

Heinz-Adalbert Krebs
Patricia Hagenweiler

Datenanonymisierung im Kontext von Künstlicher Intelligenz und Big Data

Grundlagen – Elementare Techniken
– Anwendung



Springer Vieweg

Datenanonymisierung im Kontext von Künstlicher Intelligenz und Big Data

Heinz-Adalbert Krebs ·
Patricia Hagenweiler

Datenanonymisierung im Kontext von Künstlicher Intelligenz und Big Data

Grundlagen – Elementare
Techniken – Anwendung

Heinz-Adalbert Krebs
Universität Kassel,
Wirtschaftsinformatik
Green Excellence GmbH
Düsseldorf, Deutschland

Patricia Hagenweiler
Green Excellence GmbH
Düsseldorf, Deutschland

ISBN 978-3-658-37587-4 ISBN 978-3-658-37588-1 (eBook)
<https://doi.org/10.1007/978-3-658-37588-1>

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

© Green Excellence GmbH 2022

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geographische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung: David Imgrund

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Inhaltsverzeichnis

1	Einleitung	1
2	Künstliche Intelligenz	5
2.1	Arten der künstlichen Intelligenz	6
2.2	Algorithmen	8
2.3	Machine Learning	10
2.4	Deep Learning	13
2.4.1	Neuronale Netze	14
2.4.2	Arten tiefer neuronaler Netze	16
2.5	Trainingsdaten für das KI-Modell	19
2.6	Anwendungen der künstlichen Intelligenz	26
2.6.1	Natural Language Processing	26
2.6.2	Natural Image Processing	30
2.6.3	Wissensbasierte Expertensysteme	31
2.6.4	Cognitive Computing	34
2.7	Einsatzgebiete der künstlichen Intelligenz	36
3	Big Data und Analysemethoden	43
3.1	Daten und Informationen	44
3.2	Struktur der Daten	45
3.3	Datenwertschöpfungskette	46
3.3.1	Datengewinnung	47
3.3.2	Datenspeicherung	51
3.3.3	Datenanalyse	53
3.3.4	Datenverwertung	55
3.4	Datenarchitektur	55
3.5	Methoden der Datenanalyse	56

3.5.1	Data Mining	57
3.5.2	Machine Learning	59
3.5.3	Text Mining	60
3.5.4	Web Mining	63
3.5.5	Datenvisualisierung	63
3.6	Einsatzzweck der Daten	67
4	Personenbezogene, pseudonymisierte und anonymisierte Daten	69
4.1	Personenbezogene Daten	69
4.2	Pseudonymisierte und anonymisierte Daten	70
5	Techniken der Pseudonymisierung	77
6	Anonymisierung strukturierter Daten	81
6.1	Elementare Anonymisierungstechniken	83
6.1.1	Randomisierung	83
6.1.2	Generalisierung	86
6.2	Aggregationsbasierte Verfahren	87
6.2.1	k-Anonymity	89
6.2.2	l-Diversity	92
6.2.3	t-Closeness	93
6.2.4	δ -Presence	94
6.2.5	Auswahl weiterer Anonymitätskriterien	95
6.2.6	Algorithmen für Techniken der k-Anonymity	96
6.3	Differential Privacy	97
6.4	Verfahren der Datensynthese	99
6.5	Federated Machine Learning	101
6.6	Semantische Anonymisierung	103
7	Anonymisierung unstrukturierter Daten	107
7.1	Textdaten	107
7.1.1	Anonymisierung von Textdaten auf Metadatenebene	108
7.1.2	Anonymisierung von Textdaten auf Inhaltsebene	109
7.1.3	Anonymisierung von Textdaten auf Schreibstilebene	110
7.2	Multimediatdaten	112
8	Risiken der Nutzung anonymisierter Daten	119
9	Verfahren zur Durchführung der Anonymisierung	125

10	Software zur Unterstützung der Anonymisierung	139
10.1	Anonymisierungsalgorithmen	139
10.2	Open Source-Implementierungen	141
10.3	Anonymisierungsverfahren in den Systemen der Unternehmen	145
11	Fazit und Ausblick	149
	Literatur	155

Über die Autoren

Dr. Heinz-A. Krebs ist seit 2009 geschäftsführender Gesellschafter des Unternehmens Green Excellence GmbH mit Sitz in Düsseldorf, welches auf die Beratung von Energieversorgern (Strom, Gas, Wasser) und Netzbetreibern spezialisiert ist. Die Beratungsdienstleistungen umfassen neben den Themenfeldern der Organisation und Reorganisation das Geschäfts- und Prozess-/Projektmanagement sowie die Projektentwicklung von Innovationen in den Bereichen der Energieerzeugung (Erneuerbare Energien), Energieübertragung und Energieverteilung.

Vor Übernahme der Geschäftsführung der Green Excellence GmbH war Dr. Heinz-A. Krebs über viele Jahre als Management-Consultant in der Inhouse-Beratung der RWE AG angestellt und zeichnete dort primär verantwortlich für Organisations- und Strategieprojekte in Osteuropa. Darüber hinaus lehrt er seit vielen Jahren an der Universität Kassel in regelmäßigen Blockveranstaltungen die Einführung betriebswirtschaftlicher Geschäftssysteme im Fachgebiet Wirtschaftsinformatik. Seit der Entscheidung zur Energiewende in Deutschland ist die Green Excellence GmbH weltweit in Strategie- und Umsetzungsprojekte eingebunden, welche die Erneuerbaren Energien sowie die Digitalisierung der Energiewirtschaft im Fokus der Betrachtung haben. Insbesondere im Rahmen der Themenstellung „Digitalisierung der Energiewirtschaft“ hat Dr. Heinz-A. Krebs gemeinsam mit dem Fachgebiet Anlagen- und Hochspannungstechnik sowie der Wirtschaftsinformatik der Universität Kassel Innovationsprojekte zur Thematik „Inspektionen von Freileitungen unter dem Einsatz von Unmanned Aerial Systems (UAS)“ initiiert, welche in der Wertschöpfungskette der Energiewirtschaft disruptive Entwicklungen erwarten lassen.

Bei der Umsetzung von Innovationsthemen stellt die Green Excellence GmbH im Rahmen einer stringent interdisziplinären Ausrichtung neben der Informatik,

Betriebswirtschaftslehre und Elektrotechnik zunehmend die Integration juristischer Themenstellungen in den Fokus laufender und künftiger Projekte, da sich insbesondere durch den Einsatz von neuen Informations- und Kommunikationstechnologien in der Energiewirtschaft rechtliche Fragestellungen (u. a. EnWG, GDEW, NABEG 2.0, EnLAG, MsbG, DSGVO) mit erheblichen Auswirkungen auf die Organisation, die Geschäftsprozesse und die IT-Systeme der jeweiligen Unternehmen abzeichnen.

Dr. Patricia Hagenweiler ist seit 2012 Mitarbeiterin der Green Excellence GmbH und vorwiegend für die Bereiche Datenschutz und Forschung zuständig.

Abkürzungsverzeichnis

A ⁴ NT	Adversarial Author Attribute Anonymity Neural Translation
ADM	Algorithmic Decision-Making
AEPD	Agencia Española de Protección de Datos
AGI	Artificial General Intelligence
AKI	Allgemeine Künstliche Intelligenz
ANI	Artificial Narrow Intelligence
API	Application Programming Interface
ASI	Artificial Superintelligence
ASR	Automatic Speech Recognition
BASt	Bundesanstalt für Straßenwesen
BDSG	Bundesdatenschutzgesetz
BERT	Bidirectional Encoder Representations from Transformers
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Energie
BStatG	Bundesstatistikgesetz
CAT	Cornell Anonymization Tool
CNN	Convolutional Neural Network
CPS	Cyber-Physical-Systems
CSV	Comma-separated Values
Cycle GAN	Cycle-Consistent Adversarial Networks
DCGAN	Deep Convolutional GAN
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz

DIN	Deutsches Institut für Normung
DIPS	Differentially Private Data Synthesis
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cybersecurity
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FERPA	Family Educational Rights and Privacy Act
FNN	Feedforward Neural Networks
GAN	Generative Adversarial Network
GI	Gesellschaft für Informatik
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
GPS	Global Positioning System
GPT	Generative Pretrained Transformer
GPU	Grafikprozessoren
HIPAA	Health Insurance Portability and Accountability Act
HOL	Higher Order Logic
HTML	Hypertext Markup Language
IMDB	In-Memory-Datenbanken
IoT	Internet of Things
JDBC	Java Database Connectivity
KDD	Knowledge Discovery in Databases
KI	Künstliche Intelligenz
KNIME	Konstanz Information Miner
KNN	Künstliche neuronale Netze
LDA	Latent Dirichlet Allocation
LSTM	Long Short-Term Memory
MDAV	Maximum Distance to Average Vector
MDM	MobilitätsDatenMarktPlatz
MeSH	Medical Subject Headings
MPP	Massive Parallel Processing
MRT	Magnetresonanztomografie
NIP	Natural Image Processing
NLG	Natural Language Generation
NLP	Natural Language Processing
NoSQL	Not only Structured Query Language

OCR	Optical Character Recognition
PCM	Phase Change Memory
PPML	Privacy-preserving Machine Learning
ProGAN	Progressive Growing of GAN
RAID	Redundant Arrays of Independent Disks
RFID	Radio Frequency Identification
RNN	Recurrent Neural Network
SAGAN	Self-Attention GAN
sdcMicro	Statistical Disclosure Control for Microdata
SECRETA	System for Evaluating and Comparing RELational and Transaction Anonymization
SGB	Sozialgesetzbuch
SIT	Fraunhofer-Institut für Sichere Informationstechnologie
SRGAN	Super-Resolution GAN
StyleGAN	Style-Based Generator Architecture GAN
SWAG	Situations with adversarial Generations
TIAMAT	Tool for Interactive Analysis of Microdata Anonymization Techniques
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.
TNN	Tiefes neuronales Netz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
URL	Uniform Resource Locator
VR	Virtual Reality
XML	eXtensible Markup Language

Einleitung

1

Die fortschreitende Digitalisierung, die immer höhere Verfügbarkeit des Internets in Echtzeit sowie die progressive Entwicklung der Informationstechnologie hat es Unternehmen, wissenschaftlichen Einrichtungen und Organisationen ermöglicht, Daten in einem noch nie dagewesenen Umfang und in einer Komplexität zu erzeugen, zu integrieren, zu speichern und zu analysieren, wodurch Daten einen enormen Stellen- und Marktwert erhalten haben. Diese Daten werden oftmals automatisch von zahlreichen Eingabegeräten und Sensoren, wie Mobiltelefonen, medizinischen Geräten, Scannern, Kameras oder RFID¹-Etiketten, erzeugt, zumal digitale Technologien mittlerweile in allen Bereichen des privaten sowie des beruflichen Lebens präsent sind. So haben Wirtschaftsunternehmen, Regierungsorganisationen und Forschungsinstitute sog. Data Lakes aufgebaut, in denen Daten, welche auch personenbezogen sein können, zunächst in unstrukturierter Form gesammelt werden. Inzwischen ist es möglich geworden, mithilfe maschineller Lernverfahren der künstlichen Intelligenz (KI) das in den Daten enthaltene Wissen zu extrahieren, welches bei einem verantwortungsvollen Einsatz u. a. zu Verbesserungen in der medizinischen Versorgung oder zur Erhöhung der Effektivität von maschinellen Produktions- oder Instandhaltungsprozessen führen kann. In vielen Fällen handelt es sich dabei um gesammelte Daten von Personen, welche ihr Verhalten, ihren Zustand oder ihre Handlungen beschreiben und dazu verwendet werden können, um Vorhersagen über verschiedene Aspekte der Personen in der Zukunft zu treffen. Dies können Vorhersagen über den Kauf eines Produkts, die Wahl eines Kandidaten oder eine mögliche Erkrankung sein. Außerdem kann das abstrahierte Wissen aus diesen Daten auch missbraucht werden, was insbesondere für personenbezogene Daten zu bedenken ist.²

¹ Radio Frequency Identification.

² Vgl. Kessler/Hoff/Freytag (2019) S. 1998; Engels (2020) S. 363.

Aus rechtlicher Sicht sind personenbezogene Daten zu schützen und ihre Verarbeitung zu reglementieren. Wird der Personenbezug aus den Daten entfernt, indem sie pseudonymisiert oder anonymisiert werden, besteht die Möglichkeit der freien Nutzung der Daten.³ Die personenbezogenen Daten werden durch nationale und internationale Datenschutzgesetze geschützt, wobei es um den Schutz von Personen (Betroffenen) vor der unangemessenen Verarbeitung ihrer Daten geht, sodass Betroffene das Recht haben, selbst darüber entscheiden zu können, was mit ihren persönlichen Daten geschieht und in welchem Umfang von wem ihre Daten verwendet werden dürfen. So ist auch in der Charta der Grundrechte der Europäischen Union (EU) der „Schutz personenbezogener Daten“ verankert, wonach jeder das Recht auf den Schutz der sie betreffenden personenbezogenen Daten hat, welche nur für festgelegte Zwecke und mit einer Einwilligung der betroffenen Personen oder einer sonstigen gesetzlich geregelten Grundlage verarbeitet werden dürfen.⁴ Darüber hinaus können Datenanalysen Personen betreffen, ohne deren personenbezogene Daten zu berücksichtigen oder nur zu kennen, indem u. a. Rückschlüsse einzelner Personen auf weitere Personen in einer bestimmten Region gezogen werden, obwohl diese in der Datenanalyse nicht berücksichtigt wurden und auf welche die Ergebnisse der Analysen gar nicht zutreffen. Mit Inkrafttreten der europäischen Datenschutz-Grundverordnung (DSGVO) hat der Datenschutz in der EU einen wesentlich höheren Stellenwert erhalten.⁵ Die DSGVO enthält in allen Staaten der EU unmittelbar geltendes Recht, welches im Zweifelsfall auch Vorrang vor dem nationalen Recht der Mitgliedstaaten hat, wobei die Verordnung Öffnungsklauseln beinhaltet, die von den einzelnen Mitgliedstaaten im Rahmen ihrer Gesetzgebung entsprechend angepasst werden können, ohne dass Abweichungen von der DSGVO zulässig sind. So hat in Deutschland das Bundesdatenschutzgesetz (BDSG), welches im Rahmen der Einführung der DSGVO überarbeitet wurde, die Aufgabe, die in den Öffnungsklauseln definierten Entscheidungsräume zu ergänzen. Zudem gibt es weitere deutsche Gesetze hinsichtlich des Datenschutzes, wie u. a. die Datenschutzgesetze der Bundesländer, für die Sozialdaten das Zehnte Sozialgesetzbuch (SGB X) oder den Datenschutz bei den Kirchen. Allerdings dürfen diese Gesetze die DSGVO nur konkretisieren, aber nicht ändern. Da die Schweiz nicht Teil der EU ist, ist hier die DSGVO nicht direkt anwendbar, wobei deren im Jahr 2020 überarbeitetes Datenschutzgesetz (DSG) zu wesentlichen Teilen der DSGVO entspricht.⁶

³ Vgl. Weiß/Alsabab (2020) S. 5.

⁴ Vgl. Titel II Art. 8 EU (2010); Kneuper (2021) S. 1 f.

⁵ Vgl. Kneuper (2021) S. 1, S. 4, S. 5 f.

⁶ Vgl. Kneuper (2021) S. 6 ff.

Während der Schutz der Daten in Europa durch die europäische Datenschutzgrund-Verordnung (DSGVO) geregelt wird, ist in den USA das Datenschutzrecht weitgehend in sektorspezifische Vorschriften unterteilt, wie u. a. für Krankenversicherungen im Health Insurance Portability and Accountability Act (HIPAA) oder für den Erziehungssektor im Family Educational Rights and Privacy Act (FERPA), und in China wird das Datenschutzrecht durch das mit der DSGVO vergleichbare Personal Data Protection Act reglementiert.⁷ Der amerikanische Health Insurance Portability and Accountability Act (HIPAA), welcher u. a. eine Liste von Identifikatoren enthält (Merkmale zur Identifizierung von Daten), die im Rahmen einer Basis-Anonymisierung entfernt werden müssen,⁸ und diese Liste auch in Deutschland in diesem Zusammenhang herangezogen wird, greift den Begriff der De-Identifikation (De-Identification) auf, welcher den Prozess des Schutzes von Personen vor Identifizierung umfasst, wofür es zwei Methoden gibt. So entscheidet zum einen eine Person (ein für die Verarbeitung Verantwortlicher im Sinne der DSGVO), ob das angewandte Verfahren nur sehr geringe Risiken hinsichtlich einer Re-Identifizierung der betroffenen Person(en) beinhaltet. Zum anderen müssen Informationen (sog. Identifikatoren) von betroffenen Personen entfernt werden. Die De-Identifikation nach dem HIPAA stellt keine Anonymisierung im Sinne des europäischen Rechts dar, sondern kann die Anforderungen erfüllen, die sich aus der DSGVO in Bezug auf die Pseudonymisierung ergeben.⁹ Neben den sektorspezifischen Vorschriften gibt es in den USA zudem in den einzelnen Bundesstaaten teilweise sehr unterschiedliche Regelungen, wie u. a. der seit Anfang 2020 eingeführte California Consumer Privacy Act, der im Vergleich zu den anderen Bundesstaaten sehr streng ist und insbesondere für überregionale Unternehmen eine Herausforderung darstellt. Die gesetzlichen Regelungen der USA beinhalten auch grundsätzliche Unterschiede zur DSGVO. So muss ein Unternehmen personenbezogene Daten nicht grundsätzlich schützen, sofern mit den Kunden keine entsprechenden Vereinbarungen getroffen wurden. Zudem haben Datenschutzkontrollen durch Aufsichtsbehörden oder Datenschutzbeauftragte weniger Gewicht. Da die Sicherheits- und Nachrichtendienste in den USA weitreichende Befugnisse zur Überwachung elektronischer Kommunikation haben, u. a. durch die gesetzlichen Regelungen des FISA Amendments Act of 2008, der Executive Order 12333 und des CLOUD Act, besteht kein angemessenes Datenschutzniveau gemäß der DSGVO, sodass

⁷ Vgl. Kessler/Hoff/Freytag (2019) S. 1998; Prasser/Eicher u. a. (2020) S. 1278; Kneuper (2021) S. 11 f.

⁸ Vgl. GMDS (2018) S. 17 f.; Kneuper (2020) S. 10 ff.; Kneuper (2021) S. 149 ff.

⁹ Vgl. Office for Civil Rights (2015); GMDS (2018) S. 17 f.

ein Transfer personenbezogener Daten aus der EU in die USA, z. B. im Rahmen des Cloud Computing, problematisch erscheint. Insbesondere verpflichtet der CLOUD Act Unternehmen mit Sitz in den USA, wie Internet-Firmen und IT-Dienstleister, US-Behörden Zugriff auf gespeicherte Daten zu gewährleisten, selbst wenn die Speicherung nicht in den USA, sondern in der EU erfolgt.¹⁰ So wurde auch nach dem Urteil des Europäischen Gerichtshofs (EuGH) das EU-US Privacy Shield (EU-US-Datenschutzschild) 2020 für ungültig erklärt, wodurch Übermittlungen von personenbezogenen Daten in die USA auf dieser Basis nicht mehr stattfinden können, da die Zugriffsmöglichkeiten nicht den europäischen Datenschutzanforderungen entsprechen.¹¹ Das in China am 20. August 2021 veröffentlichte und seit dem 1. November 2021 in Kraft getretene Gesetz zum Datenschutz entspricht weitgehend den Anforderungen der Datenschutz-Grundverordnung (DSGVO), wobei die Anforderungen an die Datensicherheit weitreichender sind als die der DSGVO. Das neue chinesische Gesetz regelt nicht nur die personenbezogenen Daten chinesischer Bürger, sondern auch Daten, welche für die nationale Sicherheit und die Wirtschaft Chinas wichtig sind, und enthält strengere Beschränkungen für die Datenübertragung als die DSGVO.¹²

Die vorliegende Studie befasst sich mit dem Thema der Anonymisierung im Kontext der künstlichen Intelligenz (KI) und Big Data. In den Kap. 2 und 3 werden zunächst die wesentlichen Grundlagen zur künstlichen Intelligenz (KI) und zu Big Data dargestellt, während in Kap. 4 personenbezogene, pseudonymisierte und anonymisierte Daten im Kontext der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) thematisiert werden. In Kap. 5 werden dann die Techniken der Pseudonymisierung skizziert, gefolgt von einer detaillierten Behandlung der Techniken und Verfahren der Anonymisierung in den Kap. 6 und 7. Kap. 8 erörtert die Risiken der anonymisierten Daten, während in den Kap. 9 und 10 die Vorgehensweise bei der Durchführung der Anonymisierung aus rechtlicher und technischer Sicht durch den Einsatz entsprechender Software behandelt wird. Die Studie schließt mit einem Fazit ab.

¹⁰ Vgl. Kneuper (2021) S. 11 f.

¹¹ Vgl. Theelen/Kleta u. a. (2021).

¹² Vgl. Kinast (2021).

Künstliche Intelligenz

2

Kognitive oder geistige Fähigkeiten von Computern und Maschinen, welchen menschlichen Fähigkeiten ähneln, werden als künstliche Intelligenz (KI) bezeichnet. Hierbei kann es sich um das Lernen aus Erfahrungen oder um die Lösung von Problemen handeln. Die künstliche Intelligenz eines Systems (Computers) kann mit dem sog. Turing-Test¹ analysiert werden, wobei ein Prüfer mit einem intelligenten menschlichen Experten sowie einem Computer parallel kommunizieren kann. Dem System wird dann künstliche Intelligenz zugesprochen, sobald der Prüfer nicht mehr in der Lage ist, zu unterscheiden, mit wem von beiden er kommuniziert. Die menschliche Intelligenz kann in sehr verschiedene Bereiche und Anwendungsfelder gegliedert werden und zeigt die Vielfalt von Intelligenz auf: Sprachliche Intelligenz, musikalische Intelligenz, logisch-mathematische Intelligenz, bildlich-räumliche Intelligenz, körperlich-kinästhetische Intelligenz, intrapersonale und interpersonale Intelligenz, naturalistische und existenzielle Intelligenz sowie kreative und soziale Intelligenz.²

Im Rahmen der künstlichen Intelligenz (KI) sollen Systeme entwickelt werden, die auf diesen Gebieten intelligente Leistungen erbringen können. Darüber hinaus soll anhand dieser Systeme analysiert werden, wie das menschliche Gehirn diese Intelligenzleistungen vollbringen kann. Computerprogramme der künstlichen Intelligenz (KI), bestehend aus vielen Schichten und Operatoren, erhalten Informationen aus ihrem Umfeld in Form von Bildern, Texten und Signalen, welche in Zahlenpakete verwandelt werden. Diese Zahlenpakete werden als Eingabe in den Programmen durch einfache mathematische Operationen

¹ Benannt nach dem britischen Mathematiker Alan M. Turing (1912–1954), vgl. Mainzer (2019) S. 10.

² Vgl. Kreutzer/Sirrenberg (2019) S. 2 f.; Paaß/Hecker (2020) S. 12.

(u. a. Addition, Multiplikation) in neue Zahlenpakete transformiert und als Ausgabezahlenpakete erzeugt sowie von anderen einfach strukturierten Operatoren weiterverarbeitet. Die Eingabe wird in immer abstraktere Darstellungen verwandelt, welche die wesentlichen Merkmale für die gesuchten Problemlösungen immer besser abbilden, bis der letzte Operator die gewünschte Ausgabe in einfacher Weise berechnen kann. Dieses Programm wird als tiefes neuronales Netz (TNN) bezeichnet. Das tiefe neuronale Netz enthält Parameter, welche ebenfalls ein Zahlenpaket mit einer Menge von bis zu mehreren Milliarden Zahlenwerten bilden und durch Optimierungsverfahren so angepasst werden, dass die beobachteten Daten möglichst gut reproduziert werden können.³

2.1 Arten der künstlichen Intelligenz

Bei der künstlichen Intelligenz (KI) wird zwischen einer schwachen KI (Artificial Narrow Intelligence, ANI) und einer starken (oder allgemeinen) KI (Artificial General Intelligence, AGI) unterschieden. Schwache künstliche Intelligenz (KI) fokussiert sich auf Systeme, welche Aufgaben auf mindestens menschlichem Niveau ausführen und konkrete Anwendungsprobleme lösen können, sodass nicht primär menschliche Fähigkeiten imitiert werden, sondern mithilfe von gezielt eingesetzten Algorithmen komplexe Probleme gelöst respektive besser gelöst werden, als es menschliche Fähigkeiten ermöglichen könnten. In diesem Kontext konnten in den letzten Jahren zahlreiche Durchbrüche erzielt werden, in denen KI-Systeme die Leistung von Menschen erreicht oder übertroffen haben, wobei es sich überwiegend um sensorische Fähigkeiten gehandelt hat, wie u. a. die Erkennung von Objekten in Bildern, die Übertragung von Audiosignalen in geschriebene Texte oder die Übersetzung von Texten in eine andere Sprache. Diese künstliche Intelligenz wird als schwache KI bezeichnet, weil es sich um einen Teilaspekt der menschlichen Intelligenz handelt. So fallen auch alle bislang existierenden Systeme unter die schwache KI, da sie kein tieferes Verständnis für eine Problemlösung oder ihre kausalen Zusammenhänge entwickeln. Die starke künstliche Intelligenz (KI) oder allgemeine künstliche Intelligenz (AKI) formuliert hingegen die Bestrebung, menschliche Fähigkeiten durch eine Technologie in sehr vielen Bereichen nachzubilden, zu optimieren und sogar zu übertreffen. Diese soll Problemstellungen in ungewohnten Situationen auch ohne oder mit nur wenigen Erfahrungswerten bewältigen können. Bislang können KI-Systeme nur

³ Vgl. Paaß/Hecker (2020) S. 12 f.