensdaten“. Informationen, die bei Expert:innen erhoben werden und dann in die Wissensbasis von Expertensystemen implementiert werden. Aus Geschäftsgeheimnissicht gilt betreffend ihre Geheimhaltung Gleiches was auch für die Trainingsdaten gilt.

²³ Siehe für das Thema der Geheimnisse im Zusammenhang mit KNN ausführlich und vertieft LINHART, *passim*.

Die Bedeutung von Trainingsdaten für das Funktionieren eines KNN oder eines GBA widerspiegelt sich in deren monetären Wert.²⁴ Sie wurden im zweiten Kapitel sowie in Kapitel 8 B.III. als entscheidender Schritt für die Determinierung von KNN ausgemacht. Dies begründet ein besonderes Interesse am Schutz der Daten.

Sollen Trainingsdaten durch das GeschGehG geschützt sein, dürfen sie nicht allgemein bekannt sein. Es existieren Lernformen, die auf öffentlich zugängliche Daten wie bspw. Wissenszyklopädien oder gar soziale Plattformen²⁵ zurückgreifen – oft sind dies Formen des *unsupervised learnings*. Bei solchen Trainingsdaten ist klar, dass sie bereits aufgrund ihrer Bekanntheit nicht vom GeschGehG geschützt sein können. Abgesehen von solchen Beispielen dürften Trainingsdaten generell als Geschäftsgeheimnis iSv § 2 Nr. 1 GeschGehG gelten.²⁶ Auch öffentlich zugängliche Trainingsdaten können wieder Geheimnischarakter erlangen. Wenn öffentlich zugängliche Daten gesammelt und aufbereitet werden, stellen die aufbereiteten Daten potenzielle Geschäftsgeheimnisse dar. Die Geheimhaltung von Trainingsdaten kann mittels verschiedener technischer wie auch analoger Mitteln erfolgen. Sie reichen vom physischen Schutz des Datenträgers selbst²⁷ über dessen Verschlüsselung oder Passwortschutz bis hin zur Verschlüsselung der Trainingsdaten selbst.

Der Schutz der Trainingsdaten nutzt dem Inhaber in aller Regel aber nicht, wenn das Ergebnis des Trainings – die trainierte Technologie – schutzfrei bleibt, weil sie nicht geheim ist. Dies gilt gleichermaßen für KNN wie auch für genetische Programme: In einem solchen Fall ist ein:e potenzielle:r Konkurrent:in im Besitz dessen, was sie braucht. Mit anderen Worten interessieren die Trainingsdaten die kopierende Person wenig bis nicht, wenn sie im Besitz des fertigen und funktionsfähigen Programmes ist.²⁸

²⁴ Vgl. statt vieler HACKER, GRUR 2020, 1032.

²⁵ Ein Beispiel dafür ist ChatGPT.

²⁶ HACKER, GRUR 2020, 1032.

²⁷ Tresorraum für Server bzw. Tresor für Festplatte oder gar das Abschließen des Raumes, in welchem sich der Datenträger befindet.

²⁸ Darin liegt mit unter ein Grund, dass die fertigen und funktionsfähigen Programme zu einem großen Teil cloudbasiert angeboten werden, siehe dazu oben Kap. 6, C. und Kap. 6, D., III.

Die Gewichtungsinformationen bei den KNN können in gleicher Art und Weise Gegenstand des GeschGehG werden wie Trainingsdaten, da sie ebenfalls Daten sind.

III. Sperrige Natur der Geheimhaltungsmaßnahmen

Es sei daran erinnert, dass die besprochenen Geheimhaltungsmaßnahmen über die gesamte Wertschöpfungskette und darüber hinaus bis in die Anwendungsphase aufrechterhalten werden müssen. Nur so bleibt der Geheimnischarakter bestehen. Dies führt dazu, dass der Geschäftsgeheimnisschutz äußerst starr und „unhandlich“ ist. Man denke bspw. an die Situation eines Tech-StartUps oder eines KMUs in Investorengesprächen. Zwecks Vermarktung des Produktes (der KI-Technologie) muss dieses einerseits beworben und vorgestellt werden. Andererseits muss stetig darauf geachtet werden, dass das Geheimnis (die KI-Technologie oder Teile davon) nicht derart offengelegt werden, dass es nachgebaut werden kann. Es ist offensichtlich, dass dieser Umstand zur Erhöhung der Fix- und Transaktionskosten und damit zur Effizienzminderung führt.²⁹

IV. Gesetzliche Offenlegungspflichten als Hindernis?

In den jungen und aktuellen KI-Gesetzgebungsvorhaben der EU scheint die Tendenz erkennbar, dass Offenlegungspflichten zur Regel werden. Zumindest im Vorschlag der Kommission zur Regulierung von Künstlicher Intelligenz (AI-Act/AIA-Entwurf)³⁰ sind Offenlegungspflichten explizit vorgesehen. Art. 11 Abs. 1 AIA-Entwurf sieht die Pflicht vor, bei Hochrisiko-KI-Systemen eine technische Dokumentation zu erstellen. Diese technische Dokumentation ist sodann vor Inbetriebnahme des Systems den nationalen Behörden und den notifizierten Stellen zur Verfügung zu stellen

Anhang IV zum AIA-Entwurf spezifiziert den Inhalt dieser technischen Dokumentation: die Dokumentation muss unter anderem von den „Entwurfsspezifikationen des Systems, insbesondere die allgemeine Logik des KI-Systems und der Algorithmen“ über die „Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen oder einander zuar-

²⁹ Vgl. dazu oben Kap. 6, D., I., 3.

³⁰ Oben Kap.1.

beiten und in die Gesamtverarbeitung integriert sind; zum Entwickeln, Trainieren, Testen und Validieren des KI-Systems verwendete Rechenressourcen“ bis hin zu den „Trainingsmethoden und -techniken und die verwendeten Trainingsdatensätze(n)“ reichen. Wenn auch abzuwarten ist, wie die verlangten Informationen überhaupt dargestellt werden sollen, so ist doch deutlich, dass anhand der offenzulegenden Angaben durchaus ein Nachbau erfolgen kann.³¹

Mit anderen Worten erfolgt eine komplette Offenbarung, ohne dass im Gegenzug ein Ausschließlichkeitsrecht eingeräumt wird – wie das im Patentrecht etwa der Fall ist.³² Dennoch führt diese Offenlegungspflicht nicht zu einem Verlust des Geheimnischarakters. Denn Art. 33 Abs. 6 AIA-Entwurf verpflichtet die notifizierte Behörden zur Vertraulichkeit. Art. 33 Abs. 6 AIA-Entwurf stellt klar, dass diese Vertraulichkeitspflicht Mitarbeiter:innen, Ausschüsse, Zweigstellen, Unterauftragnehmer:innen sowie alle zugeordneten Stellen oder Mitarbeiter der notifizierte Behörden sowie externer Einrichtungen trifft. Diese Personen trifft gemäß AIA-Entwurf eine berufliche Schweigepflicht. Dennoch bleibt ein Restrisiko bestehen. Je mehr Personen mit einem Geheimnis in Berührung kommen, desto größer ist die Wahrscheinlichkeit, dass das Geheimnis an die Öffentlichkeit gelangt. Zwar ist die geheimnisbrechende Person in einem solchen Fall belangbar. Aber das GeschGebG schützt nicht vor Verwendung des Geheimnisses bei fahrlässiger Unkenntnis der gesetzwidrigen Geheimniserlangung (vgl. § 4 Abs. 3 GeschGebG). Das bedeutet, dass eine Person (B) das Geheimnis verwenden (und verwerten) darf, sofern sie das Geheimnis von der unerlaubterweise geheimnisverletzenden anderen Person (A) erlangte und sie (B) von dieser rechtswidrigen Erlangung nichts weiß und auch nichts wissen müsste.

Der Entwurf zum Data-Act sieht ebenfalls eine Offenlegungspflicht für Dateninhaber auf Verlangen von öffentlichen Behörden³³ vor. Art. 14 ff. DA-Entwurf bestimmen, dass Dateninhaber:innen bei bestimmten Voraussetzungen ihre Daten öffentlichen Behörden offenlegen müssen. Kleine Unternehmen und

³¹ Dies betrifft vor allem die Systemarchitektur, die verwendeten Algorithmen sowie die Logik der KI-Technologie zusammen mit den Trainingsdatensätzen.

³² Ob dies nun sinnvoll ist bzw. ob nicht diese Offenlegungspflichten ein Schutzrecht *de lege ferenda* zu rechtfertigen vermögen, ist nicht Teil dieser Dissertation.

³³ Dabei kann es sich gemäß Art. 14 DA –Entwurf um eine öffentliche Stelle, Organ, Einrichtung oder „eine[r] sonstige[n] Stelle der Union“ handeln.

Kleinstunternehmen sind gemäß Art. 14 Abs. 2 DA-Entwurf davon ausgenommen. Art. 19 Abs. 2 DA-Entwurf greift korrigierend ein: sollten sich unter den Daten Geschäftsgeheimnisse befinden, so müssen die Daten einschränkend erhoben werden bzw. im Umfang nur soweit dies für den Zweck des Verlangens unerlässlich ist. Weiter verpflichtet Art. 19 Abs. 2 DA-Entwurf die Behörde dazu, um die Vertraulichkeit des Geschäftsgeheimnisses besorgt zu sein. Demnach führt auch die Offenlegungspflicht im DA-Entwurf nicht zum Verlust des Geheimnischarakters. Dennoch bleibt auch beim DA-Entwurf dasselbe Restrisiko wie unter dem Titel des AIA-Entwurfes.

Auch der aktuelle Vorschlag der Europäischen Kommission für eine Richtlinie des europäischen Parlamentes und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstlicher Intelligenz (Richtlinie über KI-Haftung) sieht Offenlegungspflichten im Hinblick auf KI-Technologien vor (bspw. Art. 3 des Richtlinienvorschlages). Der Richtlinien-vorschlag sieht aber ebenfalls Vertraulichkeitsverpflichtungen vor (bspw. Art. 3 Abs. 4 des Richtlinienvorschlages), sodass der Geheimnischarakter trotz Offenlegung gewahrt bleibt. Jedoch bleibt auch hier das Restrisiko der unbefugten Offenbarung des Geheimnisses durch Beteiligte.

Es ist festzustellen, dass die aktuellen Gesetzesbestrebungen im Rahmen des Digitalisierungsrechts, v.a. auf europäischer Ebene, ein gewisses Risiko für den Geschäftsgeheimnisschutz betreffend den Schutz von KI-Technologien bzw. deren Einzelteilen mit sich bringen.

Es ist wünschenswert, dass der Fortlauf der Gesetzgebungsvorhaben ein Augenmerk auf diesen Umstand legt und das Risiko zu minimieren versucht. Allerdings liegt der Grund für dieses Risiko, wie sogleich aufgezeigt wird, im (schwachen) Geschäftsgeheimnisschutz nach GeschGehG, welcher kein absolut-rechtlicher ist.

C. Erlaubte Handlungen nach GeschGehG

Im Folgenden wird auf einzelne erlaubte Handlungen von Geschäftsgeheimnissen gemäß GeschGehG eingegangen. Es handelt sich dabei um Handlungen von

anderen Personen als dem Geheimnisinhaber. Die Ausführungen sollen deutlich machen, dass der Geschäftsgeheimnisschutz nach GeschGehG im Vergleich zu einem „echten“ Ausschließlichkeitsrecht deutlich schwächer ist – vor allem in der Anwendung auf KI-Technologien.

Diese Schwäche führt zur Lückenhaftigkeit des Schutzes. Diese Lückenhaftigkeit ergibt sich jedoch nur durch die Anwendung des GeschGehG als Lückenfüller zwischen verschiedenen Immaterialgüterrechten. Oft wird nämlich auf den Geschäftsgeheimnisschutz zurückgegriffen, wenn die Prüfung der „echten“ Immaterialgüterrechte negativ ausfällt. Wenn ein Werk/Gegenstand/Erfindung nicht nach UrhG, PatG, DesignG, etc. geschützt ist, soll das GeschGehG „durch die Hintertür“ aushelfen. Diese Schwäche des GeschGehG im Vergleich zu den „echten“ Immaterialgüterrechten ist leicht zu begründen. Ziel der Einführung der Know-How-RL war *nicht* die Einführung eines neuen Schutzrechtes,³⁴ sondern unter anderem und vor allem die unionsweite Vereinheitlichung des Geschäftsgeheimnisschutzes.³⁵ Die Whistleblower-Diskussionen brachten die Gesetzgebungsvorhaben zusätzlich voran.³⁶ Das GeschGehG hat somit durchaus seine Sinnhaftigkeit – jedoch nur solange es *nicht* als neues immaterialgüterrechtliches Schutzrecht herangezogen und verstanden wird.

I. Erlaubte Handlungen und ihre Auswirkungen auf die Natur des Geschäftsgeheimnisschutzes

Neben § 5 GeschGehG³⁷ zeigt sich vor allem in den Bestimmungen von § 3 GeschGehG, dass das GeschGehG kein Ausschließlichkeitsrecht einräumt. § 3

³⁴ Auch wenn das europäische Parlament in EG 2 Know-How-Richtlinie Geschäftsgeheimnisse (neben der Ergänzung von-) durchaus als Alternative zu Rechten des geistigen Eigentumes sieht, wird in EG 16 Know-How-Richtlinie ausdrücklich festgehalten, dass die Know-How-Richtlinie „keine Exklusivrechte an als Geschäftsgeheimnis geschütztem Know-how oder als solchem geschützten Informationen begründen“ soll; BT-Drucksache, 19/4724, 25: „[...] Geschäftsgeheimnisse [werden] nicht völlig der Gemeinfreiheit entzogen und ihrem Inhaber mit Wirkung gegenüber jedermann zugeordnet, sondern es wird lediglich ein bestehender Zustand rechtlich abgesichert“.

³⁵ EG 6 ff. Know-How-Richtlinie.

³⁶ EG 18 ff. Know-How-Richtlinie, vgl. auch OHLY, GRUR 2019, 442.

³⁷ § 5 GeschGehG kann auch als whistleblower-Paragraph angesehen werden. Er regelt die Erlangung, Nutzung oder Offenbarung eines Geschäftsgeheimnisses zum Schutz eines berechtigten Interesses.

Abs. 1 GeschGehG erlaubt die Erlangung von Geschäftsgeheimnissen insbesondere durch:

- eigenständige Entdeckung oder Schöpfung (§ 3 Abs. 1 Nr. 1 GeschGehG);
- ein Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der
 - öffentlich verfügbar gemacht wurde (§ 3 Abs. 1 Nr. 2 lit. b GeschGehG) oder
 - sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt (§ 3 Abs. 1 Nr. 2 lit. b GeschGehG);
- ein Ausüben von Informations- und Anhörungsrechten der Arbeitnehmer:innen oder Mitwirkungs- und Mitbestimmungsrechte der Arbeitnehmervertretung (§ 3 Abs. 1 Nr. 3 GeschGehG).

Im Gegensatz zu § 3 Abs. 2 GeschGehG erlaubt § 3 Abs. 1 GeschGehG nur das *Erlangen* von Geschäftsgeheimnissen. § 3 Abs. 2 GeschGehG erlaubt darüber hinaus ausdrücklich auch die Nutzung und die Offenlegung des Geschäftsgeheimnisses. Aus der rechtmäßigen Erlangung nach § 3 Abs. 1 GeschGehG wird sich jedoch regelmäßig auch die Zulässigkeit einer nachfolgenden Nutzung und Offenlegung ableiten lassen.³⁸ Die nachfolgende Nutzung und Offenlegung kann jedoch nach § 4 Abs. 2 Nr. 2 bzw. Nr. 3 GeschGehG eingeschränkt sein

Zu denken ist dabei unter anderem an schuldrechtliche Verbote – individualvertraglicher Natur oder in Form von AGB. Selbstredend müssen solche Klauseln einer Inhaltskontrolle standhalten, was hier jedoch nicht weiter vertieft werden soll. Verglichen mit einem absoluten Ausschließlichkeitsrecht ist aber ein solches relatives Verbot deutlich schwächer. Nicht zuletzt aufgrund von § 4 Abs.

³⁸ BT-Drucksache, 19/4724, 25; Harte-Bavendamm/OHLY/Kalbfus, GeschGehG, § 3 Rn. 2; Heermann/Schlingloff/KAMLAH, GeschGehG, § 3 Rn. 1; etwas unbestimmt: Keller/SCHÖNKNECHT/Glinke, GeschGehG, § 3 Rn. 2.

3 GeschGehG. § 4 Abs. 3 GeschGehG verbietet die (mittelbare) Erlangung, Nutzung und Offenlegung eines Geheimnisses durch eine Person über eine andere Person nur dann, wenn die erstere im Zeitpunkt der Erlangung, Nutzung oder Offenbarung wusste und auch hätte wissen müssen, dass letztere das Geheimnis unrechtmäßig (entgegen § 4 Abs. 2 GeschGehG) genutzt oder offengelegt hatte. Angewandt auf ein vertragsrechtliches Verbot der Nutzung oder Offenlegung bedeutet das also: Eine Person (A) erlangt das Geheimnis durch eine Handlung nach § 3 Abs. 1 GeschGehG erlaubterweise. Danach nutzt diese Person (A) das Geheimnis oder legt es offen, obwohl der Nutzung oder Offenlegung individual- oder allgemeinvertragliche Vorschriften entgegenstehen. Eine andere Person (B) erlangt durch diese Vertragsverletzung der ersten Person (A) das Geheimnis. Solange jene Person (B) von der Vertragsverletzung durch Person (A) nichts wusste und auch nichts hätte wissen müssen, darf sie es selbst erlangen, nutzen und offenlegen. Der Geheimnisinhaber kann also nur gegen die Nutzung und Offenlegung von Person (A) vorgehen – nicht aber gegen die Handlungen der Person (B).

Schließlich kann die Nutzung und Offenlegung von Geschäftsgeheimnissen auch spezialgesetzlich erlaubt sein. Wesentlich im Zusammenhang mit dieser Arbeit ist, dass das Geschäftsgeheimnis nach § 3 Abs. 1 GeschGehG regelmäßig nicht bloß erlangt, sondern auch genutzt und offengelegt werden darf.

§ 3 Abs. 1 Nr. 2 GeschGehG erlaubt das sogenannte *reverse engineering*: Das Erlangen eines Geschäftsgeheimnisses durch Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands. Diese Erlaubnis zum *reverse engineering* in § 3 Abs. 1 Nr. 2 GeschGehG ist aus deutscher Sicht neu und in der Anwendung des GeschGehG auf KI-Technologien besonders relevant.³⁹ Es existieren durch das nun erlaubte *reverse engineering* verschiedene Möglichkeiten, um bspw. als Konkurrent:in erlaubterweise an ein der KI-Technologie inhärentes Geschäftsgeheimnis⁴⁰ zu gelangen. Diese Geschäftsgeheimnisse können Modelle, Architekturen, Algorithmen, Gewichtungsinformationen oder

³⁹ OHLY, GRUR 2019, 447.

⁴⁰ Je nach Technologie kann es sich dabei um die (untrainierte) Netzstruktur, das trainierte KNN, die weights oder den gesamten Programmablauf mit Algorithmus, etc. handeln.

aber auch zum Teil Trainingsdaten sein.⁴¹ Auf die Möglichkeiten des *reverse engineering*s von KI-Technologien wird weiter unten genauer eingegangen.⁴²

Besonderes Augenmerk betreffend das *reverse engineering* verdient § 3 Abs. 1 Nr. 2, zweiter Halbsatz GeschGehG. Dieser stellt die Erlaubnis des *reverse engineering*s unter den Vorbehalt, dass die rückbauende Person keiner Pflicht zur Beschränkung der Erlangung des Geheimnisses steht. Das heißt, dass das *reverse engineering* nur erlaubt ist, wenn es nicht vertraglich ausgeschlossen ist.

Ein solcher Ausschluss kann entweder individuell- oder allgemeinvertraglich ausgestaltet sein. Selbstverständlich müssen solche Klauseln auch gültig sein, was bspw. bei einem in AGB vorgesehen Verbot für ein frei auf dem Markt vertriebenem Produkt aufgrund von § 307 Abs. 2 Nr. 1 BGB zumindest zweifelhaft wäre.⁴³ Doch auch bei einer vertraglichen Beschränkung besteht das Risiko der (rechtmäßigen) fahrlässigen Erlangung von der geheimnisbrechenden Person.

Der fehlende absolut-rechtliche Charakter des Geschäftsgeheimnisschutzes zeigt sich zusammengefasst also darin, dass:

- das Gesetz mit § 3 GeschGehG eine Reihe von Handlungen vorsieht, mit welchen ein Geschäftsgeheimnis erlangt, genutzt und offengelegt werden darf. Die vorgesehenen Handlungen sind nicht abschließend aufgelistet;
- die Erlangung des Geschäftsgeheimnisses (inkl. nachfolgender Nutzung und/oder Offenlegung) über eine andere Person in fahrlässiger Unkenntnis der gesetzwidrigen Geheimniserlangung dieser Person erlaubt ist (vgl. § 4 Abs. 3 GeschGehG);

Auch an § 9 GeschGehG zeigt sich, dass das GeschGehG kein Ausschließlichkeitsrecht einräumt. Gemäß § 9 GeschGehG steht der Unterlassungsanspruch des Geheimnisinhabers unter einem Verhältnismäßigkeitsvorbehalt und ist damit – anders als bei absoluten Rechten – bedingt.

⁴¹ Siehe oben Kap. 9, B., I.

⁴² Siehe unten Kap. 9, C., II., 1.

⁴³ Siehe dazu ausführlicher OHLY, GRUR 2019, 447 f.

Bereits an dieser Stelle sei vorweggeschickt, dass das GeschGehG die Rolle als Lückenfüller für die weder durch das Urheber- noch durch das Patentrecht geschützten KI-Technologien (bzw. deren Bestandteile) nur in schwacher Form ausfüllen kann. Dies ist dem Umstand geschuldet, dass der Geschäftsgeheimnisschutz kein Exklusivrecht einräumt. In Anwendung auf die KI-Technologien bietet besonders das erlaubte *reverse engineering* ein Risiko für den Geheimnissinhaber der konkurrenzseitigen (unbefugten) Erlangung des Geschäftsgeheimnisses. Dies liegt in den technischen Gegebenheiten der KI-Technologien begründet. Zudem stehen Konkurrent:innen technische Maßnahmen zur Verfügung, die das Erlangen von KI-Technologien und deren Bestandteilen zugrunde liegenden Geschäftsgeheimnissen besonders vereinfachen. Dies wird unter nachfolgendem Titel genauer erläutert.

II. *Reverse Engineering im Besonderen*

In Kapitel 6 wurde aufgezeigt, dass KI-Technologien entweder lokal auf dem Endgerät der Nutzer:innen ablaufen können oder aber unabhängig vom Endgerät als Cloudlösung. In einem ersten Schritt werden nun die technischen Möglichkeiten erläutert, wie Konkurrent:innen mittels *reverse engineering*s an die Geschäftsgeheimnisse gelangen, die lokal ablaufenden KI-Anwendungen innewohnen.

1. *Reverse Engineering von lokalen KI-Anwendungen*

Bei genetischen Programmen ist der Maschinencode des Ziel-Programmes offen einsehbar. Der Maschinencode ist allerdings für den Menschen nicht verständlich bzw. nur sehr begrenzt nachvollziehbar. Durch Anwendung eines Dekompilierers lässt sich der Maschinencode leicht in den für Menschen les- und nachvollziehbaren Quellcode rückübersetzen. Gleiches gilt für die Einzelteile der Inferenzmaschine bei Expertensystemen. Allerdings ist diese ohne die Wissensbasis funktionsunfähig. Wird die Wissensbasis also nicht auch lokal auf dem Endgerät der Nutzer:innen zur Verfügung gestellt, sondern cloudbasiert, verlieren die Entwickler:innen das Geschäftsgeheimnis nicht gänzlich bzw. nicht in einer funktionsfähigen Art und Weise. Weil die Nutzer:innen nach wie vor noch auf die ihnen nicht lokal zur Verfügung stehende Wissensbasis angewiesen sind.

Die in ihrer Struktur komplexen KNN lassen sich mit einem gewissen technischen Aufwand ebenfalls simpel aus lokalen Anwendungen extrahieren. So kann bspw. das trainierte Modell, welches *Apples NeuralHash*-Programm verwendet, relativ einfach extrahiert werden, indem ein Dekompilierer angewendet wird.⁴⁴ Ein so extrahiertes Modell kann anschließend beliebig verwendet werden. Das extrahierte Netz ist voll funktionsfähig. Es lässt sich sogar durch Anwendung neuer Trainingsdaten umfunktionieren bzw. weiterverbessern.⁴⁵ Mit anderen Worten verlieren die Entwickler:innen so ihr Geschäftsgeheimnis.⁴⁶

Die Trainingsdaten sowie der Optimierungsalgorithmus sind in solchen Fällen zwar nicht direkt extrahierbar.⁴⁷ Das spielt für die Nutzer:innen aber keine Rolle, sofern es ihnen nur um das Kopieren oder Nachbauen des KNN geht. Weder der Optimierungsalgorithmus noch die Trainingsdaten sind bei einem trainierten Modell in der Anwendung noch notwendig für einen funktionsfähigen Ablauf⁴⁸ – außer das Modell soll sich in der Anwendung weiter anpassen. Nur in einem solchen Fall wird der bzw. ein Optimierungsalgorithmus weiterhin benötigt. Es muss sich dabei aber nicht zwingend um den gleichen Optimierungsalgorithmus handeln, der auch schon in der Entwicklung des KNN eingesetzt wurde. Die kopierende Person kann auch einen selbst gewählten oder selbst programmierten Optimierungsalgorithmus anwenden.⁴⁹ Das Extrahieren bzw. das *reverse engineering* des Optimierungsalgorithmus wäre zwar durch das GeschGehG erlaubt. Allerdings ist der Optimierungsalgorithmus in aller Regel ein

⁴⁴ Eine einfache und verständliche Anleitung dazu findet sich unter <https://github.com/AsuharietYgvar/AppleNeuralHash2ONNX>, zuletzt besucht am 9. Mai 2023.

⁴⁵ Ebenda.

⁴⁶ Vgl. dazu soeben Kap. 9, B., I.

⁴⁷ Zu den einzelnen Methoden, diese aus cloudbasierten Anwendungen zu extrahieren, siehe unten Kap. 9, C., II., 2.

⁴⁸ Dies lässt sich anhand des GPT2-Modells von OpenAI zeigen. Es handelt sich um eine OpenSource-Anwendung, bei der das Trainingsdatenset sowie die Details zum Training und damit auch der Optimierungsalgorithmus nicht veröffentlicht werden, <https://openai.com/blog/better-language-models/>, zuletzt besucht am 9. Mai 2023.

⁴⁹ <https://towardsdatascience.com/how-to-fine-tune-gpt-2-for-text-generation-ae2ea53bc272>, zuletzt besucht am 9. Mai 2023, so wurde hier bspw. ein selbst gewählter Optimierungsalgorithmus wieder das OpenSource GPT2-Modell angewandt. Die ursprünglich sehr allgemeine Textgenerierungsanwendung wurde zur Songtextgenerierung umtrainiert.

urheberrechtlich geschütztes Werk.⁵⁰ Demnach stellt das Extrahieren des Optimierungsalgorithmus ohnehin eine urheberrechtsverletzende Handlung dar.⁵¹ Um keine Urheberrechte zu verletzen, ist also ein anderer oder gar ein eigens programmierter Optimierungsalgorithmus anzuwenden.⁵²

Neben der Anwendung von Dekompilierern zur Extraktion des kompletten, bzw. trainierten KNN, lassen sich durch weitere technische Mittel auch die Architektur des (untrainierten) KNN sowie die Gewichtungsinformationen (*weights*) extrahieren.⁵³ Anhand dieser beiden Komponenten lässt sich dann auch das trainierte KNN nachbauen, ohne dass dieses selbst vorliegen muss.

Den Entwickler:innen von KI-Technologien stehen daher im Falle eines lokalen Ablaufes lediglich die technischen Schutzmaßnahmen zur Verfügung, die wir aus der „herkömmlichen“ Programmierung schon kennen. Zu diesen zählen Kopierschutz, Verschlüsselung⁵⁴, Speicherung des Modells auf einem speziell geschützten Chip, etc. Solche lassen sich aber mit mehr oder minder großem technischen Aufwand ebenfalls umgehen, was wiederum Rückbau im Sinne von § 3 Abs. 1 Nr. 2 GeschGehG darstellt.⁵⁵

Man mag einwenden, dass das Umgehen technischer Schutzmaßnahmen genauso wie das Anwenden eines Dekompilierers im Vergleich zu „herkömmlichen“ Programmiermethoden nichts Neues ist. Der Gesetzgeber trägt diesen technischen Umständen mit § 69e UrhG sowie § 108b UrhG sogar explizit Rechnung. In § 69e UrhG wird das Dekompilieren grundsätzlich verboten bzw. die zulässige Verwendung eines Dekompilierers auf Zwecke der Herstellung der Interoperabilität⁵⁶ eingeschränkt. § 108b UrhG stellt die Umgehung technischer

⁵⁰ Siehe dazu oben Kap. 8, B., III., 4.

⁵¹ Siehe dazu sogleich.

⁵² Vgl. oben Kap. 2, C., II. 3. zur technischen Bedingtheit von Optimierungsalgorithmen und dem damit einhergehenden eher geringen Schutzzumfang.

⁵³ <https://machinethink.net/blog/peek-inside-coreml/>, zuletzt besucht am 9. Mai 2023.

⁵⁴ <https://docs.microsoft.com/en-us/windows/ai/windows-ml/tutorials/advanced-tutorial-encryption>, zuletzt besucht am 9. Mai 2023.

⁵⁵ Vgl. OHLY, GRUR 2019, 447.

⁵⁶ Die Richtlinie 91/250/EWG des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen (Software-RL) definiert in EG 12 Interoperabilität als „als die Fähigkeit zum

Schutzmaßnahmen generell unter Strafe. Der entscheidende Punkt ist aber, dass das Ziel-Programm beim genetischen Programmieren und sowohl das untrainierte als auch das trainierte KNN bei den neuronalen Netzen nicht vom Urheberrecht geschützt sind.⁵⁷ Dieser Umstand lässt die Anwendungsbereiche von § 69e UrhG und von § 108b UrhG gar nicht erst eröffnen.

Mit anderen Worten ist im Falle der KNN wie auch der genetischen Programme das Umgehen technischer Schutzmaßnahmen und das Dekompilieren rechtmäßig, sofern keine urheberrechtlich geschützten Bestandteile dekompiert werden. Einzig beim Optimierungsalgorithmus (KNN), der Programmierung zwecks Generierung von Individuen und der Fitnessfunktion (genetische Programmierweise) sowie der Inferenzmaschine bei Expertensystemen handelt es sich um urheberrechtlich geschützte Werke. Damit ist das Rückbauen oder Umgehen der technischen Schutzmaßnahmen dieser Komponenten zwar nach § 3 Abs. 1 Nr. 2 GeschGehG, nicht aber nach Urheberrechtsgesetz erlaubt.

Aus Sicht der nachbauenden Person stellt dies aber kein Problem dar – zumindest nicht bei genetischen Programmen und KNN. Wie oben gesehen, wird bei KNN der Optimierungsalgorithmus nicht für die Anwendung des kopierten Modells benötigt.⁵⁸ Bei genetischen Programmen gilt für die Programmumgebung- und Fitnessfunktion Analoges. Es reicht in diesem Fall, dass das Ziel-Programm extrahiert bzw. nachgebaut werden kann, ohne urheberrechtlich geschützte Komponenten zu verwenden.

Wird der Geheimnischarakter auch bei lokalen Anwendungen bejaht oder durch spezielle Maßnahmen gewahrt, steht der rechtmäßigen Erlangung (und Nutzung sowie Offenlegung), vor allem durch *reverse engineering*, nichts im Wege. Das GeschGehG erlaubt die Erlangung der speziell geschützten Geheimnisse nach § 3 Abs. 1 Nr. 2 GeschGehG.

Austausch von Informationen und zur wechselseitigen Verwendung der ausgetauschten Informationen“ sowohl zwischen Software und Software als auch zwischen „Software und Hardware mit anderer Software und Hardware und Benutzern“ (EG 10 Software-RL).

⁵⁷ Vgl. oben Kap. 8, B. III., Kap. 8., B., III., 1., Kap. 8., B., III., 2., c).

⁵⁸ Siehe Kap. 2, C., II. 3.

Zusammenfassend ist festzuhalten, dass die Anwendung des GeschGehG auf KI-Technologien ins Leere läuft, sofern die Technologien lokal auf dem Endgerät der Nutzer:innen ablaufen. Durch das in § 3 Abs. 1 GeschGehG erlaubte *reverse engineering* können die für das Kopieren der KI-Technologien notwendigen Geschäftsgeheimnisse rechtmäßig erlangt werden. Sofern keine gültigen – vor allem vertraglichen – Verbote entgegenstehen, können die Geschäftsgeheimnisse erlangt, genutzt und offengelegt werden.

2. Reverse Engineering von cloudbasierten KI-Anwendungen am Beispiel von neuronalen Netzen

Das Geschäftsgeheimnis lässt sich aber auch mittels *reverse engineerings* erlangen, wenn die KI-Anwendung cloudbasiert angeboten wird. In solchen Fällen ist der technische Aufwand des Rückbaus allerdings höher als bei lokal ablaufenden Anwendungen.

Läuft die KI-Anwendung cloudbasiert ab, verarbeitet das Endgerät der Nutzer:innen die Anwendung nicht selber. Vielmehr werden über eine Applikation, die die Nutzer:innen bedienen, Anfragen an einen Webbrowser oder eine *API* gesendet. Der Webbrowser bzw. die *API* fungiert dabei als Mittelstelle. Sie leitet die Anfrage an die KI-Technologie weiter, die dann die Anfrage verarbeitet und die Ausgabe generiert.⁵⁹ Selbstverständlich läuft die KI-Technologie als solche auch auf einer Hardwarekomponente ab. Diese ist aber aus Sicht der Nutzer:innen unbekannt bzw. dezentral – im Herrschaftsbereich der Anbieter:innen. Die Ausgabe wird dann wieder über Webbrowser bzw. *API* an die Applikation auf dem Endgerät der Nutzer:innen geleitet.⁶⁰ Ein Beispiel für eine cloudbasiert angebotene KI-Technologie sind die *Amazon Web Services (AWS)* von *Amazon*.⁶¹

Vorteil aus Sicht der Entwickler:innen und Anbieter:innen ist bei einer solchen Lösung, dass der Maschinencode der eigentlichen Anwendung nicht auf dem Endgerät der Nutzer:innen abläuft. Auf diesen laufen nur die Codes der Applikation ab, die mit dem Webbrowser bzw. der *API* kommuniziert. Wenn der Ma-

⁵⁹ Vgl. auch oben Kap. 6, C.

⁶⁰ Siehe bereits oben Kap. 6, C.

⁶¹ <https://aws.amazon.com/de/machine-learning/>, zuletzt besucht am 9. Mai 2023.

schinencode nicht offen bzw. direkt einsehbar ist, ist auch das *reverse engineering* nicht mehr so leicht möglich wie bei den eben dargestellten lokalen Anwendungen.

Auch bei cloudbasierten KNN ist es möglich, die für einen Nachbau notwendigen Informationen via *reverse engineering* zu erlangen. Nachfolgend werden verschiedene Ansätze des *reverse engineering*s von cloudbasierten KNN aufgezeigt. So soll ein konkretes Verständnis von den Ansätzen, Möglichkeiten und notwendigen Ressourcen geschaffen werden.

Obwohl die KNN betreffend ihre Architektur, den Optimierungsalgorithmus und das Trainingsdatenset eine *Black-Box* darstellen, ist es mittels *reverse engineering*s möglich, eben diese Informationen zu erlangen. Es bestehen verschiedene Möglichkeiten – je nachdem, was vom „Ziel-KNN“ bekannt ist, wie schnell die Modellextraktion erfolgen soll und was die Ressourcen sind.

In einem Versuch des Max-Planck-Instituts Saarbrücken verwenden JOON OH/AUGUSTIN/SCHUELE/FRITZ sog. Metamodelle, um ein KNN anzugreifen.⁶² Das KNN, welches angegriffen werden soll, ist ein Bild-Klassifizierungsmodell. Die Metamodelle sind selbst auch Klassifizierungsmodelle. Sie sollen das Ziel-KNN klassifizieren bzw. testen und versuchen, die Ausgaben des Ziel-KNNs selbst korrekt vorherzusagen und damit dessen Funktionalität kopieren. Vereinfacht ausgedrückt werden ca. 10'000 schwache Modelle trainiert (sog. *low-performance classifiers* mit einer Genauigkeit von unter 98%). Vorteil dieser *low-performance classifiers* ist ihre kurze Trainingsdauer. Sie beträgt für ein Modell lediglich 5 Minuten.⁶³ Die Grundarchitektur dieser Modelle (untrainierte Netze) ist untereinander zwar jeweils ähnlich bis gleich. Sie werden aber mit unterschiedlichen Optimierungsalgorithmen und verschiedenen generischen Datensets trainiert. Damit soll Diversität zwischen den *low-performance classifiers* erreicht werden.⁶⁴ Diese *low-performance classifiers* sollen dann als Datensatz für das eigentliche Metamodell dienen, welches die Funktionalität des Ziel-KNN imitiert. Das Training der angestrebten 10'000 kleinen Modelle⁶⁵ und damit der

⁶² JOON OH/AUGUSTIN/SCHUELE/FRITZ, ICLR 2018, 2.

⁶³ JOON OH/AUGUSTIN/SCHUELE/FRITZ, ICLR 2018, 3.

⁶⁴ JOON OH/AUGUSTIN/SCHUELE/FRITZ, ICLR 2018, 3.

⁶⁵ Effektiv waren es 11'282 Modelle.

Datensatzerstellung dauert 40 GPU-Tage^{66,67} Die trainierten Modelle sollen die Ausgaben des Ziel-KNN korrekt voraussagen. Dies wird erreicht, indem ihr Output mit demjenigen des Ziel-KNN beim selben Input verglichen wird. Dabei reichen gemäß JOON OH/AUGUSTIN/SCHIELE/FRITZ bereits 100 sogenannte single-label Inputs, um die wichtigsten Informationen aus dem Ziel-KNN zu extrahieren.⁶⁸ Noch vereinfachter gesagt, wird mit der besprochenen Methode das cloudbasierte Modell angewandt und anhand der Outputs werden Rückschlüsse auf die Funktionsweise des Modelles gezogen. Um sinnvolle Rückschlüsse ziehen zu können, erfolgt das automatisiert mittels selbst trainierten *low-performance classifiers* – die dann als Datensetze für das eigentliche Metamodell dienen. Gemäß JOON OH/AUGUSTIN/SCHIELE/FRITZ können mit *dieser trial-and-error* Methode die Architektur (das untrainierte Netz), der Optimierungsalgorithmus sowie sogar das Trainingsdatenset extrahiert werden. Mit dem von JOON OH/AUGUSTIN/SCHIELE/FRITZ beschriebenen Ansatz lassen sich also sämtliche für einen Nachbau wesentliche Informationen aus einem „verdeckten“ KNN extrahieren.⁶⁹ Verdeckt sind die KNN, weil sie gänzlich cloudbasiert ablaufen und auf dem Endgerät der Nutzer:innen keine relevanten Informationen des KNN einsehbar sind bzw. gar gespeichert werden. Allerdings stellt die Anwendung des Optimierungsalgorithmus eine urheberrechtlich relevante Handlung dar⁷⁰ – weshalb auf einen selbst programmierten oder funktional ähnlichen frei verfügbaren Optimierungsalgorithmus zurückgegriffen werden dürfte bzw. sollte.⁷¹ Sofern es sich – ausnahmsweise – um urheberrechtlich geschützte Trainingsdaten handeln sollte, ist ein Ausweichen nicht mehr möglich und der Nachbau ist deutlich erschwert, weil eigene Trainingsdaten angewandt werden müssen.

⁶⁶ Die Einheit „*GPU day*“ bezeichnet die Anzahl Tage multipliziert mit der Anzahl verwendeter GPUs, also Grafikprozessoren. Selbstredend ist die Rechendauer abhängig von der Leistungsfähigkeit des verwendeten GPU. Im besprochenen Beispiel wurden *GeForce GTX TITAN*-Grafikprozessoren verwendet.

⁶⁷ JOON OH/AUGUSTIN/SCHIELE/FRITZ, ICLR 2018, 4.

⁶⁸ JOON OH/AUGUSTIN/SCHIELE/FRITZ, ICLR 2018, 9.

⁶⁹ JOON OH/AUGUSTIN/SCHIELE/FRITZ, ICLR 2018, 9.

⁷⁰ Vgl. Kap. 8, B., III., 4. zur Schutzfähigkeit des Optimierungsalgorithmus.

⁷¹ Unter Kap. 9, C. II., 1. wurde gezeigt, dass mit alternativen Optimierungsalgorithmen untrainierte KNN mit demselben Trainingsdaten zu funktional gleichwertigen trainierten KNN (um)trainiert werden können.

Neben Ansätzen wie derjenige von JOON OH/AUGUSTIN/SCHIELE/FRITZ, welche darauf abzielen, das Modell bzw. dessen Funktionalität soweit möglich *exakt* nachzubauen, existieren Ansätze, bei denen ein *funktional ähnliches* Modell extrahiert werden soll. Solche Ansätze versuchen, ein sog. *avatar model* zu konstruieren.⁷² Diese Methode wird auch verwendet, um nicht-neuronale Modelle zu extrahieren. Der Ansatz beruht eher auf Annahmen anstatt exakter Nachbildung durch Voraussagen.⁷³ Voraussetzung dafür ist aber, dass die Architektur bzw. das untrainierte KNN bekannt ist (*white-box*). Diese Architektur wird anschließend anhand der Input-Output-Regeln des Ziel-KNN so trainiert, dass es die Funktionalität des Ziel-KNN erreicht. Dies wird erzielt, indem die Input-Daten (bspw. Bilder) in ihrer Datenstruktur verändert werden.⁷⁴ Diese Veränderung ist bspw. bei einem Bild für das menschliche Auge nicht erkennbar. Hier zeigt sich auch der grundlegende Unterschied zum Ansatz von JOON OH/AUGUSTIN/SCHIELE/FRITZ. Dieser ist dazu in der Lage, selbst die Grundstruktur bzw. das untrainierte KNN sowie die Trainingsparameter (Trainingsdaten und Optimierungsvorgänge, nicht aber die Gewichtungsinformationen) vorauszusagen bzw. „zu extrahieren“. Beim *avatar* Ansatz werden bloß Annahmen zu der Grundstruktur, den Trainingsdaten und den Trainingsoptimierungen getroffen. Die avatar-Methode ist also ungenauer.⁷⁵

Die *membership inference* Methode wird dazu benutzt, zu prüfen, ob ein Datum Teil des Trainingsdatensets war.⁷⁶ Die Methode kann aber auch dazu verwendet werden, Trainingsdaten aus Modellen zu extrahieren. ATENIESE/FELICI/MACINI/SPOGNARDI/VILLANI/VITALI konnten die Trainingsdaten aus verschiedenen KI-Technologien extrahieren, indem sie ein Metamodell basierend auf einem Entscheidungsbaum nutzten. Sie konnten die

⁷² PAPERNOT/MCDANIEL/GOODFELLOW/JHA/CELIK/SWAMI, 506 ff.

⁷³ PAPERNOT/MCDANIEL/GOODFELLOW/JHA/CELIK/SWAMI, 509.

⁷⁴ PAPERNOT/MCDANIEL/GOODFELLOW/JHA/CELIK/SWAMI, 508 ff; dieser Ansatz ist vor allem von sog. *adversarial attacks* bekannt.

⁷⁵Vgl. zu den einzelnen Erfolgsquoten PAPERNOT/MCDANIEL/GOODFELLOW/JHA/CELIK/SWAMI, 510, 517.

⁷⁶ Vgl. stellvertretend MIRESHGHALLAH/GOYAL/UNIYAL/BERG-KIRKPATRICK/SHOKRI, 1.

Trainingsdaten aus KNN, *support vector machines*, *k-means* und *Hidden-Markov*-Modellen extrahieren, die nicht lokal vorlagen.⁷⁷

Die *membership inference* Methode kann nur dazu dienen, die Trainingsdaten zu extrahieren. Die *avatar* Methode verfolgt einen Ansatz, bei welchem ausgehend von einem offen vorliegenden untrainierten KNN (oder ein dazu funktional ähnliches) lediglich Annahmen getroffen werden durch einen steten Vergleich mit den input-Output-Paaren des Ziel-KNN. So sollen bei dieser Methode Rückschlüsse auf die Trainingsdaten und Optimierungsinformationen gezogen werden. Ergebnis der *avatar* Methode ist also ein funktional ähnliches Modell wie das Ziel-KNN. Demgegenüber werden mit dem Ansatz von JOON OH/AUGUSTIN/SCHUELE/FRITZ die Architektur (untrainiertes KNN), die Trainingsdaten sowie der Optimierungsalgorithmus *exakt* extrahiert. Das so extrahierte untrainierte KNN kann anhand der Trainingsdaten und des Optimierungsalgorithmus zu einem identischen, fertig trainierten Modell wie das Ziel-KNN trainiert werden. Dieser Trainingsschritt stellt nicht nur einen Zusatzaufwand dar. Die Konkurrenz, die einen Nachbau des Modells zum Ziel hat, muss aber bei allen Methoden darauf achten, keine Urheberrechte betreffend den Optimierungsalgorithmus zu verletzen. Dies lässt sich verhältnismäßig einfach umsetzen, indem ein selbst programmierter Optimierungsalgorithmus auf das untrainierte KNN angewandt wird. Gleiches kann auch mit einem frei verfügbaren Optimierungsalgorithmus erreicht werden. Solange die Trainingsdaten schutzfrei sind,⁷⁸ stellen sich keine weiteren Probleme beim Nachbau. Sind die Trainingsdaten allerdings geschützt, ist der Nachbau mittels eigenständigen Trainings umständlicher. Deshalb dürften sich *reverse engineering* Ansätze durchsetzen, bei welchen sich direkt die Trainingsergebnisse (die Gewichtungsinformationen bzw. die *weights*) sowie die schutzfreie Architektur extrahieren

⁷⁷ ATENIESE/FELICI/MANCINI/SPOGNARDI/VILLANI/VITALI, IJSN 2015, 137 ff., insb. 140: "Such technique requires no access to the potentially obfuscated software since the attack is performed in a black-box fashion."; vgl. zur Thematik der Trainingsdatenextraktion mittels *membership inference* Methode auch die Untersuchungen von CARLINI/JAGIELSKI/ZHANG/PAPERNOT/TERZIS/TRAMER; MIRESHGHALLAH/GOYAL/UNI-YAL/BERG-KIRKPATRICK/SHOKRI.

⁷⁸ Vgl. oben Kap. 8, B., V.

lassen. Wie gesehen reicht es, die *weights* auf ein untrainiertes KNN anzuwenden, um das trainierte KNN zu kopieren. Eine solche Methode wird nachfolgend vorgestellt.

TRAMER/ZHANG/JUELS/REITER/RISTENPART beschreiben verschiedene Verfahren, mit welchen sie cloudbasierte KI-Technologien „attackieren“⁷⁹. Sie zeigen, wie sie mit unterschiedlichen Methoden verschiedene KI-Technologien aus cloudbasierten Anwendungen extrahieren. Dabei funktionieren ihre Ansätze technologieunabhängig. Ihnen ist es nicht nur gelungen, ganze Modelle zu extrahieren. Es ist ihnen gelungen, die Modelle unabhängig davon zu extrahieren, ob diese auf logistischer Regression, KNN, *support vector machines* oder Entscheidungsbäumen basieren.⁸⁰ Dabei konnten sie nicht nur die Modelle selbst, sondern ebenfalls ganze Trainingsdatensätze extrahieren. In ihrem Anwendungsbeispiel konnten sie alle Gesichtsbilder rekonstruieren, die für das Training einer Gesichtserkennungsanwendung verwendet wurden.⁸¹ Es liegt auf der Hand, dass das nicht nur aus wirtschaftlichen Überlegungen aus Entwickler:innensicht, sondern insbesondere auch aus Datenschutzgründen äußerst bedenklich ist

Der Unterschied der von TRAMER/ZHANG/JUELS/REITER/RISTENPART vorgestellten Methoden zu den bereits besprochenen liegt einerseits in der bereits vorgebrachten Technologieunabhängigkeit⁸² und andererseits in der sehr hohen Genauigkeit der extrahierten Modelle. Die von TRAMER/ZHANG/JUELS/REITER/RISTENPART erreichen nach eigenen Angaben eine Genauigkeit von mehr als 99.9%.⁸³ Ein weiterer Unterschied ist, dass sich bei TRAMER/ZHANG/JUELS/REITER/RISTENPART Ansätze finden, bei welchen keine Vorkenntnisse über die Struktur des „angegriffenen“ Modells

⁷⁹ Auch für das Gelingen sog. *Adversarial Attacks* ist es notwendig, bestimmte Parameter der angegriffenen KI-Technologie zu kennen. So ist das *reverse engineering* dieser Parameter notwendiger erster Schritt für *Adversarial Attacks*.

⁸⁰ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 1.

⁸¹ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 8.

⁸² TRAMER/ZHANG/JUELS/REITER/RISTENPART, 12 ff., wobei das Paper einerseits diesbezüglich Vorbehalte macht und andererseits keine Aufschlüsse darüber gibt, ob bei KNN nur das trainierte Modell komplett oder auch dessen Einzelteile (*weights*, Architektur, Optimierungsinformationen, etc.) extrahiert werden können.

⁸³ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 2, 7, 10 f., 13 f.

vorliegen müssen.⁸⁴ Die Ansätze funktionieren mit generischen und öffentlichen (Trainings)daten, die verwendet werden, um das Ziel-Modell oder deren Trainingsdaten zu extrahieren. Die Ansätze von TRAMER/ZHANG/JUELS/REITER/RISTENPART reichen vom Lösen von Gleichungen bis zum Training von eigenen Modellen, die dann auf das Ziel-Modell angewandt werden.⁸⁵ Allerdings benötigen die Methoden von TRAMER/ZHANG/JUELS/REITER/RISTENPART mit 108'200 Anfragen⁸⁶ bei komplexen KNN deutlich mehr Anfragen an das Ziel-Modell als bspw. die 100 Anfragen bei JOON OH/AUGUSTIN/SCHUELE/FRITZ^{87,88}. Damit fallen Attacken nach den Ansätzen von TRAMER/ZHANG/JUELS/REITER/RISTENPART eher bei den Betreibern auf als Attacken gemäß dem Ansatz von JOON OH/AUGUSTIN/SCHUELE/FRITZ. Diese Menge an Anfragen ist jedoch nur bei komplexen KNN nötig, deren Aufbau gänzlich unbekannt ist.⁸⁹ Bei Modellen, die auf binärer logistischer Regression basieren, reichen durchschnittlich deren 41⁹⁰ bei „einfachen“ KNN durchschnittlich 260⁹¹, bei Modellen von AWS deren 650⁹².

Es existieren also auch bei cloudbasierten, nicht lokal vorliegenden KI-Anwendungen Möglichkeiten, an die Grundstruktur, die trainierte Technologie bzw. Anwendung, die Trainingsdaten sowie bei KNN speziell den Optimierungsalgorithmus zu kopieren. Mit der von JOON OH/AUGUSTIN/SCHUELE/FRITZ angewandten Methode lassen sich Informationen aus dem Modell extrahieren, die für einen Nachbau notwendig sind. Wir haben gesehen, dass der Aufwand mit 40 GPU-Tagen und 100 Anfragen für die Datensatzerstellung deutlich höher ist als bei *reverse engineering* Methoden bei

⁸⁴ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 11.

⁸⁵ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 5.

⁸⁶ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 13.

⁸⁷ Siehe soeben die Methode von JOON OH/AUGUSTIN/SCHUELE/FRITZ.

⁸⁸ Allerdings sei daran erinnert, dass Joon Oh/Augustin/Schuele/Fritz für ihre Methode in einem ersten Schritt noch die Metamodelle trainieren müssen, was allerdings unabhängig vom Ziel-Modell erfolgt und demnach auch ein kleineres Risiko besteht, dass das reverse engineering auf Seiten der Betreiber bemerkt wird.

⁸⁹ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 13.

⁹⁰ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 6.

⁹¹ TRAMER/ZHANG/JUELS/REITER/RISTENPART, 7.

⁹² TRAMER/ZHANG/JUELS/REITER/RISTENPART, 11

lokal ablaufenden KI-Anwendungen. Bei TRAMER/ZHANG/JUELS/REITER/RISTENPART ist der Aufwand der Extraktion nur bei komplexen KNN hoch. Ihre Ansätze ermöglichen die Modellextraktion bei verschiedenen KI-Technologien und ohne Kenntnis über die Modellart.

Es ist schließlich darauf hinzuweisen, dass diese Studien zum Teil älter als fünf Jahre sind. Demnach sind auch die angegriffenen Technologien zum Teil deutlich schwächer als KI-Anwendungen, die heute auf dem Markt sind. Dies liegt im schnellen Entwicklungstempo des Untersuchungsgegenstandes begründet.⁹³ Allerdings entwickeln sich einerseits zusammen mit den KI-Anwendungen auch die Fähigkeiten der Modelle weiter, mit welchen die KI-Anwendungen angegriffen werden. Andererseits interessieren vor allem die Funktionsweisen der *reverse engineering*-Ansätze. Diese nutzen gerade die Funktionsweise der KI-Technologien selbst sowie deren Skalierbarkeit aus – sie nutzen den fehlenden Determinismus sowie die fehlende Determiniertheit und das Funktionieren nach stochastischen Regeln aus. Sodass auch die Ansätze zum *reverse engineering* skalierbar sein dürften und die aufgezeigten Methoden auch heute mit größeren Modellen sowie stärkerer Rechenleistung funktionieren dürften.⁹⁴

III. Zwischenergebnis

Es wurde ersichtlich, was mit mehr oder minder großem Aufwand mit *reverse engineering* möglich ist. Durch das gesetzlich erlaubte Nachbauen sind Konkurrent:innen von Techunternehmen dazu in der Lage, an das Geschäftsgeheimnis – die KI-Technologie – zu gelangen. Beziehungsweise ist es ihnen durch das Nachbauen möglich, an die wesentlichen Informationen zu kommen, die sie zum Nachbau der Technologien benötigen. Aufgrund der weitgehenden immaterialgüterrechtlichen Schutzfreiheit der KI-Technologien bzw. derer Bestandteile, sind den Konkurrent:innen bis auf etwaige vertragliche Beschränkungen beinahe keine Grenzen gesetzt, wenn sie KI-Technologien kopieren und diese

⁹³ Vgl. dazu oben Kap. 6.

⁹⁴ So sind die Untersuchungen von CARLINI/JAGIELSKI/ZHANG/PAPERNOT/TERZIS/TRAMER und MIRESHGHALLAH/GOYAL/UNI-YAL/BERG-KIRKPATRICK/SHOKRI aus dem Jahr 2022.

Kopien vertreiben möchten. Der Geschäftsgeheimnisschutz ist vor diesem Hintergrund ein sehr schwacher Schutz von KI-Technologien.

Kapitel 10

Schutzlücken beim Schutz von KI-Technologien

A. Würdigung des Schutzniveaus und Schutzlücken

In den Kapiteln 1 und 6 wurde aufgezeigt, dass KI-Technologien Informationen darstellen und deshalb als solche weder exklusiv noch rival oder abnutzbar sind. Sie sind immaterielle Güter. Immaterielle Güter, deren Fixkosten in der Entwicklung sehr hoch sind bzw. sehr hoch sein können.¹ Gleichzeitig weisen Sie aber vergleichsweise niedrige Grenzkosten auf.² Damit besteht bei Schutzfreiheit von KI-Technologien ein Anreiz für Trittbrettfahrer:innen und Nachahmer:innen zur Nachahmung der KI-Technologie und diese dann zu Grenzkosten zu vertreiben. Aus Innovations- und wohlfahrtsökonomischer Sicht ist eine solche Situation unerwünscht. Sie führt auf lange Sicht zu einer Unterproduktion und damit zu einem Wohlfahrtsverlust.³

Die Marktanalyse in Kapitel 6 hat ergeben, dass Anbieter:innen von KI-Technologien auf einen faktischen Schutz zurückgreifen. Sie schützen sich mit technischen Geheimhaltungsmaßnahmen vor der Aneignung der KI-Technologien durch Trittbrettfahrer:innen. Diese umfassen neben „gewöhnlichen“ Schutzmaßnahmen wie Verschlüsselungen vor allem das Anbieten von KI-Technologien in cloudbasierter Form.

Die Technologien werden also überwiegend als Dienstleistung angeboten und nicht als Produkt. Dies bringt Anbieter:innen unter anderem⁴ – oder vor allem – den Vorteil, dass die KI-Technologie als solche nicht offengelegt werden muss,

¹ Siehe oben Kap. 6, D., I., 1.

² Siehe oben Kap. 5, B., I.

³ Vgl. oben Kap. 6, D., I., 1.

⁴ Siehe zu den anderen Vorteilen oben Kap. 6, C.

wie das im Fall einer lokalen Anwendung wäre.⁵ Allerdings erhöht eine solche Dienstleistungslösung die Fix- und Transaktionskosten. Was wohlfahrtsökonomisch ineffizient und damit unerwünscht ist. Zudem stellt eine solche Lösung eine Form von Geheimhaltung dar. Geheimhaltung von Information ist sowohl wohlfahrts- als auch innovationsökonomisch ineffizient und ebenfalls unerwünscht.⁶

Diese Ineffizienzen indizieren ein rechtliches Schutzbedürfnis. Ein Schutzrecht kann dazu beitragen, die Fix- und Transaktionskosten zu senken, und damit sowohl die statische als auch die dynamische Effizienz zu erhöhen. Ein Schutzrecht, welches die Amortisation der Investitionen ermöglicht, ließe die faktischen Schutz- bzw. Geheimhaltungsmaßnahmen obsolet werden. Damit könnten die Entwickler:innen und Anbieter:innen auf ihre faktischen Schutz- bzw. Geheimhaltungsmaßnahmen verzichten. Effizientere Preise wären die Folge und damit ein Wohlfahrtsgewinn.

Die Prüfung der Schutzfähigkeit der untersuchten KI-Technologien *de lege lata* hat ergeben, dass gewisse Schutzmöglichkeiten vorliegen. Allerdings wurde auch deutlich, dass KI-Technologien *per se de lege lata* keinen umfassenden Schutz erfahren können. Dies kann ein weiterer Grund für die vorherrschende Marktstruktur sein.⁷

In einem nächsten Schritt werden die untersuchten Schutzrechte entsprechend des im dritten Teil dargelegten Maßstabs der Innovations- und Wohlfahrtsökonomik einzeln gewürdigt. Aus dieser Würdigung werden sich Schutzlücken ergeben, an welchen ein Schutzrecht *de lege ferenda* anknüpfen kann.

I. Würdigung des patentrechtlichen Schutzes

Wie gesehen können KI-Technologien unter bestimmten Voraussetzungen patentrechtlich geschützt werden. Dies ist vor allem bei computerimplementierten KI-Technologien der Fall, wenn sie in einer technischen Vorrichtung technische Funktionen erfüllen oder Teil eines technischen Verfahrens sind. KI-

⁵ Vgl. im Genauen oben Kap. 9, C., II., 1.

⁶ Siehe zu den einzelnen Ineffizienzfaktoren im Einzelnen und Genauen oben Kap. 6, D.

⁷ Gemeint ist der Umstand, dass KI-Technologien überwiegend cloudbasiert angeboten werden.

Technologien im Sinne der bloßen Programmstruktur sind nur in Ausnahmefällen einem Patentschutz zugänglich.⁸ Diesem begrenzten Patentschutz sind zwar sämtliche KI-Technologien grundsätzlich zugänglich – unabhängig der jeweiligen Funktionsweise. Das Patentrecht schließt keine der betrachteten KI-Technologien von einem Schutz grundsätzlich aus.⁹

Doch ist ein solcher Schutz zweckmäßig? Nach der hier vertretenen Auffassung reicht das Patentrecht für sich betrachtet aus einer wohlfahrts- und innovationsökonomischen Perspektive nicht aus, was den immaterialgüterrechtlichen Schutz von KI-Technologien anbelangt – insbesondere was den Schutz der Technologie als solche betrifft. Hauptgrund dafür ist das patentrechtliche Technizitätsverständnis. Dieses schließt zahlreiche Einsatzgebiete von KI-Technologien aus.¹⁰

KI-Technologien kommen heutzutage aber auf beinahe jedem denkbaren Gebiet zum Einsatz. Der Entwicklungsaufwand für eine KI-Technologie, die nicht auf einem technischen Gebiet im patentrechtlichen Sinne zum Einsatz kommt, unterscheidet sich grundsätzlich nicht vom Entwicklungsaufwand einer KI-Technologie, deren Anwendung über Technizität im patentrechtlichen Sinne verfügt.¹¹ Durch den Ausschluss nichttechnischer KI-Technologien ergibt sich also ein Ungleichgewicht zwischen den Anwendungsgebieten, auf welchen KI-Technologien eingesetzt werden.

Darüber hinaus schützt das Patentrecht in den meisten Fällen nicht die KI-Technologie als solche, sondern deren technische Implementierung – insgesamt ein Ungleichgewicht, welches zu unbefriedigenden Ergebnissen führt, wenn wir das Ziel der hohen Produktion bzw. einer hohen dynamischen Effizienz verfolgen. Bleiben nichttechnische KI-Technologien schutzfrei, besteht ein falscher

⁸ Siehe oben Kap. 7, B., VI.

⁹ Siehe oben Kap. 7, B., I.

¹⁰ Dies, obwohl es sich bei Künstlicher Intelligenz zweifelsohne um ein Gebiet der Technik handelt. Das ergibt sich bereits aus dem informationstechnischen Wesensmerkmal.

¹¹ Der Entwicklungsaufwand einer KI-Technologie, die auf einem linguistischen Gebiet (bspw. Spracherkennung) eingesetzt wird, ist ebenso hoch wie für eine technische KI-Technologie im Sinne des Patentrechts.

Anreiz, nur noch im patentrechtlichen Sinne technische KI-Technologien zu entwickeln.

Hinzu kommt, dass die Hürden der Technizität bzw. erfinderischen Tätigkeit aufgrund des Patentierungsausschlusses von mathematischen Methoden wie auch Computerprogrammen im Verhältnis zum Entwicklungsaufwand unverhältnismäßig hoch sind. Obschon das EPA Richtlinien zur Patentierung von KI-Systemen veröffentlichte und auch auf die Rechtsprechung zur Patentierung von technisch implementierten mathematischen Methoden oder Computerprogrammen zurückgegriffen werden kann, scheint der Bereich der patentfähigen KI-Technologien noch nicht deutlich abgesteckt. Die anmeldende Person sieht sich somit vor eine erhebliche Unsicherheit gestellt und riskiert unter Umständen die Offenbarung der KI sowie der Trainingsdatensätze.¹² Diese Unsicherheit lässt sich gut an der EPA-Praxis zu Simulationsverfahren aufzeigen.¹³ Darüber hinaus kann eine solche Unsicherheit dazu führen, dass die Technologie vom Erfinder im Zweifelsfall nicht veröffentlicht, sondern geheim gehalten wird. Einerseits könnte der Erfinder gänzlich auf eine Patentanmeldung verzichten. Oder die Offenbarung erfolgt auf eine solche Art und Weise, dass nur die technische Vorrichtung oder das Verfahren beschrieben wird, für welche die KI-Technologien eingesetzt werden. Beide Szenarien machen wiederum die Weiterentwicklung der Innovation durch andere Akteur:innen unmöglich und haben somit keinen positiven Effekt auf die statische Effizienz. Schließlich sind die Trainingsdatensätze nicht durch das Patentrecht geschützt. Diese sind aber ausschlaggebend für die Qualität wie auch die Funktionsweise der Technologie und daher von hohem Wert.¹⁴ Bereits der Aufwand der Daten-

¹² So bspw. auch APEL/KAULARTZ, RD i 2020, 29.

¹³ So hat das EPA in der Entscheidung EPA GRUR-RS 2021, 49757 ff. – T 0489/14 Abstand von den bis dahin allgemein anerkannten Grundsätzen aus der Entscheidung EPA GRUR Int 2006, 59 ff. – T 1227/05 genommen und die Anforderungen an den Patentschutz computerimplementierter Simulationen erhöht. Die Große Beschwerdekammer des EPA wies darauf jedoch diese erhöhten Anforderungen (teilweise) in EPA (Große Beschwerdekammer) GRUR-RS 2021, 6335 ff. – G 1/19 zurück und erklärte den zweistufigen Ansatz („COMVIK-Ansatz“, vgl. dazu oben Kap. 7, A., III., 1.) auch bei computerimplementierten Simulationsverfahren anwendbar. Dabei verweist EPA (Große Beschwerdekammer) GRUR-RS 2021, 6335 ff. – G 1/19 an mehreren Stellen auf BGH GRUR 2000, 498 – Logikverifikation.

¹⁴ Vgl. oben Kap. 2, B.

sammlung, -trriage, -annotation und -kuration liefert aus Investitionsschutzüberlegungen genug Argumente für ein Schutzbedürfnis auch der Datensätze selbst.

Es könnte also generell die Auffassung vertreten werden, dass das Patentrecht einen Fehlanreiz schafft, weil es nicht den eigentlichen finanziellen Aufwand belohnt, sondern das Finden eines technischen Anwendungsgebietes und die Lösung eines Problems auf diesem durch das Patentrecht abgesteckten Gebiet. Diese „limitierte“ Schutzfähigkeit durch das Patentrecht ist aber zu begrüßen. Das Patentrecht soll nicht einer neuen Funktion zugeführt werden. Das Patentrecht soll weiterhin neue technische Erfindungen schützen – ob es der Erfindung großer finanzieller Aufwendungen bedurfte, darf nicht ausschlaggebendes Kriterium zwecks Beurteilung einer Patentierbarkeit sein. Es darf nicht angehen, dass eine neuartige Technologie zu einem Prinzipienbruch innerhalb einer etablierten Rechtsinstitution führt – aller Schutzbedürftigkeit zum Trotz.¹⁵

Es existieren Lehrmeinungen, welche zusätzlich die Patentierung von potenziell „gefährlicher“ KI ausschließen wollen.¹⁶ Dazu müsste in einem ersten Schritt definiert werden, was unter gefährlicher KI zu verstehen ist und ob die „Gefährlichkeit“ bereits auf Programmebene begründet ist oder erst in der Anwendung. Überhaupt ist ein solcher Ausschluss abzulehnen. Das Patentrecht soll – ausgenommen der ethisch und sittlich begründeten Ausschlussgründe in § 1a PatG – keine regulierenden Aufgaben übernehmen.¹⁷ Die Regulierung von KI muss außerhalb des Patentrechts erfolgen – nicht zuletzt auch aufgrund dessen, dass nur ein kleiner Teil von KI überhaupt erst schutzfähig ist.

Zusammengefasst ist also festzuhalten, dass das Patentrecht für sich betrachtet dem Schutzbedürfnis von KI-Technologien nicht zu genügen vermag. Es schützt lediglich technische Anwendungsgebiete im patentrechtlichen Sinn und schließt alle sonstigen Anwendungsgebiete aus. In Kapitel 6 wurde aufgezeigt, dass vor allem die vorhandenen Datenmengen, die bessere Rechenleistung und

¹⁵ So auch SCHAUB, JZ 2017, *passim*; von einer (eigentlichen) grundsätzlichen Ungeeignetheit des Patentrechts spricht im Sinne einer a.A. KKI-PAPASTEFANOU, S. 25 f.

¹⁶ Rechtshandbuch-AI- TOCHTERMANN, Kap. 7.3 Rn. 19 mit Verweis auf das Gutachten der Datenethikkommission der Bundesregierung.

¹⁷ Siehe zum Verhältnis zwischen Patentrecht und Ethik ausführlich BARTELS, *passim*, S. 63 ff.

teilweise neue Heuristiken der Entwickler:innen Treiber des Marktes für KI-Technologien sind. Mit diesen Treibern gehen auch die hohen Kosten in der Entwicklung einher. Die Kosten für diese Treiber und der damit zusammenhängende Investitionsschutz sind auch aus einer wohlfahrts- und innovationsökonomischen Perspektive wesentliches Argument für ein Schutzbedürfnis der KI-Technologien.

Aufgrund dieser Überlegungen passt auch das Patentrecht nicht gänzlich. Es belohnt eine innovative Leistung – unabhängig der dahinterstehenden Investitionen. Mit anderen Worten belohnt es im Hinblick auf KI-Technologien die Suche nach und das Finden einer technischen Einsatzmöglichkeit der Technologie und nicht das Sammeln, Aufbereiten und Kurieren von Trainingsdaten, auch nicht den Trainingsprozess als solchen und ebenso wenig die abstrakte Herangehensweise der Entwickler:innen an die Problemlösung mittels KI-Technologie und etwaiger damit zusammenhängenden Modellentwürfen. Das ist aber auch gut so. Das Patentrecht soll keineswegs dahingehend angepasst werden, dass KI-Technologien unabhängig derer Einsatzgebiete geschützt werden. Eine solche Lösung würde mit patentrechtlichen Grundprinzipien brechen und zu Widersprüchen mit dem bisher etablierten patentrechtlichen Computerprogrammenschutz führen.

II. *Würdigung des urheberrechtlichen Schutzes*

Bei Expertensystemen ist lediglich die Interferenzmaschine mit Dialogkomponente urheberrechtlich geschützt. Für die Wissensbasis kommt kein Computerprogrammenschutz infrage. Allerdings kann die Wissensbasis als Datenbankwerk geschützt sein oder Gegenstand des Datenbankherstellerrechts nach § 87 UrhG. Für die Benutzeroberfläche ist der Computerprogrammenschutz ausgeschlossen, nicht jedoch ein Schutz als Werk nach § 2 UrhG.¹⁸

Beim *genetic programming* ist neben der Fitnessfunktion nur die Programmumgebung, die die Individuen generiert, nicht aber das Ziel-Programm vom Computerprogrammenschutz erfasst. Für das Ziel-Programm kommt auch kein Schutz

¹⁸ Vgl. oben Kap. 8, B., I.

als Werk im Sinne von § 2 UrhG infrage. Grund dafür ist, dass das Ziel-Programm gänzlich autonom programmiert wird und es demnach nicht Ergebnis einer menschlich geistigen Schöpfung ist.¹⁹

Bei KNN ist die urheberrechtliche Schutzfähigkeit stark umstritten. Korrekter- und konsequenterweise sind weder untrainierte noch trainierte KNN vom urheberrechtlichen Computerprogrammenschutz erfasst.²⁰ Die Entwicklungs- und Funktionsweise von KNN lassen einen urheberrechtlichen Computerprogrammenschutz ohne Prinzipienbruch im Urheberrecht nicht zu. Untrainierte KNN sind nicht vom Computerprogrammenschutz erfasst, weil sie keine determinierte Funktion erfüllen und mithin zu abstrakt sind. Dieser Umstand schließt folgerichtig auch einen Schutz als Entwurfsmaterial eines Computerprogrammes aus.²¹ Untrainierte KNN können jedoch in Ausnahmefällen einem Schutz als sonstiges Werk nach § 2 UrhG zugänglich sein, sofern sie über ein Kommunikationselement verfügen,²² und nicht reine Funktionalitätsüberlegung zur Festlegung der Modellstruktur führten.²³

Trainierte KNN sind aufgrund mangelnder menschlich-geistiger Schöpfung ungeschützt. Der menschliche Einfluss überschreitet die Schwelle der bloßen Konzeptionierung im Hinblick auf die Funktionsaneignung des KNN nicht.²⁴ Ein Schutz von trainierten KNN als Werk im Sinne von § 2 UrhG fällt aus demselben Grund außer Betracht.²⁵ Einigkeit dürfte darüber bestehen, dass die Gewichtungsinformationen und damit die Trainingsergebnisse ebenfalls nicht geschützt sind. Einzelne Bestandteile von KNN und der Optimierungsalgorithmus können einem urheberrechtlichen Computerprogrammenschutz und als Werk im Sinne von § 2 UrhG zugänglich sein.²⁶

¹⁹ Vgl. oben Kap. 8, B., II., 2.

²⁰ Vgl. oben Kap. 8, B., III., 1., Kap. 8, B., III., 2., c).

²¹ Vgl. oben Kap. 8, B., III., 1.

²² Was selten tatsächlich der Fall sein dürfte, vgl. Kap. 8, B., IV., 1.

²³ Was ebenfalls nicht leichthin zu bejahen ist, vgl. Kap. 8, B., IV., 1.

²⁴ Vgl. oben Kap. 8, B., III., 2., b).

²⁵ Vgl. oben Kap. 8, B., IV., 2.

²⁶ Vgl. oben Kap. 8, B., III., 5.; jedoch nie als Werk nach § 2 UrhG und als Computerprogramm nach § 69a UrhG.

Trainingsdaten in ihrer Gesamtheit dürften in aller Regel nur im Einzelfall urheber- oder leistungsschutzrechtlichen Schutz genießen.

Diese Auflistung macht bereits den ersten Grund sehr deutlich, warum das geltende Urheberrecht als ungeeignet eingestuft werden muss, wenn die Schutzzfähigkeit von KI-Technologien beurteilt werden soll: KI-Technologien werden urheberrechtlich unterschiedlich behandelt – obwohl das Urheberrecht mit dem Computerprogrammschutz in § 69a UrhG eigentlich einen (technologie-neutralen) Schutz für Softwareebenen von digitalen Systemen vorsieht. Softwareebenen von *intelligenten* digitalen Systemen sind jedoch weitgehend nicht von diesem Schutzrahmen erfasst. Das Urheberrecht schließt also einzelne Technologien von einem Schutz aus. Dies führt aus wohlfahrts- und innovationsökonomischen Überlegungen zu einem Fehlanreiz.

Dieser Fehlanreiz ist umso verwerflicher, wenn man sich vor Augen führt, dass das Urheberrecht die potenteren Technologien wie genetische Programme und KNN von einem Schutz ausschließt, während die weniger potenten Technologien wie Expertensysteme oder sogar herkömmliche Softwareebenen von (nicht intelligenten) digitalen Systemen urheberrechtlich geschützt sind. Der Fehlanreiz lässt sich auch nicht dadurch lösen, den Computerprogrammschutz für trainierte KNN in einem Prinzipienbruch mit dem Urheberrecht zu bejahren.²⁷ Ziel-Programme beim *genetic programming* müssen nämlich stets schutzfrei bleiben, möchten wir nicht autonom generierten Werken generell einen Schutz zusagen und damit dem Anthropozentrismus im Urheberrecht den Rücken kehren.²⁸

Der urheberrechtliche Schutz ist also bereits deshalb als Lösung für das Schutzbedürfnis von KI-Technologien ungeeignet, weil er zu einer Ungleichbehandlung von KI-Technologien führt und lediglich die schwächeren Ansätze zu

²⁷ Die Prinzipienbrüche würden darin bestehen, dass einerseits bloße Ideen bzw. abstrakte Konzepte und andererseits Werke ohne menschlichen Schöpfer geschützt wären. Vgl. dazu oben bspw. Kap. 8, B., III. 1.; Kap. 8, B., III. 2., b).

²⁸ Vgl. stellvertretend MAAMAR, S. 209 und GRÄTZ, S. 104: Das geltende Recht bietet keinen Raum für den urheberrechtlichen Schutz von autonom generierten Werken, bei denen sich der menschliche Einfluss in der Konzeptionierungsphase erschöpft und sich der menschliche Einfluss nicht mehr in der konkreten Ausdrucksform des Werkes widerspiegelt.

schützen vermag. Potentere Technologien wie genetische Programme und KNN bleiben schutzfrei – somit liegt eine Schutzlücke vor.

Die Schutzlücke ist selbst dann noch erheblich, wenn man entgegen der hier vertretenen Meinung die urheberrechtliche Schutzfähigkeit von untrainierten sowie trainierten KNN bejahen würde. Genauer gesagt, ließe sich die erwähnte Schutzlücke durch die Bejahung des Schutzes für KNN nicht schließen.

Wie gesehen schützt das Urheberrecht nur die konkreten Ausdrucksformen einer Softwareebene – nicht aber die Funktionalität.²⁹ Die funktionale Nachahmung eines urheberrechtlichen Computerprogrammes stellt keine urheberrechtliche Verletzungshandlung dar.³⁰ Die Entwicklungs- und Funktionsweisen der betrachteten Technologien haben aber gezeigt, dass es bei der Entwicklung von KI-Technologien genau um diese Funktionalität geht. Der Mensch gibt die einzelnen konkreten Regeln der Informationsverarbeitung nicht mehr vor. Die menschliche Leistung besteht gerade nicht darin, einer Maschine den Lösungsweg für eine Aufgabe in Gestalt einer konkreten Ausdrucksform vorzugeben. Es geht viel eher darum, die Maschine in die Lage zu bringen, dass sie den Lösungsweg eigenständig finden bzw. erlernen kann.³¹

Es geht bei KI-Technologien also darum, einer Maschine eine Aufgabe zu lehren bzw. ihr eine Funktion beizubringen und nicht der Maschine eine Funktion bzw. einen Lösungsweg konkret vorzugeben. Der konkrete Lösungsweg bzw. dessen Ausdrucksform ist bei KI-Technologien nicht Ergebnis einer menschlichen Leistung. Entscheidend bei KI-Technologien ist es demnach, die Funktionalität zu erreichen. Begnüge man sich dementsprechend mit einem urheberrechtlichen Schutz von untrainierten und trainierten KNN, brähe man nicht nur mit urheberrechtlichen Prinzipien, sondern könnte Nachahmer:innen nicht davon abhalten, sich die eigentlich belohnenswerte Leistung anzueignen – die Leistung, in welche die Investitionen flossen. Nachahmer:innen wäre es bspw. möglich, das untrainierte KNN funktional nachzuahmen und auf dieses sodann die gemeinfreien Gewichtungsinformationen anzuwenden. Ergebnis wäre ein funktional ähnliches trainiertes KNN. Die Nachahmer:innen sparten

²⁹ Vgl. oben Kap. 8, A., III., 1. und GRÄTZ, S. 50 m.w.N.

³⁰ Siehe oben Kap. 8, A., III., 1.

³¹ Vgl. oben Kap. 2., A.; Kap. 2, C., IV.; Kap. 8, A., III., 1., speziell für KNN Kap. 2, C., II., 3.

sich so den aufwändigen Trainingsprozess und die Konzeptionierung der Topologie. Dabei ist wichtig zu bedenken, dass die Funktionalität der Topologie vor allem von der Anzahl Neuronen und Schichten abhängt sowie der Art der Verbindungen (progressiv, rekursiv, kombiniert, etc.). Doch sind diese Parameter bekannt, kann ein neues Modell nachgebaut werden, welches diese Parameter aufweist. Es müssen nicht zwingend sämtliche Parameter identisch übernommen werden. Es genügt, wenn nur Anhaltspunkte betreffend die Parameter bekannt sind und diese zusammen mit Annahmen im nachgebauten Modell angewandt werden. Der Umstand, dass KNN eben weder deterministisch noch determiniert, sondern probabilistisch sind und stochastisch arbeiten, ermöglicht auch in solchen Situationen eine ähnliche oder je nachdem identische Funktionalität.³² Sofern die Topologie nicht bekannt ist,³³ stellt bspw. die unter Kapitel 9.II.2. erläuterte *Avatar*-Methode ein Beispiel für funktionale Nachahmung dar.³⁴

Somit können sich Nachahmer:innen die Investitionen sparen und die nachgebaute KI-Technologie beinahe zu Grenzkosten vertreiben. Das Trittbrettfahrerproblem lässt sich also auch nicht dann vermeiden, wenn untrainierten und trainierten KNN fälschlicherweise urheberrechtlicher Schutz zugestanden wird. Grund dafür ist die Entwicklungs- und Funktionsweise von KI-Technologien. Diese ist jedoch Grund für die Potenziale von KI-Technologien gegenüber derjenigen herkömmlicher Softwareebenen.

Schließlich dauert der urheberrechtliche Schutz angesichts des v.a. mit Investitionsschutzüberlegungen begründeten Schutzbedürfnisses zu lange. Es bedarf keines Schutzes, der 70 Jahre über den Tod des (letzten Mit)urhebers dauert, um die Investitionen in die Entwicklung der KI-Technologie zu amortisieren. Die Schutzdauer im Urheberrecht ist im Hinblick auf den Schutz von KI-

³² Vgl. oben Kap. 9, C., II. 2.; vgl. auch GRÄTZ, S. 50 mit weiteren Hinweisen, welcher richtigweise ausführt, dass die Auswahl der Schichten, der Verbindungen und Neuronen nicht geschützt sein können. Er bejaht jedoch den Schutz der konkreten Ausdrucksform des untrainierten Netzes. Diese Ansicht wird hier, wie gesehen, nicht geteilt (Kap. 8, B., III., 1.) – auch nicht als Werk nach § 2 UrhG, da der konkreten Ausdrucksform des Netzes in aller Regel das erforderliche Kommunikationselement fehlt (vgl. Kap. 8, B., IV., 1.).

³³ Bspw. weil die KI-Technologie cloudbasiert angeboten wird.

³⁴ Kap. 9, C., II., 2.

Technologien auch aus Überlegungen der statischen Effizienz zu bemängeln und nicht nur aus Überlegungen der Fortschrittsgeschwindigkeit in der Entwicklung von KI-Technologien.

Das Urheberrecht ist also nicht nur deshalb für den Schutz von KI-Technologien ungeeignet, weil es diese weitestgehend gar nicht erst erfasst bzw. erfassen kann. Viel eher lassen sich die aufgezeigten Schutzbedürfnisse auch nicht dadurch decken und die Schutzlücken auch nicht schließen, indem KI-Technologien entgegen urheberrechtlichen Prinzipien in das Schutzwand des Urheberrechts gezwängt werden.

III. Würdigung des Geschäftsgeheimnisschutzes

Der Geschäftsgeheimnisschutz nach GeschGehG eignet sich nicht als Lückenfüller. Der Schutz nach GeschGehG kann nicht die Schutzlücken schließen, die schon weder der Patent- noch der Urheberschutz schließen konnten.

Einerseits ist der Schutz nach GeschGehG kein absoluter.³⁵ Andererseits knüpft er an Geheimhaltungsmaßnahmen an. Diese stellen einen Ineffizienzfaktor dar, da sie zu höheren Kosten führen. Bei KI-Technologien sind dies bspw. Kosten für Verschlüsselungen (bei lokalen KI-Anwendungen) oder Kosten für eine Cloudinfrastruktur (bei cloudbasierten KI-Anwendungen). Es ist unbefriedigend, das aufgezeigte Schutzbedürfnis nur durch Zusatzkosten abzudecken. Das Schutzbedürfnis wurde teilweise auch mit den höheren Kosten begründet, die Geheimhaltungsmaßnahmen mit sich bringen. Es sind Zusatzkosten, die bei KI-Technologien nicht aus deren Natur heraus notwendig wären. Solche Kosten führen zu ineffizienten Preisen und damit zu Wohlfahrtsverlusten. Das GeschGehG stellt damit einen Ineffizienzfaktor dar, statt effizienzfördernd zu sein, was aber gemäß dieser Arbeit Ziel eines Schutzrechtes sein sollte.³⁶

Das GeschGehG ist nicht nur aus Kostenargumenten ineffizient, sondern auch aus Sicht der statischen Effizienz zu bemängeln. Da der Schutz nach GeschGehG darauf abstellt, dass die Innovationen und die damit einhergehenden In-

³⁵ Vgl. oben Kap. 9, C., I.

³⁶ Vgl. oben Kap. 4, C.

formationen geheim gehalten werden, werden die Informationsgüter nicht verbreitet. Diese fehlende Verbreitung ist wiederum wohlfahrtsschädigend, da Folgeinnovationen nicht möglich sind.³⁷

Schließlich und vor allem ist aber der kosteneffiziente Schutz durch das GeschGehG schwach, wenn Trittbrettfahrer:innen von der Nachahmung und darauffolgenden Nutzung oder Offenlegung der KI-Technologie ausgeschlossen werden sollen. Einerseits besteht durch die relative Natur des Geschäftsgeheimnisschutzes keine Möglichkeit, Dritte³⁸ von der Erlangung und Nutzung des Geheimnisses auszuschließen, sofern und solange diese dritte Person zumindest in fahrlässiger Unkenntnis vom Geheimnisbruch handelt.³⁹ Es besteht also ein erhebliches Risiko, dass Entwickler:innen ihrer Investition verlustig gehen.

Dieses Risiko zeigt sich besonders darin, dass das GeschGehG verschiedene Handlungen vorsieht, mit welchen die Geschäftsgeheimnisse erlangt und unter Umständen gar genutzt und offengelegt werden dürfen. Im Zusammenhang mit KI-Technologien ist vor allem das in § 3 GeschGehG vorgesehene und entsprechend erlaubte *reverse engineering* zu nennen. Dieses aus deutscher Sicht neuerdings erlaubte *reverse engineering* ist aufgrund der Funktionsweise von KI-Technologien – v.a. von KNN – aus Sicht von Nachahmer:innen besonders interessant. Es ist unerheblich, ob die Technologie lokal oder cloudbasiert angeboten wird. Für Konkurrent:innen bestehen mehr oder minder aufwändige Möglichkeiten, durch *reverse engineering* an die KI-Technologie und mithin das Geschäftsgeheimnis zu gelangen. Bietet das sonstige Recht – insbesondere das Immaterialgüterrecht – keine Möglichkeit, die KI-Technologie zu schützen, gehen Entwickler:innen und Anbieter:innen ihrer Investition *qua* gesetzlicher Erlaubnis verlustig.⁴⁰ Wie aufgezeigt, bieten weder Patent- noch Urheberrecht umfassenden Schutz für KI-Technologien.⁴¹

³⁷ Vgl. oben Kap. 5, B., II.

³⁸ Im Sinne von zum Geheimnisinhaber und Geheimnisbrecher verschiedene Personen.

³⁹ Vgl. oben Kap. 9, C., I.

⁴⁰ Vgl. oben Kap. 9, C., II.

⁴¹ Vgl. oben Kap. 7, B. VI.; Kap. 8, B., VI.

Zwar ließe sich nun einwenden, dass das *reverse engineering* besonders betreffend die statische Effizienz zu begrüßen ist. Durch das *reverse engineering* können die Informationen verbreitet und Folgeinnovationen ermöglicht werden. Allerdings bietet das Schutzsystem um KI-Technologien wie gesehen zu wenig Schutz vor Nachahmer:innen. Damit ist zu bezweifeln, dass nicht eine Situation von Unterproduktion zumindest eintreten könnte.

B. Ergebnis: Schutzlücken

In Kapitel 6 wurde festgestellt, dass aus wohlfahrts- und innovationsökonomischer Sicht Anzeichen für ein Schutzbedürfnis betreffend KI-Technologien vorhanden sind. Zwar wird das volkswirtschaftliche Ziel der hohen Produktion erreicht. Die Ziele der weiten Verbreitung und niedrigen Kosten im Umgang scheinen jedoch nicht erreicht zu werden. Die Marktanalyse hat ergeben, dass vor allem hohe Investitionen in die Markttreiber der Datenakquise und -aufbereitung fließen. Daneben fließen Investitionen in die notwendige Hardware und die Vergütung der Leistungen der an der Entwicklung der Technologien beteiligten Personen.

Es sind Investitionen, die zur Schaffung der in der KI-Technologie inkorporierten Information notwendig sind. Es wurde aufgezeigt, dass KI-Technologien Charakteristika von öffentlichen Gütern aufweisen und darüber hinaus diverse Effizienzpotenziale bestehen. Effizienzpotenziale, die ein geeignetes Schutzrecht ausnutzen könnte. Die Effizienzpotenziale zeigen sich in den im *status quo* hohen Fix- und Transaktionskosten sowie in der weitgehend unterbleibenden Verbreitung der Technologien und damit der Information. Diese Potenziale spiegeln die zwei nicht erreichten volkswirtschaftlichen Ziele der weiten Verbreitung und der niedrigen Kosten im Umgang mit KI-Technologien wider.

Der aktuelle Schutzrechtsrahmen zeigt sich vor dem Hintergrund dieser Schutzbedürfnisse als wenig bis nicht geeignet, diese Effizienzpotenziale auszunutzen. Die Schutzlücken zeigen sich zusammengefasst wie folgt.

- Das Patentrecht ist zwar technologieneutral, schließt aber KI-Technologien aus, die keine Technizität im patentrechtlichen Sinne

aufweisen. Demnach sind alle KI-Technologien außerhalb technischer Einsatzgebiete grundsätzlich ausgeschlossen. Das patentrechtliche Technizitätserfordernis führt nämlich dazu, dass die eigentliche Information – die KI-Technologie als solche – in aller Regel nicht schutzbar ist, sondern nur deren Implementierung in eine technische Vorrichtung oder ein technisches Verfahren. Dies wiederum kann dazu führen, dass durch das Patentrecht trotz Offenbarungserfordernis nicht zwingend auch die Technologie als solche offengelegt wird. Oftmals wird die Offenbarung der technischen Implementierung und mithin die Beschreibung des technischen Verfahrens ausreichen. Demnach ist das Patentrecht lediglich im Bereich der Technik für KI-Technologien heranzuziehen.

- Das Urheberrecht schließt einzelne KI-Technologien aufgrund ihrer Funktionsweise aus. So sind *Ziel-Programme* beim *genetic programming* ungeschützt und bei KNN sowohl die untrainierten als auch die trainierten Netzwerke. Einzelne Bestandteile können jedoch urheberrechtlichen Schutz genießen. Bei Expertensystemen sind die Bestandteile Wissensbasis, Inferenzmaschine und Benutzeroberfläche grundsätzlich einem urheber- oder leistungsschutzrechtlichen Schutz zugänglich. Das Urheberrecht ist also im Hinblick auf KI-Technologien nicht technologie-neutral. Das ist umso stoßender, wenn man KI-Technologien als Softwareebenen von intelligenten digitalen Systemen versteht. Denn Softwareebenen (nicht intelligenter) digitaler Systeme dürften regelmäßig unter den urheberrechtlichen Computerprogrammenschutz fallen. Damit liegt ein weiteres Ungleichgewicht vor. Darüber hinaus ist das Urheberrecht auch nicht als Schutzrecht geeignet, wenn die statische Effizienz erhöht werden soll: Der eigentliche Kern der Entwicklung von KI-Technologien – die Kern-Information – ist nicht durch das Urheberrecht schutzbar. Es handelt sich um die Funktionalität von KI-Technologien. Im Unterschied zu herkömmlichen Softwareebenen ist das, was der Mensch bei KI-Technologien beeinflussen kann, diese Funktionalität. Er kann die konkrete Ausdrucksform – also das, was urheberrechtlich geschützt werden kann – nicht beeinflussen. Es geht bei KI-Technologien darum, einer Maschine eine Funktio-

nalität beizubringen. Es geht nicht wie bei der herkömmlichen Softwareentwicklung darum, einer Maschine einen funktionalen Lösungsweg vorzugeben. Der Urheberrechtsschutz ist also aus wohlfahrts- und innovationsökonomischer Sicht gänzlich ungeeignet zum Schutz von KI-Technologien. Er vermag es aber insbesondere nicht, die aufgezeigten Effizienzpotenziale auszuschöpfen. Damit bleiben auch nach der patent- und urheberrechtlichen Betrachtung die aufgezeigten Schutzbedürfnisse weitgehend ungedeckt. Es liegen also Schutzlücken vor.

- Diese Schutzlücken vermag auch der Geschäftsgeheimnisschutz nach GeschGehG nicht zu schließen. Erster und offensichtlichster Grund ist, dass das GeschGehG keinen absolut-rechtlichen Schutz einräumt. Es räumt lediglich relative Rechte ein. Zwar erfasst das GeschGehG KI-Technologien grundsätzlich technologie-neutral als Schutzgegenstände. Doch stellt der Schutz auf Geheimhaltungsmaßnahmen als Schutzvoraussetzung ab. Dieser Umstand ist wohlfahrts- und innovationsökonomisch besonders unerwünscht. Er hat eine Erhöhung der Fix- und Transaktionskosten zur Folge und führt dazu, dass die Information nicht verbreitet wird. Viel eher wird sie sogar geheim gehalten. Dies kann zu Informationsverlust führen. Der Geschäftsgeheimnisschutz ist also in erster Linie aufgrund statischer Ineffizienz ungeeignet. Ob er eine positive Wirkung auf die dynamische Effizienz hat, kann zumindest bezweifelt werden. Da er zu einer Erhöhung der Fix- und Transaktionskosten führt, kann er auch eine abschreckende Wirkung auf neue Marktteilnehmer:innen haben. Schließlich kann der Geschäftsgeheimnisschutz aus mehreren Gründen ungeeignet sein, wenn das Risiko von Nachahmer:innen und Trittbrettfahrer:innen gebannt werden soll. Dieses Risiko ist nicht nur aufgrund der fehlenden absolut-rechtlichen Natur des Schutzes erheblich. Insbesondere das gesetzlich erlaubte *reverse engineering* ermöglicht es Nachahmer:innen, erlaubterweise an die geschützte Information – die KI-Technologie – zu gelangen, diese zu nutzen und zu offenbaren.

Ohne geeigneten Schutz werden Entwickler:innen und Anbieter:innen auf Geheimhaltung zurückgreifen müssen, um ihrer Investition nicht verlustig zu ge-

hen. Sie werden zusätzliche Aufwendungen treffen müssen, um sichere Geheimhaltungsmaßnahmen ergreifen zu können. Maßnahmen, die auch ein *reverse engineering* verunmöglichen oder zumindest unrentabel werden lassen. Eine solche Entwicklung ermöglichte zwar womöglich einen wirksamen Schutz vor Nachahmer:innen und Trittbrettfahrer:innen. Allerdings wäre eine solche Lösung wohlfahrts- und innovationsökonomisch ineffizient. Die Kosten für die Geheimhaltung und die damit einhergehenden hohen Fix- und Transaktionskosten dürften eine abschreckende Wirkung auf Markteinsteiger:innen haben. Die Geheimhaltungsmaßnahmen und die hohen Transaktionskosten unterbinden eine effiziente Verbreitung der KI-Technologien und das Ziel der niedrigen Kosten im Umgang mit KI-Technologien wird selbstredend nicht erreicht.

Das Schutzbedürfnis lässt sich also *de lege lata* nicht decken. Die aufgezeigten volkswirtschaftlichen Ziele werden durch die aktuellen Schutzrechtsrahmen nicht erreicht. KI-Technologien lassen sich mit einem Schutzrecht nicht so schützen, dass:

- KI-Technologien generell technologieneutral als Schutzgegenstand in Frage kommen (primär Förderung der dynamischen Effizienz);
- die Investitionen in die Entwicklung der Technologien gesamtwirtschaftlich effizient amortisiert werden könnten (primär Förderung der dynamischen Effizienz);
- ein Schutz nicht mit einer ineffizienten Erhöhung der Fix- und Transaktionskosten verbunden ist (Förderung sowohl der dynamischen als auch der statischen Effizienz);
- ein Schutz nicht bloß die Verbreitung der KI-Technologie nicht verhindert, sondern Anreize für deren Verbreitung setzt (primär Förderung der statischen Effizienz);
- der Schutzinhaber für eine bestimmte Zeitdauer Dritte wirksam davon abhalten kann, sich die geschützte KI-Technologie anzueignen, sie zu

nutzen, zu verwerten oder investitionsschädlich offenzulegen (primär Förderung der dynamischen Effizienz).

Aus diesen Überlegungen drängt sich dementsprechend politischer Handlungsbedarf auf, um diese aufgezeigten Schutzlücken zu schließen.

Auch mit der Einführung eines neuen Schutzrechts absolut-rechtlicher Natur gehen Wohlfahrtsverluste einher. Das Schutzrecht muss derart ausgestaltet werden, dass diese Wohlfahrtsverluste geringer ausfallen als die Wohlfahrtsverluste, die sich durch die Ineffizienzen im *status quo* ergeben. Ein neues Schutzrecht muss also einen effizienten Ausgleich zwischen ausschließlicher Rechtszuweisung und Handlungsgestattungen Dritter vorsehen.

C. Weitere Argumente für die Einführung eines neuen Schutzrechts

Neben den aufgezeigten Argumenten zwecks Steigerung der statischen und dynamischen Effizienz sowie der effizienteren Kostenstruktur sprechen auch die Rechtssicherheit, das Gleichheitsgebot sowie makroökonomische Überlegungen für ein Schutzrecht an KI-Technologien.

Offensichtlicherweise sorgt ein Schutzrecht an KI-Technologien für Rechtssicherheit. Die Ausführungen im vierten Teil zeigten, dass mit der Schutzfähigkeit von KI-Technologien einige Rechtsunsicherheiten verbunden sind. Die Lehrmeinungen gehen auseinander und es finden sich Argumente auf dem gesamten Spektrum von schutzfähig bis schutzfrei. Diese Rechtsunsicherheiten führen unter anderem zu höheren Informationskosten.⁴² So kann sowohl bei der Entwicklung als auch bei der Übertragung von KI-Technologien ein Informationsaufwand anfallen, wenn die Schutzfähigkeit der entwickelten KI-Technologie abgeklärt werden soll. Damit kann ein neues Schutzrecht auch aus Rechtssicherheitüberlegungen zur Effizienzsteigerung beitragen. Vor allem

⁴² Siehe bereits oben Kap. 6, D., I., 2. und für die Thematik der KI-Erzeugnisse bereits MAAMAR, S. 128.

durch die Senkung der Informationskosten, die sich auf die Fix- und Transaktionskosten auswirken können.⁴³

Argumente aus dem Gleichheitsgebot sprechen ebenfalls für ein technologie-neutrales Schutzrecht für KI-Technologien. So soll nach Art. 3 Abs. 1 GG Gleiches gleich behandelt werden.⁴⁴ So ist es auch vor dem Hintergrund der Technologieneutralität des Urheberrechts ungerechtfertigt, die Investition in die Entwicklung von herkömmlicher Software urheberrechtlich zu schützen und die Investition in die Entwicklung intelligenter Software wie genetische Programme oder KNN nicht. Zwar lässt sich argumentieren, dass Software und intelligente Software ungleich seien. Doch handelt es sich in beiden Fällen um Informationsverarbeitung. Das *lex lata*-Ergebnis ist umso stoßender, wenn man bedenkt, dass intelligente Software in Form von genetischen Programmen oder KNN in der Lage ist, die komplexeren Probleme zu lösen als herkömmliche Programme und damit einen höheren Mehrwert mit sich bringen kann. Der Umstand der Ungleichbehandlung lässt sich auch auf dem Gebiet der KI-Technologien beobachten. So sind wie gesehen Expertensysteme geschützt, während genetische Programme und KNN schutzfrei bleiben. Auch dabei ist ersichtlich: die potentere Technologie ist schutzfrei, während die schwächere geschützt ist. Plädiert man für den Schutz von KNN, ist das stoßende Ergebnis der *lex lata*-Analyse nicht verhindert, denn genetische Programme sind einem urheberrechtlichen Schutz aufgrund des Schöpfungserfordernisses nicht zugänglich, bergen aber ähnliches Potenzial wie KNN. Aus innovationsökonomischer Sicht kann eine solche Situation zu (Fehl)Anreizen führen, nur noch in bestimmte Technologien zu investieren. Geht man von der Vergleichbarkeit der beiden Technologien aus, ergeben sich Risiken für die Gesamtwohlfahrt, indem nur gewisse Technologien geschützt werden. Zudem bräuchte ein technologie-neutrales Schutzrecht auch Rechtssicherheit betreffend noch zu entwickelnde KI-Technologien.

Schließlich spricht auch das makroökonomische Argument⁴⁵ des Standortvorteils für die Einführung eines Schutzrechtes. Mit den Marktdynamiken wurden

⁴³ Vgl. MAAMAR, S. 128.

⁴⁴ Für die Geltung des Gleichheitsgebotes im Urheberrecht vgl. Dreier/Schulze/DREIER, Einl. Rn. 39d.

⁴⁵ In Ergänzung der bislang mikroökonomisch geprägten Argumente der Markteffizienzen.

die (Wachstums)Potenziale aufgezeigt, die KI-Technologien mit sich bringen und sich positiv auf den Markt auswirken können.⁴⁶ Sowohl die Europäische Union als auch Deutschland nehmen dieses Potenzial wahr und möchten ein innovationsfreundliches Umfeld für Künstliche Intelligenz schaffen.⁴⁷ Ein Schutzrecht für KI-Technologien kann einen wichtigen Beitrag für ein solches Umfeld schaffen. Mit einem effizienten Schutzrecht kann Entwickler:innen und Investor:innen ein Anreiz geschaffen werden, ihre Tätigkeiten – vor allem Forschung und Entwicklung – in ein Land zu verlegen, in welchem ihre Innovationen bzw. Investitionen auch geschützt sind.⁴⁸ Damit sprechen auch wirtschaftspolitische Gründe für die Einführung eines Schutzrechtes an KI-Technologien in Deutschland.

⁴⁶ Siehe oben Kap. 6; vgl. auch MAAMAR, S. 133 f. m.w.N.

⁴⁷ So zum Beispiel für Deutschland statt vieler: KI-Strategie D, S. 8 und für die Europäische Union statt vieler: EG 71 AIA-Entwurf.

⁴⁸ Sogenanntes „*race to protection*“, siehe zu diesem ausführlicher MAAMAR, S. 133 ff. Siehe dort auch insbesondere den Hinweis auf eine international – v.a. aber europäisch – harmonisierte Form des Schutzrechtes. Zweifelsohne sind KI-Technologien als Teil der Digitalisierung ein globales Phänomen, das nicht an Landesgrenzen Halt macht. Dennoch ist betreffend die Harmonisierung ein Vorbehalt zu machen: unterschiedliche Schutzniveaus im internationalen Vergleich sind bereits heute bekannt. So ist es dann auch nicht notwendig, ein Schutzniveau bei KI-Technologien zu erreichen, welches demjenigen der USA entspricht. Eine vollkommene Harmonisierung auf dem EU-Binnenmarkt kann jedoch angezeigt sein – nicht zuletzt aus Binnenmarktsüberlegungen. Siehe zu den möglichen Wohlfahrtsverlusten bei unterschiedlichen Schutzniveaus ebenfalls MAAMAR, S. 134 f.

Teil 5

Schutzrecht an KI-Technologien de lege ferenda

Im Folgenden werden anknüpfend an die soeben aufgezeigten Schutzlücken die Anreizmechanismen dargelegt, welche ein neues Schutzrecht bedienen sollte und schließlich das Schutzrecht umrissen, welches eingeführt werden könnte.

Kapitel 11

Offenlegungsanreize

Die Indizien für ein Schutzbedürfnis wurden vor allem damit begründet, dass der Markt für KI-Technologien mehrere volkswirtschaftliche Ziele nicht zu erreichen scheint. Einerseits weist er hohe Kosten im Umgang mit den Technologien auf.¹ Andererseits werden die Technologien nicht weit verbreitet.² Damit unterbleibt eine Informationsverbreitung weitgehend, was sowohl aus wohlfahrts- als auch aus innovationsökonomischen Gesichtspunkten zu bemängeln ist.³

Zielverfehlungen sind zu einem großen Teil darauf zurückzuführen, dass KI-Technologien überwiegend geheim gehalten werden. Sie werden vorwiegend cloudbasiert als Dienstleistung angeboten und nicht als Produkt als solches in Form von Überlassung der Software.⁴ Ob diese Geheimhaltung mit dem Ergebnis der *lex lata*-Analyse zusammenhängt, lässt sich hier nicht abschließend beantworten. Ein fehlendes Schutzrecht begünstigt zumindest die Tendenz in Richtung Geheimhaltung.⁵

Ein Schutzrecht für KI-Technologien muss also so ausgestaltet sein, dass es Anreize setzt, die Technologien nicht geheim zu halten. So können die hohen Kosten im Umgang gesenkt und damit die Effizienz erhöht werden – die Argumente also, die in einem Schritt überhaupt für ein Schutzbedürfnis sprechen. Ob darüber hinaus auch eine aktive Offenbarung wie im Patentrecht notwendig ist,⁶ müssen ökonomische Erhebungen zeigen. Eine solche Offenbarung ist nicht

¹ Siehe dazu oben Kap. 6, D. I., 1.

² Siehe oben Kap. 6, D., II.

³ Siehe dazu oben Kap. 6, E.

⁴ Siehe oben Kap. 6, C.

⁵ Siehe oben Kap. 6, C. zu den möglichen Gründen.

⁶ Vgl. oben Kap. 7, B., III.

zwingend notwendig, um die KI-Technologie einer weiteren Verbreitung zuzuführen. Ein wirksames Schutzrecht ohne Offenbarungserfordernis kann bereits dazu beitragen, dass eine KI-Technologie in Form von Software nicht mehr lediglich cloudbasiert, sondern als Produkt angeboten wird. Mit einem Schutzrecht für KI-Technologien sind nämlich Geheimhaltungsmaßnahmen zwecks Investitionsamortisation obsolet. Über das Produkt können andere Personen als die Rechteinhaber:innen auf den Code – die zu schützende Information – zugreifen und entsprechend den Vorschriften des Schutzrechtes weiterentwickeln. Damit kann ein Schutzrecht auch ohne Offenbarungserfordernis zusätzlich zu tieferen Kosten im Umgang auch die Verbreitung der Technologie in Form von Information begünstigen. So kann ein Schutzrecht zusätzlich die statische Effizienz erhöhen. Schafft ein Schutzrecht einen Anreiz zum Verzicht auf Geheimhaltung, werden zudem Bewegungen wie *copyleft* oder *opencode* überhaupt sinnvoll ermöglicht.⁷

Das Anknüpfen eines Schutzrechts an eine Offenbarung wie im Patentrecht kann die statische Effizienz maximieren. Allerdings erfordert eine Offenbarung wie im Patentrecht eine Registerführung. Ein Offenbarungserfordernis ist also mit Kosten verbunden. Kosten, die wiederum abschreckend auf Entwickler:innen und Investor:innen wirken können und die Effizienz mindern. Solange allerdings die Geheimhaltungskosten die zusätzlichen Kosten für eine Offenbarung überwiegen, ist das Schutzrecht mit Offenbarungserfordernis nach wie vor der Schutzfreiheit vorzuziehen, weil es effizienter ist. Zudem kann eine solche Offenbarung auch als Alleinstellungsmerkmal verwendet werden. Anbieter:innen von KI-Technologien können sich mit einer Offenbarung von der Konkurrenz abheben, die möglicherweise lediglich herkömmliche Software unter dem Titel von Künstlicher Intelligenz anbietet.⁸

Ein zusätzlicher Anreiz speziell für die Produktion von KI-Technologien scheint nicht nötig zu sein. Der Markt für KI-Technologien scheint das Ziel der hohen Produktion zu erreichen.⁹ Allerdings können die Kostensenkungen, die

⁷ Siehe dazu oben Kap. 5, B. II.

⁸ Siehe dazu oben Kap. 6, D. III.

⁹ Siehe oben Kap. 6, E.

mit einem neuen Schutzrecht einhergehen, auch positiv auf die dynamische Effizienz wirken.¹⁰ Den gleichen Effekt kann ein Schutzrecht als solches ebenfalls bereits bewirken. Das bloße Bestehen eines Schutzrechts für KI-Technologien setzt *eo ipso* einen Anreiz zur Produktion von KI-Technologien. Sind die Geheimhaltungsmaßnahmen nicht mehr zwecks Investitionsamortisation nötig, können mehr Marktteilnehmer:innen auf den Markt treten, die ohne Schutzrecht von den hohen Kosten für die Geheimhaltung abgeschreckt wurden. Damit kann ein Schutzrecht für KI-Technologien auch oligopolistischen Strukturen entgegenwirken

¹⁰ Siehe bereits oben Kap. 6, E.

Kapitel 12

Schutzvoraussetzungen und Rechtsinhaber

Neben den Anreizen, die ein neues Schutzrecht schaffen soll, muss auch der vom Schutzrecht erfasste Schutzgegenstand skizziert werden. Bei der Untersuchung der immaterialgüterrechtlichen Schutzfähigkeit von KI-Technologien wäre es naheliegend schlicht KI-Technologien als Schutzgegenstand des Schutzrechts zu definieren. Im ersten Teil wurde jedoch aufgezeigt, dass mit dem Begriff der Künstlichen Intelligenz zahlreiche Unbestimmtheiten und Ungenauigkeiten verbunden sind. Als Schutzgegenstand für ein neues Schutzrecht sollen im Rahmen dieser Arbeit KI-Technologien gelten, wie sie unter Kapitel 1.B. beschrieben wurden: Softwareebenen¹, die über Autonomie im hier dargelegten Sinn² verfügen.

Es muss sich also um Softwareebenen handeln, die sich die Regeln der Informationsverarbeitung zu einem überwiegenden Teil selbst aneignen und damit über Lernfähigkeit verfügen.³ Diese Aneignung erfolgt anhand von (Trainings)Daten. Der Trainingsschritt wurde auch als ein investitionsintensiver Schritt in der Entwicklung von KI-Technologien identifiziert. Deshalb und weil das Schutzbedürfnis überwiegend mit Investitionsargumenten begründet wird,⁴ bietet es sich auch an, das Schutzrecht für KI-Technologien *de lege ferenda* von einer (erheblichen) Investition abhängig zu machen.⁵

¹ Siehe zum Begriff oben Kap. 1, A.

² Vgl. dazu oben Kap. 1, B. II.

³ Bzw. Autonomie oder Intelligenz.

⁴ Siehe oben Kap. 6, D.

⁵ Für KI-Erzeugnisse auch MUHR, S. 194 ff.

Ein solches Erfordernis ist bereits von den Leistungsschutzrechten⁶, insbesondere aber vom Datenbankherstellerrecht in § 87a ff. UrhG bekannt.⁷ Bei diesem ist die in der Datenbank verkörperte Investition Schutzgegenstand.⁸ Mit den KI-Technologien verhält es sich ähnlich: auch dort verkörpert die Technologie als solche die Investitionen, welche in der Entwicklung der Softwareebene aufgewendet werden mussten – seien dies Investitionen finanzieller oder zeitlicher Natur. Auch Investitionen in Form von Arbeit kommen in Frage⁹: Die Datenbeschaffung, die Datenaufarbeitung, die Programmierungsschritte und die Trainingsphase erfordern jeweils finanzielle, zeitliche und Arbeitsressourcen.¹⁰ Die KI-Technologien verkörpern diesen Investitionsaufwand und gerade nicht einen kreativen Ausdruck menschlichen Schaffens.¹¹

Das Investitionserfordernis – bspw. in Form des Trainingsprozesses oder der Datenakquise und -kuration – als Schutzvoraussetzung grenzt KI-Technologien sodann auch vom herkömmlichen Computerprogrammenschutz ab. Die Untersuchung hat gezeigt: je autonomer eine Technologie, desto eher ist sie nicht vom Computerprogramm- oder vom sonstigen Urheberrechtsschutz erfasst.¹² Expertensysteme können zwar als KI-Technologien aufgefasst werden. Sie verfügen auch über einen gewissen, jedoch eher geringen Grad an Autonomie.¹³ Doch ihre Entwicklung ist nicht derart investitionsintensiv wie diejenige von KNN oder genetischen Programmen. Die Entwicklung von Expertensystemen bedarf zwar auch eines Datensatzes, allerdings wird dieser *direkt* verwendet – als Wissensbasis. Der Datensatz wird nicht verwendet, um Muster oder Zusammenhänge zu erkennen und daraus neue Verhaltensregeln zu generieren, wie dies bei KNN oder genetischen Programmen erfolgt.¹⁴ Demnach wären Expertensysteme wohl nicht vom Schutzrecht *de lege ferenda* geschützt. Das ist jedoch

⁶ Siehe oben Kap. 8, A., IV.

⁷ Siehe dazu oben Kap. 8, A., IV.

⁸ Oben Kap. 8, A., IV.

⁹ Siehe oben Kap. 8, A., IV. für die Investitionsarten, die beim Datenbankherstellerrecht infrage kommen.

¹⁰ Siehe oben Kap. 6, E.

¹¹ Dies ist mitunter auch Grund für die Schutzfreiheit der Technologien, siehe oben Kap. 8, B., III., 6.

¹² Vgl. oben bspw. Kap. 10, A., II.; ausführlich Kap. 8, B.

¹³ Siehe dazu genauer oben Kap. 2, C. I.; Kap. 2, C., IV.

¹⁴ Siehe oben Kap. 2, C., IV.

nicht verwerflich: Expertensysteme bzw. deren Einzelteile sind bereits *de lege lata* ausreichend geschützt.¹⁵ Die direkte Verwendung des Datensatzes als Wissensbasis bedingt die Unabhängigkeit der einzelnen Datenbankelemente. Dies wiederum führt in Kombination mit einer erheblichen Investition zur Schutzzfähigkeit der Wissensbasis nach § 87a ff. UrhG.¹⁶

Man mag aus Gleichheitsüberlegungen¹⁷ einwenden, das Abstellen auf eine Investition sei stoßend. Zumal beim urheberrechtlichen Computerprogrammenschutz – welcher ebenfalls Softwareformen schützt – keine gesonderte Investition vorausgesetzt wird. Eine solche Ungleichbehandlung lässt sich mit dem urheberrechtlichen Anthropozentrismus rechtfertigen: In Computerprogrammen nach § 69a UrhG kommt der menschliche Geist im Schutzgegenstand selbst zum Ausdruck und ist aus diesem Grund geschützt. Bei KI-Technologien tritt das menschlich schöpferische, kreative Element in den Hintergrund und das funktionale Element in den Vordergrund. Das funktionale Element ist aber bei Computerprogrammen nicht geschützt.¹⁸ Demnach ist eine unterschiedliche Behandlung von herkömmlichen Computerprogrammen und KI-Technologien vertretbar und gerechtfertigt.

Das Investitionserfordernis ermöglicht auch die einfache Rechtszuweisung. Bei der Entwicklung von KI-Technologien sind mehr Akteur:innen beteiligt als bei der Entwicklung von herkömmlicher Software. Insbesondere die trainierende Person ist in dieser Hinsicht neu. Dies erschwert eine Zuweisung der Rechtsinhaberschaft grundsätzlich. Stellt das Schutzrecht *de lege ferenda* jedoch auf eine Investition ab, kann auch die Rechtsinhaberschaft an diese Investition geknüpft werden. Auch im Datenbankherstellerrecht nach § 87a ff. UrhG gilt nach § 87a Abs. 2 UrhG diejenige Person als Datenbankhersteller und damit als Rechtsinhaber, welche die Investition vorgenommen hat. Die Rechtsinhaberschaft kann also auch beim Schutzrecht *de lege ferenda* an das Tätigen der Investition geknüpft werden.

¹⁵ Siehe oben Kap. 8, B., I.

¹⁶ Vgl. oben Kap. 8, B., I.

¹⁷ Siehe dazu oben Kap. 10, C.

¹⁸ Siehe dazu oben Kap. 8, A., III., 1.

Kapitel 13

Schutznatur, -umfang und -dauer

Ob es sich um einen relativen oder absoluten Schutz handeln soll und wie groß der Schutzzumfang sein soll, muss sich nach der Amortisationsmöglichkeit der Investition richten. Das Schutzrecht ist also vorzugsweise so auszugestalten, dass eine wirksame Amortisation der Investition möglich ist

Ein Schutzrecht für KI-Technologien sollte absolut-rechtlicher Natur sein. Ein relativer Schutz besteht schon in Form des GeschGehG. Es wurde gezeigt, dass ein relativer Schutz die Schutzbedürfnisse nicht zu befriedigen vermag.¹ Ein relativer Abwehranspruch verhindert insbesondere nicht die Veröffentlichung und Verwertung des Schutzgegenstandes durch Dritte. Damit ist eine Amortisation der Investitionen aber wiederum nicht mehr möglich.²

Der Schutzzumfang *de lege ferenda* kann sich betreffend die zustimmungsbedürftigen Handlungen an demjenigen des Computerprogrammschutzes in § 69c UrhG orientieren: Demnach wären die (dauerhafte oder vorübergehende) Vervielfältigung, die Übersetzung, die Bearbeitung, das Arrangement und andere Umarbeiten sowie jede Form der Verbreitung und die öffentliche Wiedergabe einschließlich der öffentlichen Zugänglichmachung zustimmungsbedürftige Handlungen. Im Unterschied zum Computerprogrammschutz nach § 69a ff. UrhG sollten aber auch funktionale Nachahmungen der KI-Technologie von den zustimmungsbedürftigen Handlungen erfasst sein. Die Entwicklung von KI-Technologien ist überwiegend von funktionalen und nicht kreativen Überlegungen geprägt.³ Es geht mitunter primär darum, eine bestimmte Funktionalität zu erreichen. Die konkrete Ausdrucksform des Programmablaufs ist dabei nicht zentral und auch nicht vom Menschen beeinflusst. Der menschliche

¹ Siehe oben Kap. 9, C., III.

² Siehe oben Kap. 9, C., 1.

³ Vgl. oben Kap. 2, C., II., 3.; Kap. 2, C., III., 4.; Kap. 2, C., IV.

Einfluss bezieht sich aber auf die Wahrnehmung des zu lösenden Problems und auf das Legen der Grundlagen, die zum Erreichen der Funktionalität notwendig sind.⁴ Deshalb liefe ein Schutz der bloßen Ausdrucksform ins Leere bzw. deckt das aufgezeigte Schutzbedürfnis nicht.

Allerdings ist der Schutzzumfang auch zu begrenzen. Es sollte analog dem Datenbankherstellerrecht in § 87a ff. UrhG eine Abgrenzung “nach unten” erfolgen. Die unzulässigen Handlungen sollten nicht auch “Kleinstbestandteile” der KI-Technologien umfassen. Logische Grundsätze wie bspw. Rechenregeln müssen gemeinfrei bleiben.⁵ Ein Ansatz wäre, das Schutzrecht *de lege ferenda* analog § 87b UrhG darauf zu begrenzen, dass lediglich die zustimmungsbedürftigen Handlungen⁶ erfasst sind, die die KI-Technologie insgesamt oder einen nach Art oder Umfang wesentlichen Teil der KI-Technologie erfassen. Die Vielfältigung, Verbreitung und öffentliche Wiedergabe unwesentlicher Teile der KI-Technologie wäre demnach nicht zustimmungsbedürftig. Damit lässt sich im Sinne eines Ausgleiches zwischen Investitionsschutz und Informationsfreiheit der Wohlfahrtsverlust reduzieren.⁷

Das Erfordernis der Wesentlichkeit der vervielfältigten, verbreiteten und öffentlich wiedergegebenen Teile grenzt die vorliegende Lösung auch von derjenigen von MUHR, S. 194 ff. ab. MUHR plädiert unter dem Titel *des Schutzes von KI-Erzeugnissen* (und nicht für denjenigen der Schutzfähigkeit der KI-Technologie) für ein Leistungsschutzrecht an KI-Erzeugnissen zugunsten der Hersteller:innen von KI-Technologien.⁸ Eine solche Lösung geht einerseits zu weit, weil sie die Nutzer:innen gänzlich außer Acht lässt und namentlich bei *large language models* wie bspw. ChatGPT den Entwickler:innen die Berechtigungen an sämtlichen Erzeugnisse einräumen will. Andererseits trennt die Lösung nicht sauber zwischen dem Entwicklungs- und Anwendungszeitraum von KI-Technologien und berücksichtigt nicht die damit zusammenhängenden unter-

⁴ Vgl. oben Kap. 2, C., II., 3. und Kap. 2, C., IV.

⁵ Vgl. dazu auch oben Kap. 7, A., III.

⁶ Siehe soeben.

⁷ Vgl. Dazu für das Datenbankherstellerrecht z.B. Dreier/Schulze/DREIER, UrhG, § 87b Rn. 5.

⁸ MUHR, S.194 ff., insb. S. 202.

schiedlichen Wertungen für einen Schutz. Deshalb fordert die vorliegende Arbeit ein Leistungsschutzrecht an wesentlichen Teilen der KI-Technologie als solche – und nicht an den Erzeugnissen.

Was als wesentlicher Bestandteil zu gelten hat, wird von der Rechtsprechung zu konkretisieren sein.⁹ Die Bestimmung der Wesentlichkeit dürfte sich auch bei KI-Technologien nur im Einzelfall beantworten lassen.¹⁰ Faktoren sind einerseits von KI-Technologie zu KI-Technologie verschieden und andererseits davon abhängig, inwiefern und wie stark die Investition in einem Bestandteil der KI-Technologie verkörpert ist.¹¹ So dürften einzelne Bestandteile von genetischen Programmen eher weniger von Wert sein, da das Programm vorwiegend nur in seiner Gesamtheit funktionsfähig ist.¹² Bei KNN hingegen können bereits Einzelteile für sich funktionsfähig und somit von Wert sein bzw. die Investition (teilweise) verkörpern.¹³

Der Schutzzumfang darf nur so weit gefasst sein, dass er den Wohlfahrtsverlust der Schutzfreiheit deckt. Mit anderen Worten darf der mit dem Ausschließlichkeitsrecht einhergehende Wohlfahrtsverlust¹⁴ nicht den durch die Schutzfreiheit verursachten Wohlfahrtsverlust überwiegen. So können auch beim Schutzrecht *de lege ferenda* zustimmungsfreie Handlungen vorgesehen werden.¹⁵ Ein Ausgleich kann auch über Zwangslizenzen erreicht werden. Auch die Abwägung des Wohlfahrtsverlustes durch Schutzfreiheit mit dem Wohlfahrtsverlust durch die Einführung des Schutzrechtes (unter Berücksichtigung der zustimmungsfreien Handlungen und etwaiger Zwangslizenzen) ist Gegenstand ökonomischer empirischer Erhebungen.

Die Bestimmung der Schutzdauer sollte ebenfalls ökonomisch begründet werden. Durch die Investitionsschutzargumentation rechtfertigt sich nur eine

⁹ So bereits auch schon das für das Datenbankherstellerrecht: Dreier/Schulze/DREIER, UrhG, § 87b Rn. 5.

¹⁰ Vgl. für das Datenbankherstellerrecht Dreier/Schulze/DREIER, UrhG, § 87b Rn. 5.

¹¹ Vgl. für das Datenbankherstellerrecht Dreier/Schulze/DREIER, UrhG, § 87b Rn. 5.

¹² Vgl. oben Kap. 2, C., 2.

¹³ Siehe zu den möglichen Bestandteilen von KNN oben Kap. 8, B.III.5.

¹⁴ Monopolähnliche Stellung, siehe oben Kap. 4, B.

¹⁵ Generell Schranken oder bspw. für Computerprogramme §§ 69d f. UrhG.

Schutzdauer in der Länge der Dauer für eine Investitionsamortisation. Aus diesem Blickwinkel scheint eine Schutzdauer analog dem Urheberrecht von 70 Jahre nach dem Tod des Urhebers als weitaus zu lang.¹⁶ Die Festlegung der Mindestdauer hat sich an den Investitionsamortisationsmöglichkeiten zu orientieren.

¹⁶ Vgl. auch MUHR, S. 195.

Kapitel 14

Verortung des Schutzrechts

Schließlich gilt es vom Gesetzgeber, das Schutzrecht noch zu verorten. Möglichkeiten bestehen in der Schaffung eines eigenen Gesetzes oder aber in der Ansiedlung des Schutzrechtes in einem bestehenden Rechtsrahmen. Wenn das Schutzrecht *de lege ferenda* auf eine Investition als Schutzvoraussetzung abstellen soll, handelt es sich um ein Leistungsschutzrecht.¹ Demnach liegt es nahe, das Schutzrecht im UrhG zu verorten. Auch ohne Investitionserfordernis bietet sich eine Verortung im UrhG an. Dies ergibt sich aus der technologischen Nähe von KI-Technologien zu Computerprogrammen. Dagegen spricht allerdings der mangelnde Werkcharakter von KI-Technologien sowie die fehlende Kreativität.

¹ Vgl. oben Kap. 8, A., IV.; Kap. 12.

Kapitel 15

Zwischenergebnis

Die konkrete Ausgestaltung des Gesetzestextes für das Schutzrecht *de lege ferenda* muss interdisziplinär erfolgen. Das Schutzrecht soll einen Anreiz setzen, die KI-Technologien nicht mehr geheim zu halten. So ein Anreiz kann bereits durch die Schaffung eines explizit für KI-Technologien zugeschnittenen Schutzrechts geschaffen werden. Maximiert könnte ein Offenbarungsanreiz und damit die statische Effizienz durch ein Offenbarungserfordernis wie im Patentrecht: „Schutzrecht gegen Offenbarung“. Schutzgegenstand *de lege ferenda* sollen autonome Softwareebenen sein: Software, die sich die Regeln der Informationsverarbeitung selbständig aneignet. Da das Schutzbedürfnis zu einem großen Teil mit Investitionsschutzargumenten begründet wurde, ist es folgerichtig, den Schutz von einer erheblichen Investition analog dem Datenbankherstellerrrecht abhängig zu machen. Der Schutz soll darüber hinaus lediglich die Technologie insgesamt sowie wesentliche Teile der Technologie erfassen. Nicht erfasst werden sollten nicht wesentliche Bestandteile der Technologie, insbesondere aber logische Abläufe und Rechenregeln. Ein relatives Schutzrecht vermag die aufgezeigten Schutzbedürfnisse nicht zu decken, weshalb das Schutzrecht *de lege ferenda* Ausschließlichkeitscharakter aufweisen sollte. Ein Ausgleich zwischen Ausschließlichkeitsrecht und Informationsfreiheit kann insbesondere mittels Schranken und Zwangslizenzen erreicht werden. Die Schutzdauer muss sich an der Dauer der Amortisation der Investition orientieren

Ergebnisse der Untersuchung

Der Begriff der Künstlichen Intelligenz umschreibt ein interdisziplinäres Forschungsfeld, das sich mit der Nachahmung menschlicher Intelligenz mittels technischer Mittel befasst. Es handelt sich um einen sehr weiten, oft sehr ungenau verwendeten Begriff. Er ist vielmehr Schlagwort als Arbeitsbegriff. Der Untersuchungsgegenstand sind KI-Technologien. KI-Technologien sind Softwareebenen, die so entwickelt werden, dass ihnen die Regeln zur Informationsverarbeitung nicht von Programmierer:innen direkt vorgegeben werden. Sie erlernen diese Regeln – zumindest teilweise – selbstständig. Die Fähigkeit, sich die Regeln der Informationsverarbeitung selbst zu setzen, wird im Rahmen dieser Arbeit als Autonomie verstanden.

Es existieren zahlreiche verschiedene Technologien, die über Autonomie verfügen. Die Autonomiegrade – und damit das Maß an selbstbestimmter Regelsetzung – unterscheiden sich dabei. Diese unterschiedlichen Autonomiegrade zeigen sich mehrheitlich an den verschiedenen Entwicklungsansätzen und daran, wie die verschiedenen Technologien funktionieren. Den autonomen Technologien ist gemein, dass zusätzlich zum Programmierungsschritt noch ein weiterer Entwicklungsschritt hinzukommt – in Form des Trainings. Dieses Training erfolgt anhand von Daten. Beispiele für autonome Technologien sind Expertensysteme, KNN und genetische Programme.

Expertensysteme werden im Vergleich zu KNN und genetischen Programmen nicht im eigentlichen Sinne trainiert. Sie sind auch nicht auf Trainingsdaten angewiesen. Bei ihnen handelt es sich vielmehr um Wissensdaten, auf welche sie direkt zugreifen. Ihre Autonomie besteht darin, dass sie sich neue Verknüpfungen innerhalb der Wissensebene erschließen und damit Wissen anders interpretieren können als von den Entwickler:innen vorgegeben. Darüber hinaus können sie neues Wissen herleiten. Dennoch sind sie eher am unteren Ende der Autonomieskala anzusiedeln. Zudem verwenden sie in erster Linie die ihnen zur Verfügung gestellten Daten *direkt* zur Aufgabenlösung und leiten nicht aus den Daten die Regeln der Informationsverarbeitung *indirekt* ab. KNN und genetische Programme sind demgegenüber wesentlich autonomer und erschließen sich aus den Trainingsdaten in einem *trial and error*-Verfahren die Regeln der

Informationsverarbeitung. Sie verwenden die Trainingsdaten demnach indirekt. Bei herkömmlichen Softwareebenen wird dem Computer eine Funktion Schritt für Schritt in einer für den Computer verständlichen Form beigebracht bzw. vorgegeben. Bei KI-Technologien hingegen wird dem digitalen System das notwendige Werkzeug – unter anderem in Form von Trainingsdaten – bereitgelegt und die konkrete Funktion eignet sich das System in einem zweiten Schritt selbst- bzw. eigenständig an. Das Charakteristikum der Autonomie sowie das Erfordernis der Trainings- bzw. Wissensdatenmenge sind also die wesentlichen Unterschiede bei der Entwicklung von KI-Technologien im Vergleich zu herkömmlichen Softwareebenen.

Bevor die Frage nach der Schutzfähigkeit von KI-Technologien beantwortet werden konnte, war zu erörtern, ob KI-Technologien überhaupt eines Schutzes bedürfen. KI-Technologien verarbeiten Informationen und stellen als solche selbst Informationen dar – mithin handelt es sich bei KI-Technologien um immaterielle Güter. Deshalb wurden im zweiten Teil die Rechtfertigungsansätze des Immaterialgüterrechts dargelegt. Es wurde aufgezeigt, dass in einem modernen Verständnis die Zuordnung von immateriellen Gütern mittels Ausschließlichkeitsrechten weitgehend ökonomisch gerechtfertigt wird. Demnach wurde auch für die vorliegende Arbeit ein ökonomischer Ansatz gewählt.

Dieser Ansatz wurde im dritten Teil vertieft, indem der Markt für KI-Technologien ökonomisch analysiert worden ist. Das Ergebnis dieser Analyse zeigt, dass der Markt für KI-Technologien Indizien für ein rechtliches Schutzbedürfnis aufweist. Dazu wurde an die ökonomischen Rechtfertigungstheorien aus dem zweiten Teil angeknüpft. Als rechtfertigendes Ziel von Schutzrechten an KI-Technologien wurde die wohlfahrtsökonomische Effizienzsteigerung festgelegt. Ausgehend von den Marktversagensgründen, die in einer juristischen Arbeit nicht bewiesen werden können, wurden drei wohlfahrtsökonomische Effizienzziele ausgearbeitet, die als normativer Maßstab für die Marktanalyse dienen. Demnach wird im Rahmen dieser Arbeit ein Markt für Güter als effizient und damit nicht als schutzbedürftig erachtet, wenn er folgende drei Ziele erreicht: (i) eine hohe Produktion von neuen Gütern (dynamische Effizienz), (ii) eine weite Verbreitung dieser Güter (statische Effizienz) und (iii) niedrige Kosten im Umgang mit den Gütern.

Der Markt für KI-Technologien wurde ausgehend von seinen Charakteristika, seiner Treiber sowie der Produkte des Marktes in seiner Effizienz bewertet. Die Bewertung erfolgte anhand jener drei genannten volkswirtschaftlichen Ziele. Die Bewertung des Marktes für KI-Technologien ergab, dass der Markt bei Schutzfreiheit von KI-Technologien ineffizient hohe Kosten aufweist. Diese hohen Kosten sind auf den Umstand zurückzuführen, dass die Mehrheit der Anbieter:innen von KI-Technologien ihr Produkt lediglich cloudbasiert anbieten und nicht als Produkte, welche lokal auf den Endgeräten der Nutzer:innen ablaufen. Cloudanwendungen bringen mit sich, dass die KI-Technologie als solche nicht verbreitet wird – sie wird geheim gehalten bzw. zumindest nicht offengelegt. Das Anbieten von KI-Technologien als Cloudlösung führt zu zusätzlichen Kosten, die nicht direkt mit der Entwicklung dieser Technologien zusammenhängen und auch nicht aus der Natur der Technologien hervorgehen. Es kann nicht eindeutig beurteilt werden, ob das überwiegende Cloudangebot ausschließlich auf Geheimhaltungsmotivationen der Anbieter:innen oder auch noch auf andere Überlegungen wie bspw. fehlende Rechenkapazitäten zurückzuführen ist. Die Antwort auf diese Frage ist aber für den Ausgang der vorliegenden Arbeit nicht von Relevanz: Einerseits entwickeln sich diese Rechenkapazitäten nach dem *Moore'schen Gesetz* weiter. Andererseits wird trotzdem ein Teil der KI-Anwendungen auch lokal angeboten. Zudem führt die vorherrschende Situation – unabhängig der Ursache – dazu, dass die Güter nicht verbreitet werden. Das Ziel der statischen Effizienz wird also nicht erreicht. Die Situation zeigt sich im *status quo* zuletzt so, dass Kosten bei der Mehrheit der Marktteilnehmer:innen aufgewendet werden, die nicht mit der Entwicklung von KI-Technologien zusammenhängen. Das Ziel der niedrigen Kosten im Umgang scheint demnach ebenfalls nicht erreicht zu werden. Bei (ineffizient) hohen Kosten muss sodann auch hinterfragt werden, ob die Potenziale der dynamischen Effizienz gänzlich ausgeschöpft werden. Die hohen Kosten können nämlich eine abschreckende Wirkung auf potenzielle Markteinsteiger:innen haben.

Das Ergebnis der Marktanalyse deutet also auf mehrere Indizien von Ineffizienzen hin und spricht damit für das Vorliegen eines Schutzbedürfnisses für KI-Technologien. Dieses Schutzbedürfnis ergibt sich vor allem aus dem Mangel an Schutz der für die Entwicklung von KI-Technologien notwendigen Investitionen. Die anschließende Untersuchung der rechtlichen Schutzmöglichkeiten *de lege lata* ergab, dass dieses Schutzbedürfnis nicht gedeckt werden kann.

Das Patentrecht bietet zwar grundsätzlich technologieneutrale Schutzmöglichkeiten. Allerdings sind die Patentierungsanforderungen für KI-Technologien als solche sehr hoch. Viel eher dürfen sich die Patente auf dem Gebiet der KI-Technologien auf technische Implementierungen von KI-Technologien beschränken. Das führt einerseits dazu, dass nichttechnische Anwendungsgebiete von KI-Technologien einem patentrechtlichen Schutz nicht zugänglich sind. Andererseits führt es dazu, dass bei Patentierung von technisch implementierten KI-Technologien die Technologie als solche gar nicht zwingend zu offenbaren ist. Unter Umständen genügt das Beschreiben der technischen Vorrichtung oder des technischen Verfahrens. In solchen Fällen verhilft das Patentrecht nicht zur Steigerung der Güterverbreitung bzw. der statischen Effizienz.

Die urheberrechtliche Schutzfähigkeit von KI-Technologien lässt sich nicht technologieneutral beantworten. Das liegt einerseits im urheberrechtlichen Computerprogramm-begriff und andererseits an den verschiedenen Entwicklungs- und Funktionsweisen der unterschiedlichen KI-Technologien begründet. Damit ist auch die erste Schwäche des urheberrechtlichen Schutzes von KI-Technologien offenbart: Obwohl das Urheberrecht technologieneutral ausgestaltet ist bzw. sein sollte, behandelt es nicht alle KI-Technologien und damit auch nicht alle Softwareebenen gleich: herkömmliche (nicht intelligente) Softwareebenen sind von einem Schutz erfasst, intelligente Softwareebenen überwiegend nicht. Dies kann zu Fehlanreizen führen. Expertensysteme sind in ihren einzelnen Bestandteilen von einem urheberrechtlichen (Leistungs)Schutz erfasst: Die Wissensbasis dürfte regelmäßig vom Datenbankherstellerrecht in §§ 87a ff. UrhG erfasst sein. Die Inferenzmaschine dürfte regelmäßig urheberrechtlichen Computerprogramm-schutz im klassischen Sinne nach §§ 69a ff. UrhG genießen. Die Benutzeroberfläche kann hingegen nur in ihrer konkreten Gestaltungsform als Werk nach § 2 UrhG geschützt sein, nicht aber als Computerprogramm nach §§ 69a ff. UrhG. Bei der genetischen Programmierweise gestaltet sich die Situation aus Sicht der Entwickler:innen und Anbieter:innen prekärer: Zwar ist die Programmierumgebung, welche die einzelnen Programme (Individuen) generiert, regelmäßig vom urheberrechtlichen Computerprogramm-schutz nach §§ 69a ff. UrhG erfasst. Die Fitnessfunktion kann ebenfalls Schutz nach §§ 69a ff. UrhG genießen. Das Ergebnis der genetischen Programmierweise – das Ziel-Programm – kann aber keinen urheberrechtlichen Schutz erfahren. Das gilt auch für sämtliche Vorgänger des Ziel-Programmes. Sie sind weder als

Computerprogramm nach § 69a UrhG noch als sonstiges Werk nach § 2 UrhG einem urheberrechtlichen Schutz zugänglich. Dies liegt hauptsächlich darin begründet, dass sie nicht das Ergebnis einer menschlichen individuellen geistigen Schöpfung sind. Der Schutz der Programmierumgebung sowie der Fitnessfunktion ist aus Sicht der Entwickler:innen und Anbieter:innen jedoch wertlos, wenn das Ergebnis der Entwicklung – das Ziel-Programm – schutzfrei ist. Nur dieses Ziel-Programm geht in die Anwendung. Die Programmierumgebung sowie die Fitnessfunktion sind in der Anwendungsphase unerheblich. In Bezug auf genetische Programme stellt das Urheberrecht also kein wirksames Mittel für den Investitionsschutz dar. Dieser Schluss gilt auch für den Schutz von KNN. Weder untrainierte noch trainierte neuronale Netze sind gemäß hier vertretener Ansicht einem urheberrechtlichen Computerprogrammschutz zugänglich. Die Trainingsergebnisse im Sinne der Gewichtungseinstellungen der Neuronen sind ebenfalls urheberrechtlich schutzfrei. Sie können weder Gegenstand des Computerprogrammschutzes nach §§ 69a ff. UrhG noch des Datenbankherstellerrechts nach §§ 87a ff. UrhG sein. Ebenfalls außer Betracht fällt ein Schutz als Datenbankwerk nach § 4 UrhG oder als sonstiges Werk nach § 2 UrhG. Untrainierte KNN können unter Umständen einen Schutz als sonstiges Werk im Sinne von § 2 UrhG genießen, nicht aber als Computerprogramm geschützt sein. Voraussetzung für einen Schutz als sonstiges Werk nach § 2 UrhG ist aber in jedem Fall, dass sie über ein Kommunikationselement verfügen. Einzelne Bestandteile von neuronalen Netzen können einem urheberrechtlichen Computerprogrammschutz zugänglich sein. Ebenso wie der Optimierungsalgorithmus. Das aus Sicht der Entwickler:innen und Anbieter:innen Wesentliche – untrainierte KNN, trainierte KNN sowie die Gewichtungsinformationen – bleibt aber einem urheberrechtlichen Schutz unzugänglich. Selbst wenn man trainierten KNN einen Schutz zusprechen möchte, lässt sich die Investition über das Urheberrecht nicht schützen. Das liegt darin begründet, dass das Urheberrecht jeweils nur die konkrete Ausdrucksform eines Werkes schützt. Weder die dem Werk zugrundeliegenden Ideen noch die Funktionalität eines Computerprogrammes können geschützt sein. Das führt dazu, dass sich selbst bei Schutzzfähigkeit eines trainierten KNN dieses relativ einfach lediglich funktional – und damit urheberrechtlich zulässig – nachahmen lässt. Dies ist vergleichsweise einfach möglich, da das untrainierte KNN sowie die Gewichtungsinformationen schutzfrei sind. Trainingsdaten kann jedoch in ihrer Gesamtheit unter Umständen im Einzelfall ein urheberrechtlicher Schutz nach § 2 Abs. 1 Nr.

7 UrhG oder § 4 UrhG und leistungsschutzrechtlicher Schutz gemäß §§ 87a ff. UrhG zugesprochen werden. Das Urheberrecht vermag also – außer bei den Expertensystemen – die in Teil drei der Arbeit dargelegten Schutzbedürfnisse nicht zu befriedigen. Demnach ergeben sich auch nach Betrachtung des Urheberrechts Schutzlücken.

Das Geschäftsgeheimnisrecht in Form des GeschGehG vermag diese Lücken nicht zu schließen. Erstens bietet es als relatives Recht lediglich einen schwachen Schutz, der nicht absolut vor Nachahmer:innen schützt. Zudem knüpft dieser schwache Schutz an Geheimhaltungsmaßnahmen – und damit Zusatzkosten – an. Der Geschäftsgeheimnisschutz senkt damit aktiv die Effizienz, indem er die Kosten im Umgang mit den Geheimnisgütern erhöht. Drittens ermöglicht das GeschGehG durch die Erlaubnis zum *reverse engineering* Nachahmer:innen aktiv, an das Geschäftsgeheimnis und in diesem Falle an die KI-Technologie zu gelangen. Nachahmer:innen können so an die KI-Technologie gelangen und diese darüber hinaus nutzen und offenbaren. Schließlich ist der Geschäftsgeheimnisschutz auch vor dem Hintergrund der statischen Effizienz zu bemängeln. Da er auf Geheimhaltung abstellt, wird die Information in Form der KI-Technologie nicht verbreitet – ein wohlfahrtsökonomisch ungewünschtes Ergebnis.

Das Ergebnis der Schutzfähigkeitsprüfung sind Schutzlücken. Es existiert *de lege lata* keine Schutzmöglichkeit, die KI-Technologien derart schützt, dass:

- KI-Technologien generell technologieneutral als Schutzgegenstand in Frage kommen (primär Förderung der dynamischen Effizienz);
- die Investitionen in die Entwicklung der Technologien gesamtwirtschaftlich effizient amortisiert werden könnten (primär Förderung der dynamischen Effizienz);
- ein Schutz nicht mit einer ineffizienten Erhöhung der Fix- und Transaktionskosten verbunden ist (Förderung sowohl der dynamischen als auch der statischen Effizienz);

- ein Schutz nicht bloß die Verbreitung der KI-Technologie nicht verhindert, sondern Anreize für deren Verbreitung setzt (primär Förderung der statischen Effizienz);
- der Schutzinhaber für eine bestimmte Zeitdauer Dritte wirksam davon abhalten kann, sich die geschützte KI-Technologie anzueignen, zu nutzen, zu verwerten oder investitionsschädlich offenzulegen (primär Förderung der dynamischen Effizienz).

Aufgrund dieser Überlegungen drängt sich politischer Handlungsbedarf auf, um die aufgezeigten Schutzlücken zu schließen. Ergebnis des vierten Teiles der Arbeit ist also die rechtspolitische Forderung nach der Schaffung eines Schutzrechtes, welches die obgenannten Punkte erfüllt. Diese Forderung wird durch weitere in Teil vier der Arbeit genannte Argumente unterstrichen: Rechtssicherheit, Gleichbehandlungs- sowie makroökonomische Überlegungen.

Im fünften und letzten Teil der Arbeit wird diese rechtspolitische Forderung aufgegriffen. Es wird jedoch kein konkreter Vorschlag für eine *de lege ferenda*-Lösung verfasst. Es werden lediglich Eckpunkte eines einzuführenden Schutzrechtes besprochen, an welche zukünftige Untersuchung anknüpfen können:

- Ein Schutzrecht an KI-Technologien *de lege ferenda* soll einen Anreiz zur Offenlegung der KI-Technologie – weg von Geheimhaltungsmaßnahmen – setzen.
- Schutzgegenstand sollen KI-Technologien sein – Softwareebenen intelligenter digitaler Systeme. Geschützt sein sollen demnach solche Softwareebenen, die über Autonomie verfügen und sich die Regeln zur Informationsverarbeitung selbst setzen und nicht direkt von einer programmierenden Person vorgegeben erhalten. Da für die Untersuchung überwiegend Investitionsschutzargumente herangezogen wurden und zwecks Abgrenzung nach unten, bietet es sich an, einen Schutz von einer wesentlichen Investition abhängig zu machen. Dies ist bereits aus dem Datenbankherstellerrecht nach §§ 87a ff. UrhG bekannt. Schutzrechts-

inhaber könnte demnach auch diejenige Person sein, welche die Investition aufwendet. Vorliegend wird also für die Einführung eines Leistungsschutzrechtes plädiert.

- Das Schutzrecht muss einen absolut-rechtlichen Charakter aufweisen. Zu starke Monopolstellungen lassen sich durch die Einräumung von Zwangslizenzen und Schranken korrigieren. Sollte eine Investitionsamortisation auch durch einen wirksamen relativrechtlichen Schutz möglich sein, ist ein solcher relativer Schutz wohlfahrtsökonomisch vorzuziehen. Der Schutzzumfang hinsichtlich der zustimmungsbedürftigen Handlungen kann sich am Computerprogrammenschutz (§§ 69a ff. UrhG) sowie dem Datenbankherstellerrecht (§§ 87a ff. UrhG) im UrhG orientieren. Die Konkretisierung dieser zustimmungsbedürftigen Handlungen wäre sodann Aufgabe der Rechtsprechung.
- Systematisch wäre ein Schutzrecht *de lege ferenda* im Urheberrecht zu verorten.

Literaturverzeichnis

- AGGARWAL CHARU C.*, Neural Networks and Deep Learning, Yorktown Heights 2018.
- Agrawal Ajay / Gans Joshua / Goldfarb Avi (Hrsg.), The Economics Of Artificial Intelligence, Chicago 2019 (zitiert als: BEARBEITER:IN, in: The Economics Of Artificial Intelligence, S.)
- ALAM TANWEER / QAMAR SHAMIMUL / DIXIT AMIT / BENAIDA MOHAMED*, Genetic Algorithm: Reviews, Implementations, and Applications, iJEP 2020.
- ANTOINE LUCIE*, Entwurfsmaterial im Schutzsystem der Software-Richtlinie, Chancen und Herausforderungen, CR 2019 1 ff.
- APEL SIMON / KAULARTZ MARKUS*, Rechtlicher Schutz von Machine Learning-Modellen, RD 2020, 24 ff.
- ARORA ASHISH / FOSFURI ANDREA / GAMBARDELLA ALFONSO*, Markets for Technology, The Economics of Innovation and Corporate Strategy, Cambridge London 2002.
- ATENIESE GIUSEPPE / FELICI GIOVANNI / MANCINI LUIGI / SPOGNARDI ANGELO / VILLANI ANTONIO / VITALI DOMENICO*, Hacking Smart Machines with Smarter Ones: How to Extract Meaningful Data from Machine Learning Classifiers, IJSN 2015, 137 ff.
- BARTELS MARVIN*, Ethik und Patentrecht, Verhältnisse und Wechselwirkungen zwischen Ethik und Patentrecht vor dem Hintergrund innovativer Biotechnologien, Diss., Tübingen 2020
- BEIER FRIEDRICH-KARL*, Die herkömmlichen Patentrechtstheorien und die sozialistische Konzeption des Erfinderrechts, GRUR Int. 1970, 1 ff.
- Benkard Georg (Hrsg.), Patentgesetz, 11., neubearbeitete Auflage, München 2015 (zitiert als: Benkard/BEARBEITER:IN, PatG, § Rn.)
- BECKER MAXIMILIAN*, Absolute Herrschaftsrechte, Habil., Tübingen 2022
- BESSEN JAMES / IMPINK STEPHEN MICHAEL / REICHENSPERGER LYDIA / SEAMANS ROBERT*, The role of data for AI startup growth, Research Policy, Volume 51, Issue 5, June 2022
- BESSEN JAMES E.*, The Business of AI Startups, Boston University School of Law, Law & Economics Series Paper No. 18-28

- BOMHARD DAVID/GAJECK NICLAS A., Softwareentwicklung durch künstliche Intelligenz, RDi 2021, 472 ff.
- BROY MANFRED/SPANIOL OTTO, VDI-Lexikon Informatik und Kommunikationstechnik, 2. Auflage, Berlin Heidelberg 1999, zitiert als: VDI-Informatiklexikon, S.)
- CARLINI NICHOLAS/JAGIELSKI MATTHEW/ZHANG CHIYUAN/PAPERNOT NICOLAS/TERZIS ANDREAS/TRAMER FLORIAN, The Privacy Onion Effect: Memorization is Relative, NeurIPS 2022
- CERUZZI PAUL E., Computing: A Concise History, Cambridge/London 2012
- COBBE JENNIFER/SINGH JATINDER, Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges, Forthcoming in Computer Law & Security Reviews, April 12 2021
- COOTER ROBERT/ULEN THOMAS, Law and Economics, 6. Auflage, 2. Buch, Berkeley 2016
- CORMEN THOMAS/LEISERSON CHARLES E./RIVEST RONALD/STEIN CLIFFORD, Algorithmen – eine Einführung, 4., durchgesehene und korrigierte Auflage, München 2013
- CUKIER KENNETH/MAYER-SCHOENBERGER VIKTOR, The rise of big data: how it's changing the way we think about the world, in: Council on Foreign Relations, Inc. (Hrsg.), Foreign Affairs, Volume 92, 3. Auflage, New York 2013
- DELTORN JEAN-MARC/LEMÉNAGER GODEFROY, La protection de l'intelligence artificielle en France et en Europe, Réalités industrielles Novembre 2020, 34 ff.
- Depenheuer Otto / Peifer Klaus-Nikolaus (Hrsg.), Geistiges Eigentum: Schutzrecht oder Ausbeutungstitel?: Zustand und Entwicklungen im Zeitalter von Digitalisierung und Globalisierung, Berlin, Heidelberg 2008 (zitiert als: Depenheuer/Peifer/BEARBEITER:IN, S.)
- Dreier Thomas/Schulze Gernot (Hrsg.), Urheberrechtsgesetz Verwertungsgesellschaftengesetz Kunsturhebergesetz, 6. Auflage, 2018 München (zitiert als: Dreier/Schulze/BEARBEITER:IN, UrhG, § Rn.)
- Ebers Martin / Heinze Christian / Krügel Tina / Steinrötter Björn (Hrsg.), Künstliche Intelligenz und Robotik Rechtshandbuch, München 2020 (zitiert als: KI-Rechtshandbuch-BEARBEITER:IN, § Rn.)
- EHINGER PATRICK/STIEMERLING OLIVER, Die urheberrechtliche Schutzfähigkeit von Künstlicher Intelligenz am Beispiel von Neuronalen Netzen – Welche Strukturelemente und welche Entwicklungsphasen sind urheberrechtlich geschützt?, CR 2018, 761 ff.

- EHINGER PATRICK*, Urheberrechtlicher Schutz von neuronalen Netzen und Erzeugnissen von K.I.-Software, Beilage 1 zu Heft 7/8 K & R 2019, 12 ff.
- EIBEN A. E. / SMITH J. E.*, Introduction to Evolutionary Computing, 2. Auflage, Berlin Heidelberg 2015
- EIDENMÜLLER HORST*, Effizienz als Rechtsprinzip, Möglichkeiten und Grenzen der ökonomischen Analyse des Rechts, 4. Auflage, Tübingen 2015
- EMMERICH DAVID*, Die Auswirkungen künstlicher Intelligenz auf die erfinderische Tätigkeit und das Erfinderprinzip, Diss., Berlin 2021
- ERTEL WOLFGANG*, Grundkurs Künstliche Intelligenz: Eine praxisorientierte Einführung, 5. Auflage, Wiesbaden 2021
- FOGEL DAVID B.*, Evolutionary Computation – Toward a New Philosophy of Machine Intelligence, 3. Auflage, New Jersey 2006
- GODDAR HEINZ*, Patent Solutions for AI and IoT Inventions, GRUR 2021, 196 ff.
- GOODFELLOW IAN / BENGIO, YOSHUA / COURVILLE, AARON*, Deep Learning, Cambridge 2016
- GOOS GERHARD*, Vorlesungen über Informatik. 1, Grundlagen und funktionales Programmieren, 4. Auflage, 2006
- GRÄFE HANS-CHRISTIAN / KAHL JONAS*, KI-Systeme zur automatischen Texterstellung: Urheber- und medienrechtliche Einordnung von Textgeneratoren in Journalismus und E-Commerce, MMR 2021, 121 ff.
- GRÄTZ AXEL*, Künstliche Intelligenz im Urheberrecht: Eine Analyse der Zurechnungskriterien und der Prinzipien der Verwandten Schutzrechte vor dem Hintergrund artifiziieller Erzeugnisse, Diss., Wiesbaden 2021
- GROTH OLIVER*, Künstliche Intelligenz 2019 – Eine Analyse zwischen Fakten und Hype, Kommunikation & Recht 2019, Heft 7-8, Beilage S. 3 f.
- GULL ISABEL / SCHRÄDE-GRYTSENKO LISA / LUNDBORG MARTIN*, Cloud-Lösungen und KI-as-a-Service – Aktuelle und potenzielle Anwendungsszenarien und Marktentwicklungen, WIK Diskussionsbeitrag Nr. 469, Bad Honnef 2020
- GUSAROV KONSTANTINS*, An Analysis on Java Programming Language Decompiler Capabilities, Applied Computer Systems 2018 (2), 109 ff.

- HACKER, PHILIPP / ENGEL ANDREAS / MAURER MARCO*, Regulating ChatGPT and other Large Generative AI Models, Working Paper, Version vom 8. Mai 2023
- HACKER, PHILIPP*, Immaterialgüterrechtlicher Schutz von KI-Trainingsdaten, GRUR 2020, 1025 ff.
- HAEDICKE MAXIMILLIAN W.*, Patentrecht, 6. Auflage, Köln 2022
- Harte Bavendamm Henning / Ohly Ansgar / Kalbfus Björn (Hrsg.), Kommentar zum Gesetz zum Schutz von Geschäftsgeheimnissen, München 2020 (zitiert als: Bavendamm/Ohly/Kalbfus/BEARBEITER:IN, GeschGehG, § Rn.)
- HARTMANN FRANK / PRINZ MATTHIAS*, Immaterialgüterrechtlicher Schutz von Systemen Künstlicher Intelligenz, in: Taeger Jürgen (Hrsg.), Rechtsfragen digitaler Transformationen. Gestaltung digitaler Veränderungsprozesse durch Recht, Edewecht, 2018
- HARTMANN MATTHIAS* (Hrsg.), KI & Recht kompakt, Berlin 2020 (zitiert als: KI & Recht kompakt-BEARBEITER:IN, S.)
- HAUCK RONNY / CEVC BALTASAR*, Patentschutz für Systeme Künstlicher Intelligenz?, ZGE 2019, 134 ff.
- HAUGELAND JOHN*, Artificial Intelligence: The Very Idea, Cambridge 1985
- Heermann Peter / Schlingloff Jochen (Hrsg.), Münchener Kommentar zum Lauterkeitsrecht, 3. Auflage, München 2020 (zitiert als: Heermann/Schlingloff/BEARBEITER:IN, Gesetz, § Rn.)
- HERBERGER MAXIMILLIAN*, «Künstliche Intelligenz» und Recht – ein Orientierungsversuch, NJW 2018, 2825 ff.
- Hetmank Sven / Rechenberg Constantin (Hrsg.), Kommunikation, Kreation und Innovation – Recht im Umbruch?, Leipzig 2019 (zitiert als: KKI-BEARBEITER:IN, S.)
- HICKS JOHN RICHARD*, The Foundations of Welfare Economics, The Economic Journal 1939, 696 ff.
- HILTY RETO / HOFFMANN JÖRG / SCHEUERER STEFAN*, Intellectual Property Justification for Artificial Intelligence, Max Planck Institute for Innovation and Competition Research Paper 20-02

HOHENDORF THOMAS, Know-How-Schutz und geistiges Eigentum, Ein Beitrag zur systematischen Einordnung des Geheimnisschutzes in das Recht des geistigen Eigentums, Tübingen 2020

JIN WANG/MCELHERAN, Economies before Scale: Survival and Performance of Young Plants in the Age of Cloud Computing, Rotman School of Management Working Paper No. 3112901, 2017

JOON OH SEONG / AUGUSTIN MAX / SCHIELE BERNT / FRITZ MARIO, Towards Reverse-Engineering Black-Box Neural Networks, ICLR 2018

KALDOR NICHOLAS, Welfare Propositions of Economics and Interpersonal Comparisons of Utility, *The Economic Journal* 1939, 549 ff.

KAULARTZ MARTIN / BRAEGELMANN TOM (Hrsg.), *Rechtshandbuch Artificial Intelligence und Machine Learning*, München 2020 (zitiert als: *Rechtshandbuch-AI-BEARBEITER:IN*, Kap. Rn.)

KEINER ALEXANDRA E., Algorithmen als Rationalitätsmythos, in: *Leineweber Christan / de Witt Claudia* (Hrsg.): *Algorithmisierung und Autonomie im Diskurs – Perspektiven und Reflexionen auf die Logiken automatisierter Maschinen*, Hagen 2020, 47 ff.

Keller Erbard / Schönknecht Marcus / Glinke Anna (Hrsg.), *Beck'scher Kurzkommentar zum Geschäftsgeheimnisschutzgesetz*, München 2021 (zitiert als: *Keller/Schönknecht/Glinke/BEARBEITER:IN*, *GeschGehG*, § Rn.)

KÖHLER HELMUT / BORNKAMM JOACHIM / FEDDERSEN JÖRN / ALEXANDER CHRISTIAN (Hrsg.), *Gesetz gegen den unlauteren Wettbewerb*, *GeschGehG*, *PAngV*, *UKlaG*, *DL-InfoV*, *P2B-VO*, 41., neu bearbeitete Auflage, München 2023, (zitiert als: *Köhler/Bornkamm/Feddersen/Alexander/BEARBEITER:IN*, *Gesetz*, § Rn.)

KONERTZ ROMAN/SCHÖNHOF RAOUL, *Das technische Phänomen "künstliche Intelligenz" im allgemeinen Zivilrecht: Eine kritische Betrachtung im Lichte von Autonomie, Determinismus und Vorhersehbarkeit*, Baden-Baden 2020

KRASSER RUDOLF/ANN CHRISTOPH, *Patentrecht*, 7., neubearbeitete Auflage, München 2016

KRAUSEN JEAN-MARCEL, *Künstliche Intelligenz als Erfindung und Erfinder, patentrechtliche Auswirkungen des Fortschritts auf dem Gebiet der künstlichen Intelligenz*, Diss., Tübingen 2023

KRUSE RUDOLF / BORGELT CHRISTIAN / BRAUNE CHRISTIAN / KLAWONN FRANK / MOEWES CHRISTIAN / STEINBRECHER MATTHIAS, *Computational Intelligence: Eine methodische*

- Einführung in Künstliche Neuronale Netze, Evolutionäre Algorithmen, Fuzzy-Systeme und Bayes-Netze, 2., überarbeitete und erweiterte Auflage, Wiesbaden 2015
- KÜPPERS E.W. UDO*, Eine transdisziplinäre Einführung in die Welt der Kybernetik – Grundlagen, Modelle, Theorien und Praxisbeispiele, Wiesbaden 2019
- LANDES WILLIAM M. / POSNER RICHARD A.*, The Economic Structure of Intellectual Property Law, Cambridge London 2003
- LAUBER-RÖNSBERG ANNE / HETMANK SVEN*, The Concept of Authorship and Inventorship under Pressure: Does Artificial Intelligence Shift Paradigms, GRUR Int. 2019, 641 ff.
- LEGG SHANE / HUTTER MARCUS*, Universal Intelligence: A Definition of Machine Intelligence, Minds & Machines 2007, 391 ff.
- LETTL TOBIAS*, Gewerblicher Rechtsschutz, München 2019
- LINHART ANDREA*, Information Künstlicher Neuronaler Netze zwischen Geheimnisschutz und Transparenz, Diss., im Erscheinen
- LINKE DAVID*, „Künstliche Intelligenz“ und Urheberrecht – Quo vadis?, Diss., Baden-Baden 2021
- Loewenheim Ulrich / Leistner Matthias / Ohly Ansgar (Hrsg.), Urheberrecht, UrhG, KUG, VGG, 6. Neu bearbeitete Auflage, 2020 München (zitiert als: Schrickler/Löwenheim/BEARBEITER:IN, UrhG, § Rn.)
- LUHMANN NIKLAS*, Systemtheorie der Gesellschaft, Berlin 2017
- MAAMAR NIKLAS*, Computer als Schöpfer: Der Schutz von Werken und Erfindungen künstlicher Intelligenz, Diss., Tübingen 2021
- MCCARTHY JOHN / MINSKY MARVIN / ROCHESTER NATHANIEL / SHANNON CLAUDE*, A Proposal For The Dartmouth Summer Research Project On Artificial Intelligence, 31.08.1955
- MELULLIS KLAUS-J.*, Zur Patentfähigkeit von Programmen für Datenverarbeitungsanlagen, GRUR 1998, 843 ff.
- MENIERE YANN / PIHLAJAMAA HELI*, Künstliche Intelligenz in der Praxis des EPA, GRUR 2019, 332 ff.
- MERGES ROBERT*, Justifying Intellectual Property, Cambridge London 2011

- MES PETER*, Patentgesetz Gebrauchsmustergesetz, 5., neubearbeitete Auflage, München 2020
- MESSIER RIC*, Operating system forensics, Waltham 2016 (Mackay Kevin, technischer Hrsg.)
- MIRESHGHALLAH FATEMEHSADAT / GOYAL KARTIK / UNIYAL ARCHIT / BERG-FITZPATRICK TAYLOR / SHOKRI REZA*, Quantifying Privacy Risks of Masked Language Models Using Membership Inference Attacks, Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing 2022
- MOORE GORDON E.*, Cramming more components onto integrated circuits, Electronics 1965, Vol. 38, Nr. 8
- MUHR MONIKA*, KI-Schöpfungen im Urheberrecht, Diss., Berlin 2022
- MÜLLER FERDINAND / KIRCHNER ELSA / SCHÜSSLER MARTIN*, „Ein “KI-TÜV” für Europa? Eckpunkte einer horizontalen Regulierung Algorithmischer Entscheidungssysteme”, in: Assmussen Sven / Golla Sebastian / Kuschel Linda (Hrsg.), Tagungsband GRUR Jr. 2020, Baden-Baden 2020, S. 85 ff.
- MÜLLER FERDINAND*, Einsatz digitaler Agenten im Rechtsverkehr, Diss., im Erscheinen
- NÄGERL JOEL / NEUBURGER BENEDIKT / STEINBACH FRANK*, Künstliche Intelligenz: Paradigmenwechsel im Patentsystem, GRUR 2019, 336 ff.
- NILSSON NILS J.*, The Quest for Artificial Intelligence, Cambridge, 2009
- NISSEN VOLKER*, Einführung in Evolutionäre Algorithmen: Optimierung nach dem Vorbild der Evolution, Braunschweig; Wiesbaden 1997.
- OHLY, ANSGAR*, Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, 441 ff.
- PAPASTEFANOUS STEFAN*, Genetic Breeding Algorithms als Form des «Machine Learning» im Urheber- und Patentrecht – Rechtliche Herausforderungen beim Schutz von Algorithmen des Genetic Breeding Models, CR 2019, 209 ff.
- PAPERNOT NICOLAS / MCDANIEL PATRICK / GOODFELLOW IAN / JHA SOMESH*, Practical Black-Box Attacks against Machine Learning, in: Celik Z. Berkay / Swami Ananthram Karri Ramesh / Sinanoglu Ozgur / Sadeghi Ahmad-Reza / Yi Xun (Hrsg.), Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, New York 2017
- PEUKERT ALEXANDER*, Urheberrecht und verwandte Schutzrechte, 19. Auflage, München 2023

- PIERSON MATTHIAS / AHRENS THOMAS / FISCHER KARSTEN*, Recht des geistigen Eigentums: Gewerblicher Rechtsschutz, Urheberrecht, Wettbewerbsrecht, 4. Auflage, Tübingen 2018
- POSNER RICHARD A.*, Economic Analysis of Law, 9. Auflage, New York 2014
- PRIDDY KEVIN L. / KELLER PAUL E.*, Artificial Neural Networks: An Introduction, 2005 Bellingham
- PUPPE FRANK*, Einführung in Expertensysteme, 2. Auflage, Heidelberg 1991
- REDEKER HELMUT*, IT-Recht, 7., neubearbeitete Auflage, München 2020
- REHBINDER MANFRED / PEUKERT ALEXANDER*, Urheberrecht und verwandte Schutzrechte, 18. vollständig neu bearbeitete Auflage, München 2018
- ROJAS RAUL*, Neural Networks, A Systematic Introduction, Berlin Heidelberg 1996
- RUSSEL STUART / NORVIG PETER*, Artificial Intelligence – A Modern Approach, 4. Auflage, Harlow, 2022
- Sassenberg Thomas / Faber Tobias (Hrsg.), Rechtshandbuch Industrie 4.0 und Internet of Things, 2. Auflage, München 2020 (zitiert als: Rechtshandbuch Industrie 4.0-BEARBEITER:IN, § Rn.)
- SCHACK HAIMO*, Urheber- und Urhebervertragsrecht, 10., neu bearbeitete Auflage, Tübingen 2021
- SCHÄFER HANS-BERND / OTT CLAUS*, Lehrbuch der ökonomischen Analyse des Zivilrechts, 6., überarbeitete Auflage, Wiesbaden 2020
- SCHAUB RENATE*, Interaktion von Mensch und Maschine: Haftungs- und immaterialgüterrechtliche Fragen bei eigenständigen Weiterentwicklungen autonomer Systeme, JZ 7/2017, 342 ff.
- SCHEJA KATHARINA*, Schutz von Algorithmen in Big Data Anwendungen: Wie Unternehmen aufgrund der Umsetzung der Geschäftsgeheimnis-Richtlinie ihre Algorithmen wie auch Datenbestände besser schützen können, CR 2018, 485 ff.
- SCHERER MATTHEW U.*, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, Harv. J.L. & Tech 2016, 353 ff.
- SCHWARZ CLAUDIA / KRUSPIG SABINE*, Computerimplementierte Erfindungen – Patentschutz von Software?, 2. Auflage, Köln 2018

- SEITZ JAN / RITZMANN KAY*, Internet der Dinge – Internet Of Things (IOT), Grundlagen, Anwendungsbereiche, Potentiale, 2022
- SHAVELL STEVEN*, Foundations of Economic Analysis of Law, Cambridge London 2004
- SIEBER ULRICH*, Informationsrecht und Recht der Informationstechnik - Die Konstituierung eines Rechtsgebietes in Gegenstand, Grundfragen und Zielen, NJW 1989, 2569 ff.
- SÖBBING THOMAS*, Algorithmen und urheberrechtlicher Schutz, CR 2020, 223 ff.
- SPECHT LOUISA / HEROLD SOPHIE*, Roboter als Vertragspartner? Gedanken zu Vertragsabschlüssen unter Einbeziehung automatisiert und autonom agierender Systeme, MMR 2018, 40 ff.
- SPIECKER GEN. DÖHMANN INDRA*, Staatliche oder private Algorithmenregulierung?, in: Bitbürger Gespräche, Jahrbuch 2020, S. 37 ff.
- Springer Gabler* (Hrsg.), Kompakt-Lexikon Wirtschaft, 4.500 Begriffe nachschlagen, verstehen, anwenden, 11., aktualisierte Auflage, Wiesbaden 2013
- STANFORD UNIVERSITY*, Human-Centered Artificial Intelligence, Artificial Intelligence Index Report 2022
- STIERLE MARTIN*, Das nicht-praktizierte Patent, Diss., Tübingen 2018
- STYCZYNSKI ZBIGNIEW A. / RUDION KRYSZTOF / NAUMANN ANDRÉ*, Einführung in Expertensysteme: Grundlagen, Anwendungen und Beispiele aus der elektrischen Energieversorgung, Wiesbaden 2017
- TOWFIGH EMANUEL V. / PETERSEN NIELS*, Ökonomische Methoden im Recht, eine Einführung für Juristen, 2. überarbeitete und aktualisierte Auflage, Tübingen 2017
- TRAMÈR FLORIAN / ZHANG FAN / JUELS ARI / REITER MICHAEL K. / RISTENPART THOMAS*, Stealing Machine Learning Models via Prediction APIs, Usenix 2016
- TURING ALAN M.*, Computing Machinery And Intelligence, Mind, Vol. 59 (1950), Issue 236, 433 ff.
- VILLALOBOS PABLO / SEVILLA JAMES / BESIROGLU TAMAY / HEIM LENNART / HO ANSON / HOBBAHN MARIUS*, Machine Learning Model Sizes and the Parameter Gap, Cornell University, 2022

- Wandtke Artur-Axel / Bullinger Winfried* (Hrsg.), *Praxiskommentar Urheberrecht*, 5. Neuarbeitete und erweiterte Auflage, München 2019 (zitiert als: *Wandtke/Bullinger/BEARBEITER:IN*, UrhG, § Rn.)
- XULI TANG / XIN LI / YING DING / MIN SONG / YI BU*, The pace of artificial intelligence innovations: Speed, talent, and trial-and-error, *Journal of Infometrics*, 2020, Volume 14, 4. Auflage
- ZECH HERBERT*, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, in: *Ständige Deputation des Deutschen Juristentags* (Hrsg.), *Verhandlungen des 73. Deutschen Juristentags Hamburg 2020/Bonn 2022*, Band I, München 2020, aktualisiert 2022 (zitiert als *ZECH*, Gutachten, S.)
- ZECH HERBERT*, Risiken digitaler Systeme: Robotik, Lernfähigkeit und Vernetzung als aktuelle Herausforderungen für das Recht, *Weizenbaum Series*, 2, Berlin 2020 (zitiert als *ZECH*, Risiken, S.)

Materialien

Gesetzesentwurf der Bundesregierung vom 4. Oktober 2018, Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, Deutscher Bundestag, BT Drucksache 19/4724

Herausforderungen der künstlichen Intelligenz – Bericht der interdepartementalen Arbeitsgruppe „Künstliche Intelligenz“ an den Bundesrat vom 13.12.2019, abrufbar unter: <https://www.sbfi.admin.ch/sbfi/de/home/bfi-politik/bfi-2021-2024/transversale-themen/digitalisierung-bfi/kuenstliche-intelligenz.html> (zuletzt besucht am 09. Mai 2023) (zitiert als KI-Bericht CH)

Strategie Künstliche Intelligenz der Bundesregierung (Deutschland), Stand November 2018, abrufbar unter: https://www.bmbf.de/bmbf/shareddocs/downloads/files/nationale_ki-strategie.pdf?__blob=publicationFile&v=2 (zuletzt besucht am 09. Mai 2023) (zitiert als KI-Strategie D)

The State of AI: Divergence 2019, MMC Ventures, abrufbar unter: <https://www.state-of-ai2019.com> (zuletzt besucht am 09. Mai 2023)

Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM (2021) 206 final)

WIPO, Technology Trends 2019, Artificial Intelligence

Pablo Schumacher

Schutzfähigkeit Künstlicher Intelligenz

Eine urheber-, patent- und geschäftsgeheimnisschutzrechtliche Untersuchung der Schutzfähigkeit verschiedener KI-Technologie. Der Autor würdigt die Schutzfähigkeit de lege lata unter wohlfahrtsökonomischen Gesichtspunkten. Ergebnis sind Schutzlücken de lege lata.