Robotik und Recht 26

Paul Vogel

Künstliche Intelligenz und Datenschutz

Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potentielle Regulierungsansätze

Nomos

Robotik und Recht

Herausgegeben von

Prof. Dr. Dr. Eric Hilgendorf, Universität Würzburg
Prof. Dr. Susanne Beck, LL.M., Universität Hannover

Band 26

Paul Vogel

Künstliche Intelligenz und Datenschutz

Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potentielle Regulierungsansätze

Nomos

Onlineversion
Nomos eLibrary

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

Zugl.: Würzburg, Univ., Diss., 2021

ISBN 978-3-8487-8703-6 (Print)
ISBN 978-3-7489-3095-2 (ePDF)

1. Auflage 2022

Meinen Eltern

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht, Rechtstheorie, Informationsrecht und Rechtsinformatik an der Julius-Maximilians-Universität Würzburg. Sie wurde im Wintersemester 2019/20 von der Juristischen Fakultät als Dissertation angenommen. Der Arbeit liegt die bei Fertigstellung im Januar 2020 geltende Rechtslage zugrunde; ausgewählte Literatur und gesetzgeberische Bestrebungen wurden bis Herbst 2021 berücksichtigt.

Mein besonderer Dank gilt meinem Doktorvater Herrn Professor Dr. Dr. *Eric Hilgendorf*, der mir bereits zu Beginn meiner juristischen Ausbildung im Jahr 2012 als studentische Hilfskraft an seinem Lehrstuhl die Beschäftigung mit dem Datenschutzrecht empfohlen und meine Ausbildung seither begleitet hat. Für seine langjährige Unterstützung und die hervorragende Betreuung bin ich ihm herzlich verbunden.

Herrn Professor Dr. *Eckhard Pache* danke ich für die zügige Erstellung des Zweitgutachtens.

Weiterer Dank gilt meinen Freunden und (ehemaligen) Kollegen am Lehrstuhl und an der Forschungsstelle RobotRecht. Besonders zu erwähnen sind Dr. *Christian Haagen*, Dr. *Anna Lohmann*, *Annika Schömig*, *Max Tauschhuber* sowie *Nicolas Woltmann* für ihre ungebrochene Bereitschaft zu Fachdiskussionen und für eine unvergessliche Zusammenarbeit. Für gewinnbringende Gespräche sei auch Dr. *Christoph Ritzer* und Dr. *David Roth-Isigkeit* herzlich gedankt.

Für ihren Rückhalt und stets aufbauende Worte ist *Marina Reitz* ganz besonders hervorzuheben.

Schließlich danke ich von Herzen meiner Familie, allen voran meinen Eltern *Gabriele* und *Peter Vogel* für ihre bedingungslose Unterstützung in jeder erdenklichen Lebenslage. Ihnen ist diese Arbeit gewidmet.

Würzburg, im November 2021 *Paul Vogel*

Inhaltsverzeichnis

Abkürzungsverzeichnis 15

Einführung 21

Teil 1: Grundlagen 29

Kapitel 1: Begriffliche und technische Grundlagen 29
I. Kurze Geschichte der Künstlichen Intelligenz 29
II. Begriffliche Klärung 34
III. Grundlagen der Maschinenintelligenz 36
1. Techniken des maschinellen Lernens 38
a) Überwachtes Lernen 39
b) Nicht-überwachtes Lernen 40
c) Verstärkungslernen 42
2. Modelltypen des maschinellen Lernens 42
a) Entscheidungsbäume 43
b) Tiefes Lernen in künstlichen neuronalen Netzen 45
IV. Bedeutung von Daten und ihrer Qualität für lernende Systeme 49

Kapitel 2: Einsatzszenarien lernender Systeme 54
I. Einsatz durch Private 54
II. Einsatz durch staatliche Stellen 58
1. Vorausschauende Gefahrenabwehr 59
2. Unterstützung bei Bewährungsentscheidungen 61

Teil 2: Das Datenschutzrecht als Regulierungsinstrument für Künstliche Intelligenz? 64

Kapitel 1: Vorüberlegungen 64
I. Diskriminierungen und andere Rechtsverstöße 66
II. Zentrales Problem: Intransparenz 70
III. Schlüsselbegriffe und Begutachtungsperspektiven 72
IV. Gründe für das Erfordernis von Nachvollziehbarkeit und Erklärbarkeit 73

Kapitel 2: Anwendungsbereich des Datenschutzrechts 76
I. Räumlicher Anwendungsbereich 76
II. Sachlicher Anwendungsbereich 78
1. Personenbezogene Daten 78
2. Automatisierte und nichtautomatisierte Verarbeitung 84
III. Zwischenergebnis 84

Teil 3: Vereinbarkeit von Künstlicher Intelligenz mit den Grundprinzipien des Datenschutzrechts (*de lege lata*) 86

Kapitel 1: Bedeutung und Rechtsnatur der Verarbeitungsgrundsätze 87

Kapitel 2: KI und Rechtmäßigkeit 89
I. Einwilligung des Betroffenen 90
II. Erforderlichkeit der Verarbeitung zur Vertragserfüllung 94
III. Überwiegende Interessen des Verantwortlichen 95
IV. Verarbeitung besonderer Kategorien personenbezogener Daten 100
V. Geltendmachung von Betroffenenrechten 101
VI. Zwischenergebnis 103

Kapitel 3: KI und Treu und Glauben 104

Kapitel 4: KI und Transparenz 106
I. Grundsätze des Transparenzprinzips 107
II. Das Verbot automatisierter Einzelentscheidungen (Art. 22 DSGVO) 109
1. Einordnung und historischer Kontext der Vorschrift 110
a) Geschichte und verfassungsrechtlicher Hintergrund des Verbots automatisierter Entscheidungen im Einzelfall 110
aa) Art. 15 DSRL 110
bb) § 6a BDSG a.F. 113
b) Normcharakter des Art. 22 DSGVO 114
2. Anwendungsbereich der Vorschrift 116
a) Automatisierte Einzelfallentscheidung 116
aa) Entscheidung auf Grundlage einer automatisierten Verarbeitung 117
bb) Unterwerfung des Betroffenen 119
cc) Ausschließliches Beruhen 120

b) Rechtliche Wirkung oder erhebliche Beeinträchtigung durch die Entscheidung 122
aa) Rechtliche Wirkung 123
(1) Grundsätzliches 123
(2) Beschränkung des Anwendungsbereichs auf negative rechtliche Wirkungen 123
(3) Zwischenfazit 127
bb) Erhebliche Beeinträchtigung in ähnlicher Weise 127
(1) Grundsätzliches 127
(2) Insbesondere: Personalisierte Preisdifferenzierung 129
(3) Zwischenfazit 132
c) Ausnahmetatbestände 132
aa) Abschluss oder Erfüllung eines Vertrages 133
bb) Öffnungsklausel für unionsrechtliche und mitgliedstaatliche Regelungen 134
(1) § 37 BDSG 135
(2) § 31 BDSG 138
cc) Ausdrückliche Einwilligung des Betroffenen 139
dd) Erforderliche Schutzmaßnahmen 140
3. Zwischenergebnis: Auswirkungen auf den Einsatz lernender Systeme 141
III. Informationspflichten und Auskunftsansprüche bei automatisierten Einzelentscheidungen 142
1. Grundsätzliches 142
a) Inhaltliche Anforderungen und Zeitpunkt der Informationserteilung 143
b) Formale Anforderungen 144
2. Pflicht zur Information und Auskunft über den Einsatz von KI *de lege lata* 144
a) Bestehen einer automatisierten Entscheidungsfindung („Ob“) 145
b) Einzelheiten der automatisierten Entscheidungsfindung („Wie“) 147
IV. Allgemeine Erfordernisse des Transparenzgrundsatzes abseits von Art. 22 DSGVO 149
V. Zwischenergebnis 151
Kapitel 5: KI und Zweckbindung 151
I. Inhalt des Zweckbindungsgrundsatzes 152

II. Zweckbindung bei der Verarbeitung personenbezogener Daten zum Zwecke des maschinellen Lernens 153
1. Anforderungen an die Konkretisierung des Zwecks 153
2. Weiterverarbeitung zu Zwecken des maschinellen Lernens 154
a) Fortentwicklung eines intelligenten Systems als „wissenschaftliche Forschung“ 155
b) Kompatibilitätstest gemäß Art. 6 Abs. 4 DSGVO 157
3. Risikoorientierte Auslegung des Zweckbindungsgrundsatzes 158
III. Zwischenergebnis 159

Kapitel 6: KI und Datenminimierung sowie Speicherbegrenzung 160
I. KI und Datenminimierung 161
II. KI und Speicherbegrenzung 163

Kapitel 7: Zwischenfazit – Vereinbarkeit von KI mit den Datenschutzgrundsätzen 165

Teil 4: Regulierungsansätze für einen transparenten Einsatz von KI 172

Kapitel 1: Ein subjektives „Recht auf Erklärung“ des Betroffenen? 172
I. Vorteile eines solchen Rechts 173
II. Normative Verortung eines Rechts auf Erklärung 175
III. Argumente gegen ein Recht auf Erklärung 177
1. Vergleich mit der früheren Rechtslage 177
2. Entgegenstehende Rechte und Interessen des Verantwortlichen 179
a) Geistiges Eigentum 179
b) Geschäftsgeheimnisse 181
c) Einschränkung der Beschränkungen 183
3. Faktischer Nutzen einer umfassenden Auskunft 183
IV. Zwischenfazit 185
V. Konturierung eines Rechts auf Erklärung mit Hilfe des risikobasierten Ansatzes der DSGVO 186
1. Ursprung und Charakter des risikobasierten Ansatzes 186
2. Eignung des risikobasierten Ansatzes zur Präzisierung eines Rechts auf Erklärung 187
VI. Inhalt des Rechts auf Erklärung 193
1. Abgrenzung nach Bezugspunkt und maßgeblichem Blickwinkel 193

2. Anforderungen an die Begründung einer konkreten Entscheidung 196
a) Ermittlung der Begründungstiefe aus der Perspektive ihres Zwecks 197
b) Vergleich mit dem Begründungserfordernis hoheitlichen Handelns 199
VII. Ergebnis: Ein Recht auf Erklärung algorithmischer Entscheidungen 201

Kapitel 2: Pflichten der Betreiber intelligenter Systeme 205
I. Zulassungskontrolle 206
II. Fortwährende ergänzende Algorithmenkontrolle 210
1. Kontrollrechte der Untersuchungsbehörden 211
2. Mitwirkungspflichten des Betreibers 212
III. Kennzeichnung algorithmischer Entscheidungen 214
IV. Pseudonymisierung und Anonymisierung personenbezogener Daten 216
1. Regelungen der DSGVO zu Pseudonymisierung und Anonymisierung 217
a) Pseudonymisierung 217
b) Anonymisierung 219
2. Insbesondere: Anonymisierungstechniken beim maschinellen Lernen 221
a) K-Anonymisierung 222
b) Differential Privacy 223
c) Homomorphe Verschlüsselung 224
3. Zwischenfazit 225
V. Freiwillige Selbstverpflichtung und Zertifizierungsmöglichkeiten 227

Kapitel 3: Aufsichtsbehördliche Sanktionsmöglichkeiten und individueller Rechtsschutz 229
I. Datenschutzrechtliche Sanktionsmöglichkeiten 229
II. Möglichkeiten individuellen Rechtsschutzes 230

Teil 5: Fazit 232

Kapitel 1: Thesen zu einem datenschutzkonformen Einsatz intelligenter Systeme 232

Kapitel 2: Ausblick 237

Literaturverzeichnis 243

Abkürzungsverzeichnis

a.A.	andere Ansicht
a.F.	alte Fassung
ABl. EG	Amtsblatt der Europäischen Gemeinschaften
ABl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz/Absätze
ACM	Association for Computing Machinery
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGG	Allgemeines Gleichbehandlungsgesetz
AI	Artificial intelligence
Alt.	Alternative
Anm. d. Verf.	Anmerkung des Verfassers
AO	Abgabenordnung
AöR	Archiv des öffentlichen Rechts
APuZ	Aus Politik und Zeitgeschichte
Art.	Artikel
Aufl.	Auflage
BayPAG	Bayerisches Polizeiaufgabengesetz
BDSG	Bundesdatenschutzgesetz
BeckOGK	beck-online.GROSSKOMMENTAR
BeckOK	Beck'scher Online-Kommentar
BeckRS	beck-online.RECHTSPRECHUNG
Begr.	Begründer
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BMBF	Bundesministerium für Bildung und Forschung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BremDSGVOAG	Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung
BT-Drucks.	Bundestagsdrucksache

BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
bzw.	beziehungsweise
CCPA	California Consumer Privacy Act
CDU	Christlich Demokratische Union Deutschlands
CR	Computer und Recht
CSU	Christlich-Soziale Union in Bayern
d.h.	das heißt
DAR	Deutsches Autorecht
DARPA	Defense Advanced Research Projects Agency
DB	DER BETRIEB
ders.	derselbe
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
dies.	dieselbe(n)
DÖV	Die Öffentliche Verwaltung
DSGVO	Datenschutz-Grundverordnung
DSGVO-E	Vorschlag des Europäischen Parlaments und des Rates einer Datenschutz-Grundverordnung (= KOM[2012], 11 endgültig)
DSRITB	Deutsche Stiftung für Recht und Informatik – Tagungsband Herbstakademie
DSRL	Datenschutzrichtlinie (= Richtlinie 95/46/EG)
dt.	deutsch
DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
Ed.	Edition
EDPL	European Data Protection Law Review
EG	Europäische Gemeinschaft
Einf.	Einführung
Einl.	Einleitung
ErwGr.	Erwägungsgrund/Erwägungsgründe
et al.	et alii
EU	Europäische Union
EuGH	Europäischer Gerichtshof

EUV	Vertrag über die Europäische Union
EuZA	Europäische Zeitschrift für Arbeitsrecht
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
f.	folgende
FDA	Food and Drug Administration
ff.	folgende
Fn.	Fußnote
FS	Festschrift
GA	Generalanwalt/Generalanwältin
gem.	gemäß
gen.	genannt
GeschGehG	Geschäftsgeheimnisgesetz
GeschGehRL	Geschäftsgeheimnisrichtlinie (= Richtlinie [EU] 2016/943)
GG	Grundgesetz
ggf.	gegebenenfalls
GRCh	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
h.M.	herrschende Meinung
Hervorh. d. Verf.	Hervorhebung durch Verfasser
HK	Heidelberger Kommentar
Hrsg.	Herausgeber
Hs.	Halbsatz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
i.E.	im Ergebnis
i.S.d.	im Sinne des/der
i.V.m.	in Verbindung mit
IDPL	International Data Privacy Law
IEEE	Institute of Electrical and Electronics Engineers
InTeR	Zeitschrift zum Innovations- und Technikrecht
IT	Informationstechnologie
ITRB	IT-Rechtsberater
JI-RL	EU-Richtlinie für Justiz und Inneres (= Richtlinie [EU] 2016/680)
JZ	JuristenZeitung

K&R	Kommunikation und Recht
Kap.	Kapitel
KI	Künstliche Intelligenz
KI-VO-E	Vorschlag für ein „Gesetz über Künstliche Intelligenz“ (= COM[2021] 206 final)
lit.	littera
m. Anm.	mit Anmerkung
m.w.N.	mit weiteren Nachweisen
MMR	Multimedia und Recht
MPG	Medizinproduktegesetz
MPVO	Medizinprodukteverordnung (= Verordnung [EU] 2017/745)
n.F.	neue Fassung
Nachw.	Nachweis(e)
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
NK	Nomos-Kommentar
NPOG	Niedersächsisches Polizei- und Ordnungsbehördengesetz
Nr.	Nummer(n)
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
NZKart	Neue Zeitschrift für Kartellrecht
o.Ä.	oder Ähnlichem
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OLG	Oberlandesgericht
PinG	Privacy in Germany
PolG BW	Polizeigesetz Baden-Württemberg
PolG NRW	Polizeigesetz des Landes Nordrhein-Westfalen
RatSWD	Rat für Sozial- und Wirtschaftsdaten
RDV	Recht der Datenverarbeitung
RL	Richtlinie
Rn.	Randnummer(n)
Rs.	Rechtssache
S.	Satz/Sätze
S.	Seite(n)

Slg.	Sammlung der Rechtsprechung des Gerichtshofes und des Gerichts Erster Instanz
sog.	sogenannte(n/r/s)
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
StIGH	Ständiger Internationaler Gerichtshof
TÜV	Technischer Überwachungsverein
UAbs.	Unterabsatz
UKlaG	Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz)
US	United States
USA	United States of America
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	von
v.a.	vor allem
Var.	Variante
vgl.	vergleiche
VO	Verordnung
Vol.	Volume
vs.	versus
VuR	Verbraucher und Recht – Zeitschrift für Wirtschafts- und Verbraucherrecht
VwVfG	Verwaltungsverfahrensgesetz
WpHG	Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz)
XAI	Explainable Artificial Intelligence (Erklärbare Künstliche Intelligenz)
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZD-Beil.	Zeitschrift für Datenschutz – Beilage
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
zit.	zitiert
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

Einführung

In jüngerer Zeit lässt sich eine weltweit zunehmende, branchenübergreifende Verwendung intelligenter Systeme beobachten. Ebenso wie automatisierte und autonome Systeme dienen sie dazu, den Menschen bei Tätigkeiten zu unterstützen, die er selbst beispielsweise aufgrund damit verbundener Gefahren oder anderen Unwägbarkeiten nicht selbst ausführen möchte. Darüber hinaus sind solche Systeme auf speziellen Gebieten aber auch in der Lage, den Menschen – etwa aufgrund seiner körperlichen oder geistigen Grenzen – zu übertreffen und in einzelnen Anwendungsszenarien bessere Ergebnisse als dieser zu erzielen. Beispielhaft seien hierzu die Systeme in Erinnerung gerufen, die in ihren Bereichen exponierte Persönlichkeiten aus Fleisch und Blut in den Schatten stellten – sei es beim Schach, dem Spiel *Go* oder in der Quizshow *Jeopardy*.

Auch aus diesem Grund bestehen in der Gesellschaft teils erhebliche Bedenken im Hinblick auf die Entwicklung und den Einsatz Künstlicher Intelligenz (KI). Sogar führende Branchenspezialisten mahnen Vorsicht bei der Fortentwicklung intelligenter Systeme an. Technologiepionier *Elon Musk* bezeichnete KI als „wahrscheinlich größte existenzielle Bedrohung" der Menschheit.[1] *Stephen Hawking* formulierte, dass KI das Beste oder das Schlechteste sein könne, das der Menschheit je zugestoßen ist.[2] Es kursieren „Schreckbilder von Systemen, die sich selbst über menschliches Maß hinaus verbessern, sich unserer Kontrolle entziehen, uns im besten Fall in den Kaninchenstall sperren, weil wir ihnen zu dumm sind, und im schlimmsten zu Büroklammern verarbeiten, einfach, weil sie darauf programmiert sind, immer mehr davon herzustellen".[3]

Als – je nach persönlicher Einstellung – zu erstrebendes oder befürchtendes Endziel wird das Erreichen der Singularität propagiert. Dieser Begriff beschreibt im Kontext des technologischen Fortschritts den Zeitpunkt, ab dem intelligente Systeme sich in einem solchen Tempo selbst verbessern können, dass menschliche Intelligenz nicht mehr erforderlich

1 Zitiert bei *Gibbs*, Elon Musk: artificial intelligence is our biggest existential threat, The Guardian online vom 27.10.2014.
2 *Hawking*, Kurze Antworten auf große Fragen, S. 230 f.
3 *Lenzen*, Künstliche Intelligenz, S. 13.

ist.[4] *Vernor Vinge* postulierte in den 1990er-Jahren plakativ, dass kurz darauf die Ära der Menschheit zu Ende sein würde.[5]

Auf der anderen Seite erhofft sich die Gesellschaft von dem wachsenden Potential intelligenter Systeme zu Recht Vorteile in vielen Bereichen des täglichen Lebens. Pflegeroboter versprechen ein selbstbestimmtes Altern, medizinische Diagnosesoftware kann Krankheiten feststellen, die ein Arzt erst zu einem späteren Zeitpunkt oder gar nicht erkannt hätte und Prognoseprogramme können Sicherheits- und Polizeibehörden bei der Kriminalitätsprävention und Verbrechensaufklärung unterstützen. Die Mehrheit der Bundesbürger hält KI als solche daher mehr für eine Chance als für eine Gefahr.[6] Insofern verwundert es nicht, dass die großen IT-Konzerne dieser Welt Unsummen in die Entwicklung der Maschinenintelligenz investieren. *Google* hat 2016 mit seiner „AI first"-Strategie den Beginn des KI-Zeitalters propagiert und setzt fortan in jedem seiner Produktbereiche auf Künstliche Intelligenz.[7]

Der Digitalverband *Bitkom* prognostiziert eine Verfünffachung des europäischen KI-Marktes bis 2022 – dann sollen in Europa zehn Milliarden Euro für KI ausgegeben werden (2018: zwei Milliarden Euro).[8] In Zeiten stets zunehmender Rechenkapazität, verbunden mit gleichzeitig sinkenden Kosten für Speicherplatz und hohen Forschungsinvestitionen, ist KI mittlerweile im Alltag angekommen.[9]

Maschinen treffen also vermehrt Entscheidungen, die bislang von Menschen getroffen wurden. Dazu gehören auch Entscheidungen über das Schicksal von Individuen, wie es sich etwa am Beispiel der vollautoma-

---

4 *Söffner*, Tech-Euphoriker sehen eine neue Apokalypse kommen – ist das ernst zu nehmen?, NZZ.ch vom 31.05.2018. *Ray Kurzweil*, Director of Engineering bei *Google*, erwartet den Eintritt der Singularität innerhalb der nächsten 30 Jahre, voraussichtlich noch vor 2045, vgl. *Reedy*, Kurzweil Claims That the Singularity Will Happen by 2045, Futurism vom 05.10.2017.

5 *Vinge*, The Coming Technological Singularity: How to Survive in the Post-Human Era, 1993.

6 *Bitkom*, Künstliche Intelligenz: Bundesbürger sehen vor allem Chancen, Pressemitteilung vom 27.11.2018.

7 *Dignan*, Google bets on AI-first as computer vision, voice recognition, machine learning improve, ZDNet vom 17.05.2017.

8 *Bitkom*, Europäischer KI-Markt verfünffacht sich binnen fünf Jahren, Pressemitteilung vom 07.01.2019, Angaben beruhen auf einer Studie des *European Information Technology Observatory*.

9 *Leenes/De Conca*, Artificial intelligence and privacy – AI enters the house through the Cloud, in: Barfield/Pagallo (Hrsg.), Research Handbook on the Law of Artificial Intelligence, S. 280.

tisierten Kreditvergabe zeigt. Kommt das Computerprogramm aufgrund einer Vielzahl von ihm zur Verfügung stehenden Parametern und Attributen zu dem Ergebnis, dass der Antragsteller nicht kreditwürdig sei, kann das für ihn gravierende Konsequenzen haben. Natürlich ist es durchaus möglich (wenn nicht gar wahrscheinlich), dass die maschinelle Entscheidung genauer und in einem objektiven Sinne „richtiger" ist als die eines menschlichen Sachbearbeiters, weil das Programm die Ausfallwahrscheinlichkeit und infolgedessen die Bonität des Antragstellers aufgrund statistischer Wahrscheinlichkeiten und zur Verfügung stehender Parameter genauer berechnen kann.

Allerdings fehlt Algorithmen zum jetzigen Zeitpunkt das, was gemeinhin als „gesunder Menschenverstand" bezeichnet wird, ebenso wie ein moralisches Bewusstsein.[10] Bescheidet das System Kreditanträge von Frauen oder dunkelhäutigen Personen generell negativ, weil in vergangenen Fällen, auf deren Grundlage der Algorithmus trainiert wurde, diese Personengruppen ihren Kredit häufiger als andere nicht bedienen konnten, und stützt es sich dabei nur oder hauptsächlich auf diese statistische Variable, handelt es sich um eine ungerechtfertigte Diskriminierung, der zwingend mit technischen und rechtlichen Mitteln begegnet werden muss.

Problematisch ist, dass bei besonders fortschrittlichen technischen Methoden häufig nicht nachvollzogen werden kann, wie und aus welchen Gründen eine konkrete Entscheidung zustande gekommen ist. Die soeben erwähnte Ungleichbehandlung kann, mit anderen Worten, nicht als solche identifiziert werden, weil für den menschlichen Betrachter nicht ersichtlich ist, dass sich das System allein auf den Parameter der ethnischen Herkunft oder des Geschlechts gestützt hat, als es seine ablehnende Entscheidung getroffen hat.

Nicht nur private Unternehmen verfolgen die fortschreitende Entwicklung intelligenter Algorithmen. Auch im öffentlichen Sektor ist ein zunehmendes Interesse an „smarten" Systemen zu beobachten. Beispielsweise werden in den Vereinigten Staaten schon heute Richter bei der Entscheidung über die Aussetzung der Freiheitsstrafe zur Bewährung durch lernende Algorithmen unterstützt, die auf Basis einer großen Datenmenge Aussagen über die Sozialprognose des Verurteilten treffen können.[11] In Deutschland und weiteren Ländern werden Systeme getestet, die unter dem Schlagwort „predictive policing" Vorhersagen über die Wahrschein-

10 *Lenzen*, Künstliche Intelligenz, S. 47 f.; *Dreyer/Schmees*, CR 2019, 758 (761).
11 *Garber*, When Algorithms Take the Stand, The Atlantic online vom 30.06.2016.

lichkeit der Begehung von Straftaten an konkreten Orten (oder in Zukunft auch durch konkrete Personen) treffen.[12]

Was, wenn die Konsequenz einer maschinellen Entscheidung nicht nur ein versagtes Darlehen ist, sondern eine polizeiliche Gefährderansprache oder gar ein Widerruf der Strafaussetzung zur Bewährung? Als unmittelbarer Grundrechtsverpflichteter muss sich der Staat höheren Anforderungen stellen als private Unternehmen. Insbesondere sind staatliche Institutionen umso mehr verpflichtet, dafür Sorge zu tragen, dass der Einzelne nicht zum bloßen „Objekt" der maschinellen Entscheidungsfindung gerät[13] und Ungleichbehandlungen unterworfen wird, die weder der Betroffene noch eine Kontrollinstanz erkennen kann.

Hier und da geäußerte Vorbehalte gegenüber lernenden Systemen beziehen sich vornehmlich auf diese Intransparenz der Entscheidungsfindung.[14] Insbesondere die Technik des *Deep Learning* zeichnet sich durch eine Vielzahl von Verarbeitungsebenen aus, deren Auswirkungen auf das Ergebnis im Einzelnen kaum bestimmbar sind.[15] Für sie ist charakteristisch, dass häufig selbst der Programmierer des jeweiligen Algorithmus nicht erklären kann, wie das ausgeworfene Ergebnis im Einzelnen zustande gekommen ist.[16]

Um diesen Bedenken auf ethischer, rechtlicher und regulatorischer Ebene zu begegnen, steht das Phänomen der KI auch auf der Agenda der Europäischen Union. In diversen Papieren bekräftigen verschiedene Unionsorgane das Bedürfnis einer gemeinsamen Vorgehensweise der Mitgliedstaaten, auch um im Wettbewerb vor allem mit China und den USA, die ihrerseits kräftig in die Entwicklung von Robotik und KI investieren, mitzuhalten.[17] Die *Europäische Kommission* betont, dass KI bereits Teil unseres

---

12 *Krempl*, Predictive Policing: Die Polizei arbeitet verstärkt wie ein Geheimdienst, heise online vom 29.03.2018.

13 Vgl. insoweit auch *Datenschutzkonferenz*, Hambacher Erklärung zur Künstlichen Intelligenz, S. 3.

14 *Bitkom*, Künstliche Intelligenz. Von der Strategie zum Handeln, Präsentation vom 27.11.2018, S. 9.

15 Zu den technischen Grundlagen sogleich Teil 1 Kap. 1.

16 *Temme*, EDPL 3 (2017), 473 (475); *Gleß/Weigend*, ZStW 126 (2014), 561 (564).

17 Vgl. nur *Europäische Kommission*, Künstliche Intelligenz: Kommission beschreibt europäisches Konzept zur Förderung von Investitionen und Entwicklung ethischer Leitlinien, Pressemitteilung vom 25.04.2018; *Europäisches Parlament*, Bericht über eine umfassende europäische Industriepolitik in Bezug auf künstliche Intelligenz und Robotik vom 30.01.2019 (2018/2088(INI)), S. 4.

täglichen Lebens und nicht bloß Science-Fiction sei.[18] Aus diesem Grund hatte sie mit der *High-Level Expert Group on Artificial Intelligence* eine interdisziplinäre Expertenkommission eingesetzt, die ethische, rechtliche und soziologische Vorgaben für den gesellschaftlich akzeptablen Einsatz von KI entwickeln sollte, welche ihrerseits als Grundlage eines europäischen Rechtsrahmens für KI dienen können.[19]

Anfangs konzentrierten sich die öffentliche Diskussion wie auch die rechtswissenschaftliche Forschung zu intelligenten Systemen auf Fragen der zivil-[20] und strafrechtlichen Haftung für die „Handlungen" eines intelligenten Systems[21] sowie auf Zurechnungsfragen von Willenserklärungen beim Vertragsschluss mittels intelligenter Agenten.[22] Daneben lohnt sich aber auch ein Blick auf datenschutzrechtliche Implikationen des Einsatzes solcher Systeme. Dass eine Entscheidung wie im oben beschriebenen Szenario nicht erklärt werden kann, ruft im Falle der Verarbeitung personenbezogener Daten erhebliche Konflikte mit dem Datenschutzrecht hervor.

Doch damit nicht genug: Maschinelles Lernen als wichtigstes Teilgebiet der KI funktioniert nur mit einer gewaltigen Datenmenge als Basis des Lernprozesses.[23] Allein durch die Auswertung massenhafter Daten (*Big Data*) kann ein System in die Lage versetzt werden, Muster und Korrelationen zu erkennen und daraus Vorhersagen zu treffen oder Klassifikationsaufgaben zu erledigen. Gerade vor dem Hintergrund der kürzlich abgeschlossenen – zumindest geplanten[24] – Vollharmonisierung des europäischen Datenschutzrechts ist zu klären, ob rechtliche Regelungen für das Phänomen selbstlernender Algorithmen existieren und diesem möglicher-

---

18 *Europäische Kommission*, Mitteilung „Artificial Intelligence for Europe" vom 25.04.2018, COM(2018) 237 final.

19 Vgl. https://ec.europa.eu/futurium/en/european-ai-alliance/ai-hleg-steering-group-european-ai-alliance.html (13.11.2021). Die Ergebnisse liegen mittlerweile vor und sind auf der Webseite der *Europäischen Kommission* abrufbar, vgl. https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai (13.11.2021)

20 Statt vieler *Zech*, ZfPW 2019, 198 ff.; *Borges*, NJW 2018, 977 (980 ff.); *Wendt/Oberländer*, InTeR 2016, 58 ff.

21 Vgl. *Lewke*, InTeR 2018, 207 (209). Zur strafrechtlichen Verantwortlichkeit etwa *Hilgendorf*, Autonome Systeme, künstliche Intelligenz und Roboter, in: FS-Fischer, S. 99 ff.; zur Strafbarkeit von Herstellern automatisierter Fahrzeuge *Schuster*, DAR 2019, 6 ff.

22 Vgl. etwa *Specht/Herold*, MMR 2018, 40 ff.; *Pieper*, InTeR 2018, 9 (13 f.).

23 *Lenzen*, Blackbox im Labor, in: P.M. Thema 1/2019, S. 38 (40).

24 Ob das Ziel der Vollharmonisierung tatsächlich erreicht wurde, wird angesichts diverser Ausgestaltungsspielräume für die Mitgliedstaaten mitunter bezweifelt, vgl. etwa *Kühling/Martini*, EuZW 2016, 448 (454).

weise sogar im Wege stehen. Zudem müssen Diskriminierungen, wie sie sich in Szenarien wie dem oben beschriebenen Fallbeispiel ereignen, durch die Rechtsordnung verhindert werden.

Die vorliegende Arbeit will an dieser Stelle ansetzen und die Konsequenzen der Intransparenz bestimmter algorithmischer Entscheidungen aus juristischer Perspektive untersuchen. Zu ermitteln ist, ob das geltende Recht auf diesen sogenannten Blackbox-Charakter des tiefen Lernens und die sich aus diesem ergebenden Gefahren vorbereitet ist. Daraus ergibt sich die Folgefrage, ob das geltende Datenschutzrecht, dem in weiten Teilen seit der zweiten Hälfte des 20. Jahrhunderts dieselben Grundsätze zugrunde liegen, im Zeitalter von Künstlicher Intelligenz als Musterbeispiel neuer, disruptiver Technologien überhaupt noch Bestand haben kann oder nicht vielmehr einer umfassenden Revision bedarf.

Nach dem vorliegenden Problemaufriss sollen in einem Grundlagenteil die technische Funktionsweise intelligenter Systeme erläutert und maßgebliche Begriffe geklärt werden. Was sind lernende Systeme? Wie funktionieren sie? Welche Methoden des maschinellen Lernens gibt es? Wann ist ein Computer eigentlich „intelligent“? Da der Fokus der vorliegenden Untersuchung auf den datenschutzrechtlichen Herausforderungen des Einsatzes von KI liegt, ist vor allem die Bedeutung von Daten als Grundlage maschineller Lernprozesse zu beleuchten. Weiterhin sind denkbare Einsatzszenarien intelligenter Algorithmen zu beschreiben, die das praktische Bedürfnis einer datenschutzkonformen Verarbeitung veranschaulichen.

Im zweiten Teil der Arbeit ist die Bedeutung des Datenschutzrechts für den legalen Einsatz von KI zu verdeutlichen. Dabei ist vor allem dem Umstand Rechnung zu tragen, dass sich einige maschinelle Lernverfahren durch eine besondere Intransparenz ihrer Entscheidungsfindung auszeichnen. Das wirft beispielsweise auch aus der Perspektive der zivilrechtlichen Haftung für „Handlungen“ intelligenter Systeme Probleme auf, sofern die eindeutige Zuweisung der Verantwortlichkeit aufgrund fehlender Einblicke in die internen Abläufe eines intelligenten Systems Schwierigkeiten bereitet. Aus der Sicht des Datenschutzrechts wird diese Intransparenz vor allem zum Problem, wenn das Subjekt der algorithmischen Datenverarbeitung nicht hinreichend über das Ob und Wie der Verarbeitung informiert werden kann – ggf. verhindert bereits dieser Umstand einen datenschutzrechtskonformen Einsatz intelligenter Algorithmen.

Diese und weitere Fragen sind im ersten Hauptteil der vorliegenden Untersuchung zu klären, der die Vereinbarkeit von KI-Anwendungen mit den datenschutzrechtlichen Grundprinzipien *de lege lata* analysiert (Teil 3). Es wird festzustellen sein, dass die teilweise bereits seit den 1980er-Jahren

etablierten Datenschutzgrundsätze mit den Besonderheiten intelligenter Algorithmen nicht nur unerheblich konfligieren. Das gilt namentlich vor allem für den Grundsatz der transparenten Verarbeitung, der dem sog. Blackbox-Charakter bestimmter intelligenter Systeme schon begrifflich diametral zuwiderläuft. Zudem stellt die Notwendigkeit riesiger Datensammlungen als Grundlage maschineller Lernprozesse die Grundsätze der Rechtmäßigkeit, Fairness, Zweckbindung, Datenminimierung und Speicherbegrenzung auf die Probe.

Im zweiten Hauptteil der Arbeit ist sodann zu untersuchen, wie ein datenschutzrechtskonformer Einsatz intelligenter KI-Systeme aussehen könnte (Teil 4). Besonderes Augenmerk ist auf die Frage zu legen, ob und inwieweit das europäische Datenschutzrecht dem Verarbeitungssubjekt ein „Recht auf Erklärung" algorithmischer Entscheidungen gewährt. Ein solches Recht würde, wollte man es in einem umfassenden Sinne verstehen, aufgrund seiner faktischen Unerfüllbarkeit in vielen Fällen zu einer datenschutzrechtlichen Illegalität des Einsatzes bestimmter KI-Anwendungen führen. Das Datenschutzrecht würde somit zu einem kaum zu rechtfertigenden Hemmschuh für Innovation durch KI geraten.

Daneben sind weitere Bausteine eines regulativen Rahmens für KI zu erarbeiten, der einen rechtssicheren und datenschutzrechtskonformen Einsatz intelligenter Systeme ermöglicht. Ein solches Regelungssystem muss stets die Rechte und Freiheiten des von einer maschinellen Entscheidung Betroffenen im Blick haben. Es geht mit anderen Worten um die Entwicklung eines datenschutzrechtlichen Rahmens, der es ermöglichen soll, die Vorteile von KI bestmöglich zu nutzen, der gleichzeitig aber dafür sorgt, ihre Nachteile und Gefahren unter Kontrolle zu behalten. Aufgrund der neuen europäischen Vorgaben zum Datenschutz durch Technikgestaltung (*privacy by design*) ist jedem Entwickler und Anbieter intelligenter Systeme zu raten, sich frühzeitig mit den datenschutzrechtlichen Fragestellungen auseinanderzusetzen und gegebenenfalls erforderliche Prozesse und Mechanismen möglichst rasch zu implementieren, um nicht mit dem beachtlichen Sanktionssystem des europäischen Datenschutzrechts in Konflikt zu geraten.

Problematisch ist, dass bisherige Lösungsansätze häufig entweder auf der einen Seite den Datenschutz substantiell beeinträchtigen, oder aber auf der anderen Seite die Vorteile und Chancen von KI maßgeblich einschränken – oder sogar beide Folgen hervorrufen.[25] Es ist daher zu erörtern, welche Lösungsansätze bereits existieren, worauf sie beruhen und inwieweit

25 *Kuner et al.*, IDPL 8 (2018), 289 (291).