STIFTUNG DATENSCHUTZ

# POTENZIALE VON KÜNSTLICHER INTELLIGENZ MIT BLICK AUF DAS DATENSCHUTZRECHT

## Gutachten


AUTOR

Prof. Dr. Georg Borges, Universität des Saarlandes

# INHALT

**Kapitel F**

HERAUSFORDERUNGEN DER INDIVIDUELLEN KOMMUNIKATION DURCH KI-SYSTEME



**Kapitel G**

**Kapitel A**

# DAS VERHÄLTNIS VON KÜNSTLICHER INTELLIGENZ UND DATENSCHUTZ

## I. POTENZIALE UND HERAUSFORDERUNGEN DURCH KÜNSTLICHE INTELLIGENZ AUS SICHT DES DATENSCHUTZRECHTS

Mit dem Begriff der künstlichen Intelligenz[1] verbinden sich in der aktuellen Diskussion größte Erwartungen. Künstliche Intelligenz als Teilgebiet der Informatik, das der Erforschung von Mechanismen des intelligenten menschlichen Verhaltens gewidmet ist,[2] oder als „Eigenschaft eines IT-Systems, ‚menschenähnliche', intelligente Verhaltensweisen zu zeigen"[3], und ebenso KI-Systeme, also Systeme bestehend aus Software und ggf. Hardware, in denen Technologien der künstlichen Intelligenz zum Einsatz kommen, faszinieren.

Dies gilt vor allem für den Bereich des maschinellen Lernens, der in der letzten Dekade auch die Aufmerksamkeit der breiten Öffentlichkeit erreicht hat. Leistungen von KI-Systemen wie AlphaGo und AlphaGo Zero, ebenso Technologien wie autonome Fahrzeuge, wecken weitreichende Fantasien und Erwartungen.

Das Potenzial der künstlichen Intelligenz und der KI-Systeme wird, sicher zu Recht, als überaus groß eingeschätzt. So werden enormes Wirtschaftswachstum und Wohlfahrtssteigerungen erwartet.[4] Im Bereich der medizinischen Forschung werden wesentliche Forschungserfolge etwa in der Bekämpfung von Krankheiten erhofft.[5] Nicht minder wichtig sind die erhofften Fortschritte in der Versorgung pflegebedürftiger Menschen sowie im Bereich der Gesundheitsfürsorge für jedermann.[6] Die Steigerung von Produktivität in nahezu allen Bereichen soll unter anderem zu einer verbesserten Versorgung der Menschheit mit Nahrung[7] und anderen lebenswichtigen Gütern führen.

Künstliche Intelligenz ist datenhungrig. Die Entwicklung von KI-Systemen beruht, insbesondere im Fall des maschinellen Lernens, häufig entscheidend auf der Nutzung großer Mengen an Daten. Wenn man das zentrale Charakteristikum des maschinellen Lernens darin sieht, dass ein System anhand von großen Datenmengen Muster erkennt und hieraus Informationen ableitet, wird deutlich, dass die Datenverarbeitung zum Kern der Entwicklung von KI-Systemen gehört.

Auch in den Anwendungen erfolgt häufig eine massive Datennutzung, KI-Systeme verwenden häufig zur Ausführung ihrer Funktionalität große Mengen an Daten. Wenn etwa ein hochautomatisiertes Fahrzeug mit Kamera, Lidar und Radar seine Umgebung wahrnimmt und darüber hinaus mit Informationen durch die Verkehrsinfrastruktur, andere Fahrzeuge sowie durch eine gegebenenfalls laufend aktualisierte Karte versorgt wird, wird intuitiv deutlich, wie stark die Verbindung von KI-Systemen und Datenverarbeitung typischerweise ist.

Das Datenschutzrecht, das erhebliche organisatorische und technische Anforderungen an die Verarbeitung von (personenbezogenen) Daten formuliert und diese zudem empfindlich einschränkt, steht in einem natürlichen Spannungsverhältnis zur künstlichen Intelligenz. Zu Recht wird die Frage aufgeworfen, inwieweit Datenschutz ein Hemmnis für die Entwicklung und Nutzung von künstlicher Intelligenz und KI-Systemen darstellt und damit der Realisierung der damit verbundenen Poten-

1 Der Begriff der KI wird in großer Vielfalt definiert; siehe einen kleinen Überblick etwa bei Kaulartz/Braegelmann in Kaulartz/Braegelmann, Kap. 1 Rn. 2 ff.

2 So eine Hauptströmung des Begriffsverständnisses, stellvertretend hier zitiert nach Wichert, Künstliche Intelligenz, in: Lexikon der Neurowissenschaften (Leitung: Hartwig Wanser), hrsg. von Spektrum Akademischer Verlag, 2000, abrufbar unter https://www.spektrum.de/lexikon/neurowissenschaft/kuenstliche-intelligenz/6810 (zuletzt abgerufen am 14.11.2021).

3 So eine zweite Hauptströmung, stellvertretend zitiert nach Bitkom/DFKI, Künstliche Intelligenz, Ziff. 3.2. (S. 28).

4 Bericht Enquete-Kommission KI, BT-Drs. 19/23700, S. 168 f.; Begleitforschung PAiCE, Ziff. 4.3.1. (S. 32ff.), Ziff. 7.1 (S. 51); PwC, Auswirkungen der Nutzung von künstlicher Intelligenz in Deutschland, 2018, S. 12 f., PwC Deutschland_Auswirkungen der Nutzung von künstlicher Intelligenz in Deutschland.pdf (forum-institut.de), zuletzt abgerufen am 28.11.2021.

5 Bericht Enquete-Kommission KI, BT-Drs. 19/23700, S. 248 ff.; Krumm/Dwertmann, S. 161 f.

6 Bericht Enquete-Kommission KI, BT-Drs. 19/23700, S. 253 ff.; Plattform Lernende Systeme (Hrsg.) , Lernende Systeme im Gesundheitswesen – Bericht der Arbeitsgruppe Gesundheit, Medizintechnik Pflege, 2019, S. 8 ff., abrufbar unter Lernende Systeme im Gesundheitswesen:- Grundlagen, Anwendungsszenarien und Gestaltungsoptionen - PLS (plattform-lernende-systeme.de), zuletzt abgerufen am 28.11.2021; zu Einsatzmöglichkeiten von KI i.R.d. Covid-19-Pandemie s. Bericht Enquete-Kommission KI, BT-Drs. 19/23700, S. 110 f.

7 Zur Steigerung des Ertrags in der Landwirtschaft durch KI: BT-Drs. 19/23700, S. 155 f.

ziale für Wirtschaftswachstum und Wohlfahrt entgegensteht.

Künstliche Intelligenz löst auch vielfältige Ängste aus. Die Angst vor dem Verlust von Arbeitsplätzen durch Einsatz von KI-Systemen, die vor einigen Jahren durch entsprechende Prognosen befeuert wurde, wird intensiv diskutiert.[8] Die Gefahr von Schäden an Leib und Leben, die etwa am Beispiel autonomer Fahrzeuge intuitiv deutlich wird, wurde insbesondere seit dem weltweit beachteten Unfall eines Uber-Fahrzeugs im Jahre 2018[9] stark diskutiert.

Ängste und Sorgen lösen auch die offensichtlichen Gefahren aus der Anwendung von KI-Systemen im Bereich der Überwachung einerseits, der Beeinflussung, gar Manipulation, andererseits aus. So können KI-Systeme durch Informationsgewinnung zur weitreichenden Überwachung von Menschen eingesetzt werden, etwa durch autonome Identifizierung.

KI-Systeme können, angefangen bei individualisierter Werbung über die Beeinflussung in von KI-Systemen geführten Dialogen bis zur gezielten Erzeugung oder Verbreitung von Nachrichten, durch Informationsüberlegenheit und Manipulation tiefgreifend Einfluss sowohl auf den Einzelnen als auch auf gesellschaftliche und politische Diskurse nehmen.

Nicht von ungefähr sind derartige Risiken Gegenstand der rechtspolitischen Diskussion und wurden beispielsweise von der EU-Kommission im kürzlich veröffentlichten Vorschlag eines KI-Gesetzes aufgegriffen.

## II. DATENSCHUTZ ALS ANTIPODE ODER PARTNER VON KÜNSTLICHER INTELLIGENZ?

Angst vor Überwachung ist auch eine historische Grundlage des Datenschutzrechts. Das europäische Datenschutzrecht in seiner derzeit vorherrschenden Prägung wurde in den 60er Jahren unter maßgeblicher Beteiligung Deutschlands entwickelt. Dem hessischen Datenschutzgesetz von 1970[10] gebührt der Ruhm, das erste Datenschutzgesetz dieser Art zu sein.[11] Schon in seiner Geburtsphase bezweckte das Datenschutzrecht den Schutz des Einzelnen, daneben aber auch der Gesellschaft und der staatlichen Institutionen.[12]

Das europäische Datenschutzrecht hat sich seit seiner Geburtsstunde enorm entwickelt. Es regelt heute nicht nur den Schutz gegen die Datenverarbeitung des Staates, sondern enthält eine umfassende Regelung des Umgangs mit Informationen, die ihren Schwerpunkt in der Abwehr von Gefahren durch Datenverarbeitung privatwirtschaftlicher Akteure hat und selbst den Einzelnen in seiner privaten Tätigkeit adressiert.

Während die Notwendigkeit von Datenschutz in Deutschland allgemein anerkannt ist und sich das Datenschutzrecht in seiner derzeitigen Prägung als Regelung bereits der bloßen Verarbeitung personenbezogener Daten weltweit zu etablieren scheint, wächst zugleich das Unbehagen demgegenüber. Datenschutz wird verbreitet als Beispiel ausufernder Bürokratie, als Verhinderer von Innovation sowie als Beschränkung von Freiheit wahrgenommen.

Das Verhältnis von künstlicher Intelligenz und Datenschutz ist eine notwendige Frage der sogenannten digitalen Gesellschaft. Es bedarf eines tieferen Verständnisses dieses facettenreichen Verhältnisses und auch einer - derzeit noch nicht abgeschlossenen – adäquaten gesetzlichen Regelung zur Gewährleistung eines angemessenen Interessenausgleichs.

8 Siehe hierzu etwa Südekum, Digitalisierung und die Zukunft der Arbeit, WPZ Analyse Nr. 19, 26.07.2018, PA19DigitalisierungZukunftArbeit20180726.pdf (wpz-fgn.com), zuletzt abgerufen am 28.11.2021.

9 FAZ, Fußgängerin stirbt nach Unfall mit selbstfahrendem Auto von Uber, 2018, Frau stirbt nach Unfall mit selbstfahrendem Auto von Uber (faz.net), zuletzt abgerufen am 28.11.2021; Heise, Tödlicher Unfall mit autonomem Auto: Uber-Fahrerin angeklagt, 2020, Tödlicher Unfall mit autonomem Auto: Uber-Fahrerin angeklagt | heise online, zuletzt abgerufen am 28.11.2021.

10 Datenschutzgesetz [Hessen] vom 7.10.1970, GVBl. Hessen 1970 I 625.

11 Simitis/Hornung/Spieker-Simitis/Hornung/Spieker, Einl. Rn. 1.

12 Simitis/Hornung/Spieker-Simitis/Hornung/Spieker, Einl. Rn. 6 ff., 22 ff.

## III. GEGENSTAND UND GANG DER UNTERSUCHUNG

Die vorliegende Untersuchung nimmt gemäß ihrem Titel „Potenziale von Künstlicher Intelligenz mit Blick auf das Datenschutzrecht“ das Spannungsverhältnis von technischer Innovation und Datenschutz in den Blick. Als Leitgedanke sollen hier zum einen die Frage dienen, inwieweit das Datenschutzrecht eine Grundlage für die erfolgreiche Nutzung der Potenziale von KI darstellt, indem es eine Grundlage für die Akzeptanz von KI und KI-Systemen darstellt, und zum anderen die Frage, inwieweit Datenschutz eine Beschränkung für die Nutzung dieser Potenziale bewirkt.

Die Hypothese dieser Untersuchung ist insoweit, dass Datenschutz weder einseitig als Grundlage noch als Hemmschuh für die Entwicklung von KI und KI-Systemen anzusehen ist, sondern letztlich einen von mehreren Bausteinen des – noch nicht abschließend entwickelten – rechtlichen Rahmens für künstliche Intelligenz darstellt.

Dabei sollen im Wege einer Bestandsaufnahme aktuelle Herausforderungen und Probleme, zugleich aber auch – positiver – Ergebnisse in der Anwendung des Datenschutzrechts auf KI benannt werden. Weiterhin soll untersucht werden, inwieweit Änderungsbedarf im Datenschutzrecht besteht, um die Potenziale von maschinellem Lernen und KI insgesamt besser zur Geltung kommen zu lassen. Zudem soll aufgezeigt werden, ob und wie der Datenschutz bereits dazu beiträgt oder künftig dazu beitragen kann, dass datenbasierte Diskriminierung von Menschen durch KI-Anwendungen vermieden wird.

Die umfassende wissenschaftliche Erörterung des Verhältnisses von KI und Datenschutz bedarf eines Forschungsprogramms. Das Anliegen dieser Untersuchung kann es daher nur sein, diese Fragestellung anhand ausgewählter aktueller Themenbereiche anzureißen, die verschiedene Aspekte der KI und ihres Verhältnisses zum Datenschutzrecht beleuchten. Im Einzelnen sollen folgende Aspekte angesprochen werden:

### Datenschutzrecht als Schutz vor Risiken für Rechte und Freiheiten natürlicher Personen durch Künstliche Intelligenz

In einem ersten Abschnitt (sogleich B) soll die Leistungsfähigkeit des geltenden Datenschutzrechts in Bezug auf die spezifischen Risiken für Rechte und Freiheiten natürlicher Personen durch künstliche Intelligenz im Überblick analysiert werden. Dazu sollen spezifische Risiken, die von dem Einsatz von mit künstlicher Intelligenz ausgestatteten Systemen ausgehen, dargestellt werden. Darauf aufbauend werden, am Beispiel der Informationsgewinnung durch KI-Systeme, die Schutzinstrumente des Datenschutzrechts im Hinblick auf ihre Leistungsfähigkeit in Bezug auf die zuvor identifizierten spezifischen Risiken überprüft. Dabei zeigt sich, dass einzelne der mit KI verbundenen Risiken durch das Datenschutzrecht sehr intensiv adressiert werden, andere hingegen nicht oder nur sehr eingeschränkt.

### Beschränkung von Forschung und Anwendung Künstlicher Intelligenz durch Datenschutz

In einem weiteren Abschnitt (unten C) werden potenziell problematische Beschränkungen, die sich aus dem Datenschutzrecht für die Forschung und Anwendung von künstlicher Intelligenz ergeben, systematisch zusammengestellt und im Hinblick auf Plausibilität grob evaluiert.

### Möglichkeiten und Grenzen des Verzichts auf personenbezogene Daten beim maschinellen Lernen

Im Hinblick auf mögliche Lösungen des Spannungsverhältnisses zwischen Datenschutz und Forschung wird am Beispiel des maschinellen Lernens untersucht, welche Potenziale und Schwierigkeiten mit einem Verzicht auf den Einsatz personenbezogener Daten verbunden sind (unten D).

### Fehlerhafte Entscheidungen durch Künstliche Intelligenz

Die Risiken fehlerhafter Bewertungen natürlicher Personen durch KI-Systeme und die Gefahr von Diskriminierung sind zu Recht ein zentraler Aspekt der Diskussion zu KI-Systemen. Daher bildet die Betrachtung dieser Fragestellung mit Blick auf die Rolle des Datenschutzrechts einen Schwerpunkt der Untersuchung (unten E).

### Herausforderungen durch Verwendung von Echtzeitdaten

Durch die Verwendung von Echtzeitdaten können, etwa bei Techniken des dynamic pricing oder beim predictive policing, aber auch bei individueller Werbung, Grundlagen für automatisierte oder auch manuelle Entscheidungen geschaffen werden, die für den Betroffenen u. U. erhebliche Bedeutung haben können.

Die Verwendung von Echtzeitdaten betrifft teilweise klassische Aspekte des Datenschutzrechts, etwa das Vorliegen von personenbezogenen Daten und die Rechtfertigung der Verarbeitung personenbezogener Daten, geht aber auch darüber hinaus, namentlich unter dem Aspekt der Informationsasymmetrie und der daraus ggf. resultierenden Wissensüberlegenheit. Daher soll diese Fallgruppe zur Beschreibung der Bedeutung einerseits, der Grenzen des Datenschutzrechts andererseits, in Bezug auf die mit KI verbundenen Risiken beleuchtet werden (unten F).

### Leistungsfähigkeit des Datenschutzrechts und Regelungsbedarf

Abschließend wird eine Bewertung der Leistungsfähigkeit des Datenschutzrechts zur Abwehr von Gefahren durch KI-Systeme versucht und, aufsetzend auf den im Rahmen der Untersuchung ermittelten Lücken, Regelungsbedarf sowohl innerhalb des Datenschutzrechts als auch darüber hinaus benannt (unten G).

**Kapitel B**

# DATENSCHUTZRECHT ALS SCHUTZ VOR RISIKEN FÜR RECHTE UND FREIHEITEN NATÜRLICHER PERSONEN DURCH KÜNSTLICHE INTELLIGENZ

## I. RISIKEN FÜR RECHTE UND FREIHEITEN NATÜRLICHER PERSONEN DURCH KÜNSTLICHE INTELLIGENZ

### 1. KI-SYSTEME ALS GEGENSTAND DER RECHTLICHEN REGELUNG

Der rechtliche Rahmen für Künstliche Intelligenz ist in jüngster Zeit Gegenstand intensiver Diskussion.[13] In Europa treibt die Europäische Kommission, insbesondere seit Veröffentlichung ihrer KI-Strategie 2018[14], die Entwicklung eines spezifischen Rechtsrahmens für KI voran. Insbesondere wurde eine ganze Reihe von Expertengruppen gegründet, die ethischen und rechtlichen Aspekten der künstlichen Intelligenz gewidmet waren und im Februar 2020 in zwei Veröffentlichungen der Kommission mündeten: Während die Kommission in ihrem Weißbuch zur künstlichen Intelligenz[15] die Bedeutung des ethischen und rechtlichen Rahmens von künstlicher Intelligenz betonte, konkretisiert sie in ihrem Bericht zur Sicherheit und Haftung für Intelligenz, Internet der Dinge und Robotik[16] ihre Strategie zu zentralen Rechtsfragen. Im April 2021 veröffentliche die Kommission ihren Vorschlag für ein „Gesetz über künstliche Intelligenz".[17] Der Verordnungsvorschlag, der sofort weltweite Aufmerksamkeit gewann, regelt – entgegen der anmaßenden Bezeichnung als „KI-Gesetz" – zentrale Aspekte der Sicherheit von KI-Systemen und setzt hier, wie der am gleichen Tag veröffentliche Entwurf einer neuen Maschinenverordnung[18], die künftige europäische Grundlage des Produktsicherheitsrechts, weitgehend auf das aus dem Produktsicherheitsrecht bekannte System einer Sicherheitsprüfung durch den Hersteller, das zu einem umfassenden Risikomanagement ausgebaut wird.

Gegenstand des KI-Gesetzes ist nicht die „künstliche Intelligenz", sondern sind „KI-Systeme". Der Begriff des KI-Systems, der sich in der europäischen Diskussion durchzusetzen scheint, wird in Art. 3 Nr. 1 des KI-Gesetz-Entwurfs definiert. KI-Systeme sind danach „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". Im Anhang I des Entwurfs sind die bekannten Techniken und Konzepte, die zur Künstlichen Intelligenz im Sinne eines Teilgebiets der Informatik gezählt werden, aufgeführt. KI-Systeme sind danach also letztlich Computerprogramme, die mit Techniken der künstlichen Intelligenz erzeugt wurden.

Die Bezugnahme auf KI-Systeme als Gegenstand der Regelung überzeugt, da sich die besonderen Gefahren durch künstliche Intelligenz erst in funktionsfähigen Produkten zeigen. Die Herstellung und Nutzung derartiger Produkte ist daher zu Recht ein wichtiger Gegenstand des Rechtsrahmens für KI. Das – ausgesprochen weite – Verständnis des KI-Gesetz-Entwurfs von KI-Systemen wird auch in dieser Untersuchung zugrunde gelegt.

KI-Systeme können Schäden an Rechtsgütern natürlicher Personen verursachen. Soweit physische Maschinen durch KI-Systeme gesteuert werden,

13 Siehe einen Überblick etwa bei Borges, A legal Framework for Autonomous Systems, Ziff. 1.1.
14 Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen Künstliche Intelligenz für Europa vom 25.4.218, COM(2018) 237 final.
15 Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen vom 19.2.2020, COM(2020) 65 final.
16 Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss, Bericht über die Auswirkungen künstlicher Intelligenz, des Internet der Dinge und der Robotik im Hinblick auf Sicherheit und Haftung vom 29.1.2020, COM(202) 64 final.
17 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 vom 21.4.2021, COM(2021) 206 final.
18 Proposal for a Regulation of the European Parliament and of the Council on machinery products vom 21.4.2021, COM(2021) 202 final.

etwa hochautomatisierte Fahrzeuge, Drohnen, ec., ist das Risiko für Rechtsgüter durch Unfälle offensichtlich. Derartige Gefahren von Personen- und Sachschäden werden derzeit sowohl aus der Perspektive der Haftung als auch der Produktsicherheit betrachtet. Auch der Entwurf des KI-Gesetzes widmet sich diesen Aspekten.

Aus der Perspektive des Datenschutzrechts sind vor allem Risiken für die Persönlichkeit von Interesse, ebenso das Spannungsverhältnis zwischen Persönlichkeitsschutz und Innovationsschutz. Aus systematischer Sicht können die vielgestaltigen Risiken in Gruppen zusammengefasst werden.

## 2. ERZEUGUNG UND AGGREGATION VON INFORMATION DURCH KI-SYSTEME

Als eine erste Fallgruppe soll die Informationsgewinnung durch KI-Systeme betrachtet werden. Chancen und Risiken aus der Sammlung und Aggregation von Informationen werden zu Recht unter dem Stichwort „Big Data“ diskutiert, es handelt sich nicht um eine spezifische Fragestellung der künstlichen Intelligenz. Jedoch werden KI-Systeme zur Informationsgewinnung eingesetzt. Ein intuitives Beispiel liefert etwa die Gesichtserkennung durch KI-Systeme, durch die natürliche Personen identifiziert oder einzelne Merkmale von Personen erfasst werden. Neue Informationen können auch durch die Auswertung vorhandener Informationen zu natürlichen Personen, etwa durch Bewertung jeglicher Art, erfolgen.

Die Informationsgewinnung durch KI-Systeme erfolgt typischerweise durch Auswertung bereits vorhandener Information. So liegt der Gesichtserkennung das Bildnis einer Person zugrunde, bei Scoring oder Bewertung von Videoaufnahmen eines Bewerbungsgesprächs erfolgt die Bewertung anhand der dem KI-System zur Verfügung gestellten Daten.

Daher sind in Bezug auf Informationsgewinnung durch KI-Systeme zwei Aspekte zu unterscheiden: zum einen die Verarbeitung personenbezogener Daten als solche und zum anderen die Bewertung als solche, die im Hinblick auf ihre Zulässigkeit oder ihre Qualität zu betrachten ist. Dieser zentralen Unterscheidung folgend sollen hier unter dem Gesichtspunkt der Informationsgewinnung die Verarbeitung personenbezogener Daten als klassische datenschutzrechtliche Fragestellung untersucht (dazu sogleich II.) und die Aspekte der Bewertung als eigene Fallgruppe erfasst werden.

## 3. ALGORITHMISCHE ENTSCHEIDUNGEN ÜBER PERSONEN

Mit dem Begriff der algorithmischen Entscheidung sowie verwandten Begriffen wie „maschinelle Entscheidung“ werden im Kern Entscheidungen durch Maschinen über Rechtsträger bezeichnet, von Steuerbescheiden und anderen Verwaltungsakten bis zu Auswahlentscheidungen und Bewertungen (dazu unten E.I).

Entscheidungen und Bewertungen zu Personen durch Maschinen hängen typischerweise zusammen: Eine Bewertung entsteht in einem Vorgang (Bewertungsvorgang), als dessen Bestandteil man die Entscheidung ansehen kann, dem Entscheidungsobjekt ein bestimmtes Bewertungsergebnis zuzuordnen. Wenn eine Maschine ein Scoring zu der Verhaltensweise einer natürlichen Person oder eine Bewertung in Bezug auf die Eignung für einen Arbeits- oder Studienplatz abgibt, so kann man hierin eine Entscheidung sehen (dazu unten E.I). Der Begriff der algorithmischen Entscheidung wiederum meint nicht die Entscheidung eines hochautomatisierten Fahrzeugs, rechts oder links abzubiegen, sondern bezeichnet die Zuordnung von Rechtsfolgen oder von Bewertungen; enthalten ist also eine Bewertung im soeben genannten Sinne.

In beiden Fällen bestehen charakteristische Risiken, die sich auf den Inhalt der Entscheidung oder Bewertung beziehen. Der Steuerbescheid und ebenso eine Bewertung über die Eignung für einen Arbeitsplatz können inhaltlich fehlerhaft sein, etwa eine Diskriminierung enthalten oder aufgrund eines Rechenfehlers einen nicht zutreffenden Punktewert aufweisen.

Die möglichen Fehler einer von einer Software verfassten Bewertung oder Entscheidung sind unterschiedlicher Art und können sich in sehr unterschiedlichen Rechtsverhältnissen auswirken. Es ist daher erforderlich, die Fehler von algorithmischen Entscheidungen sowie von Bewertungen zu systematisieren und sodann die rechtlichen Aspekte der Fehler systematisch zu erfassen. Dies soll in dieser Untersuchung für Entscheidungen und Bewertungen gemeinsam erfolgen (unten E).

### 4. WISSENSÜBERLEGENHEIT UND BEEINFLUSSUNG DURCH KI-SYSTEM

Ein wesentlicher Aspekt möglicher Gefahren durch künstliche Intelligenz betrifft den Bereich der Überlegenheit, insbesondere der Wissensüberlegenheit von KI-Systemen gegenüber dem Menschen und der Beeinflussung von natürlichen Personen durch KI-Systeme. Zu den offensichtlichen Gefahren gehört etwa die Manipulation von Menschen durch Maschinen, die etwa in Artikel 5 Abs. 1 lit. a) und b) des vorgeschlagenen KI-Gesetzes adressiert wird.

Auch die personalisierte Ansprache, etwa in Form von personalisierter Werbung oder individuellen Preisangaben, kann Risiken für Persönlichkeitsrechte aufweisen und wird zu Recht diskutiert (dazu unten F).

Der Themenbereich der Wissensüberlegenheit kann im Rahmen dieser Untersuchung bei weitem nicht ausgelotet werden, soll aber, im Hinblick vor allem auf das Datenschutzrecht, jedenfalls anhand relevanter Beispiele untersucht werden (unten F I.2).

## II. ASPEKTE DES VERHÄLTNISSES VON DATENSCHUTZ UND KÜNSTLICHER INTELLIGENZ

### 1. ZIELSETZUNG UND SCHUTZINSTRUMENTE DES DATENSCHUTZRECHTS

Das Datenschutzrecht soll vor allem die Persönlichkeit des Einzelnen vor Risiken aus der Verarbeitung seiner Daten schützen. Das Datenschutzrecht ist also seiner Intention nach nicht das Recht der künstlichen Intelligenz. Jedoch steht es in einem engen und vielfältigen Verhältnis zur Anwendung von künstlicher Intelligenz. Dies ist unmittelbar der Fall, soweit KI-Systeme personenbezogene Daten verarbeiten. Hier wirkt das Datenschutzrecht als Begrenzung der Nutzung von KI, steht also in einem Spannungsverhältnis zur künstlichen Intelligenz. KI-Systeme können auch zum Schutz von Persönlichkeitsrechten eingesetzt werden, entsprechend insoweit also den Schutzzielen des Datenschutzrechts, und kann ggf. sogar Datenschutz unterstützen.[19]

Da das Datenschutzrecht in erster Linie Schutzfunktion zugunsten des Einzelnen hat und nicht, wie etwa das Immaterialgüterrecht, Rechte an Daten begründet, ist zu vermuten, dass die Funktion des Datenschutzrechts als Begrenzung der Nutzung von Technologien überwiegt. Ob diese Begrenzung problematisch ist oder aber eine wesentliche Grundlage für die Akzeptanz und Zulässigkeit der Nutzung von KI darstellt, ist die entscheidende Frage im Verhältnis von KI und Datenschutzrecht.

Das Datenschutzrecht enthält ein breites Schutzinstrumentarium. Der zentrale materiellrechtliche Grundsatz des Datenschutzrechts, dass die Verarbeitung personenbezogener Daten der Rechtfertigung bedarf, wird durch zahlreiche Pflichten der Verarbeiter personenbezogener Daten ergänzt, die sich vor allem auf die Transparenz sowie auf die Sicherheit der Datenverarbeitung beziehen.

Das Datenschutzrecht gewährt dem Betroffenen umfassende Rechte. Kernelement ist hier die Befugnis, durch Gewährung, Einschränkung oder Widerruf seiner Einwilligung den Umfang der Datenverarbeitung zu beeinflussen. Dieses Recht wird durch eine breite Palette an Rechten zur Durchsetzung begleitet. Schließlich wird die Datenverarbeitung einer intensiven staatlichen Kontrolle unterworfen. Diese Schutzinstrumente des Datenschutzrechts sind auch bei Verarbeitung von Daten durch KI-Systeme umfassend anwendbar.

### 2. SPEZIFISCHE DATENSCHUTZRECHTLICHE SCHUTZINSTRUMENTE FÜR KI-SYSTEME?

Das Datenschutzrecht enthält bisher keine spezifischen Instrumente in Bezug auf KI-Systeme, sodass sich die Frage stellt, ob das Datenschutzrecht in Bezug auf die spezifischen Risiken durch KI-Systeme adäquaten Schutz bietet, ob es modifiziert werden sollte oder ob der Persönlichkeitsschutz im Hinblick auf die Risiken durch KI-Systeme durch andere Gesetze zu ergänzen ist. Dabei dürfte unstreitig sein, dass der rechtliche Rahmen für künstliche Intelligenz über Datenschutz weit hinausgeht, auch in Bezug auf den Schutz von Persönlichkeitsrechten.

Ein spezifisches Regelungssystem zum Schutz der Persönlichkeitsrechte gegen Gefahren aus KI-Sys-

19 Dazu etwa Meents in Kaulartz/Braegelmann.

temen wird sich vor allem durch das vorgeschlagene KI-Gesetz ergeben. So enthält der Entwurf des KI-Gesetzes der EU-Kommission eine ganze Reihe von Regeln, die ausdrücklich Risiken für Persönlichkeit durch KI-Systeme adressieren. Dies gilt nicht zuletzt für die in Art. 5 Abs. 1 des Entwurfs vorgesehenen Verbote der Nutzung von KI-Systemen, die die in lit. a) und b) zur schädigenden Beeinflussung von Personen, in lit. c) social scoring untersagt. Auch im Fall des in Art. 5 Abs. 1 lit. d) des Entwurfs geregelten Einschränkung der Nutzung biometrischer Echtzeit-Fernidentifizierungssysteme zu Strafverfolgungszwecken hat einen starken Bezug zu Persönlichkeitsrechten. Auch im Bereich der Hochrisiko-KI-Systeme, dem zentralen Regelungsgegenstand des KI-Gesetz-Entwurfs, sind Risiken für Persönlichkeitsrechte adressiert. So soll der Anhang III des Gesetzes vor allem Anwendungen erfassen, in denen Persönlichkeitsrechte betroffen sind, angefangen bei Systemen zur biometrischen Fernidentifizierung (Anhang III Ziff. 1. b), über KI-Systeme zur Entscheidung über den Zugang natürlicher Personen zu Einrichtung der Bildung (Anhang III Ziff. 3 a) oder Bewertung von Schülern in solchen Einrichtungen (Anhang III Ziff. 3 b) und KI-Systeme, die für die Einstellung oder Auswahl von Bewerbern für Beschäftigungsverhältnisse (Anhang III Ziff. 4 a) oder Entscheidungen im Rahmen von Beschäftigungsverhältnissen (Anhang III Ziff. 4 b) sowie von KI-Systemen zur Kreditwürdigkeitsprüfung (Anhang III Ziff. 4 b) bis hin zu KI-Systemen im Rahmen der Strafverfolgung (Anhang III Ziff. 6 lit. a) bis g) oder staatlichen Eingriffen im Rahmen der Migration und Grenzkontrollen (Anhang III Ziff. 7 lit. a) bis d), bei denen jeweils automatisierte Bewertungen von Personen im Vordergrund der Regelung stehen.

In Bezug auf die zuvor genannten Risiken von KI-Systemen für Persönlichkeitsrechte lässt sich bereits eine Abstufung hinsichtlich der Bedeutung des Datenschutzrechts erkennen: So betrifft die Fallgruppe der Informationsgewinnung und -aggregation durch KI-Systeme den Kern des Datenschutzrechts, soweit, wie häufig, personenbezogene Daten verarbeitet werden. Insoweit ist also von entscheidender Bedeutung, ob das Datenschutzrecht adäquate Lösungen bietet.

In Bezug auf den Inhalt einer maschinellen Entscheidung oder Bewertung ist bereits fraglich, inwieweit das Datenschutzrecht reicht. Auch wenn die DSGVO mit ihrem Artikel 22 und den korrespondierenden Informationspflichten in den Artikeln 13, 14 algorithmische Entscheidungen adressiert (dazu unten E.III), sind die Grenzen des Datenschutzrechts offensichtlich und ist ein komplementäres Verhältnis zum KI-Gesetz sowie zu anderen, gegebenenfalls noch zu schaffenden Regeln zu erwarten.

Im Folgenden soll der Aspekt der Informationsgewinnung erörtert werden; die übrigen Aspekte werden in späteren Abschnitten der Untersuchung erörtert.

## III. INFORMATIONSGEWINNUNG DURCH KI-SYSTEME

### 1. EINFÜHRUNG. BILDAUSWERTUNG ALS BEISPIEL FÜR INFORMATIONSGEWINNUNG DURCH KI-SYSTEME

Der Themenbereich der Gewinnung und Aggregation von Information durch KI-Systeme ist von unendlicher Vielfalt und kann nur exemplarisch untersucht werden. Ziel dieser Untersuchung ist es, KI-spezifische Besonderheiten herauszuarbeiten und zu prüfen, ob das geltende Datenschutzrecht auf diese adäquat reagiert. Diese Aufgabe soll am Beispiel der Gesichtserkennung erfolgen, die häufig durch KI-Systeme durchgeführt wird.

Das wohl prominenteste Beispiel ist die Facebook-Gesichtserkennung, die 2012 erstmals eingeführt, zwischenzeitlich in Europa und Kanada deaktiviert, 2018 erneut aktiviert und 2021 wiederum deaktiviert wurde.[20] Technisch basiert die Facebook-KI auf einer Auswertung von Fotos, auf denen Personen markiert wurden; beim Hochladen weiterer Fotos hat das System sodann automatisch geprüft, ob bereits „bekannte“ Personen auf den neu hochgeladenen Fotos zu erkennen sind.[21]

Es wird eine ganze Reihe an Diensten im Zusammenhang mit Gesichtserkennung per Internet angeboten. So bietet auch Google eine Bil-

20 Vgl. die Mitteilung von Facebook vom 2.11.2021, abrufbar unter https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/.
21 Vgl. die Angaben auf der Hilfeseite von Facebook zur Gesichtserkennung (zwischenzeitlich abgeschaltet); die letzte veröffentliche Version vom 28.10.2021 ist einsehbar über https://web.archive.org/web/20211028095307/https://de-de.facebook.com/help/122175507864081.

der-Rückwärtssuche an. Diese findet, wenn als Suchobjekt ein Bild hochgeladen oder die Bildquelle angegeben wird, ähnliche Bilder und listet zudem Internetseiten auf, auf denen die Bildquelle ebenfalls verwendet wird. Auf ähnlichen Mechanismen basieren auch auf Gesichtserkennung spezialisierte Suchmaschinen, die etwa von Unternehmen wie Clearview[22] oder PimEyes[23] angeboten werden. Während sich Clearview vor allem im Bereich der Strafverfolgung profiliert,[24] stellt PimEyes eine kostenpflichtige Suchmaschine zur Rückwärtssuche bereit. Die Suchmaschine PicTriev[25] hingegen sucht nach dem Upload eines Fotos nach ähnlich aussehenden (überwiegend prominenten) Personen aus einer Datenbank und schätzt zugleich das Geschlecht und das Alter der Person, die auf dem vom Nutzer hochgeladenen Foto abgebildet ist. Die Angebote sind letztlich recht unterschiedlich. Bei den für jedermann zugänglichen, kostenfreien Diensten wird also durchaus nicht stets eine Identifizierung der abgebildeten Person angeboten.

Aus rechtlicher Sicht kann man die wesentliche Aufgabe von KI-Systemen im Zusammenhang mit Gesichtserkennung wohl auf den Identitätsvergleich zurückführen. Mit diesem Wort soll der Begriff der Identitätsprüfung vermieden werden, der meist im Sinne von Identifizierung verstanden wird. Mit dem Begriff der Identifizierung wird typischerweise die Feststellung der bürgerlichen Identität einer natürlichen Person bezeichnet. Dies ist ein wichtiger Zweck der Gesichtserkennung und gilt für den Einsatz von Gesichtserkennung bei fast allen Anwendungen der Zugangskontrolle, sei es beim Zugang zu einem Staatsgebiet oder bei Zugang zu einem geschützten Gebäude oder Raum, ebenso bei dem umstrittenen Dienst von Facebook, soweit diese ihre Identität gegenüber Facebook preisgegeben haben.

Identitätsvergleich meint hier dagegen den der Identifizierung zugrunde liegenden Schritt, nämlich schlicht die Überprüfung der Übereinstimmung – im Sinne der ursprünglichen Bedeutung des Begriffs „Identität“[26] – zweier Bildnisse einer Person. Im Rahmen von Gesichtserkennung wird vom System ein Bildnis einer Person mit einem Vergleichsgegenstand auf hinreichende Übereinstimmung untersucht. Vergleichsgegenstand und hinreichende Übereinstimmung können dabei letztlich, je nach dem Zweck der Gesichtserkennung, frei bestimmt werden.

In wichtigen Anwendungsbereichen, etwa bei Zugangskontrolle, wird das zu vergleichende Bildnis mit bereits bekannten Bildnissen von Personen verglichen, um festzustellen, ob die Bilder in der Weise als übereinstimmend bezeichnet werden können, dass mit hinreichender Sicherheit festgestellt werden kann, dass die Bildnisse dieselbe natürliche Person abbilden. Dabei geht es nicht um Ähnlichkeit der Bildnisse, sondern um hinreichend starke Ähnlichkeit der aus den Bildern ableitbaren Merkmale der augenscheinlich auf beiden Bildern gezeigten Person.

Ein Vergleich kann sich aber auch auf einzelne Merkmale einer Person beziehen. So kann ein Vergleich etwa – wie im Fall des kostenlosen Tools von PicTriev[27] – darauf gerichtet sein, das augenscheinliche Geschlecht oder das ungefähre Alter einer Person festzustellen, was für Werbezwecke ausreichend sein kann. Damit wird deutlich, dass Gesichtserkennung nicht notwendigerweise zur Identifizierung im Sinne der Feststellung der bürgerlichen Identität einer Person genutzt werden muss.

KI-Systeme zur Gesichtserkennung werfen zahlreiche Rechtsfragen auf. Zu Recht adressiert auch der Entwurf des KI-Gesetzes Gesichtserkennung in mehrfacher Weise. So spielt Gesichtserkennung eine Rolle im Rahmen der von Artikel 5 ausgesprochenen Verbote bestimmter KI-Anwendungen. Vor allem aber sind Gesichtserkennungssysteme häufig Bestandteil von Anwendungen, die als Hochrisiko-KI-Systeme einzuordnen sind und damit besonderen Pflichten in Bezug auf das Risikomanagement und zudem einer öffentlichen Aufsicht unterliegen sollen.

Aus datenschutzrechtlicher Sicht wirft Gesichtserkennung in vermutlich allen Aspekten des Datenschutzes schwierige Fragen auf, die für KI-Systeme typisch sind.

22 Die Unternehmenswebsite ist abrufbar unter https://www.clearview.ai/.
23 Die Unternehmenswebsite ist abrufbar unter https://pimeyes.com/.
24 Vgl. etwa die kritische Berichterstattung über das weltweite Angebot an Polizeibehörden unter https://netzpolitik.org/2021/ueberwachungstechnik-clearview-bietet-umstrittene-gesichtserkennung-polizeien-weltweit-an/.
25 Abrufbar unter http://www.pictriev.com/.
26 Dazu Meyer, S. 24 f.
27 Vgl. oben Fn. 25.

## 2. PROBLEME DES ANWENDUNGSBEREICHS DES DATENSCHUTZRECHTS AM BEISPIEL VON BILDNISSE

### a. Bildaufnahmen in der personalisierten Werbung

Strittige Fragen ergeben sich etwa beim Anwendungsbereich des Datenschutzrechts. So ist zu fragen, ob es sich bei den Bildnissen, die durch eine Kamera erzeugt und dem Gesichtserkennungssystem zum Identitätsvergleich zugeleitet werden, um personenbezogene Daten handelt. Dieser Aspekt wird etwa im Rahmen von personalisierter Werbung (dazu unten F.I.1) relevant, soweit Systeme die Personalisierung anhand von Bildnissen vornehmen.

Ein Beispiel für personalisierte Werbung anhand von Personenaufnahmen lieferte die Supermarktkette real, die von Herbst 2016 bis Juni 2017 in 41[28] Filialen individuelle Werbung im Kassenbereich einsetzte. Dabei wurden den im Kassenbereich wartenden Kunden auf Bildschirmen Werbung angezeigt. Die Auswahl der den Kunden angezeigten Werbung wurde von einer Auswertung von Daten des Kunden abhängig gemacht. Konkret wurde durch eine Kamera der im Blickkontakt mit dem Bildschirm stehende Kunde erfasst, das Bild wurde mittels Software ausgewertet. Nach bestimmten Kriterien, unter anderem dem geschätzten Alter und Geschlecht des Kunden, wurde die ihm anzuzeigende Werbung ausgewählt.[29] Derartige Techniken sind in anderen Ländern stärker verbreitet. So sind etwa in Japan seit 2012 verbreitet Verkaufsautomaten im Einsatz, die aufgrund einer Kameraaufnahme personalisierte Angebote für Kunden aussuchen und auf einem Monitor anzeigen (dazu unten F.I.1).

Die bürgerliche Identität des Werbeadressaten war weder im Fall der japanischen Verkaufsautomaten noch im Beispiel der real-Supermärkte irgendeinem Beteiligten bekannt. Im Fall der real-Werbung wurden die Bilder nach Unternehmensangaben nur für 150 Millisekunden auf dem Server gespeichert und vollständig automatisiert ausgewertet, zudem seien lediglich Metadaten zu den Bildern übertragen worden.[30]

### b. Bildaufnahmen als personenbezogene Daten per se?

Die in diesen Beispielen illustrierte Fragestellung lautet, ob Bildaufnahmen als personenbezogene Daten zu bezeichnen sind, wenn zu keinem Zeitpunkt eine Identifizierung der abgebildeten Person realistischerweise möglich ist. Diese Fragestellung stellt sich nicht nur bei KI-Systemen, sondern generell. Unterliegen etwa alle Fotos, die ein Tourist von einer Sehenswürdigkeit macht, dem Datenschutzrecht, weil notgedrungen – ihm unbekannte – Passanten oder andere Touristen auf dem Bild zu sehen sind? Die Frage ist aber für KI-Systeme in besonderer Weise relevant: Dies gilt nicht nur für das hier herangezogene Beispiel der Gesichtserkennung, sondern für zahlreiche KI-Systeme, die in Maschinen verwendet werden. So sind autonome Fahrzeuge, ebenso alle anderen hochautomatisierten Verkehrsmittel, regelmäßig mit Kameras ausgestattet, die zur Ausführung ihrer Funktionen, etwa Fahren im öffentlichen Verkehr, auch Bilder von natürlichen Personen erzeugen.[31]

Bei KI-Systemen stellt sich im Zusammenhang mit der Qualifikation von Kameraaufnahmen als personenbezogenen Daten noch eine weitere Frage, die am Beispiel der Dashcam-Entscheidung des Bundesgerichtshofs[32] deutlich wird. Hier ging es anlässlich eines Streits um das Verschulden eines Verkehrsunfalls um die Frage, ob es sich bei den von der Dashcam eines Unfallbeteiligten erzeugten Aufnahmen des anderen am Verkehrsunfall beteiligten Fahrzeugs um personenbezogene Daten handelte. Der BGH qualifizierte das Bildnis eines Autos unter Einschluss des Kfz-Kennzeichens als personenbezogenes Datum dessen Halters.[33] Diese Einstufung, die datenschutzrechtliche Laien zu Recht erstaunen dürfte, wird in der datenschutzrechtlichen Literatur nahezu einhellig gebilligt.[34] Der BGH begründete dies damit, dass in der konkreten Situation eines Verkehrsunfalls der Beteiligte je-

28 real, Ende des Echion-Tests zur Blickkontakterfassung, 27.6.2017, online verfügbar: Ende des Echion-Tests zur Blickkontakterfassung - Pressemitteilung |real-markt.de, zuletzt abgerufen am 28.11.2021.

29 Frankfurter Allgemeine Zeitung, Supermarktkette Real analysiert Kundengesichter, online verfügbar: Supermarktkette Real testet Gesichtserkennung (faz.net), zuletzt abgerufen am 10.11.2021; Legal Tribune Online (LTO), Vorsicht, Kamera!, online verfügbar: Gesichtserkennung im Supermarkt: Dürfen die das? (lto.de), zuletzt abgerufen am 10.11.2021; Weser Kurier, Supermarkt scannt Kunden, online verfügbar: Supermarkt scannt Kunden - WESER-KURIER, zuletzt abgerufen am 10.11.2021.

30 Frankfurter Allgemeine Zeitung, Supermarktkette Real analysiert Kundengesichter, online verfügbar: Supermarktkette Real testet Gesichtserkennung (faz.net), zuletzt abgerufen am 10.11.2021; Weser Kurier, Supermarkt scannt Kunden, online verfügbar: Supermarkt scannt Kunden - WESER-KURIER, zuletzt abgerufen am 10.11.2021.

31 Schröder, ZD 2021, 302 f.

32 BGH Urteil vom 15.05.2018 – VI ZR 233/17 – BGHZ 218, 348.

33 BGH Urteil vom 15.05.2018 – VI ZR 233/17 – BGHZ 218, 348, 357.

34 Gola-Gola, DS-GVO Art. 4 Rn. 5; BeckOK DatenschutzR/Schild, DSGVO Art. 4 Rn. 21; Strauß, NZV 2018, 554, 557; allgemein zustimmend zu Entscheidung bspw. Krämer, NZV 2018, 146; Schmidt, JA 2018, 869.

weils die Identität des Halters des anderen beteiligten Fahrzeugs durch eine Halterabfrage feststellen könne.[35] Diese zentrale Einschränkung wird vielfach übersehen.

Bejaht man den Personenbezug beim Auto, muss man konsequenterweise annehmen, dass auch jedes Bildnis eines Wohnhauses ein personenbezogenes Datum dessen Bewohners und vielleicht sogar zugleich dessen Eigentümers darstellt, soweit es sich dabei um eine natürliche Person handelt.[36] Tatsächlich wird, etwa im Zusammenhang mit Aufnahmen von Google für den in Google Maps integrierten Dienst Google Street View, verbreitet angenommen, dass Aufnahmen von Wohnungen personenbezogene Daten seien, wenn mit einer Adresse versehen bzw. georeferenziert[37] sind[38]

Je nachdem wie man diesen Aspekt verallgemeinert, wird jedes Bildnis einer Sache, die in irgendeiner rechtlichen Beziehung zu einer Person steht, zum personenbezogenen Datum. Ob eine solche Annahme, die offenbar verbreitet ist, wirklich zutrifft, ist eine grundlegende Frage des Datenschutzrechts, die hier nicht erörtert werden kann.

Die Frage nach der Personenbezogenheit von Bildern von Sachen ist kein Spezifikum von KI-Systemen. KI-Systeme legen aber den Finger in die Wunde des Datenschutzrechts, das um seine Grenzen, den Anwendungsbereich, nicht so recht weiß. Dies gilt insbesondere für die im Fall der Gesichtserkennung und der Nutzung der Daten für die Steuerung einer Maschine (z.B. eines hochautomatisierten Fahrzeugs) verwendeten Bildaufnahmen natürlicher Personen. Hier kommt es darauf an, ob Bildaufnahmen von natürlichen Personen per se, also auch dann, wenn eine Identifizierung im Sinne der Feststellung der bürgerlichen Identität der Person ausgeschlossen ist, als personenbezogene Daten zu bezeichnen sind.

Diese Frage ist meines Erachtens zu verneinen. Wenn etwa die Kamera eines Fahrzeugs mit Parkassistent beim Einparken eine Person aufnimmt, liegt kein personenbezogenes Datum vor, ebenso wenig, soweit ein hochautomatisiertes Fahrzeug Kameraaufnahmen allein zur Steuerung seines Fahrverhaltens verwendet. Verallgemeinert geht es um Fälle, in denen ein Bildnis einer Person nur zum Zweck der Steuerung einer Maschine, unabhängig von der Persönlichkeit der aufgenommenen Person, verwendet wird. Hier liegen offensichtlich keine Gefahren für die Persönlichkeit der aufgenommenen Person vor.

### c. Automatisierte Bildauswertung

Bei der personalisierten Werbung im Supermarkt liegt ein schwieriger Grenzfall vor. Hier wurde durch den Supermarktbetreiber zu keinem Zeitpunkt die Identität der Person festgestellt noch die Identifizierung für Dritte ermöglicht.

Dies spricht entscheidend gegen die Annahme eines Personenbezugs der Aufnahme. Gleichwohl mag man intuitiv geneigt sein, den Anwendungsbereich des Datenschutzrechts als eröffnet anzusehen und folglich das Vorliegen personenbezogener Daten zu bejahen. Dies dürfte auf dem Umstand beruhen, dass ein Schutzbedarf offensichtlich ist, denn anhand der aus dem Bild ausgelesenen Merkmale der Person (z.B. Geschlecht, ungefähres Alter) wurde eine Einschätzung der Person vorgenommen, und aus dieser wurden Folgen, nämlich die Auswahl der angezeigten Werbung, abgeleitet. Diese Einschätzung wurde auch Dritten mitgeteilt, für die die personalisierte Werbung und mittelbar auch die der Auswahl zugrunde liegende Einschätzung sichtbar waren.

Wenn einem Mädchen Werbung für klassische „Jungenartikel“ angezeigt wird, mag dies der betroffenen Person angenehm, vielleicht aber auch unangenehm sein. Dieser Effekt wird den Schutzinstinkt des Datenschützers wachrufen. Aus systematischer Sicht ist gleichwohl zu fragen, ob dieser Aspekt durch das Datenschutzrecht zu lösen ist. Persönlichkeitsschutz wird bekanntlich durch vielfältige Instrumente des Rechts bewirkt, das Datenschutzrecht ist hier nicht alleinzuständig.

Eine abschließende Stellungnahme fällt schwer, hierzu bedarf es tiefergehender Untersuchungen. Es ist aber offensichtlich, dass sich das Datenschutzrecht sehr weit von seinem Ursprung entfernt, denn das Unbehagen beruht hier nicht auf der Erhebung und Verwendung der Bildaufnahme, wie das Beispiel des Parkassistenten belegt, sondern auf der ausgesendeten Information.

35 BGH, Urteil vom 15.05.2018 – VI ZR 233/17 – BGHZ 218, 348, 357.
36 Vgl,. in Bezug auf grundstücksgezogene Daten, Arzt, DuD 2000, 204, 206;
37 Gemeint ist die Verknüpfung des Bildes mit einem geografisch definierten Ort der Erdoberfläche.
38 Kühling/Buchner-Klar/Kühling, Art. 4 Nr. 1 Rn. 38.

Die automatisierte Bildauswertung und deren Berücksichtigung ist für viele KI-Anwendungen wichtig. So wird man etwa von einem hochautomatisierten Fahrzeug verlangen, dass es aufgrund der Merkmale der Person, die sich aus der Auswertung der Kameras ergeben, unterschiedlich reagiert. Damit ist nicht die Diskussion gemeint, ob ein hochautomatisiertes Fahrzeug entscheiden soll, ob es bei einem unvermeidbaren Unfall eher ein junges Mädchen oder eine alte Frau überfährt, [39] sondern die notwendige Frage, ob ein Auto den Umstand berücksichtigen soll, dass es kleine Kinder auf der Straße erkennt. Ebenso wie in dieser Situation von menschlichen Fahrern ein spezifisches Verhalten – erhöhte Vorsicht, ggf. Geschwindigkeitsverminderung – erwartet wird, muss auch beim automatisierten Fahren eine entsprechende Reaktion und folglich auch eine darauf bezogene Bildauswertung erfolgen. Ruft dies das Datenschutzrecht auf den Plan? Dies ist zu verneinen. Es geht um Sicherheit, nicht um Persönlichkeit von Personen.

Die Facebook-Gesichtserkennung wirft eine andere Frage auf, nämlich die, ob Fotos von Personen schon deshalb als personenbezogenes Datum anzusehen sind, weil die abgebildete Person durch Nutzung des Dienstes – unterstellt, der Dienst von Facebook oder ein vergleichbarer Dienst stünde noch zur Verfügung – identifiziert werden kann.

Im Unterschied zur vorgenannten Fallgruppe liegen hier gespeicherte Bildnisse vor, die vom Besitzer des Bildnisses jedenfalls faktisch frei verwendet werden können. In der aktuellen Diskussion wird das Vorliegen eines personenbezogenen Datums, soweit erkennbar, bejaht. Die zugrunde liegende Annahme ist zutreffend: Das Foto einer natürlichen Person ist nach allgemeinen Grundsätzen ein personenbezogenes Datum, soweit seinem Besitzer eine realistische Möglichkeit zur Identifizierung zur Verfügung steht, deren Nutzung keinen unverhältnismäßigen Aufwand verursacht.

Ob jedermann eine technische Möglichkeit zur Verfügung steht, beliebige Fotos von Menschen einer konkreten Person zuzuordnen, ist eine andere Frage. Angesichts der überaus großen Fortschritte im Bereich der Gesichtserkennung und automatisierten Gesichtserkennung und der Verfügbarkeit von Diensten wie Google Reverse Image Search besteht eine solche Möglichkeit jedenfalls in vielen Fällen.

### d. Ergebnis

Entsprechend ist zu differenzieren: Bildaufnahmen von Personen sind nicht per se personenbezogene Daten (insbesondere wenn das Gesicht der Person nicht erkennbar ist), weil nicht jede Bildaufnahme eine Identifizierung der Person ermöglicht. Eine Identifizierungsmöglichkeit besteht aber sehr häufig. Für die Praxis bedeutet dies, dass Bildaufnahmen von Personen im Zweifel als personenbezogene Daten anzusehen sind, soweit nicht nach Lage der Dinge, insbesondere durch entsprechende technische Vorkehrungen wie im Fall von real, eine Identifizierung ausgeschlossen wird.

## 3. RECHTFERTIGUNG DER DATENVERARBEITUNG DURCH KI-SYSTEME

Unabhängig von der Reichweite der DSGVO bei Bildverarbeitung durch KI-Systeme ist offensichtlich, dass KI-Systeme in hohem Maße personenbezogene Daten verarbeiten. Dies gilt vor allem, soweit KI-Systeme gezielt zur Verarbeitung personenbezogener Daten eingesetzt werden, wie etwa bei der Nutzung von KI-Systemen zur Identifizierung oder zur Bewertung von Personen. Soweit man von personenbezogenen Daten ausgeht, wenn KI-Systeme personenbezogene Daten für die Steuerung ihrer Funktionen nutzen, etwa im Fall des hochautomatisierten Fahrzeugs, stellt sich die Frage nach der Rechtfertigung ebenso.

Die Notwendigkeit der Rechtfertigung der Datenverarbeitung ist kein Spezifikum von KI-Systemen. Gleichwohl zeigt sich hier die besondere Bedeutung des Datenschutzrechts: Wäre die Verarbeitung personenbezogener Daten schrankenlos zulässig, könnten dystopische Vorstellungen von KI-Anwendungen leichter Realität werden.

Betrachtet man die in den Rechtfertigungsgründen zu berücksichtigenden Interessen näher, zeigen sich Fragen, die für KI-Anwendungen durchaus typisch sind. Nicht zuletzt kommt es auf die typisierten Interessen des Betroffenen an, die etwa im Rahmen der Abwägung nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO zu berücksichtigen sind. Davon sollen hier zwei zentrale Interessen herausgegriffen werden, die für die Gesichtserkennung und ebenso für viele KI-Anwendungen von Bedeutung sind: Das Interesse des Betroffenen, dass Abbildungen (Bild, Ton, Radar etc.) der eigenen Person nicht erzeugt und vor allem nicht gespeichert werden, zum einen

39 Grundlegend zu Dilemmasituationen beim autonomen Fahren Bonnefon/Shariff/Rahwan, 352 Science (2016), 1573 ff. sowie die Implementierung einer „moral machine“ durch das Massachusetts Institute of Technology (MIT) ist abrufbar https://www.moralmachine.net.

und das Interesse, dass aus den Abbildungen keine Schlüsse gezogen werden, zum anderen. Als ein Beispiel für eine Schlussfolgerung in diesem Sinne wird hier auch die Identifizierung der Person angesehen, ebenso aber die Bildung von Persönlichkeits- oder Interessenprofilen, anhand derer etwa individualisierte Werbung erstellt wird.

In beiden Fällen gleichermaßen ist von Bedeutung, welches Gewicht dem jeweiligen Interesse im Rahmen der Interessenabwägung beizumessen ist. Es versteht sich von selbst, dass die Frage letztlich stets im Kontext der konkreten Interessenabwägung, etwa nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO, zu beantworten ist. Es versteht sich auch, dass Bildaufnahmen anders als Radaraufnahmen zu bewerten sind und dass es bei einem Foto auf die Auflösung (Satellitenbild vs. Nahaufnahme) ankommen kann. Es gibt aber allgemeine Fragen, deren wichtigste sicherlich ist, welche Bedeutung dem Interesse, im öffentlichen Raum nicht abgebildet zu werden, beizumessen ist. Diese Frage wurde in anderen Bereichen des Persönlichkeitsschutzes, namentlich beim Recht am eigenen Bild, intensiv diskutiert. Dort ist anerkannt, dass die Frage differenziert zu beantworten ist und dass in vielen Fällen ein schutzwürdiges Interesse an der Nichtaufnahme, dass eine Unzulässigkeit der Aufnahme zur Folge hätte, nicht besteht.

Da auch das Recht am eigenen Bild dem Schutz der Persönlichkeit dient, spricht einiges dafür, diese Wertung in das Datenschutzrecht zu übernehmen und dem Interesse des Betroffenen an der Nichtaufnahme kein größeres Gewicht beizumessen als dort.

Diese Frage, die keinen spezifischen Bezug auf KI-Systeme aufweist, kann hier nicht im Einzelnen erörtert werden. Aus Sicht von KI-Systemen wird aber deutlich, dass die Erzeugung und ggf. auch die Verwertung von Bildnissen von Personen häufig zulässig sein werden, da dem etwaigen Interesse des Betroffenen, dass keine Bildaufnahme seiner Person erzeugt wird, nicht per se ein hohes Gewicht beizumessen ist.

Eine zweite Fallgruppe ist für KI-Systeme von besonderer Relevanz. Greift man einmal die Identifizierung heraus, die etwa im Fall der Facebook-Gesichtserkennung von Bedeutung ist, so zeigt sich ein völlig anderes Bild: Hier ist von Bedeutung, welches Gewicht dem Interesse des Betroffenen an der Anonymität, also der Nicht-Identifizierung, beizumessen ist. Dieses Interesse wird von der Rechtsordnung als besonders schutzwürdig eingestuft. So enthält etwa § 19 Abs. 2 TTDSG, wie zuvor § 13 Abs. 6 TMG a. F., die Pflicht, die Nutzung von Telemedien anonym zu ermöglichen, soweit dies dem Anbieter zumutbar ist.

Das Ergebnis der Interessenabwägung muss dem konkreten Einzelfall vorbehalten bleiben, eine allgemeingültige Abwägung anzustellen soll hier nicht versucht werden. Wie könnte auch das Interesse eines Jünglings, der gern wüsste, wer auf einer Veranstaltung wenige Plätze neben ihm und doch unerreichbar fern saß, von der akademischen Kanzel herab angemessen gewichtet werden? Auch das Interesse des Fußballfans oder der Polizei, zu wissen, wer an einem bestimmten Tag in der Fankurve des 1. FC Fußball stand, ist sicher im Einzelfall zu würdigen.

Schwierig wird es in Bezug auf die Rechtfertigung bei Dienstleistungen, etwa der Facebook-Gesichtserkennung, soweit der Dienstleister selbst als Verantwortlicher und nicht als Auftragsverarbeiter tätig wird. Offensichtlich wird man hier ähnlich wie beim Scoring und anderen Dienstleistungen zur Rechtfertigung auf die Interessenlagen desjenigen abzustellen haben, dem die Dienstleistung zugutekommt.

Als Zwischenergebnis aus der hier notwendigerweise unvollkommenen Betrachtung sei hier gezogen, dass die Identifizierung von Personen aus vorhandenen Daten, die für die Gesichtserkennung, aber auch für andere Anwendungen von KI-Systemen von Bedeutung oder gar prägend ist, häufig nicht gerechtfertigt sein wird, da dem Interesse an der Anonymität häufig ein großes Gewicht beizumessen ist. Weitere Verallgemeinerung verbietet sich angesichts des Umstandes, dass die Identifizierung in vielen Fällen auch zulässig ist, etwa bei der Zugangskontrolle.

## 4. FAZIT

Als ein übergreifendes Ergebnis lässt sich aus den hier angesprochenen Fragen wohl herleiten, dass KI-Systeme das Datenschutzrecht vor Herausforderungen stellen, die jedenfalls derzeit noch nicht als gelöst anzusehen sind.

In Bezug auf die Anwendbarkeit des Datenschutzrechts bei Datenverarbeitungsvorgängen, die für KI-Systeme typisch sind, etwa Bildaufnahmen

durch Kameras von KI-Systemen, besteht zum einen erhebliche Rechtsunsicherheit, die aus Sicht von Herstellern und Nutzern von KI-Systemen problematisch ist. Insoweit bedarf das Datenschutzrecht der Fortentwicklung. Zum anderen zeichnet sich am Beispiel der von KI-Systemen vorgenommenen und an Dritte übermittelte Einschätzungen ab, dass typische Gefahren für die Persönlichkeit durch KI-Systeme über traditionelle Fragen des Datenschutzes hinausgehen (dazu unten F.II.5).

In Bezug auf die Rechtfertigung der Datenverarbeitung von KI-Systemen ist von Bedeutung, dass das Interesse Betroffener, von Sensoren von KI-Systemen, einschließlich einer Kamera, nicht erfasst zu werden, in vielen Fällen gegenüber dem Interesse an der Nutzung der Daten zur Steuerung der KI-Systeme zurückstehen muss. Dem Interesse des Betroffenen, nicht durch KI-Systeme identifiziert zu werden, ist hingegen hohes Gewicht beizumessen. Auch wenn die Identifizierung natürlicher Personen mittels KI-Systeme(n) in vielen Fällen, etwa bei der Zugangskontrolle, gerechtfertigt sein kann, ist eine solche außerhalb derartiger Rechtfertigung regelmäßig unzulässig.

**Kapitel C**

# BESCHRÄNKUNG VON FORSCHUNG UND ANWENDUNG KÜNSTLICHER INTELLIGENZ DURCH DATENSCHUTZ

## I. DATENSCHUTZ ALS HINDERNIS FÜR KÜNSTLICHE INTELLIGENZ?

Künstliche Intelligenz und Datenschutz stehen, wie eingangs gesagt, in einem notwendigen Spannungsverhältnis. Schon bei der Forschung und Entwicklung von KI-Anwendungen werden, insbesondere beim maschinellen Lernen, personenbezogene Daten benötigt. Auch in der Anwendung von KI-Systemen werden in vielen Fällen personenbezogene Daten verarbeitet. In beiden Fällen sind die Regeln des Datenschutzrechts zu beachten.

Dem Datenschutzrecht wird häufig innovationshemmende Wirkung bescheinigt.[40] Insbesondere wird oft die Befürchtung geäußert, die DSGVO könne die Entwicklung selbstlernender Systeme behindern.[41] In der rechtspolitischen Diskussion werden dazu mitunter starke Worte verwendet. So betitelte der Bundestagsabgeordnete Andreas Steier einen Blogbeitrag anlässlich des Inkrafttretens der DSGVO mit der Aussage „KI und Machine Learning: Warum wir mit dem Datenschutz von heute die Zukunft verspielen“[42]. Insbesondere im Bereich der KI-Forschung in der Medizin wird das Datenschutzrecht als bedeutende Hürde angesehen.[43]

Allerdings besteht in Bezug auf die Bedeutung der innovationshemmenden Wirkung des Datenschutzrechts erhebliche Unsicherheit. Von Interesse ist insoweit eine aktuelle Umfrage des Bitkom in Bezug auf die künftige ePrivacy-Verordnung, in der zwar 38% der befragten Unternehmen Wettbewerbsnachteile europäischer KI-Anbieter sahen, allerdings nur 21% eine innovationshemmende Wirkung vermuteten.[44]

Mitunter wird eine innovationshemmende Wirkung des Datenschutzrechts ausdrücklich bestritten und diesem gar eine innovationsfördernde Wirkung zugeschrieben. So äußerte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, kürzlich in einer öffentlichen Sitzung der Enquete-Kommission des Deutschen Bundestags, Datenschutz sei keineswegs ein Hemmnis für Innovation im Bereich der KI, sondern könne ein „Innovationsmotor“ und „ein Alleinstellungsmerkmal für die Etablierung einer KI made in Europe“ sein.[45]

Eine differenzierte Betrachtung tut not. Es bedarf keiner Frage, dass Datenschutz einen hemmenden Effekt auf die Entwicklung und Nutzung neuer Technologien ausübt, soweit diese mit der Verarbeitung personenbezogener Daten einhergehen.

Soweit – und dies ist nicht selten – Datenschutz die Nutzung von Technologien untersagt, etwa im oben diskutierten Fall der Facebook-Gesichtserkennung, wirkt sich dies unmittelbar und erheblich auf die Nutzung und damit mittelbar auf die Herstellung derartiger Systeme sowie die Entwicklung der zugrunde liegenden Technologien aus.

Auch soweit das Datenschutzrecht die Entwicklung, Herstellung und Nutzung von KI-Systemen nicht untersagt, führt die Beachtung des Datenschutzrechts zu einem hohen Aufwand für den Verantwortlichen und andere Beteiligte (z.B. Auftragsverarbeiter), der sich auf die Forschung nachteilig auswirkt.[46]

40 Vgl. Marsch, DGRI-Jahrbuch 2018, S. 175, 188.

41 Siehe z.B. Stolton, MEP: Datenschutz kann die Entwicklung künstlicher Intelligenz einschränken, 27.8.2019, abrufbar unter https://www.euractiv.de/section/digitale-agenda/interview/mep-datenschutz-kann-die-entwicklung-kuenstlicher-intelligenz-einschraenken/, zuletzt abgerufen am 29.11.2021.

42 Steier, KI und Machine Learning: Warum wir mit dem Datenschutz von heute die Zukunft verspielen, 24.5.2018, Blogbeitrag, abrufbar unter https://digitaleweltmagazin.de/en/2018/05/24/ki-und-machine-learning-warum-wir-mit-dem-datenschutz-von-heute-die-zukunft-verspielen/, zuletzt abgerufen am 29.11.2021.

43 Brautzsch, Wie KI-Forschung in der Medizin trotz Datenschutz gelingen kann, 18.6.2021, Blogbeitrag, abrufbar unter https://www.mdr.de/wissen/kuenstliche-intelligenz-medizin-datenschutz-100.html, zuletzt abgerufen am 29.11.2021.

44 Bitkom, DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, 2019, abrufbar unter https://www.bitkom.org/sites/default/files/2019-09/bitkom-charts-pk-privacy-17-09-2019.pdf, zuletzt abgerufen am 29.11.2021; dazu: Fischer, ZD-Aktuell 2020, 07361.

45 Zit. nach Deutscher Bundestag, Im Spannungsfeld zwischen Datenschutz und Künstlicher Intelligenz, 2020, https://www.bundestag.de/dokumente/textarchiv/2020/kw03-pa-enquete-kuenstliche-intelligenz-673918, zuletzt abgerufen am 5.2.2021.

46 Schürmann, KI im Rahmen der Digitalisierungsstrategie – die DSGVO als Innovationsbremse?, t3n, 17.3.2019, abrufbar unter https://t3n.de/news/ki-rahmen-dsgvo-1148992/, zuletzt abgerufen am 29.11.2021.

Das Datenschutzrecht steht daher stets unter einem hohen Rechtfertigungsdruck. Es ist zu fragen, ob der vom Datenschutzrecht bezweckte – in seinem Grundanliegen unstreitige – Schutz den dafür erforderlichen Aufwand rechtfertigt. Auch wenn die Notwendigkeit von Datenschutz unbestritten und Datenschutz in jüngerer Zeit weltweit als wertvolles Gut anerkannt ist, so bestehen in vielen Aspekten berechtigte Zweifel an der Ausgewogenheit der bisher erzielten Abwägung von Datenschutz und Innovationsförderung.

Zu Recht wird nach Lösungen gesucht. Teilweise wird ausdrücklich auch eine Fortentwicklung des Datenschutzrechts gefordert. So fordert etwa der Sachverständigenrat Gesundheitswesen in seinem kürzlich vorgelegten Gutachten „Digitalisierung für Gesundheit", Datenschutz müsse „im Sinne eines umfassenden Patientenschutzes neu gedacht werden".[47] Speziell in Bezug auf die medizinische Forschung fordert das Gutachten unter anderem eine gesetzliche Neuregelung der Einwilligungsverfahren und Weiterentwicklung von Forschungsklauseln.[48]

Als eine Lösung zur Linderung der durch datenschutzrechtliche Anforderungen bedingten Forschungshemmnisse wird derzeit die Einschaltung von sog. Datentreuhändern diskutiert,[49] die nicht zuletzt für maschinelles Lernen von Interesse sein kann. Auch hier sind die Meinungen indes gespalten: Während die Datenethikkommission hier großes Potential sieht,[50] weisen andere Studien darauf hin, dass sich aus Datentreuhändermodelle auch neue Probleme ergeben können.[51]

Die vorliegende Untersuchung kann die weitverzweigte Fragestellung nicht ausloten. Nachfolgend werden zunächst drei Aspekte der Diskussion skizziert: die Einschränkung von Forschung durch Datenschutz (sogleich 2.), die Einschränkung der Nutzung von KI-Systemen durch Datenschutz (unten 3.) und die Unterstützung der Entwicklung und Nutzung von KI-Systemen durch Datenschutz (unten 4.).

## II. EINSCHRÄNKUNGEN DER FORSCHUNG UND ENTWICKLUNGEN VON KI-SYSTEMEN DURCH DATENSCHUTZ

Die Einschätzung, dass Datenschutz unmittelbar zu Einschränkungen der Forschung und Entwicklung von KI-Systemen führt, wird in Medienberichten wird auf unterschiedliche Anforderungen des Datenschutzrechts zurückgeführt. So soll das Transparenzprinzip, Art. 5 Abs. 1 lit. a) DSGVO, für die Entwicklung problematisch sein, da etwa beim maschinellen Lernen die Vorgänge im Einzelnen selbst dem Programmierer nicht bekannt seien.[52] Der Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c) DSGVO, könne die Entwicklung hemmen, da KI große Datenmengen benötigen.[53] Auch der Grundsatz der Zweckbindung führe beim maschinellen Lernen zu Schwierigkeiten.[54]

Probleme des Datenschutzes können sich nicht zuletzt in Bezug auf die Qualität des maschinellen Lernens ergeben. So wird in einem Blogbeitrag ein Wissenschaftler wie folgt zitiert: „Stellen Sie sich vor, es ist ein Datensatz falsch annotiert: Es wird festgestellt, dass angeblich ein Lungenödem auf dem Bild ist, dabei ist tatsächlich das Herz vergrößert. Dann lernt der entsprechende Algorithmus natürlich etwas Falsches. Und gerade wenn ich nicht den Zugriff auf die Originaldaten habe, dann fällt es schwer, die Datenqualität zu wahren."[55]

47 SVR Gesundheitswesen, Gutachten 2021, Executive Summary Ziff. 6, S. XXVI und Kap. 5.5.1, Ziff. 509 f., S. 232.
48 SVR Gesundheitswesen, Gutachten 2021, Executive Summary Ziff. 23, S. XXVIII und Kap. 5.1.1., Ziff. 509, S. 232.
49 Siehe aus datenschutzrechtlicher Sicht etwa Kühling/Sackmann/Schneider.
50 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Kap. E 4, Zusammenfassung der wichtigsten Handlungsempfehlungen, Ziff. 21, S. 140.
51 So etwa SVR Gesundheitswesen, Gutachten 2021, Kapp. 5.5.1, Ziff. 510, S. 233.
52 Heß, Künstliche Intelligenz und DSGVO, 14.6.2018 / 12.5.2021, Blogbeitrag, abrufbar unter https://www.fonial.de/blog/artikel/lesen/kuenstliche-intelligenz-und-dsgvo-394/, zuletzt abgerufen am 29.11.2021.
53 Dirksen, Künstliche Intelligenz und Datenschutz, 23.6.2020, Blogbeitrag abrufbar unter https://www.liebenstein-law.de/kuenstliche-intelligenz-und-datenschutz/, zuletzt abgerufen am 29.11.2021; ähnlich Steier, KI und Machine Learning, Warum wir mit dem Datenschutz von heute die Zukunft verspielen, 24.5.2018, Blogbeitrag, abrufbar unter https://digitaleweltmagazin.de/en/2018/05/24/ki-und-machine-learning-warum-wir-mit-dem-datenschutz-von-heute-die-zukunft-verspielen/, zuletzt abgerufen am 29.11.2021.
54 Schürmann, KI im Rahmen der Digitalisierungsstrategie – die DSGVO als Innovationsbremse?, t3n, 17.3.2019, abrufbar unter https://t3n.de/news/ki-rahmen-dsgvo-1148992/, zuletzt abgerufen am 29.11.2021.
55 Prof. Dr. Andreas Maier, Friedrich-Alexander-Universität Erlangen-Nürnberg, zit. Brautzsch, Wie KI-Forschung in der Medizin trotz Datenschutz gelingen kann, 18.6.2021, Blogbeitrag, abrufbar unter https://www.mdr.de/wissen/kuenstliche-intelligenz-medizin-datenschutz-100.html, zuletzt abgerufen am 29.11.2021.

## III. VERBOTE UND EINSCHRÄNKUNGEN DER NUTZUNG VON KI DURCH DATENSCHUTZ

Das Datenschutzrecht schränkt die Nutzung von KI-Anwendungen direkt und indirekt ein. Eine direkte Einschränkung ergibt sich aus dem Verbot der automatisierten Entscheidungen des Art. 22 DSGVO.[56] Das Verbot schränkt die Nutzung solcher Systeme in vielfältiger Weise ein. Zwar sind die Einschränkungen nach hiesigem Verständnis letztlich nicht sonderlich groß, jedoch begründet die Norm schon aufgrund der vielen Unklarheiten, die zu entsprechenden Meinungsstreiten geführt haben, Risiken, die aus Sicht der Nutzer in ihrem eigenen Risikomanagement zu berücksichtigen sind und entsprechende negative Effekte auslösen. Auch die angesichts der komplexen Rechtslage notwendige Rechtsberatung verursacht Kosten.

Indirekte Einschränkungen für die Nutzung von KI-Anwendungen ergeben sich aus den allgemeinen, nicht KI-spezifischen Anforderungen des Datenschutzrechts. Die aktuelle Diskussion um Videokonferenzsysteme wie MS Teams und Zoom verdeckt das eigentliche Drama des Datenschutzrechts bei innovativen Technologien. Bei der Nutzung von Technologien mit breitem Anwendungsbereich und großen Märkten werden die Kosten für Datenschutzprüfungen die Nutzung nicht verhindern. Das Datenschutzrecht gilt aber in gleicher Weise für Nischenanwendungen. Die Vornahme komplexer datenschutzrechtlicher Prüfungen ist nicht nur für kleine Unternehmen oder Verbraucher oft unmöglich und führt bekanntlich zu einem breiten Feld notgedrungener Nichtbeachtung des Datenschutzrechts. Diese Rechtsunsicherheit aber schlägt auf die Forschung und Entwicklung und vor allem die Markteinführung von Produkten zurück. Die in der Tagespresse genannte Einschätzung, dass Datenschutzrecht ein Hemmnis darstellt, ist daher plausibel.

## IV. DATENSCHUTZ ALS UNTERSTÜTZUNG FÜR KI

Datenschutz wird teilweise als Unterstützung für die Entwicklung von KI gesehen. In der eingangs zitierten Stellungnahme bezeichnet der BfDI, Ulrich Kelber, Datenschutz gar als „Innovationsmotor" für KI und mögliches „Alleinstellungsmerkmal" einer „KI made in Europe". Diese These wird jedoch nicht begründet.

Was das „Alleinstellungsmerkmal" angeht, ist möglicherweise gemeint, dass der in Europa geltende Datenschutz ein Vertriebsargument darstellen könne. Der Slogan „Datenschutz Europe" als Vertriebsargument wurde vor einigen Jahren im Bereich des Cloud Computing genutzt. Das Vorhandensein eines Serverstandorts in Deutschland wurde etwa von der Deutschen Telekom und Microsoft bei Eröffnung einer „Geman Cloud" im Jahr 2015 als entscheidender Vorteil bezeichnet. Inzwischen hat Microsoft dieses Geschäft aber aufgegeben. Auch Gaia-X als „Cloud made in Europe" hat durchaus mit Gegenwind zu kämpfen.

Die These, dass europäischer Datenschutz per se ein Marketingvorteil sei, dessen Wert die Kosten durch Erfüllung der Datenschutzanforderungen übersteigt, erscheint daher nicht per se plausibel.

Mit dem Stichwort „Innovationsmotor" soll möglicherweise die recht häufig genannte Erwartung bezeichnet werden, dass durch die strengen Anforderungen der DSGVO ein Innovationsdruck entstehe, der Unternehmen dazu zwinge, bessere bzw. innovativere Lösungen zu entwickeln.[57] Ob damit eine verbreitete Nutzung oder gar wirtschaftlicher Erfolg einhergehen, ist freilich eine andere Frage. Der Verfasser erinnert sich an den mit dem neuen Personalausweis ermöglichten elektronischen Identitätsnachweis, der durch hochkomplexe technische Konzepte und umfangreiche rechtliche und organisatorische Maßnahmen mit einem Höchstmaß an Datenschutz ausgestattet wurde, aber jedenfalls bisher keine nennenswerte Verbreitung fand.

56 S. dazu Stolton, MEP: Datenschutz kann die Entwicklung künstlicher Intelligenz einschränken, 27.8.2019, https://www.euractiv.de/section/digitale-agenda/interview/mep-datenschutz-kann-die-entwicklung-kuenstlicher-intelligenz-einschraenken/, zuletzt abgerufen am 29.11.2021.

57 Schürmann, KI im Rahmen der Digitalisierungsstrategie – die DSGVO als Innovationsbremse?, t3n, 17.3.2019, abrufbar unter https://t3n.de/news/ki-rahmen-dsgvo-1148992/, zuletzt abgerufen am 29.11.2021.

Man wird zu differenzieren haben: Die verbreitete Annahme, dass Datenschutz wesentlich zur Akzeptanz von KI-Anwendungen beiträgt,[58] erscheint plausibel. Könnte der Einzelne nicht darauf vertrauen, dass die Nutzung seiner Daten in KI- Anwendungen rechtlichen Grenzen unterläge, wäre das Misstrauen gegen die Nutzung von künstlicher Intelligenz – zu Recht – weitaus größer. Daher kann Datenschutz zu Recht als eine notwendige Grundlage für eine erfolgreiche Nutzung von künstlicher Intelligenz angesehen werden.

Jedoch ist das Datenschutzrecht nicht die alleinige Grundlage des Vertrauens in künstliche Intelligenz. Die entscheidende Frage ist daher, ob der Nutzen die durch das Datenschutzrecht in seiner gegenwärtigen Ausprägung verursachten Kosten übersteigt, und ob nicht ein hinreichender Schutz vor den durch KI-Systeme ausgehenden Gefahren zu geringeren Kosten zu erreichen wäre. Diese Frage ist völlig offen und damit auch die Frage, ob das gegenwärtige Datenschutzrecht eher ein Hemmnis oder eine Unterstützung der Entwicklung und Nutzung von KI-Systemen in Europa darstellt.

58 Vgl. etwa Rosenthal, Künstliche Intelligenz – trotz DSGVO ein Markt der Zukunft?!, 5.9.2018, Blogbeitrag, abrufbar unter https://www.srd-rechtsanwaelte.de/blog/kuenstliche-intelligenz-dsgvo/, zuletzt abgerufen am 29.11.2021.

**Kapitel D**

# MÖGLICHKEITEN UND GRENZEN DES VERZICHTS AUF PERSONENBEZOGENE DATEN BEIM MASCHINELLEN LERNEN

Angesichts der – vor allem durch Rechtsunsicherheit bedingten (soeben C.II. und III) – Einschränkungen, die sich durch datenschutzrechtliche Anforderungen für das maschinelle Lernen ergeben, kommt der Möglichkeit eines Verzichts auf die Verwendung personenbezogener Daten beim maschinellen Lernen große Bedeutung zu. Dabei werden insbesondere zwei Ansätze diskutiert, die auch die Datenethikkommission in ihrem Gutachten hervorgehoben hat[59]: die Anonymisierung personenbezogener Daten zum einen, die Verwendung synthetischer Daten zum anderen.

## I. ANONYMISIERUNG

Die Anonymisierung von Daten ist seit jeher ein zentraler Ansatz, um personenbezogene Daten für die Forschung nutzen zu können.

Der Begriff der Anonymisierung spielte im BDSG a.F. eine große Rolle. § 3 Abs. 6 BDSG a.F. definierte die die Anonymisierung als das „Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können."

Entsprechend hat sich in der deutschen Diskussion der Begriff der anonymisierten Daten als Gegenbegriff zu den personenbezogenen Daten etabliert. Anonymisierte Daten sind danach solche, die keinen Personenbezug aufweisen und entsprechend nicht dem Datenschutzrecht unterliegen.

Die DSGVO, wie zuvor die Datenschutzrichtlinie, enthält den Begriff der Anonymisierung nicht. Es besteht aber Einigkeit darin, dass auch diese von der Möglichkeit nicht-personenbezogener Daten ausgeht, freilich ohne den Begriff der Anonymität zu verwenden. Ebenso wenig verneint die DSGVO die Möglichkeit eines Vorgangs, der personenbezogene Daten in nicht-personenbezogene Daten umwandelt, anerkennt also die Möglichkeit der Anonymisierung.

In der Literatur wird darauf hingewiesen, dass die Anonymisierung ihrerseits eine Datenverarbeitung darstellt, die der DSGVO unterliegt,[60] und folglich die Anonymisierung nicht per se zur Vermeidung der Anwendbarkeit des Datenschutzrechts führt.[61]

Bedeutung hat die Frage vor allem, wenn die Daten unmittelbar im Zusammenhang mit der Erhebung anonymisiert werden, also nicht zuvor gespeichert werden. So kann es etwa bei personalisierter Werbung liegen.

Angenommen, die Kameraaufnahmen von Kunden, die zum Zwecke der personalisierten Werbung erzeugt werden (dazu oben B.III.1), werden durch Software so verrauscht, dass eine Identifizierung unmöglich wird – liegen dann zu irgendeinem Zeitpunkt personenbezogene Daten vor? Diese Frage ist zu verneinen. Die schon von vornherein anonymisierte Speicherung als Verarbeitung personenbezogener Daten zu verstehen, ist gedanklich möglich, aber datenschutzrechtlich nicht sinnvoll, denn es droht keine Gefahr für Persönlichkeitsverletzungen durch die Verarbeitung personenbezogener Daten. Die Frage hat für die Praxis möglicherweise wenig Bedeutung, weil die Anonymisierung in derartigen Fällen stets gerechtfertigt sein sollte.

Das entscheidende Problem betrifft die Anforderungen an die Anonymisierung: Wenn als Ergebnis der Anonymisierung Daten ohne Personenbezug entstehen sollen, richten sich die Anforderungen an die Anonymisierung notwendigerweise nach dem

59 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Ziff. 4.2 (S. 129 ff.).
60 Hornung/Wagner, ZD 2020, 223, 224; Valkanova, in: Kaulartz/Braegelmann (Hrsg.), Kap. 8.1 Rn. 12.
61 Ebenso Lutz, ZD 2020, 450, 452.

Personenbezug von Daten. Angesichts der schier unabsehbaren Weite des Personenbezugs, wie sie derzeit vielfach vertreten wird, gerät die Anonymisierung indes häufig zur „mission impossible". Entsprechend groß ist die Rechtsunsicherheit in dieser zentralen Frage.

Mit der Frage nach den Anforderungen an die Anonymisierung korreliert ein Problem, das aus technischer Sicht mitunter angesprochen wird: die Datenqualität. Diese Problematik stellt sich nicht zuletzt im Bereich der medizinischen Forschung, bei der umfassende Daten zu einem Krankheitsverlauf erforderlich sind, die kaum einmal anonym sein können.[62] Entsprechend beklagt der Sachverständigenrat Gesundheitswesen in seinem Gutachten, dass mit der Anonymisierung von Daten „ein hoher Informationsverlust verbunden" sei.[63]

Angesichts der großen Datenmengen, die für das maschinelle Lernen in einigen Bereichen, etwa bei der Entwicklung automatisierter Fahrzeuge, erforderlich ist, wird jedenfalls eine manuelle Anonymisierung von Bildern auch als kaum durchführbar angesehen.[64]

Angesichts dieser Schwierigkeiten wird man nicht feststellen können, dass die Möglichkeit der Anonymisierung von Daten nach gegenwärtiger Rechts- und Diskussionslage ein vielversprechendes Mittel darstellt, um KI-Forschung datenschutzkonform und zugleich effizient zu betreiben.

## II. SYNTHETISCHE DATEN

Als eine Möglichkeit zum Verzicht auf personenbezogene Daten beim maschinellen Lernen wird die Verwendung synthetischer Daten diskutiert.[65] Die Datenethikkommission setzt in ihrem Gutachten sogar stark auf diese Möglichkeit und empfiehlt der Bundesregierung, die Forschung im Bereich synthetischer Daten zu fördern.[66]

Der Begriff der synthetischen Daten wird durchaus unterschiedlich verwendet. Auch wenn der Begriff teilweise als „Daten, die künstlich generiert und nicht unmittelbar in der realen Welt erhoben wurden"[67] definiert wird, ist ein deutlich engerer Begriff gemeint.

Im Kern ist mit dem Begriff ein Ansatz gemeint, bei dem künstlich erzeugte Daten Eigenschaften aufweisen, die realen Datensätzen hinreichend gleichkommen, so dass sie für dieselben Zwecke wie „reale" Daten verwendet werden und diese folglich ersetzen können.[68] Daher kann von der „Repräsentation" realer Datensätze durch künstlich erzeugte Daten gesprochen werden.[69] „Künstliche" Datensätze sind solche, die nicht durch Abbildung der Realität gewonnen, sondern durch Software erzeugt werden. Zufallsdaten sind auch künstlich in diesem Sinne, sollen aber nicht reale Daten repräsentieren.

Die Erzeugung derartiger „repräsentativer" Daten ist durchaus anspruchsvoll und komplex. Das Ziel, tatsächlich „repräsentative" und nicht nur zufällige Daten zu erzeugen, setzt eine nachweisbare, hinreichende Ähnlichkeit zwischen den künstlich erzeugten und realen Daten voraus.[70]

Synthetische Daten können durch unterschiedliche Verfahren der Künstlichen Intelligenz erzeugt werden, wobei die Nutzung maschinellen Lernens wichtige Vorteile bietet.[71] Ein in jüngerer Zeit viel beachtetes Konzept zur Erzeugung derartiger synthetischer Daten verwendet Generative Adversarial Networks (GAN), bei dem ein neuronales Netz, der Generator, Datensätze erzeugt und das andere Netz, der Diskriminator, versucht, die erzeugten Datensätze von realen Datensätzen zu unterscheiden.[72]

Der Grundgedanke der Verwendung synthetischer Daten ist aus datenschutzrechtlicher Sicht

62 Brautzsch, Wie KI-Forschung in der Medizin trotz Datenschutz gelingen kann, 18.6.2021, https://www.mdr.de/wissen/kuenstliche-intelligenz-medizin-datenschutz-100.html, zuletzt abgerufen am 28.11.2021.
63 SVR Gesundheitswesen, Gutachten 2021, Executive Summary Ziff, 22, S. XXII
64 Lutz, ZD 2020, 450, 452; ähnlich Valkanova, in Kaulartz/Braegelmann, Kap. 8.1 Rn. 13.
65 Raji, DuD 2021, 303, 305 ff.
66 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Ziff. 4.2.3 (S. 132).
67 So Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Ziff. 4.2.3. (S. 132).
68 Siehe einen Überblick bei Drechsler/Jentzsch, S. 7 ff.
69 Paal in Kaulartz/Braegelmann, Kap. 8.7 Rn. 28.
70 S. dazu Drechsler/Jentzsch, S. 17 f. m.w.Nachw.
71 Siehe dazu Drechsler/Jentzsch, S. 11 ff.
72 Siehe eine anschauliche Erklärung etwa bei Raji, DuD 2021, 303, 305; s. auch Drechsler/Jentzsch, S. 13 f. m.w.Nachw.

bestechend. In der Literatur werden auch mögliche datenschutzrechtliche Bedenken[73] diskutiert, etwa unter welchen Voraussetzungen synthetische Daten als anonyme Daten anzusehen sind.[74] Dabei wird teilweise darauf hingewiesen, dass die Synthetisierung von Daten ein Instrument zur Depersonalisierung von Daten darstellt, das jedoch nicht zwangsläufig dazu führe, dass die erzeugten (synthetischen) Daten ihrerseits vollständig anonym seien.[75]

Die in Abhängigkeit vom gewählten Verfahren bestehende Möglichkeit, in bestimmten Fällen von den synthetischen Daten auf die personenbezogenen Ausgangsdaten zurückzuschließen,[76] schließt aber gerade nicht aus, dass Daten ohne derartige Rückbeziehung erstellt werden, insbesondere bei Verwendung maschinellen Lernens.[77]

Der Aufwand zur Erzeugung synthetischer Daten mit guter Repräsentationseignung ist allerdings hoch, zudem verbleibt stets das Risiko unzureichender Repräsentation. Die Erzeugung synthetischer Daten kann daher jedenfalls nicht als Lösung der datenschutzrechtlichen Problematik mit breitem Anwendungsbereich angesehen werden.

Das eigentliche Ziel der Erzeugung synthetischer Daten liegt indes nicht in der Vermeidung datenschutzrechtlicher Anforderungen. Ein zentraler Vorteil liegt darin, dass durch die künstliche Erzeugung von Daten eine Knappheit an realen Daten überwunden werden kann.[78] Dies hat große Bedeutung beim maschinellen Lernen, das auf eine hohe Anzahl an Daten angewiesen ist. Hier können synthetische Daten, die in beliebiger Menge produziert werden können,[79] benutzt werden. Besonders wichtig ist dies für die Simulation von bisher nicht oder selten vorkommenden Situationen (z.B. kritische Verkehrssituationen beim automatisierten Fahren).[80]

## III. FAZIT

Aus den Überlegungen zur Anonymisierung von Daten und zur Verwendung synthetischer Daten wird deutlich, dass der Verzicht auf personenbezogene Daten für Forschung und Entwicklung im Bereich der künstlichen Intelligenz, insbesondere in Bezug auf das maschinelle Lernen, keine Lösung mit breitem oder gar umfassendem Anwendungsbereich darstellen kann. Der Aufwand für die Erstellung anonymer oder synthetischer Daten kann sehr hoch sein. Die Verwendung derartiger Daten kann zu Qualitätseinbußen führen, die ihrerseits problematisch sein können.

Vielmehr werden personenbezogene Daten in hohem Umfang für die Forschung und Entwicklung im Bereich der künstlichen Intelligenz benötigt. Die zuvor geschilderten Probleme sind daher innerhalb des Datenschutzrechts, nicht zuletzt durch eine sachgerechte Bestimmung des Anwendungsbereichs, konkret des Begriffs des Personenbezugs von Daten, sowie, de lege lata, über eine interessengerechte Berücksichtigung der Forschungsinteressen im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO zu suchen.

73 Dazu etwa Raji, DuD 2021, 303, 307 ff.
74 S. dazu etwa Heinemeyer, CR 2019, 147, 151; Paal in Kaulartz/Braegelmann, Kap. 8.7. Rn. 28; Raji, DuD 2021, 303, 307 f.
75 Paal in Kaulartz/Braegelmann, Kap. 8.7. Rn. 28.
76 Dazu Drechser/Jentzsch, S. 10 f. mit Verweis auf weiterführende Literatur.
77 Darauf weisen Drechsler/Jentzsch, S. 10 f. ausdrücklich hin.
78 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Ziff. 4.2.3 (S. 132); Heinemeyer, CR 2019, 147, 150; Raji, DuD 2021, 303, 305.
79 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Ziff. 4.2.3 (S. 132).
80 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Ziff. 4.2.3 (S. 132).

**Kapitel E**

# FEHLERHAFTE ENTSCHEIDUNGEN DURCH KÜNSTLICHE INTELLIGENZ

## I. GEGENSTAND UND GLIEDERUNG DER UNTERSUCHUNG

Die Risiken durch fehlerhafte Bewertungen natürlicher Personen durch KI-Systeme und die Gefahr von Diskriminierung sind zu Recht ein zentraler Aspekt der Diskussion zu KI-Systemen. Die Fragestellung ist äußerst vielschichtig und wird in den verschiedenen Disziplinen in unterschiedlicher Weise erörtert. So wird etwa neben dem Begriff der Diskriminierung, der seinerseits unterschiedlich verstanden wird, häufig auch auf Bias oder Fairness Bezug genommen. Auch der Gegenstand der Betrachtung wird unterschiedlich bezeichnet. So wird teilweise von „algorithmischen Entscheidungen" gesprochen, teilweise auch von Entscheidungen durch „künstliche Intelligenz" oder „KI-Systeme".

Im Vordergrund des Interesses stehen Entscheidungen sowie Bewertungen über natürliche Personen, die von einem KI-System, also von einer Software oder einem System bestehend aus Soft- und Hardware, vorgenommen werden. Insoweit wird hier in Anlehnung an eine Studie zu algorithmischen Entscheidungen der Gesellschaft für Informatik[81] der Begriff „algorithmische Entscheidung" (sogleich II.1) verwendet, der auch Bewertungen umfasst. Da es aus Sicht des Betroffenenschutzes und insbesondere des Datenschutzrechts nicht entscheidend ist, ob das System, das eine algorithmische Entscheidung vornimmt, seinerseits die Anforderungen an den Begriff der künstlichen Intelligenz erfüllt, sollen hier auch sonstige maschinelle Entscheidungen betrachtet werden.

Angesichts der umfangreichen und komplexen Fragestellungen muss sich die Analyse auf wenige Aspekte beschränken. Zunächst sollen die Begriffe und Zielrichtungen der Diskussion, insbesondere die Begriffe der Diskriminierung, des Bias und der Fairness, für die Zwecke dieser Untersuchung (sogleich 2. a.) und sodann der Bereich der Fehler in algorithmischen Entscheidungen beschrieben werden (unten 2. b.–d.). Anschließend wird die Bedeutung des Art. 22 DSGVO, der im Zusammenhang mit der hier interessierenden Fragestellung häufig genannt wird, näher untersucht (unten 3.). Anschließend werden die Verwendung fehlerhafter Daten in algorithmischen Entscheidungen (4.), Diskriminierung durch algorithmische Entscheidungen (5.) und Fehler in der Datengrundlage, der sog. „bias in the data" (6.), jeweils mit besonderem Blick auf die Rolle des Datenschutzrechts, untersucht. Abschließend wird ein kurzes Fazit zum Potenzial des Datenschutzrechts in Bezug auf fehlerhafte algorithmische Entscheidungen gezogen (7.).

## II. FEHLER IN ALGORITHMISCHEN ENTSCHEIDUNGEN

### 1. TERMINOLOGIE

Der Begriff der algorithmischen Entscheidung wird durchaus unterschiedlich definiert. In einer interdisziplinären, von der Gesellschaft für Informatik erstellten Studie wird der Begriff der algorithmischen Entscheidungsfindung als ein Prozess definiert, bei dem eine Aktion aus mehreren Alternativen auf Basis qualitativer und quantitativer Attribute durch einen Algorithmus ausgewählt wird.[82] Andere Definitionen gehen dahin, dass „algorithmen-determinierte" Entscheidungen vollständig automatisiert und ohne menschliches Handeln getroffen werden.[83] Auch insoweit wird unter einer Entscheidung die Auswahl zwischen Handlungsmöglichkeiten unter Berücksichtigung von deren Merkmalen verstanden,[84] was auch den Kern der Definition der GI-Studie darstellt.

81 Gesellschaft für Informatik, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Gutachten der Fachgrupp Rechtsinformatik der Gesellschaft für Informatik e.V. im Auftrag des Sachverständigenrats für Verbraucherfragen (Hrsg.),
82 Vgl. GI-Studie, Ziff. 3.1, S. 17.
83 Hoffmann-Riem in Eifert, Digitale Disruption und Recht, 2020, S. 143, 162 f.
84 Hoffmann-Riem in Eifert, Digitale Disruption und Recht, 2020, S. 143, 162.

Dieser Begriff wird auch hier zugrunde gelegt, wobei die Bewertung einer Person auch als Entscheidung verstanden wird. Formal kann dies damit begründet werden, dass die Bewertung die Entscheidung enthält, dem Gegenstand der Bewertung eines von mehreren möglichen Bewertungsergebnissen zuzuweisen. Soweit also eine Bewertung von Software vorgenommen wird, handelt es sich auch um eine algorithmische Entscheidung.

Die hier interessierenden Problembereiche lassen sich als „fehlerhafte" algorithmische Entscheidungen in dem Sinne verstehen, dass sie unerwünscht sind, etwa gegen ein rechtliches Gebot (z.B. Diskriminierungsverbot) verstoßen.

Der Begriff des Fehlers in einer Entscheidung im Zusammenhang mit algorithmischen Entscheidungen wurde in der GI-Studie verwendet und systematisiert.[85] Die Studie, die auf Beurteilungen von Personen durch Maschinen fokussiert ist, weist zu Recht darauf hin, dass die Bewertung einer Beurteilung als „fehlerhaft" in mehrfacher Hinsicht von der Perspektive und den Zielen des Bewertenden abhängt,[86] und verdeutlicht dies am Beispiel der Berücksichtigung des Alters bei der Personalauswahl. Dort mag der Entscheider, etwa im Hinblick auf Präferenzen der Kollegen, eine altersgemäße Homogenität des Personals für wichtig halten, der deswegen abgelehnte Bewerber mag hierin eine Altersdiskriminierung sehen, der Vorgesetzte des Entscheiders wegen einer Präferenz für altersgemischte Teams die Entscheidung für eine fachlich unqualifizierte Entscheidung halten.[87]

Diese Abhängigkeit der „Fehlerhaftigkeit" einer algorithmischen Entscheidung von der Perspektive ist auch aus rechtlicher Sicht von Bedeutung: Eine wesentliche Zielsetzung des Rechts ist es, Abweichungen von rechtlichen Anforderungen zu identifizieren und zu vermeiden, zu sanktionieren oder negative Folgen auszugleichen. Insoweit wird der Fehler als Abweichung von rechtlichen Anforderungen definiert. Das Recht adressiert aber auch Fehler als Abweichung von den eigenen Zielen des Entscheiders, besonders deutlich etwa im Beispiel der vertraglichen Gewährleistung für die Mangelhaftigkeit eines Systems.

Aus datenschutzrechtlicher Perspektive sind Verstöße algorithmischer Entscheidungen gegen rechtliche Vorgaben von besonderem Interesse. Dies ist etwa der Fall, wenn ein rechtlich unzulässiges Entscheidungskriterium verwendet wird, wie es bei der Diskriminierung der Fall ist, oder wenn der Beurteilende eine Information übersieht, dessen Berücksichtigung rechtlich geboten ist.

## 2. BEWERTUNG EX ANTE UND EX POST

Im Hinblick auf die rechtliche Bewertung algorithmischer Entscheidungen ist eine weitere Unterscheidung nach der Perspektive und dem Wissensstand der Person zu treffen, die die Beurteilung als fehlerhaft oder fehlerfrei zu bewerten hat.

Diese Unterscheidung kann mit dem Begriffspaar „ex ante" und „ex post" gekennzeichnet werden.[88] Mit dem Begriff „ex ante" wird meistens die Situation des Entscheidenden, insbesondere dessen Wissensstand und Erkenntnismöglichkeiten, bezeichnet, wogegen mit dem Begriff „ex post" die Perspektive eines mit Zusatzwissen ausgestatteten Dritten beschrieben wird, der die Beurteilung bewertet. Musterfall ist die Perspektive eines Gerichts, das über die Fehlerhaftigkeit einer Beurteilung zu entscheiden hat.[89]

Beide Perspektiven sind aus rechtlicher Sicht von Bedeutung. Die ex-post-Betrachtung ist typischerweise relevant, wenn es um die Feststellung der Fehlerhaftigkeit einer Entscheidung als solcher geht. So berücksichtigt ein Gericht für die Beurteilung der Fehlerhaftigkeit einer Entscheidung jeweils das gesamte, ihm zur Verfügung stehende Wissen, nicht zuletzt sowohl das Wissen des Entscheiders als auch Dritter, selbst bei lang zurückliegenden Entscheidungen. Dies gilt auch, soweit bei einer Entscheidung ein Beurteilungsspielraum zugebilligt wird. Die Frage, ob sich eine Entscheidung innerhalb oder außerhalb des Beurteilungsspielraums bewegt, wird wiederum aus der Perspektive des Gerichts mit dem gesamten, diesem zur Verfügung stehenden Wissen getroffen.

Die ex-ante-Perspektive wird insbesondere für die Frage eines Verschuldens hinsichtlich der fehlerhaften Entscheidung herangezogen. So liegt ein Verschulden hinsichtlich einer fehlerhaften Ent-

85 Siehe dazu GI-Studie, Ziff. 5.3, S. 82 ff.
86 GI-Studie, Ziff. 5.2, S. 81 f.
87 GI-Studie, Ziff. 5.2, S. 81.
88 GI-Studie, Ziff. 5.2.2, S. 82.
89 GI-Studie, Ziff. 5.2.2, S. 82.

scheidung nicht vor, wenn der – ex post als solcher identifizierte – Fehler aus Sicht des Entscheiders nicht erkennbar war.

Die Kategorie des Verschuldens ist indes auf Maschinen nach herrschender Ansicht nicht anwendbar.[90] Auf die hochinteressante Frage, ob Maschinen verschuldensfähig sind oder die Regelungen zum Verschulden analog auf Maschinen anwendbar sind,[91] kann im Rahmen dieser Untersuchung nicht eingegangen werden.

In Bezug auf KI-Systeme ist diese ex-ante-Sicht, auf die etwa das Gewährleistungsrecht (vgl. §§ 434, 633 / 437, 634 BGB), aber auch das Produkthaftungsrecht (vgl. § 1 ProdHaftG) abstellt, für die Beurteilung der Fehlerhaftigkeit der Maschine maßgeblich.

Der Entwurf des KI-Gesetzes knüpft im Rahmen der Pflicht zur Qualitätssicherung und zum Risikomanagement grundsätzlich an die ex-ante-Perspektive an, etwa wenn in Art. 26 auf den Zeitpunkt des Inverkehrbringens abgestellt wird. Später erlangtes Wissen muss der Hersteller im Rahmen des Risikomanagements jedoch ebenfalls berücksichtigen (Art. 9 Abs. 2 lit. c).

## 3. ARTEN VON FEHLERN

Eine allgemeingültige Systematik der Fehlerhaftigkeit algorithmischer Entscheidungen existiert bisher nicht, zum Teil wird zwischen Fehlern in der Entscheidungsfindung, der Entscheidungsgrundlage und der Würdigung der Entscheidungsgrundlagen unterschieden.[92] In Anlehnung an die GI-Studie zu algorithmischen Entscheidungen[93] wird hier wie folgt unterschieden:

### a. Unzulässigkeit der algorithmischen Entscheidung

Die Fehlerhaftigkeit einer algorithmischen Entscheidung kann schon in der Vornahme als solcher liegen. Ein solches Verbot einer algorithmischen Entscheidung wird etwa in Art. 22 DSGVO geregelt (dazu unten 3.). Nach § 35a VwVfG sind automatisierte Entscheidungen etwa für Ermessensentscheidungen oder Entscheidungen mit Beurteilungsspielraum unzulässig, zudem muss die Automatisierung durch Rechtsvorschrift zugelassen sein. Im Anwendungsbereich eines solchen Verbots wäre eine gleichwohl vorgenommene Entscheidung fehlerhaft im hier genannten Sinne und zugleich rechtswidrig.

### b. Intransparenz der Entscheidung

Eine algorithmische Entscheidung kann, unabhängig vom Entscheidungsinhalt, bereits wegen Intransparenz fehlerhaft sein. Dies ist etwa dann der Fall, wenn die Entscheidung öffentlich zu erfolgen hat oder, etwa dem Betroffenen, die Entscheidungsgrundlagen mitzuteilen sind. Als Fallgruppe der Intransparenz lässt sich auch das Fehlen einer gebotenen Begründung verstehen.

### c. Fehler der Entscheidungsfindung

Eine Entscheidung kann fehlerhaft sein, weil sie Anforderungen an die Entscheidungsfindung, also an das zur Entscheidung führende Verfahren, verletzt. Der GI-Studie folgend soll hier die Ermittlung der tatsächlichen Entscheidungsgrundlage als eigene Fallgruppe (sogleich dd.) bezeichnet werden. Andere Anforderungen an ein Entscheidungsverfahren, die etwa aus staatlichen Verfahren bekannt sind, betreffen etwa die Gelegenheit zur Stellungnahme oder die Auswahl des Entscheiders, sei es hinsichtlich der generellen Eignung (Qualifikation) oder der Eignung im konkreten Fall, die etwa wegen Befangenheit fehlen kann.

Derartige Anforderungen gelten grundsätzlich auch für algorithmische Entscheidungen. Es ist aber offensichtlich, dass insoweit nicht einfach die Anforderungen an menschliche Entscheidungen übertragen werden können.

So wird ein KI-System keine Examina oder Studienabschlüsse vorweisen müssen. Es lassen sich jedoch maschinenspezifische, funktional äquivalente Anforderungen formulieren. So ist naheliegend, dass ein KI-System, das für automatisierte Entscheidungen eingesetzt werden soll, mit einer Bestätigung über einen durchgeführten Test versehen sein muss. Diesem Konzept entsprechend verlangt etwa der Entwurf des KI-Gesetzes die Vergabe des CE-Kennzeichens durch den Hersteller (vgl. Art. 16 lit. i) KI-Gesetz), das bei Hochrisiko-KI-Systemen die Bestätigung über die Einhaltung der vom KI-Gesetz gestellten Anforderungen an Hochrisiko-KI-Systeme enthält.

90 BeckOK IT-Recht-Hilber, BGB § 278 Rn. 5 ausdrücklich zu KI-Systemen; Horner/Kaulartz, CR 2016, 7; Zech, ZfPW 2019, 198, 211.
91 Siehe zur analogen Anwendbarkeit des § 278 BGB etwa Linardatos, Autonome und vernetzte Aktanten im Zivilrecht, 2021, S. 205 ff.; zur analogen Anwendung des § 831 BGB auf KI etwa Zech, ZfPW 2019, 198, 211.
92 EHKS/Ebers, § 3 Rn. 26.
93 Vgl. GI-Studie, Ziff. 5.3., S. 82 ff.

Auch kann die Besorgnis der Befangenheit, die bei menschlichen Entscheidern etwa aus einem Verwandtschaftsverhältnis zum Betroffenen abgeleitet wird, keine Rolle spielen. Möglicherweise wird man aber in ganz ähnlicher Weise annehmen, dass ein System, das eine Entscheidung über eine Person trifft, nicht von einer dem Betroffenen nahestehenden Person programmiert oder eingestellt werden darf.

#### d. Fehler der Entscheidungsgrundlage

Als Fehler der Entscheidungsgrundlage werden hier, der GI-Studie folgend, Fehler bei der Sammlung der Entscheidungsgrundlagen, insbesondere der für die Beurteilung zugrunde liegenden Tatsachenbasis, verstanden.[94] Diese Fallgruppe ist für die Diskriminierung von Bedeutung. So liegt ein Fehler der Entscheidungsgrundlage etwa bei Heranziehung unzulässiger Tatsachen vor, wie es bei Diskriminierung (vgl. dazu unten 5.) der Fall ist.

Eine fehlerhafte Entscheidungsgrundlage liegt aber auch bei Heranziehung unzutreffender Tatsachen oder bei einer unvollständigen Sammlung von Tatsachen vor (dazu unten 4.), deren Vermeidung insbesondere ein Kernanliegen des Verfahrensrechts ist. Wenn etwa der Richter verpflichtet ist, alle relevanten Tatsachen zu berücksichtigen, so dient dies der Vermeidung eines solchen Fehlers. Und wenn eine Entscheidung auf einer fehlerhaften Tatsachengrundlage beruht, stellt dies sowohl in Gerichtsverfahren als auch im Verwaltungsverfahren einen Grund zur Aufhebung dar.

Auch das Datenschutzrecht adressiert diese Fallgruppe, etwa durch den Anspruch des Betroffenen auf Korrektur von Daten, ebenso das Strafrecht (z.B. § 263 StGB), das Deliktsrecht sowie das Vertragsrecht.

#### e. Fehlerhafte Würdigung der Entscheidungsgrundlagen

Fehler können sich schließlich bei der Würdigung der Entscheidungsgrundlagen ergeben.[95] Einfache Beispiele sind Rechenfehler, etwa bei der Addition von Punkten für eine Gesamtbewertung. Häufiger, aber auch komplexer, sind unangemessene Gewichtungen von Tatsachen im Rahmen der Entscheidungsfindung. Aus rechtlicher Sicht sind derartige Fehler aus verschiedenen Gründen nicht leicht fassbar. Dem menschlichen Entscheider wird ein erheblicher Beurteilungsspielraum zugebilligt, in dessen Rahmen Bewertungen rechtlich nicht angreifbar sind. Wie bereits gesagt, gelten auch hier Grenzen, etwa bei Nichtberücksichtigung, also vollständiger Außerachtlassung, relevanter Tatsachen. Inwieweit die bestehenden für menschliche Entscheidungen entwickelten Grundsätze auf algorithmische Entscheidungen übertragbar sind, ist noch weitgehend offen, die Diskussion ist hier erst am Anfang.

Als ein spezifischer Aspekt fehlerhafter algorithmischer Entscheidungen ist wohl die Fragestellung des sog. bias in the data einzuordnen, bei der es um „fehlerhafte“ oder jedenfalls unfaire, ggf. auch diskriminierende Entscheidungen im Einzelfall geht, die ihre Ursache in der Datengrundlage im maschinellen Lernen haben. Daher soll diese Fragestellung jedenfalls im Überblick (unten 6.) betrachtet werden.

## III. ENTSCHEIDUNGEN ÜBER MENSCHEN DURCH MASCHINEN? DIE BEDEUTUNG DES ART. 22 DSGVO FÜR ALGORITHMISCHE ENTSCHEIDUNGEN

### 1. DAS VERBOT DER AUSSCHLIESSLICH AUTOMATISIERTEN ENTSCHEIDUNG, ART. 22 DSGVO

Art. 22 Abs. 1 DSGVO gewährt jeder betroffenen Person „das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung […] beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“. Dies gilt nach Abs. 2 jedoch nicht in den Ausnahmen der Abs. 2 lit. a)–c).

Dieser Norm, die den Einzelnen davor schützen soll, durch automatisierte Entscheidungen beeinträchtigt zu werden,[96] wird mitunter erhebliche Bedeutung im Zusammenhang mit algorithmischen Entscheidungen bescheinigt. Jedoch ist ihre Bedeutung in allen zentralen Aspekten unklar und vielfach umstritten.

94 GI-Studie, Ziff. 5.3.4., S. 84.
95 Siehe dazu GI-Studie, Ziff. 5.3.4, S. 84.
96 Kühling/Buchner-Buchner, Art. 22 Rn. 1 m.w.N; Simitis/Hornung/Spiecker-Scholz, DSGVO Art. 22 Rn. 3.

Trotz anderslautenden Gesetzeswortlauts besteht offenbar Einigkeit darin, dass Art. 22 Abs. 1 ein Verbot automatisierter Entscheidungen ausspricht.[97] Unklarheiten und umstrittene Auslegungsfragen bestehen in Bezug auf den Tatbestand der Norm, vor allem hinsichtlich des Gegenstands des Verbots, der mit dem Begriff der „ausschließlich automatisierten Entscheidung" zusammengefasst wird. Hier ist insbesondere umstritten, welcher Grad an Automatisierung das Verbot hervorruft, ob eine Bewertung der betroffenen Person vorausgesetzt wird und ob bloße Bewertungen überhaupt erfasst sind.

Als Beispiele für die Fragestellung werden in der Diskussion etwa die automatisierte Kreditentscheidung genannt, die man sich etwa bei einem per Internet zu beantragenden „Sofort-Kredit" vorstellen kann, oder die automatisierte Vorauswahl von Bewerbern für einen Arbeitsplatz. Als Gegenbeispiel kann aber auch gefragt werden, ob die Entscheidung eines Geldautomaten, nach Vorlage einer Kreditkarte und Eingabe des zugehörigen Passworts den gewünschten Geldbetrag auszugeben, unter Art. 22 DSGVO fällt.[98]

Nachfolgend werden zunächst die wesentlichen Aspekte der Norm kurz analysiert und sodann Art. 22 DSGVO in Bezug auf algorithmische Entscheidungen evaluiert.

## 2. DIE AUSSCHLIESSLICH AUTOMATISIERTE ENTSCHEIDUNG

Da sich Art. 22 nur auf „ausschließlich" automatisierte „Entscheidungen" bezieht, kommt es für die praktische Bedeutung der Norm entscheidend darauf an, welcher Automatisierungsgrad maßgeblich ist und wann eine „Entscheidung" vorliegt.

### a. Der maßgebliche Automatisierungsgrad

Erwägungsgrund 71 der DSGVO spricht in Satz 1 von Entscheidungen „ohne jegliches menschliche Eingreifen" und nennt als Beispiel die „automatische Ablehnung eines Online-Kreditantrags", was auf ein enges Verständnis hinweist. Entsprechend wird bisher nahezu einhellig angenommen, dass Art. 22 nur dann eingreift, wenn eine Entscheidung mit rechtlicher Wirkung oder sonst erheblicher Beeinträchtigung unmittelbar und ausschließlich von einer Maschine getroffen wird,[99] nicht aber, wenn die Entscheidung von der Maschine lediglich vorbereitet und letztlich von einem Menschen getroffen wird.[100] Von dieser engen Auslegung geht auch die Datenethikkommission in ihrem Gutachten aus.[101]

Entscheidend ist nach diesem Verständnis, unter welchen Voraussetzungen eine von einer Maschine vorbereitete Entscheidung von einem Menschen „getroffen" wird. Insoweit wird teilweise verlangt, dass die Mitwirkung der natürlichen Person „nicht lediglich formaler", sondern „inhaltlicher Art" sein müsse.[102] Es bleibt jedoch unklar, unter welchen Voraussetzungen eine inhaltliche Mitwirkung vorliegen soll. Vielfach wird eine Überprüfung von Entscheidungen aufgrund von Plausibilität für ausreichend gehalten, soweit sich diese nicht auf Stichproben beschränkt.[103] Andere hingegen halten eine Plausibilitätskontrolle nicht für ausreichend.[104]

Unklarheiten und Meinungsdivergenzen bestehen auch bei Einzelfällen. So wird die Kreditentscheidung wird nach herrschender Meinung nur dann vollständig automatisiert getroffen, wenn das System auch die abschließende Entscheidung trifft, nicht aber, wenn ein menschlicher Sachbearbeiter aufgrund eines automatisch errechneten Scorewertes[105] entscheidet.[106] Eher vereinzelt wird – durchaus konsequent – vertreten, die Kreditentscheidung sei als vollständig automatisiert anzusehen, wenn der menschliche Kreditsachbearbeiter die Entscheidung „ganz überwiegend" aufgrund eines negativen Scorewertes treffe.[107]

Die schwierige Abgrenzung weist bereits auf das grundlegende Dilemma des Art. 22 hin: die Unklarheit in der entscheidenden Frage, was eigentlich von Art. 22 verlangt wird. Bei algorithmischen

97 Unstr. siehe nur Kumkar/Roth-Isigkeit, JZ 2020, 277, 278; Sydow-Helfrich, DSGVO Art. 22 Rn. 39; Spindler/Schuster-Spindler/Horváth, DSGVO Art. 22 Rn. 5; BeckOK IT-Recht-Steinrötter DSGVO Art. 22 Rn. 5; Taeger/Gabel-Taeger, Art. 22 Rn. 7, 23 f.

98 GI-Studie, Ziff. 5.5.2, S. 95.

99 So Auernhammer-Herbst, DSGVO Art. 22 Rn. 5; Simitis/Hornung/Spicker-Scholz, DSGVO Art. 22 Rn. 26; BeckOK IT-Recht-Steinrötter, Art. 22 Rdn. 7; Gola-Schulz, DSGVO Art. 22 Rn. 12.

100 So Schwartmann/Jaspers/Thüsing/Kugelmann-Atzert, DSGVO Art. 22 Rn. 75; Ehmann/Selmayr-Hladik, DSGVO Art. 22 Rn. 6; Simitis/Hornung/Spiecker-Scholz, DSGVO Art. 22 Rn. 28.

101 Vgl. Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, S. 185.

102 Kühling/Buchner-Buchner, Art. 22 Rn. 15; Auernhammer-Herbst, DSGVO Art. 22 Rn. 6; Simitis/Hornung/Spiecker-Scholz, Art. 22 Rn. 26; Spindler/Schuster-Spindler/Horváth, DSGVO Art. 22 Rn. 5.

103 Kühling/Buchner-Buchner, Art. 22 Rn. 15; BeckOK DatenschutzR-Lewinski, DSGVO Art. 22 Rn. 25.1.

104 Paal/Pauly-Martini, DSGVO Art. 22 Rn. 19; Simitis/Hornung/Spiecker-Scholz, Art. 22 Rn. 27.

105 Zur Eigenschaft des Scorewertes als Entscheidung i.S. des Art. 22 siehe sogleich bb.

106 So etwa Gola-Schulz, DSGVO Art. 22 Rn. 15; ebenso, zu § 6a BDSG a.F., BGHZ 200, 38 Rn. 34.

107 Simitis/Hornung/Spiecker-Scholz, Art. 22 Rn. 27.

Entscheidungen wird das Erfordernis einer vollautomatisierten Entscheidung durchaus einmal vorliegen, so dass der Norm insoweit eine praktische Bedeutung zukommen kann.

### b. Bewertungen als Entscheidung i.S. des Art. 22 DSGVO?

Die wichtigere Frage dürfte indes nicht sein, wann eine Entscheidung „ausschließlich" durch eine Maschine getroffen wird, sondern was unter dem Begriff der „Entscheidung" zu verstehen ist.

Nach bisher offenbar allgemeiner Auffassung rekurriert das Gesetz auf die abschließende Entscheidung in einer Angelegenheit, nicht auf deren Vorbereitung. So wird die automatisierte Vorauswahl von Bewerbern im Rahmen der Stellenbesetzung als bloße Entscheidungshilfe angesehen, auf die Art. 22 DSGVO nicht anwendbar ist,[108] obwohl die Entscheidung für die abgelehnten Bewerber ja durchaus endgültig ist. Etwas anderes soll nur gelten, wenn die Absage durch das System selbst ausgesprochen wird.[109]

Danach würde eine bloße Bewertung von Eigenschaften einer Person nicht unter den Begriff der Entscheidung fallen. Zwingend ist dies nicht: Wenn etwa ein KI-System im Rahmen der Personalauswahl einen Kandidaten als ungeeignet einstuft und dieser daraufhin vom menschlichen Entscheider aussortiert wird, könnte durchaus anzunehmen sein, dass die Bewertung gegenüber dem Kandidaten zwar keine unmittelbare rechtliche Wirkung entfaltet, ihn aber „in ähnlicher Weise erheblich beeinträchtigt". Eine Bewertung könnte ohne logische Verrenkung durchaus als Unterfall einer „Entscheidung" erfasst werden.

Derartige Bewertungen werden von der DSGVO mit dem Begriff des „Profiling" bezeichnet. Der in Art. 22 Abs. 1 DSGVO verwendete Begriff umfasst nach der Definition des Art. 4 Nr. 4 DSGVO jede Verarbeitung personenbezogene Daten zur Bewertung bestimmter persönlicher Aspekte einer natürlichen Person. Art. 4 Nr. 4 DSGVO nennt als Beispiele unter anderem die Analyse oder Vorhersage von Arbeitsleistung, der wirtschaftlichen Lage oder der Gesundheit. Damit ist jede automatisierte Bewertung von natürlichen Personen anhand deren Merkmalen und personenbezogener Daten ein „Profiling" im Sinne des Art. 22 DSGVO.

Die entscheidende Frage ist, ob Profiling, das per Definition automatisiert erfolgt, als solches eine „Entscheidung" i.S. des Art. 22 DSGVO darstellt. Nimmt man das an,[110] fiele etwa die Erstellung eines Kreditscoring als solche unter das Verbot des Art. 22 Abs. 1 DSGVO. Nach ganz herrschender Meinung der Literatur ist jedoch das eine Entscheidung lediglich vorbereitende Profiling von Art. 22 Abs. 1 DSGVO im Ergebnis nicht erfasst.[111] Folgt man der h.M., sind isolierte Bewertungen nicht als „Entscheidungen" anzusehen.[112] Angesichts des starren Verbots des Art. 22 DSGVO ist dies überzeugend. Jedoch ergeben sich Schutzlücken im Bereich der automatisierten Bewertungen (dazu unten e) bb).

## 3. RECHTSWIRKUNG ZULASTEN ODER BENACHTEILIGUNG DES BETROFFENEN

Der Tatbestand des Art. 22 Abs. 1 DSGVO setzt weiter voraus, dass die Entscheidung Rechtswirkung gegenüber dem Betroffenen entfaltet oder ihn anderweitig erheblich benachteiligt.

Die alternative Formulierung wird verbreitet dahin verstanden, dass jede Entscheidung, die Rechtswirkung entfaltet, per se dem Verbot des Abs. 1 unterliegt, ohne Rücksicht darauf, ob sie eine „erhebliche Beeinträchtigung" darstellt.[113] Nach anderer Auffassung greift das Verbot auch bei Entscheidungen mit Rechtswirkung nur bei einer erheblichen Beeinträchtigung ein.[114]

Eine rechtliche Wirkung in diesem Sinne soll vorliegen, wenn die Rechtsstellung des Betroffenen in irgendeiner Weise verändert wird.[115] Dies wird etwa bei einer positiven Entscheidung über den Abschluss oder die Kündigung eines Vertrags,[116]

108 Simitis/Hornung/Spiecker-Scholz, Art. 22 Rn. 27.
109 Simitis/Hornung/Spiecker-Scholz, Art. 22 Rn. 27.
110 So wohl Franzen/Gallner/Oetker-Franzen, Art. 22 Rn. 25
111 Plath-Kamlah, Art. 22 Rn. 2; Kumkar/Roth-Isigkeit, JZ 2020, 277, 278; BeckOK IT-Recht-Steinrötter, DSGVO Art. 22 Rn. 10; Taeger/Gabel-Taeger, DSGVO Art. 22 Rn. 35.
112 So ausdrücklich für Kreditscoring etwa Taeger/Gabel-Taeger, Art. 22 Rn. 32, 35.
113 So etwa Sydow-Helfrich, Art. 22 Rn. 47 ff.; BeckOK IT-Recht-Steinrötter, DSGVO Art. 22 Rn. 11.
114 Auernhammer-Herbst, DSGVO Art. 22 Rn. 14; Hennemann/Kumkar in Linardatos, § 13 Rn. 13.
115 Plath-Kamlah, DSGVO Art. 22 Rdn. 7a; Kumkar/Roth-Isigkeit, JZ 2020, 277, 279; Paal/Pauly-Martini, DSGVO Art. 22 Rn. 26; Spindler/Schuster-Spindler/Horváth, DSGVO Art. 22 Rn. 7.
116 Auernhammer-Herbst, DSGVO Art. 22 Rn. 16; Kumkar/Roth-Isigkeit, JZ 2020, 277, 279.

über den Erlass eines Verwaltungsakts[117] oder über den Erlass einer ordnungsrechtlichen Verfügung[118] angenommen. Die Ablehnung eines Vertragsschlusses hingegen soll nach einer Mindermeinung der Literatur nicht unter Art. 22 Abs. 1 fallen,[119] was insoweit merkwürdig ist, als hier besondere Schutzbedarf (z.B. Ablehnung einer Kreditgewährung) besteht. Die herrschende Ansicht der Literatur sieht die Vertragsablehnung zu Recht als Entscheidung i.S. des Art. 22 Abs. 1 DSGVO an. [120]

Als ungeschriebene Voraussetzung wird teilweise angenommen, dass die Entscheidung eine für den Betroffenen nachteilige Komponente haben müsse,[121] mit der Folge, dass Entscheidungen, die einem Begehren des Betroffenen in vollem Umfang entsprechen, nicht unter das Verbot des Art. 22 Abs. 1 fallen sollen.[122]

Eine erhebliche Beeinträchtigung liegt nach h.M. vor, wenn der Betroffene durch die Entscheidung in seiner wirtschaftlichen oder persönlichen Tätigkeit nachhaltig gestört wird.[123] Als Beispiel werden in der Literatur die Kündigung eines Kredits sowie die Gewährung eines Kredits zu erhöhtem Zinssatz genannt,[124] Dies soll auch bei der Ablehnung eines Vertragsangebots gelten, jedoch nur, soweit die Ablehnung eine erhebliche Beeinträchtigung darstellt.[125]

## 4. VERBOT NACHTEILIGER ENTSCHEIDUNGEN AUFGRUND EINER BEWERTUNG DES BETROFFENEN

Als weitere, ungeschriebene Voraussetzung des Art. 22 wird in der Literatur überwiegend angenommen, dass die Entscheidung auf einer Bewertung eines Aspekts der Person beruht,[126] so wie etwa im § 6a BDSG a.F., der die Vorgängernorm des Art. 22, Art. 15 der Datenschutz-Richtlinie, umsetzte. Eine entsprechende Einschränkung war im Verordnungsvorschlag der Kommission und des Europäischen Parlaments noch enthalten, entfiel jedoch im weiteren Gesetzgebungsverfahren.[127] Darauf verweisend lehnt die Gegenmeinung ein solches Erfordernis ab.[128] Die h.M. ist gleichwohl überzeugend, da ansonsten auch automatisierte Entscheidungen erfasst würden, die aus anderen Gründen getroffen werden, etwa die Ablehnung eines Vertragsangebots allein aus Kapazitätsgründen.

Dieses Erfordernis schärft das Verständnis des Art. 22 wesentlich. Es geht nicht um die Verhinderung einer nachteiligen Entscheidung durch Maschinen, sondern um die Verhinderung einer Bewertung von Personen durch Maschinen, die sich in einer nachteiligen Entscheidung von erheblicher Bedeutung niederschlägt.

Dieses Ziel, das als solches zu begrüßen ist, wird in der bisherigen Fassung des Gesetzes aber unzureichend umgesetzt, da maschinelle Bewertungen, die nicht sogleich in eine automatisierte Entscheidung münden, nicht erfasst sind.

Fragen ergeben sich auch bei KI-gestützten Bewertungen, die gar nicht die einzelne Person betreffen, aber für die Entscheidung über ihr Schicksal Bedeutung haben.

Wenn etwa angeboten wird, Abschlussnoten von Schulen oder Universitäten durch KI-Systeme zu bewerten und auf dieser Grundlage die konkrete Note eines Bewerbers um einen Arbeits- oder Studienplatz zu gewichten,[129] liegt weder ein Personenbezug noch eine automatisierte Entscheidung über Personen vor. Gleichwohl ist das Bedürfnis nach einer Qualitätskontrolle derartiger Bewertungen offensichtlich.

117 BeckOK DatenschutzR- Lewinski, Art. 22 Rn. 30; Gola-Schulz, DSGVO Art. 22 Rn. 23.
118 Kühling/Buchner-Buchner, Art. 22 Rn. 24.
119 Gola-Schulz, Art. 22 Rn. 25
120 Kühling/Buchner-Buchner, Art. 22 Rn. 26a; Simitis/Hornung/Spiecker-Scholz, DSGVO Art. 22 Rn. 36; Taeger/Gabel-Taeger, DSGVO Art. 22 Rn. 44.
121 Kühling/Buchner-Buchner, Art. 22 Rn. 25; Kumkar/Roth-Isigkeit, JZ 2020, 277, 279; Plath-Kamlah, DSGVO Art. 22 Rn. 7e; BeckOK DatenschutzR-Lewinski, DSGVO Art. 22 Rn. 33.
122 Kühling/Buchner-Buchner, Art. 22 Rn. 25; Plath-Kamlah, DSGVO Art. 22 Rn. 7e.
123 Spindler/Schuster-Spindler/Horváth, DSGVO Art. 22 Rn. 8; BeckOK IT-Recht-Steinrötter, DSGVO Art. 22 Rn. 13.
124 So zur Kündigung: Ehmann/Selmayr-Hladjik, DSGVO Art. 22 Rn. 9; Spindler/Schuster-Spindler/Horváth, DSGVO Art. 22 Rn. 8; zum erhöhten Zinssatz: Auernhammer-Herbst, DSGVO Art. 22 Rn. 17; BeckOK IT-Recht-Steinrötter, DSGVO Art. 22 Rn. 13.
125 Kühling/Buchner-Buchner, Art. 22 Rn. 26a; ähnlich Paal/Pauly-Martini, DSGVO Art. 22 Rn. 27; Teager/Gabel-Taeger, DSGVO Art. 22 Rn. 44.
126 Kühling/Buchner-Buchner, Art. 22 Rn. 19; BeckOK DatenschutzR-Lewinski, Art. 22 Rn. 12; Paal/Pauly-Martini, DSGVO Art. 22 Rn. 15c; Gola-Schulz, DSGVO Art. 22 Rn. 20.
127 Siehe dazu Kühling/Buchner-Buchner, Art. 22 Rn. 17.
128 Dammann, ZD 2016, 307, 312.
129 So etwa beim CASE-Score des Anbieters candidate select, siehe die Beschreibung auf der Website des Anbieters unter https://case-score.de/. Dazu Spiegel, Wie gut ist Ihr Schulabschluss, 2021, abrufbar unter https://www.spiegel.de/start/ki-bewertet-uni-noten-wie-gut-ist-ihr-hochschulabschluss-a-5b4176c9-0b46-4675-8537-3344397373fd, zuletzt abgerufen am 6.12.2021.

## 5. AUSNAHMEN VOM VERBOT DER AUTOMATISIERTEN ENTSCHEIDUNG

Auch wenn das Verbot der automatisierten Entscheidung in Art. 22 Abs. erhebliche Einschränkungen erfährt, ist die Streubreite des Verbots gleichwohl sehr groß, insbesondere wenn – entgegen der hier vertretenen Ansicht – alle Entscheidungen mit rechtlicher Wirkung darunter gefasst werden.

Es erstaunt daher nicht, dass Abs. 2 umfangreiche Ausnahmen vom Verbot regelt. Die automatisierte Entscheidung ist nicht verboten, wenn der Betroffene ausdrücklich einwilligt (Abs. 2 lit. c), oder wenn sie für den Abschluss oder die Durchführung eines Vertrags zwischen dem Betroffenen und dem Verarbeiter erforderlich ist (lit. a). Der Begriff der Erforderlichkeit wird in der Literatur denkbar weit ausgelegt. Die Entscheidung soll stets erforderlich sein, wenn sie „in unmittelbarem Zusammenhang mit der Entscheidungs- und Kalkulationsgrundlage" für ein bestimmtes Rechtsgeschäft steht.[130] Dies ist zweifellos ein interessanter Ansatz, der das Verbot des Art. 22 im vertraglichen Bereich weitestgehend aushebelt.

Dies wird besonders deutlich, wenn eine Erforderlichkeit in diesem Sinne vorliegen soll, wenn eine Kreditentscheidung auf der Grundlage eines Scoring getroffen wird.[131] Konsequent weitergeführt, können dann auch Arbeitsplätze vollständig automatisiert aufgrund einer ebenfalls automatisierten Bewertung von Kandidaten vergeben werden.

Angesichts der damit ausgelösten Schutzdefizite mag dieser Befund erschrecken. Jedoch bedeutet es lediglich, dass die Automatisierung im Bereich der vertraglichen Beziehungen nicht eingeschränkt wird und dass das Datenschutzrecht insbesondere nicht die formale Einschaltung menschlicher Mitarbeiter als Träger einer „Entscheidung" verlangt. Dies ist zu begrüßen. Zugleich wird deutlich, dass Art. 22 nicht geeignet ist, materiellen Schutz gegen fehlerhafte algorithmische Entscheidungen zu gewähren.

Darüber hinaus greift das Verbot automatisierter Entscheidungen nach Abs. 2 lit. b) nicht, soweit diese durch Rechtsvorschriften der Union oder der Mitgliedstaaten zugelassen sind und die Rechtsvorschriften angemessene Maßnahmen zum Schutz der Betroffenen enthalten. Diese recht unbestimmte Öffnungsklausel, die bei kritischer Betrachtung kaum mehr als ein qualifizierter Gesetzesvorbehalt für automatisierte Entscheidungsverfahren ist, belegt die ungeheure Schwierigkeit eines Verbots automatisierter Entscheidungen.

Die Lösung der DSGVO ist daher in gewisser Weise von Weisheit geprägt, denn die Öffnungsklausel des Abs. 2 lit. b) nimmt das von Abs. 1 normierte Verbot so stark zurück, dass der nationale Gesetzgeber die Chance hat, innovationsfeindliche Wirkungen zu vermeiden. Der Preis hierfür ist freilich die Zersplitterung der Rechtslage auch innerhalb der Union, die ihrerseits erhebliches Potenzial zur Innovationshemmung hat, gerade im Hinblick auf die Entwicklung neuer KI-Anwendungen.

## 6. DIE BEDEUTUNG DES ART. 22 DSGVO FÜR ALGORITHMISCHE ENTSCHEIDUNGEN

Versucht man eine Gesamtbetrachtung der sehr komplexen Regelung des Art. 22 und ihrer Bedeutung für algorithmische Entscheidungen, bleibt wie eingangs angedeutet vor allem viel Ungewissheit. Zu Recht sieht die Datenethik-Kommission in ihrem Gutachten Klarstellungs- und Konkretisierungsbedarf.[132]

### a. Eingeschränkte Reichweite des Verbots

Offensichtlich ist, dass Art. 22 nach dem bisherigen Normverständnis gravierende Schutzlücken hinterlässt: Ist eine lediglich formale Mitwirkung einer natürlichen Person ausreichend, wird materieller Schutz nicht bewirkt. Welcher Art die menschliche Mitwirkung sein muss, ist umstritten und unklar.

Weitere, ggf. noch gravierendere Defizite bestehen in Bezug auf Bewertungen, die nach h.M. von Art. 22 DSGVO nicht erfasst werden. Dies gilt insbesondere in Bezug auf die Nutzung von KI-Systemen für Bewertungen. Insoweit bestehen grundlegende Schwierigkeiten. Insbesondere kann der Entscheider, wenn eine Bewertung zugeliefert wird, diese kaum überprüfen. Wenn etwa ein Sachbearbeiter bei einer Kreditentscheidung eine Kreditwürdigkeitseinschätzung einer Ratingagentur vor sich hat, kann er diese schon deswegen nicht überprüfen, weil ihm weder die zugrunde liegenden Tatsachen noch die Berechnungsgrundlage bekannt ist. Dieses Problem gilt insbesondere bei Bewertungen

130 Kühling/Buchner-Buchner, Art. 22 Rn. 30; Plath-Kamalath, DSGVO Art. 22 Rn. 8; BeckOK IT-Recht-Steinrötter, DSGVO Art. 22 Rn. 18.
131 So ausdrücklich Kühling/Buchner-Buchner, Art. 22 Rn. 30.
132 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Executive Summary Nr. 52 (S. 28).

durch KI-Systeme, die auf maschinellem Lernen beruhen. Aufgrund des „Black-Box-Effekts“ des maschinellen Lernens besteht wenig Aussicht auf Überprüfung der Entscheidung über eine Plausibilitätsschätzung hinaus.

Diese Schutzlücke ist, wie dargestellt, letztlich richtig, weil die viel zu allgemeine Regelung der DSGVO nicht geeignet ist, hier eine sinnvolle Abgrenzung zu liefern. Zu Recht setzt der Gesetzgeber, wie in den sehr spezifischen Verboten von KI-Anwendungen in Art. 5 des KI-Gesetzes, auf differenzierende Lösungen.

### b. Gesetzlicher Handlungsbedarf

Das Anliegen des Art. 22 ist richtig: Wesentliche Entscheidungen über Menschen sollten nicht durch Maschinen getroffen werden. Ein „Robo(t) Judge“ sollte ebenso undenkbar sein wie eine Verwaltung, die wesentliche Entscheidungen allein von Maschinen treffen lässt.

#### aa). Flexible Regelung statt starren Verbots

Die gesetzliche Vorschrift des Art. 22 ist jedoch misslungen und bedarf der Nachbesserung. Fehlerhaft ist insbesondere die Wahl des starren Verbots in Abs. 1, die dem Grundanliegen widerspricht, das doch eine flexible, auf die Bedeutung der Angelegenheit abstellende Intensität menschlicher Beteiligung verlangt. Auch ist zu überlegen, ob die Norm nicht, entsprechend ihrem Wortlaut, als Anspruch auf menschliche Entscheidung denn als Verbot verstanden werden sollte.

Die wichtigste Nachbesserung wäre zweifellos die Abkehr vom Verbotsprinzip zugunsten einer flexiblen, risikobasierten Regelung, wie es auch die Datenethikkommission empfiehlt.[133] Insoweit wird hier vorgeschlagen, in Art. 22 Abs. 1 die automatisierte Entscheidung nicht zu verbieten, sondern ein der Bedeutung der Angelegenheit entsprechendes Maß an menschlicher Mitwirkung zu verlangen.

Mit etwas Mut ist dieses Verständnis sogar auf der Grundlage der derzeitigen Gesetzeslage realisierbar: Zwar lässt der Begriff der Ausschließlichkeit nach seinem Wortlaut kaum Interpretationsspielraum zu, jedoch zeigt schon die bisherige Diskussion, die zwischen einer lediglich formalen und einer inhaltlichen Befassung unterscheiden will, dass hier eine wertende Betrachtung gefordert ist. De lege lata ist daher anzunehmen, dass eine ausschließlich automatisierte Entscheidung i.S. des Art. 22 Abs. 1 DSGVO vorliegt, wenn eine Entscheidung von erheblicher Bedeutung für eine natürliche Person, die eine Bewertung von Eigenschaften dieser Person impliziert, nicht in einem der Bedeutung der Entscheidung entsprechenden Maße von einem menschlichen Entscheider geprägt wird.

#### bb). Ergänzung des Rechtsschutzes in Bezug auf automatisierte Bewertungen

Eine wesentliche Lücke des durch Art. 22 DSGVO bewirkten Rechtsschutzes betrifft automatisierte Bewertungen, die von der Norm nicht erfasst werden. Insbesondere fehlen Regeln zur Qualität automatisierter Bewertungen und von Systemen zur Erzeugung derartiger Bewertungen. Dieser wichtige Bereich sollte nicht im Datenschutzrecht, sondern in eigenständigen Regeln erfasst werden.

Der Entwurf des KI-Gesetzes erfasst einen wichtigen Teilbereich des Rechts automatisierter Bewertungen, da sich das Risikomanagement für Hochrisiko-KI-Systeme auch auf den Schutz der Persönlichkeit bezieht und insoweit der Hersteller von Systemen zur Erzeugung automatisierter Bewertungen adressiert wird. Jedoch werden weder qualitative Anforderungen an automatisierte Bewertungen noch Betreiber von Systemen, die solche Bewertungen erzeugen und vertreiben, erfasst. Angesichts des hilflosen Umgangs des Gesetzgebers mit Scoring und Rating, das in der DSGVO gar nicht spezifisch geregelt ist und mangels eines spezifischen gesetzlichen Rahmens in einem Umfeld größter Rechtsunsicherheit betrieben wird, besteht hier Handlungsbedarf, nicht zuletzt Forschungsbedarf zur Vorbereitung eines spezifischen Rechtsrahmens für automatisierte Bewertungen.

#### cc). Entwicklung eines Rechtsrahmens für automatisierte Entscheidungen

Automatisierte Bewertungen sind letztlich nur ein Spezialfall des größeren Feldes automatisierter Entscheidungen. Auch insoweit gilt das zu Bewertungen Gesagte: Das Verbot des Art. 22 DSGVO, der ein Fremdkörper im Gesetz ist und im Kern keine spezifisch datenschutzrechtlichen Fragen adressiert, ist zu ersetzen durch einen umfassenderen Rechtsrahmen für automatisierte Entscheidungen, der auch die nachfolgenden Aspekte der inhaltlichen Angemessenheit von Entscheidungen adressiert. In einem solchen rechtlichen Rahmen erhielte der von Art. 22 DSGVO intendierte Schutz

133 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, Executive Summary Nr. 52 (S. 28).

des Einzelnen vor einer maschinellen Bestimmung seiner Lebensverhältnisse in Form eines Gebots angemessener Beteiligung menschlicher Entscheider in wichtigen Entscheidungen seinen adäquaten Platz.

## IV. VERWENDUNG FEHLERHAFTER DATEN IN ALGORITHMISCHEN ENTSCHEIDUNGEN

### 1. FALLGRUPPEN

Die Verwendung fehlerhafter Daten in algorithmischen Entscheidungen kann in ganz unterschiedlicher Hinsicht von Bedeutung sein. Von Interesse sind insbesondere falsche Angaben zu Tatsachen, die in eine Entscheidung eingehen und ggf. deren Ausgang beeinflussen.

So können fehlerhafte Daten des Betroffenen, der Gegenstand der Entscheidung ist, verwendet werden. Wenn etwa bei Personalentscheidungen eine falsche Examensnote verwendet wird, bei Kreditentscheidungen oder Kreditwürdigkeitseinschätzungen ein unzutreffendes Einkommen zugrunde gelegt wird oder bei Entscheidungen zur Zulassung zu altersabhängigen Diensten ein unzutreffendes Alter zugrunde gelegt wird, ist offensichtlich, dass die Entscheidung fehlerhaft im Sinne der Abweichung von den Zielen des Entscheiders, ebenso auch rechtswidrig sein kann, indem sie etwa dem Betroffenen rechtliche Vorteile verwehrt, auf die er einen Anspruch hat oder die ihm bei Verwendung richtiger Daten gewährt worden wären. Auch sonstige, nicht auf den Betroffenen bezogene Daten können zu fehlerhaften Entscheidungen führen, etwa falsche Examensnoten von Konkurrenten bei einer Auswahlentscheidung.

Hiervon gedanklich zu unterscheiden sind Fehler in den Entscheidungskriterien selbst. Zu dieser Fallgruppe gehört etwa der Fall der Diskriminierung, bei der einem bestimmten Datum unzulässigerweise eine Bedeutung für die Entscheidungsfindung beigemessen wird. Hierzu gehören auch, über die Diskriminierung hinaus, Aspekte, die als „bias“ bezeichnet werden können. Wenn etwa ein Entscheider meint, dass die Farbe der Krawatte eines Bewerbers oder dessen Zugehörigkeit zu einer bestimmten politischen Partei Entscheidendes über die Eignung als Richter oder Datenschutzbeauftragter aussage, würde man wohl von einem bias ausgehen.

Diese Arten von Fehlern betreffen nicht die tatsächliche Entscheidungsgrundlage, sondern die Würdigung der Tatsachen. Sehr deutlich wird dies bei der Diskriminierung: Hier ist das Datum richtig, unzutreffend ist die Bedeutung, die diesem in der Entscheidung beigemessen wird.

Während die meisten der hier genannten Fragen keinen spezifischen Bezug zu algorithmischen Entscheidungen haben, ergibt sich für den Bereich der Diskriminierung und des bias eine Besonderheit, die mit dem Stichwort „bias in the data“ bezeichnet wird. Dabei geht es um Voreingenommenheit aufgrund der beim maschinellen Lernen verwendeten Datengrundlage. Man kann daher von einem Fehler in der Datengrundlage sprechen. Da diese Daten aber nicht als solche in die Entscheidung eingehen, ist diese Fallgruppe von der hier interessierenden zu unterscheiden und wird (unten 6.) separat erörtert.

Im Zusammenhang mit Fehlern in der tatsächlichen Entscheidungsgrundlage sind zwei Fragestellungen von besonderem Interesse: zum einen, inwieweit die Berichtigung oder Löschung falscher Tatsachen geboten ist und gegebenenfalls von Betroffenen einer Entscheidung verlangt werden kann, und zum anderen, inwieweit die Entscheidung als solche wegen einer fehlerhaften Tatsachengrundlage angreifbar ist.

### 2. BERICHTIGUNG UND LÖSCHUNG FEHLERHAFTER TATSACHENGRUNDLAGEN

In Bezug auf die Berichtigung und Löschung fehlerhafter Tatsachengrundlagen ist die Rechtslage entscheidend unterschiedlich, je nachdem, ob es sich um personenbezogene Daten des von der Entscheidung Betroffenen handelt oder um sonstige Daten. Daher werden diese Fallgruppen separat erörtert.

#### a. Fehlerhafte Daten zu Betroffenen in Entscheidungen

Soweit Daten verarbeitet werden, die als personenbezogene Daten des von der Entscheidung Betroffenen anzusehen sind, unterliegt diese Datenverarbeitung und damit auch die gesamte Ent-

scheidungsfindung dem Datenschutzrecht. Insbesondere greifen die datenschutzrechtlichen Regeln zu fehlerhaften Tatsachen ein. Da der Bereich des personenbezogenen Datums extrem weit ist, sind kaum Daten vorstellbar, die in eine algorithmische Entscheidung zu einer natürlichen Person eingehen und nicht in irgendeiner Weise Personenbezug aufweisen. Allemal sind Angaben zur Person und zu den Umständen des Betroffenen erfasst.

In dieser Fallgruppe hat das Datenschutzrecht zweifellos eine große Stunde. Die Verwendung korrekter personenbezogener Daten gehört zu den Grundsätzen des Datenschutzrechts. Art. 5 Abs. 1 lit. d) DSGVO beschreibt den Grundsatz der Richtigkeit von Daten; danach sind sachlich richtige und erforderlichenfalls aktuelle Daten zu verarbeiten, Daten, die im Hinblick auf die Verwendung unrichtig sind, müssen unverzüglich gelöscht oder berichtigt werden.

Zur praktischen Umsetzung des Grundsatzes der Richtigkeit der Daten gewährt die DSGVO dem Betroffenen weitreichende Rechte. So regelt Art. 16 DSGVO das Recht des Betroffenen auf Berichtigung fehlerhafter Daten. Soweit nach dem Zweck der Datenverarbeitung erforderlich, schließt das Recht, wie S. 2 ausdrücklich bestimmt, auch einen Anspruch auf Vervollständigung der Daten ein.

Bei fehlerhaften Daten kann dem Betroffenen ein Anspruch auf Löschung aus Art. 17 DSGVO zustehen. So fehlt es bei fehlerhaften Daten regelmäßig an der Notwendigkeit deren Verarbeitung, sodass sich der Anspruch aus Art. 17 Abs. 1 lit. a) DSGVO ergibt. Da, wie bereits dargestellt, die Datenverarbeitung meist auch unrechtmäßig ist, ergibt sich ein Löschungsanspruch ferner aus Art. 17 Abs. 1 lit. d) DSGVO.[134] Der Betroffene hat das Recht zur Wahl zwischen Berichtigung und Löschung.[135]

Die Rechte aus Artt. 16 und 17 DSGVO stehen jeweils „dem“ Betroffenen zu, also der Person, als deren personenbezogene Daten die fehlerhaften Daten anzusehen sind. Der Betroffene kann daher wohl nicht die Korrektur oder Löschung von Daten anderer Betroffener verlangen. Im Beispiel fehlerhafter Daten von Konkurrenten in einer Auswahlentscheidung hat der Betroffene daher die Rechte aus Artt. 16 und 17 nicht.

Unabhängig vom Datenschutzrecht wird sich ein Anspruch auf Korrektur oder Löschung fehlerhafter Daten regelmäßig aus dem Rechtsverhältnis ergeben, in dessen Rahmen die Entscheidung ergeht. So wird man aus dem vorvertraglichen Rechtsverhältnis einer Bewerbung um einen Arbeitsplatz das Recht herleiten können, dass der Arbeitgeber korrekte Daten des Bewerbers zugrunde legt.

Ob sich aus dem Persönlichkeitsrecht ein allgemeiner Anspruch auf Verwendung korrekter Daten ergibt, ist, soweit ersichtlich, nicht geklärt. Im Anwendungsbereich der DSGVO ist auch fraglich, ob ein solcher Anspruch neben der DSGVO anwendbar wäre.

Die hier genannten Grundsätze gelten uneingeschränkt für algorithmische Entscheidungen.

### b. Sonstige fehlerhafte Daten in Entscheidungen

Soweit in Entscheidungen zu einer natürlichen Person fehlerhafte Daten eingehen, die nicht als personenbezogen anzusehen sind, greift das Datenschutzrecht nicht ein. Datenschutzrechtliche Ansprüche des Betroffenen bestehen, wie soeben gezeigt, ferner nicht bei Daten mit Bezug zu anderen Personen. In diesen Fällen sind Ansprüche auf Verwendung korrekter Daten aus anderer Rechtsgrundlage von größerer Bedeutung.

Die Frage, ob und inwieweit sich ein allgemeiner Anspruch auf Verwendung einer korrekten Datengrundlage etwa aus dem Persönlichkeitsrecht des Betroffenen ergibt, ist, soweit ersichtlich, nicht geklärt. Man wird einen solchen Anspruch wohl nicht annehmen können, da sonst die Freiheit desjenigen, der Daten verarbeitet, zu stark eingeschränkt wäre. Auch ein allgemeiner Anspruch auf „korrekte Tatsachengrundlage“ bei Bewertung oder sonstigen Entscheidungen über eine natürliche Person lässt sich wohl nicht aus dem allgemeinen Persönlichkeitsrecht des Betroffenen ableiten. Vielmehr kann sich ein solcher Anspruch nur aus der konkreten Situation ergeben. Im Vordergrund stehen dabei Rechte aus einem Rechtsverhältnis, in dessen Rahmen eine Entscheidung getroffen wird. Hier, etwa in einem Arbeits- oder Dienstverhältnis, hat der Betroffene regelmäßig einen Anspruch auf Berücksichtigen korrekter Tatsachen bei ihn betreffenden Entscheidungen.

134 Kühling/Buchner-Herbst, Art. 17 Rn. 29.
135 Kühling/Buchner-Herbst, Art. 17 Rn. 29.

Diese Fragen, die offensichtlich nicht spezifisch für algorithmische Entscheidungen sind, sondern sich bei menschlichen Entscheidungen ebenso stellen, können im Rahmen dieses Gutachtens nicht im Einzelnen untersucht werden. Festzuhalten ist aber, dass derartige Pflichten zur Verwendung korrekter Tatsachengrundlagen, die sich etwa aus dem Arbeitsrecht, ebenso in Verwaltungsverfahren ergeben, uneingeschränkt auch für algorithmische Entscheidungen gelten.

### 3. FEHLERHAFTE TATSACHENGRUNDLAGE UND RECHTMÄSSIGKEIT EINER ENTSCHEIDUNG

Eine weitere höchst schwierige Frage ist, inwieweit eine Entscheidung bei Verwendung einer fehlerhaften Tatsachengrundlage ihrerseits rechtswidrig oder angreifbar ist. Eine allgemeine gesetzliche Regelung besteht insoweit nicht.

Ohne Zweifel ist eine Entscheidung rechtswidrig, wenn die Verwendung fehlerhafter Tatschen dazu führt, dass die Entscheidung inhaltlich gegen rechtliches Gebot verstößt, etwa einen Anspruch versagt, der nach der objektiven Tatsachenlage bestünde. Die Verwendung fehlerhafter Tatsachen als solche führt andererseits meist nicht zur Rechtswidrigkeit der Entscheidung, wenn diese auch bei Zugrundelegung der korrekten Tatsachen in der gleichen Weise hätte getroffen werden können.

Da die Frage der Rechtswidrigkeit oder der Angreifbarkeit einer Entscheidung von zahlreichen Faktoren abhängt, insbesondere bei staatlichen Entscheidungen wie Verwaltungsentscheidungen und gerichtlichen Entscheidungen, und nicht zuletzt auch das Vertrauen in den Bestand der Entscheidung[136] zu schützen ist, lässt sich eine allgemeingültige Antwort auf die Frage nach dem Ob und den Voraussetzungen der Rechtswidrigkeit oder Angreifbarkeit einer Entscheidung nicht geben.

Dieser Befund scheint auch für algorithmische Entscheidungen zu gelten. Indes ist de lege ferenda zu fragen, ob algorithmische Entscheidungen in Bezug auf die Verwendung fehlerhafter Daten wirklich wie menschliche Entscheidungen zu behandeln sind oder ob es eines spezifischen Rechtsrahmens bedarf. Ausgangspunkt dieser Frage ist die Eigentümlichkeit maschineller im Vergleich zu menschlichen Entscheidungen. Dazu gehört der Umstand, dass maschinelle Entscheidungen im Grundsatz reproduzierbar sind. Auch bei KI-Systemen, die ihre Fähigkeiten aufgrund maschinellen Lernens erworben haben, wird das System unter denselben tatsächlichen Voraussetzungen dieselbe Entscheidung treffen, jedenfalls soweit es sich nicht weiter verändert hat. Die damit verbundene Aussicht auf das Testen von maschinellen Entscheidungen sollte auch Auswirkungen auf das Recht auf Überprüfung von Entscheidungen haben, jedenfalls soweit nicht andere Grundsätze, wie etwa der Vertrauensschutz in die getroffene Entscheidung, dies verbieten.

Diese Fragestellung hat, soweit ersichtlich, noch keine größere Beachtung gefunden, was angesichts der derzeit noch eher geringen praktischen Erfahrungen mit dem Einsatz algorithmischer Entscheidungen nicht verwundert. Es darf erwartet werden, dass die Frage nach Überprüfung algorithmischer Entscheidungen auf deren Korrektheit im Hinblick auf die Tatsachengrundlage künftig intensiver zu diskutieren sein wird.

### 4. AUSKUNFT ÜBER DIE TATSÄCHLICHE ENTSCHEIDUNGSGRUNDLAGE

Ein praktisches Kernproblem des Schutzes gegen fehlerhafte Entscheidungen betrifft die Kenntnis der Tatsachengrundlage des durch die Entscheidung Betroffenen. Soweit diesem die Tatsachengrundlage nicht bekannt ist, kann er sich gegen Fehler derselben nicht effektiv zur Wehr setzen, soweit er die Darlegungs- und Beweislast für das Vorliegen eines solchen Fehlers trägt.

Soweit es um personenbezogene Daten des Betroffenen geht, hilft das Datenschutzrecht zumindest zum Teil: Art. 15 Abs. 1 DSGVO gewährt dem Betroffenen ein umfassendes Auskunftsrecht über die Verarbeitung der ihn betreffenden personenbezogenen Daten. Art. 15 Abs. 3 DSGVO erweitert das Recht um den Anspruch auf Herausgabe einer Kopie der Daten, die Gegenstand der Verarbeitung sind.

Ob und inwieweit Artikel 15 DSGVO das Recht gewährt, die tatsächliche Grundlage einer konkreten Entscheidung zu erfahren, ist zweifelhaft. Art. 15 Abs. 1 enthält jedenfalls kein derartiges Recht, sondern beschränkt sich auf die in lit. a) bis h) genannten Informationen. Art. 15 Abs. 3 verpflichtet

136 Die ZPO lässt die Wiederaufnahme rechtskräftig abgeschlossener Verfahren nur aus den in §§ 579, 580 ZPO geregelten Gründen zu; die Zugrundelegung falscher Tatsachen gehört nur indirekt dazu, wenn diese wegen einer falschen Urkunde (§ 580 Nr. 2 ZPO) oder falschen eidlichen Aussage (§ 580 Nr. 1) berücksichtigt wurde.

zwar zur Bereitstellung einer Kopie der Daten, die Gegenstand „der" Verarbeitung sind. Auch damit ist indes die Gesamtheit der vom Verantwortlichen verarbeiteten Daten des Betroffenen gemeint, nicht die Auswahl der für eine bestimmte Entscheidung herangezogenen Daten.

Ein Anspruch auf Mitteilung der für eine konkrete Entscheidung herangezogenen Tatsachen ergibt sich häufig aus dem Rechtsverhältnis, in dessen Rahmen die Entscheidung ergangen ist. So ist im Verwaltungsverfahren die Behörde häufig zur Begründung ihrer Entscheidung verpflichtet. Ein wesentliches Element der Begründung ist die Darstellung der tatsächlichen Entscheidungsgrundlage. Im Privatrecht ist die Fragestellung wesentlich differenzierter: Ein allgemeiner Anspruch auf Begründung einer Entscheidung besteht nicht, ebenso wenig ein Anspruch auf Darstellung der tatsächlichen Entscheidungsgrundlage.

Diese Rechtslage gilt auch für algorithmische Entscheidungen. Auch insoweit ist zu überlegen, ob bei algorithmischen Entscheidungen de lege ferenda eine andere Rechtslage anzustreben ist; konkret, ob eine Pflicht zur Dokumentation der tatsächlichen Entscheidungsgrundlage und ein Anspruch des Betroffenen auf Auskunft gelten sollten.

Der Grund für eine solche Sonderregel im Unterschied zu menschlichen Entscheidungen ist offensichtlich: Es ist bei Entscheidungen, die von Maschinen getroffen werden, mit wesentlich geringerem Aufwand möglich und daher unter geringeren Voraussetzungen zumutbar, die tatsächliche Grundlage einer Entscheidung zu speichern und mitzuteilen. Dies muss Auswirkungen auf den vom Recht vorzunehmenden Interessenausgleich haben. Auch insoweit ist indes Augenmaß geboten. Schon aus Gründen des Datenschutzes, aber auch aus Gründen der Ressourcenschonung, sollten nicht blindlings alle in algorithmische Entscheidungen eingehenden Daten auf unabsehbare Zeit gespeichert werden. Insoweit besteht offensichtlich noch erheblicher Forschungsbedarf.

## V. DISKRIMINIERUNG IN ALGORITHMISCHEN ENTSCHEIDUNGEN

### 1. SORGE VOR DISKRIMINIERUNG DURCH KI-SYSTEME

Die Angst vor Diskriminierung durch algorithmische Entscheidungen gehört zu den in der Öffentlichkeit besonders intensiv diskutierten Risiken von KI-Systemen. Sie wird insbesondere dann relevant, wenn KI-Systeme zur Bewertung von Menschen eingesetzt werden. Weithin bekannt ist das US-amerikanische COMPAS-System, das zur Ermittlung der Rückfallwahrscheinlichkeit von Strafgefangenen eingesetzt wurde.[137] Ähnlich liegt es, wenn KI-Systeme eine Vorauswahl von Bewerbern treffen oder in einem Jobportal darüber entscheiden, welche offenen Stellen einem Nutzer angezeigt werden.

Das System COMPAS wurde bekannt, als eine Untersuchung nachwies, dass die Hautfarbe der Strafgefangenen auffällig stark mit der Einschätzung der Rückfallwahrscheinlichkeit korrelierte und daraus ableitete, dass die Hautfarbe ein wesentlicher Faktor für die Einschätzung der Maschine war.[138] War die Hautfarbe tatsächlich maßgebend für die Bewertung und damit mittelbar für die Entscheidung über die Haftentlassung, liegt eine Diskriminierung vor.

Auch bei automatisierten Auswahlentscheidungen, etwa im Arbeitsbereich, bestehen Risiken der Diskriminierung durch KI-Systeme, die derzeit Gegenstand der Forschung sind.

### 2. DER BEGRIFF DER DISKRIMINIERUNG

Eine zentrale Problematik der Forschung besteht darin, dass der Begriff der Diskriminierung im rechtlichen Sinne nicht leicht zu fassen ist. Das Gesetz verwendet den ihn nur in seltenen Ausnahmefällen,[139] typischerweise spricht das Gesetz von „Benachteiligung".[140] Das entscheidende und charakteristische Merkmal der Diskriminierung ist der Grund für die Benachteiligung. Das Grundgesetz etwa wendet sich ausdrücklich gegen die Benachteiligung aus bestimmten Motiven, etwa

137 Dressel/Farid, Science Advances 2018 (4), 1 ff.

138 Angwin/Larson/Mattu/Kirchner, Machine Bias, 2016, abrufbar unter Machine Bias — ProPublica, zuletzt abgerufen am 6.12.2021; kritisch dagegen etwa Flores/Lowenkamp/Bechtel, False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks.", Federal Probation 2016 (80), 38 ff., abrufbar unter: 80_2_6_0.pdf (uscourts.gov); ebenfalls kritisch Dressel/Farid, Science Advances 2018 (4), 1 ff.

139 So etwa in der amtlichen Überschrift zu § 4 TzBfG, nicht hingegen im Normtext.

140 So insbesondere in § 3 AGG, der zwischen unmittelbaren (Abs. 1) und mittelbaren (Abs. 2) Benachteiligungen unterscheidet.

wegen des Geschlechts oder wegen der religiösen Anschauungen (Art. 3 Abs. 3 GG). Ein Verbot der Benachteiligung aufgrund des Alters („Altersdiskriminierung") hingegen ist im Grundgesetz nicht explizit geregelt,[141] wohl aber im Unionsrecht[142] Eine Unterscheidung etwa anhand des Alters ist in vielen Fällen jedoch völlig unbedenklich: Dass Gesetze zu Zwecken des Kinder- und Jugendschutzes an das Lebensalter anknüpfen, liegt in der Natur der Sache.

Daher kann der Begriff der Diskriminierung aus rechtlicher Sicht als eine nicht gerechtfertigte Benachteiligung aufgrund eines unzulässigen Differenzierungsmerkmals definiert werden.

Indes: Auch eindeutige Diskriminierung ist in vielen Fällen erlaubt. Artikel 3 des Grundgesetzes verbietet zwar Diskriminierung in dem hier definierten Sinne, bindet unmittelbar aber nur den Staat, nicht den Bürger, und damit weder Vermieter noch Arbeitgeber. Das „Allgemeine Gleichbehandlungsgesetz" (AGG), das auch den Bürger bindet, gilt im Arbeitsrecht und darüber hinaus in wichtigen Bereichen, insbesondere bei sogenannten Massengeschäften. Für die meisten Rechtsgeschäfte gilt das Gesetz jedoch nicht.

Damit wird offensichtlich, dass das Vorliegen einer Diskriminierung im rechtlichen Sinne das Ergebnis einer unter Umständen komplexen Prüfung ist.

## 3. DISKRIMINIERUNG DURCH KI-SYSTEME

Diskriminierung durch KI-Systeme ist leicht vorstellbar, wenn diese zur Entscheidung über natürliche Personen oder zur Vorbereitung einer solchen eingesetzt werden. Wenn ein KI-System zur Selektion von Bewerbern um eine Mietwohnung oder einen Arbeitsplatz alle Kandidaten mit ausländischer Staatsangehörigkeit oder oberhalb eines bestimmten Alters verwirft,[143] ist dies regelmäßig nicht zu rechtfertigen, und in diesen Beispielen verbietet das AGG, soweit es im konkreten Fall anwendbar ist, die darin liegende Benachteiligung.

Derartige Diskriminierung durch KI ist keine lediglich theoretische Möglichkeit. Die aktuelle Forschung zu algorithmic bias oder fehlerhaften algorithmischen Entscheidungen verweist vielfach darauf, dass die KI beim maschinellen Lernen vorhandene Diskriminierung oder Voreingenommenheit (bias) tradieren könnte.

Die Gefahr verborgener Voreingenommenheit ist mit dem maschinellen Lernen untrennbar verbunden. Maschinelles Lernen beruht auf der Erkennung von Mustern aus Daten. Im Trainingsprozess wird das künstliche neuronale Netz das stabilste Muster wählen, das zur jeweiligen Klassifikationsentscheidung passt. Das kann leicht „schiefgehen": Ein sehr bekanntes Beispiel ist das KI-gestützte Erkennen von Pferden auf Fotos: Hier erkannte das neuronale Netz Pferde anhand des Copyright-Vermerks, der auf den Fotos enthalten war. Die Trefferquote war sehr hoch innerhalb der Trainingsdaten. Das System versagte aber, als Fotos ohne solchen Vermerk zu beurteilen waren.[144]

Das Beispiel illustriert das ungeheure Fehlerpotenzial des maschinellen Lernens: Es gibt keine a-priori-Garantie, dass das stabilste Muster den gewünschten Entscheidungsgründen entspricht. Folglich kann nicht ausgeschlossen werden, dass das System beim Training ein für die Trainingsdaten stabiles, aber diskriminierendes Unterscheidungsmerkmal (z.B. Hautfarbe) erlernt.

Das ist unproblematisch, wenn KI-Systeme zur Erzeugung von Kunstwerken eingesetzt werden, kann aber nicht hingenommen werden, wenn KI-Systeme Bewertungen zu natürlichen Personen mit für diese nachteiligen Folgen treffen.

## 4. DATENSCHUTZ UND DISKRIMINIERUNGSSCHUTZ

Aus der Sicht des Datenschutzrechts ist von Interesse, ob und inwieweit Diskriminierung durch KI-Systeme durch das Datenschutzrecht verhindert oder eingeschränkt werden kann.

Eine erste Schranke ergibt sich aus dem Verbot automatisierter Entscheidungen nach Art. 22 DSGVO: Soweit damit eine Kontrolle durch eine natürliche Person gewährleistet ist, besteht insoweit eine

141 Für ein implizites Verbot etwa v. Mangoldt/Klein/Starck-Baer/Markard, Art. 3 Rn. 551 f.; gegen ein „Quasi-Diskriminierungsverbot" aber BeckOK GG-Kischel, Art. 3 Rn. 140.

142 Vgl. hier insbesondere Art. 19 Abs. 1 AEUV, Art. 21 Abs. 1 GRCh.

143 Siehe zu möglichen Szenarien eines KI-Einsatzes mit Diskriminierungspotential Zweig/Hauer/Raudonat, Anwendungsszenarien KI-Systeme im Personal- und Talentmanagement, 2020, abrufbar unter https://testing-ai.gi.de/fileadmin/PR/Testing-AI/ExamAI_Publikation_Anwendungsszenarien_KI_HR.pdf, zuletzt abgerufen am 7.12.2021.

144 Hierzu Lapuschkin/Wäldchen/Binder/Montavon/Samek/Müller, Nature Communications 10, 1096 (2019), abrufbar unter https://www.nature.com/articles/s41467-019-08987-4.pdf, zuletzt abgerufen am 7.12.2021.

Chance auf Fehlerkorrektur. Dieses Schwert dürfte jedoch recht stumpf sein: Da KI-Systeme, soweit ihre Entscheidung oder Einschätzung auf maschinellem Lernen beruht, ihre Entscheidungsgründe nicht mitteilen, ist die Überprüfung der Entscheidung schwierig. Die Forschung zu Explainable AI versucht, hier Abhilfe zu schaffen, steckt aber noch in den Kinderschuhen.[145] Derzeit wird vor allem daran gearbeitet, Diskriminierung durch das Testen von KI-Systemen aufzudecken.[146] Die erforderliche Testinfrastruktur besteht derzeit aber noch nicht.

Eine entscheidende Frage geht dahin, ob dem Datenschutzrecht materielle Diskriminierungsverbote entnommen werden können. Diese Frage ist eindeutig zu verneinen, insoweit gelten spezielle Regeln.

Das Datenschutzrecht bietet mittelbaren Schutz vor Diskriminierungen. An einer Datenverarbeitung, die zu rechtswidrigen Ergebnissen führt, besteht etwa im Rahmen des Art. 6 Abs. 1 S. 1 lit. f) DSGVO regelmäßig kein legitimes Interesse, und vor allem stehen Betroffeneninteressen entgegen.[147] Auch dient der besondere Schutz besonderer Kategorien von personenbezogenen Daten in Art. 9 DSGVO der Vermeidung von Diskriminierung.[148]

Von Bedeutung ist auch, dass dem Datenschutzrecht durchaus Anforderungen an die Qualität automatisierter Bewertungsverfahren zu entnehmen sind. Das klassische Beispiel ist hier das Scoring, das sowohl im BDSG a.F. als auch im BDSG n.F. eine besondere Regelung erfahren hat. Interessant ist, dass zwar § 31 BDSG n.F. mangels Öffnungsklausel in der DSGVO unanwendbar ist,[149] dieselben Anforderungen aber aus Art. 6 DSGVO abgeleitet werden können.[150] Wenn dem so ist, können entsprechende Anforderungen auch für andere Fälle automatisierter Bewertung abgeleitet werden.

Auch hier gilt aber, dass es materieller Anforderungen bedarf, an denen das Datenschutzrecht anknüpfen kann. Soweit etwa eine Diskriminierung rechtlich nicht untersagt ist, ist schwer vorstellbar, dass sich aus Art. 6 DSGVO Anforderungen an die Vermeidung der Diskriminierung ableiten lassen.

## 5. FAZIT

Damit ergibt sich, dass das Datenschutzrecht durchaus wirksame Mittel zur Bekämpfung diskriminierender oder sonst fehlerhafter Bewertungen von Menschen durch KI-Systeme bietet. Diese laufen jedoch leer, soweit die materiellrechtlichen Anforderungen in Bezug auf eine Diskriminierung an die konkrete Datenverarbeitung nicht klar sind.

Der bessere Ansatzpunkt sind Grundsätze zum Risikomanagement in Bezug auf Diskriminierung, wie sie im Entwurf des KI-Gesetzes angelegt sind. KI-Systeme, die eine Bewertung zu natürlichen Personen erzeugen, sind regelmäßig als Hochrisiko-KI-Systeme im Sinne des vorgeschlagenen KI-Gesetzes einzustufen, wenn die Bewertung zu Entscheidungen über den Zugang zu Bildungseinrichtungen,[151] zu selbstständiger oder unselbstständiger Arbeit[152] oder zu grundlegenden privaten und öffentlichen Diensten und Leistungen[153] herangezogen wird, ebenso hinsichtlich der Durchführung individueller Risikobewertungen bei der Strafverfolgung[154] oder der Abschätzung von Risiken im Zusammenhang mit Migration, Asyl und Grenzkontrollen.[155] und unterliegen den dort geregelten Pflichten auch in Bezug auf den Persönlichkeitsschutz. Auch insoweit ist derzeit noch unklar, welche konkreten Pflichten in Bezug auf die Vermeidung von Diskriminierung bestehen.

145 Siehe einen Überblick etwa bei Langer/Oster/Speith et al., What do we want from Explainable Artificial Intelligence (XAI)? – A stakeholder perspective on XAI and a conceptual model guiding interdisciplinary XAI research, AI 296 (2021), 103473.

146 Dies ist Gegenstand etwa des vom Bundesministerium für Arbeit und Soziales geförderten Forschungsprojekts „ExamAI: KI Testing und Auditing"; siehe hierzu den Abschlussbericht des Projekts (2021), abrufbar unter https://gi.de/fileadmin/PR/Testing-AI/Abschlussbericht_ExamAI_-_KI_Testing_und_Auditing.pdf, zuletzt abgerufen am 7.12.2021.

147 Vgl. Erwägungsgrund 75 DSGVO; s. ferner Ehmann/Selmayr-Heberlein, DSGVO, 2. Aufl. 2018, Art. 6 Rn. 28.

148 Martini/Nink, NVwZ 2017, 681, 682; BeckOK DatenschutzR-Schild, Art. 4 DSGVO Rn. 188.

149 H.M.; Kühling/Buchner-Buchner/Petri, Art. 6 DSVO Rn. 161; Auer-Reinsdorff/Conrad-Conrad, § 34 Rn. 763; Moos/Rothkegel, ZD 2016, 561, 568 f.; Piltz, § 31 BDSG Rn. 38.

150 Nach verbreiteter Ansicht soll § 31 BDSG n.F. als „Auslegungshilfe" zu Art. 6 DSGVO dienen; vgl. Kühling/Buchner-Buchner, § 31 BDSG Rn. 6; Auer-Reinsdorff/Conrad-Conrad, § 34 Rn. 766; Plath-Kamlah, § 31 Rn. 6.

151 Vgl. Anhang III, Ziff. 3 des KI-Gesetzes.

152 Anhang III, Ziff. 4 des KI-Gesetzes.

153 Anhang III, Ziff. 5 des KI-Gesetzes.

154 Anhang III, Ziff. 6 lit. a) des KI-Gesetzes.

155 Anhang III, Ziff. 7 des KI-Gesetzes.

## VI. BIAS IN THE DATA – FEHLER IN DER DATENGRUNDLAGE LERNENDER SYSTEME

### 1. DIE BEDEUTUNG DER DATENGRUNDLAGE FÜR DAS MASCHINELLE LERNEN

Das Stichwort „bias in the data" weist auf ein Problem hin, das sich beim maschinellen Lernen ergeben kann. Beim maschinellen Lernen wird, anders als bei herkömmlicher Programmierung, das Programm nicht vorab festgelegt. Vielmehr wird ein sogenanntes neuronales Netz mit einem Ziel ausgestattet, und das Netz erzeugt den Algorithmus, nach dem es vorgeht, letztlich selbst.[156] Dieser wiederum ist für Menschen nur sehr eingeschränkt – de facto nicht – lesbar, woraus sich der gefürchtete Black-Box-Effekt von Systemen, die auf maschinellem Lernen beruhen, ergibt.[157]

Der Lernvorgang beim maschinellen Lernen beruht entscheidend auf der Mustererkennung anhand von Daten, den sogenannten Trainingsdaten.[158] So kann etwa ein neuronales Netz anhand zahlreicher Fotos von Pferden lernen, den auf einem Foto dargestellten Gegenstand als Pferd zu klassifizieren, indem es typische Muster der Abbildungen identifiziert.[159] Natürlich sind Fehler möglich und kommen häufig vor, wie etwa in dem (oben 5.) schon genannten Fall, in dem ein neuronale Netz die Klassifikation nicht aus den Eigenschaften der abgebildeten Pferde, sondern aus einem auf den Bildern enthaltenen Copyright-Vermerk ableitete.

Entscheidend für maschinelles Lernen ist also die Qualität der Trainingsdaten.[160] Das in der Diskussion immer wieder genannte Beispiel betrifft das bereits im Zusammenhang mit Diskriminierung genannte System COMPAS (dazu oben V.1). Nimmt man hier an, dass die Hautfarbe ein wesentlicher Faktor für die Einschätzung der Maschinen war, wies die Einschätzung der Rückfallwahrscheinlichkeit einen „bias" auf.[161] Ein solcher bias in Entscheidungen eines auf maschinellem Lernen beruhenden KI-Systems beruht auf einem – typischerweise nicht bekannten – Muster in den im Lernprozess verwendeten Daten. Daher wird mitunter von einem „bias in the data" gesprochen.[162]

### 2. DIE RECHTLICHE EINORDNUNG EINES BIAS IN THE DATA

Die rechtliche Einordnung eines solchen bias hängt entscheidend vom Gegenstand und dem Ziel der Betrachtung ab. Sie ist schon deswegen schwierig, weil es sich nicht um einen Rechtsbegriff handelt, ebenso wie der verwandte, in der Informatik verwendete Begriff der „algorithmic fairness".[163] Übersetzt man den Begriff des bias mit „Voreingenommenheit" oder „Fehlerhaftigkeit", so ist der natürliche Bezugspunkt zunächst die Entscheidung des KI-Systems, die an einem solchen bias leiden mag.[164]

Als ein möglicher Fehler einer solchen Entscheidung ist hier also eine Voreingenommenheit des Entscheiders zu prüfen; insoweit kann auf die vorangegangenen Ausführungen zu Fehlern in algorithmischen Entscheidungen, insbesondere zur Diskriminierung, verwiesen werden (oben V.3). Dabei zeigte sich, dass das Datenschutzrecht sich nicht auf den Inhalt der Entscheidung bezieht, sondern lediglich auf die Richtigkeit der Tatsachengrundlage (oben V.4).

Ein weiterer Ansatzpunkt für die rechtliche Betrachtung eines bias ist das KI-System selbst, dessen Entscheidungen an einem bias leiden; darauf weist der Begriff des „machine bias" hin.[165] Anforderungen an ein KI-System werden sich aus dem geplanten KI-Gesetz ergeben, das Anbietern von Hochrisiko-KI-Systemen umfassende Pflichten zu einem Risikomanagement auferlegt.[166] Dabei werden Pflichten in Bezug auf Persönlichkeitsrechte durchaus erfasst, wie sich etwa aus Art. 7 Abs. 1 lit. b) ergibt [167]

156 Vgl. zum angewendeten Verfahren der „backpropagation" etwa EHKS-Niederée/Nejdl, § 2 Rn. 70.
157 Martini, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, 2019, S. 41 ff.
158 Martini, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, 2019, S. 50.
159 Lapuschkin/Wäldchen/Binder/Montavon/Samek/Müller, Nature Communications 10, 1096 (2019), abrufbar unter https://www.nature.com/articles/s41467-019-08987-4.pdf, zuletzt abgerufen am 7.12.2021.
160 EHKS-Niederée/Nejdl, § 2 Rn. 95; Stevens, CR 2020, 73, 74.
161 So insbesondere die Folgerung bei Angwin/Larson/Mattu/Kirchner, Machine Bias, 2016, abrufbar unter https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, zuletzt abgerufen am 7. 12.2021.
162 Valera, S. 15, 20.
163 Zu den Herausforderungen der Gewährleistung von Fairness algorithmischer Entscheidungsfindung etwa Hauer/Adler/Zweig.
164 In diesem Sinne auch EHKS-Niederée/Nejdl, § 2 Rn. 120.
165 Martini, Blackbox Algorithmus, S. 47.
166 Siehe hierzu Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1190; Spindler, CR 2021, 361, 366; Valta/Vasel, ZRP 2021, 142, 144.
167 Siehe auch Erwägungsgründe 35–38, die die Vermeidung von Diskriminierungen als Ziel des KI-Gesetzes nennen.

Das vom KI-Gesetz geforderte Risikomanagement schließt die Vermeidung von bias ein. Die zum Training, ebenso zum Validieren oder Testen verwendeten Datensätze sind auf bias zu untersuchen (vgl. Art. 10 Abs. 2 lit. f) KI-Gesetz). Zudem werden Hersteller von Hochrisiko-KI-Systemen zum Testen von Hochrisiko-KI-Systemen verpflichtet (vgl. Art. 9 Abs. 5 KI-Gesetz).

Ob und inwieweit eine fehlerhafte Entscheidung eines KI-Systems zu einer konkreten Rechtsverletzung oder Verletzung von Rechtsgütern Betroffener führt, hängt entscheidend vom Einsatzgebiet des KI-Systems und seiner Funktion ab. Wie schon das Beispiel des COMPAS-Systems zeigt, geht es bei dem Thema eines bias in the data weniger um Risiken für die körperliche Integrität von Personen oder Sachen, sondern um die Beurteilung von Personen.

Eine fehlerhafte Bewertung in Bezug auf eine Person stellt indes nicht stets eine Persönlichkeitsrechtsverletzung dar und ist selbst innerhalb von Sonderrechtsverhältnissen wie einem Vertragsverhältnis oder einer Bewerbungssituation oder im Rahmen eines Verwaltungsverfahrens nur in recht engen Grenzen angreifbar. Als Gegenstand einer Rechtsverletzung, die von einem Risikomanagement umfasst sein könnte, kommt aber etwa eine Diskriminierung in Betracht. Jedenfalls im Anwendungsbereich eines gesetzlichen Diskriminierungsverbots sollte sich das Risikomanagement von KI-Systemen, wie es im Entwurf des KI-Gesetzes vorgesehen ist, auch auf die Vermeidung einer solchen Diskriminierung erstrecken.

Zu den Möglichkeiten, bias oder Voreingenommenheit in KI-Systemen festzustellen, wird derzeit intensiv geforscht. Dabei richtet sich die Aufmerksamkeit aus rechtlicher Sicht vor allem auf das Testen von KI-Systemen.[168]

Ein anderer Ansatz folgt aus Überlegungen zur Explainable AI, bei der Entscheidungen von KI-Systemen in dem Sinne erklärbar werden sollen, als die Entscheidungsfaktoren und ihr Gewicht für die Entscheidung deutlich gemacht werden sollen. Dazu können teilweise sog. „Heatmaps“ eingesetzt werden, mit denen beispielsweise die entscheidenden Pixel eines Bildes sichtbar gemacht werden können, die zu einer bestimmten Klassifikation führen.[169] Mit diesem Verfahren wurde etwa im erwähnten Beispiel (oben 1) die Klassifikation von Pferden anhand von Copyright sichtbar gemacht.[170] Ob und inwieweit eine solche Erklärbarkeit von KI-Systemen möglich und für Zwecke der rechtlichen Überprüfung nutzbar sein wird, ist Gegenstand der Forschung.[171]

Inwieweit bias im allgemeinen Deliktsrecht, insbesondere unter dem Gesichtspunkt einer Persönlichkeitsrechtsverletzung, von Bedeutung ist, ist unklar. Wie dargestellt, ist selbst im Sonderfall der Diskriminierung noch durchaus unklar, ob und in welchen Fällen eine Persönlichkeitsrechtsverletzung vorliegt.

Wie das Stichwort „bias in the data“ zeigt, kann Gegenstand der Betrachtung auch die Datengrundlage sein, die das fehlerhafte Muster enthält. Das Stichwort „bias in the data“ legt nahe, nach der Verantwortung für die Trainingsdaten, auf denen die Funktion eines neuronalen Netzes wesentlich beruht, zu fragen. Als fiktives, aber naheliegendes Beispiel sei genannt, dass ein zur Auswahl von Kandidaten für eine freie Stelle verwendeter Algorithmus Kandidaten mit schwarzer Hautfarbe aussortiert, weil in den Trainingsdaten die besseren Kandidaten stets weiße Hautfarbe hatten.

Stellt man insoweit auf die Verantwortung für die Trainingsdaten ab, stellt sich die Frage, wie die Anforderungen an die Qualität von Trainingsdaten zu bestimmen sind, konkret, wann der bias in the data vorliegt. Ob Daten einen bias haben, hängt entscheidend von der Verwendung der Daten ab. Man mag Fotos von Pferden, Abbildungen von Leberflecken oder Fotos der Gemälde alter Meister im Rahmen des maschinellen Lernens zu ganz verschiedenen Lernzielen heranziehen, und es ist offensichtlich, dass die Frage, ob die Daten fehlerhaft sind oder einen bias enthalten, entscheidend vom Lernziel abhängen.

Dies spricht dafür, dass der bias in the data oder der Fehler von Daten stets erst durch die Zweckbestimmung und die Auswahl der Daten erfolgt. Diese Auswahl und Zweckbestimmung sind Teil des Trainings des neuronalen Netzes und werden von demjenigen vorgenommen, der das neuronale Netz

168 Dies ist Gegenstand etwa des vom Bundesministerium für Arbeit und Soziales geförderten Forschungsprojekts „ExamAI: KI Testing und Auditing“; siehe hierzu den Abschlussbericht des Projekts (2021), abrufbar unter https://gi.de/fileadmin/PR/Testing-AI/Abschlussbericht_ExamAI_-_KI_Testing_und_Auditing.pdf.

169 Siehe hierzu Samek/Binder/Montavon/Lapuschkin/Müller.

170 S. hierzu Lapuschkin/Wäldchen/Binder/Montavon/Samek/Müller.

171 Siehe hierzu etwa Langer/Oster/Speith et al.

trainiert. Dies spricht dafür, dass die Verantwortung für die Daten – und damit für den Fehler oder bias– bei dem zu sehen ist, der das Netz trainiert, nicht bei dem, der die Daten bereitstellt.

Die weitere Frage ist dann, wie ein „Fehler“ in Daten zu bestimmen ist und welche Verantwortung denjenigen, der ein neuronales Netz trainiert, insoweit trifft. Soweit neuronale Netze in Produkte Eingang finden, kann das Produkt einen Fehler im Sinne des Produkthaftungsrechts aufweisen und die Produkthaftung des Herstellers auslösen. Diese bezieht sich indes nicht auf Persönlichkeitsrechtsverletzungen, die hier im Vordergrund stehen.

## 3. BIAS IN THE DATA IM DATENSCHUTZRECHT

Aus Sicht des Datenschutzrechts kommen zwei Ansatzpunkte in Betracht. So ist zu fragen, ob Daten, in denen ein neuronales Netz fehlerhafte Muster erkennt, als solche falsch im Sinne des Datenschutzrechts sind. Dies ist, wie bereits angedeutet, zu verneinen. Wenn, wie im Beispiel, beim Training für eine Kandidatenauswahl Muster erkannt werden, die auf Geschlecht, Hautfarbe oder anderen diskriminierungsrelevanten Merkmalen beruhen, sind die Daten, wenn es sich insoweit überhaupt um personenbezogene Daten handelt, als solche nicht notwendigerweise falsch. Die Verwendung von Daten zu fehlerhaften Schlüssen ist indes keine Frage, die vom Datenschutzrecht adressiert wird.

Auch die Pflicht zur datenschutzfreundlichen Gestaltung von Systemen nach Art. 25 DSGVO muss leerlaufen, soweit das Datenschutzrecht fehlerhafte Muster in Daten oder das Erlernen problematischer Schlüsse aus Daten nicht adressiert.

Der Ansatzpunkt für die rechtliche Erfassung von „bias“ muss sich daher aus dem rechtlichen Rahmen von Entscheidungen als solchem ergeben, ggf. auch aus einem spezifischen Rechtsrahmen für maschinelle Entscheidungen. Wie bereits (oben 3.) dargestellt, besteht insoweit erhebliches Potenzial: Der bereits genannte Umstand, dass maschinelle Entscheidungen im Ausgangspunkt wiederholbar sind, ist der Ansatzpunkt für derzeitige Überlegungen, das Testen von KI-Systemen in den Mittelpunkt des Risikomanagements zu stellen. Insbesondere ist zu erwarten, dass sich Fehler wie Diskriminierung in maschinellen Beurteilungen durch Testen feststellen lassen.

Die Fragen rund um einen „bias in the data“ bestätigen damit die These, dass es eines spezifischen rechtlichen Rahmens für algorithmische Entscheidungen bedarf, der die Besonderheiten maschineller Entscheidungen in den Blick nimmt und insoweit auch das Potenzial der Wiederholbarkeit maschineller Entscheidungen nutzt.

**Kapitel F**

# HERAUSFORDERUNGEN DER INDIVIDUELLEN KOMMUNIKATION DURCH KI-SYSTEME

## I. INDIVIDUELLE KOMMUNIKATION DURCH KI-GESTÜTZTE VERWENDUNG VON ECHTZEITDATEN

Zu den aktuellen Herausforderungen von KI-Systemen, die an Beispielen des predictive policing, der individuellen Werbung und der individuellen Preise diskutiert werden, gehört die Nutzung von KI-Systemen im Rahmen der Echtzeitverarbeitung personenbezogener Daten und die Ableitung von Folgen hieraus, die ggf. erhebliche Nachteile für den Betroffenen zur Folge haben können.

Derartige Datennutzung hat einen potenziell sehr breiten Anwendungsbereich und wirft eine feine Vielzahl von Rechtsfragen unterschiedlicher Art auf. Soweit etwa KI-Systeme zur Überwachung eingesetzt werden, insbesondere im Zusammenhang mit Sanktionen durch staatliche Gewalt, sind offensichtlich Aspekte des Grundrechtsschutzes und des Verhältnisses von Bürger und Staat angesprochen. Die KI-gestützte Echtzeitverarbeitung von Daten kann auch zur Beeinflussung von Personen, von der Manipulation bis zu Lehre und Erziehung, eingesetzt werden, offensichtlich mit ganz unterschiedlicher rechtlicher Relevanz.

Die Beispiele der individualisierten Werbung und der individualisierten Preise zeigen, dass derartige Systeme auch in der Kommunikation zwischen Privatrechtssubjekten eine erhebliche Rolle spielen können. Maßgeblich sind hier nicht zuletzt Aspekte des Datenschutzrechts und der KI-Regulierung sowie des Persönlichkeitsschutzes, aber auch des Wettbewerbsrechts.

### 1. ERSCHEINUNGSFORMEN UND RECHTSFRAGEN PERSONALISIERTER WERBUNG

Die Individualisierung oder Personalisierung von Werbung ist ein Charakteristikum der Werbung im World Wide Web sowie auf Plattformen, etwa sozialen Netzwerken. Im Onlinemarketing hat die personalisierte Werbung die traditionelle, aus Medien wie der (gedruckten) Presse und dem klassischen Fernsehen bekannte Werbung mit einheitlicher Werbebotschaft für alle Adressaten weitgehend verdrängt.[172] Die Personalisierung von Werbung erfolgt durch unterschiedliche Methoden. Ein schon klassischer Weg erfolgt durch Profiling mittels sogenannter Cookies.[173]

Die Personalisierung von Werbung ist auch in der „Offline-Kommunikation“ möglich. In Deutschland wird diese derzeit noch sehr verhalten eingesetzt, nicht zuletzt wegen datenschutzrechtlicher Bedenken.

In Deutschland wurde die personalisierte Werbung durch Anzeige auf Monitoren im öffentlichen Bereich vor allem durch das schon erwähnte Beispiel der real-Supermärkte aus dem Jahr 2016/2017 bekannt, in denen den im Kassenbereich wartenden Kunden, beruhend auf einer Auswertung einer Bildaufnahme des jeweiligen Kunden, personalisierte Werbung angezeigt wurde (dazu oben B.III.2.a). Nach einer Prüfung durch das Bayerische Landesamt für Datenschutzaufsicht und kritischer Berichterstattung in der Tagespresse stellte real diese Praxis wieder ein.

In anderen Staaten ist die Nutzung personalisierter Werbung weit stärker vorangeschritten. So werden, wie bereits (oben B.III.2) erwähnt, in Japan schon seit 2012 Verkaufsautomaten zur personalisierten Werbung eingesetzt. Vorreiter waren hier Verkaufsautomaten für Getränke, die aufgrund von Gesichtserkennung Merkmale, konkret ungefähres Alter und Geschlecht, erfassten und in Abhängigkeit davon bestimmte Produkte empfohlen.[174] In

172 Baumgartner/Hansch, ZD 2020, 435.
173 Kreutz, MMR 2016, 364, 368; Weidert/Klar, BB 2017, 1858, 1861.
174 Reuters, Japan vending machine recommends drinks to buyers, Meldung 15.11.2010, abrufbar unter https://www.reuters.com/article/us-japan-machines-idUSTRE6AE0G720101115

jüngerer Zeit sind Taxis zunehmend mit Bildschirmen ausgestattet, die von den Passagieren auf den Rücksitzen eingesehen werden können. Auf die Bildschirme wird durch Software automatisiert personalisierte Werbung eingeblendet. Auch hier erfolgt die Personalisierung aufgrund von Aufnahmen der Passagiere durch eine Kamera im Taxi und anschließender automatisierter Auswertung, insbesondere nach geschätztem Alter und Geschlecht der Passagiere.[175]

Personalisierte Werbung wirft zahlreiche datenschutzrechtliche Fragen auf. Die datenschutzrechtliche Diskussion ist bisher auf die Sammlung der Informationen fokussiert; zum Einsatz von Cookies existiert eine umfangreiche Diskussion in der Literatur.

Die Erfassung von Informationen im Rahmen von Gesichtserkennung wird, wie bereits dargestellt (oben B.III.2), derzeit intensiv diskutiert. Die damit verbundene Frage nach dem Einsatz von Kameras gehört zu den Klassikern der Datenschutzdiskussion in den beiden vorangegangenen Dekaden.

Eine zentrale Frage bei personalisierter Werbung lautet häufig, ob es sich bei den zur Personalisierung genutzten Daten um personenbezogene Daten handelt. Diese Frage wurde etwa in Bezug auf Cookies intensiv diskutiert.[176] Ein wichtiges Problem in der Praxis ist bei Einsatz von Kameras, wie häufig, die Erfüllung der Informationspflicht nach Art. 13 DSGVO.

Die datenschutzrechtliche Frage nach der Rechtfertigung der Datenverarbeitung wird vergleichsweise wenig diskutiert. Bei der Datenerhebung im Internet hat sich das Erfordernis der Einwilligung als einzig maßgeblicher Rechtfertigungsgrund durchgesetzt.

Bei personalisierter Werbung durch Anzeigen von Werbebotschaften auf Monitoren im öffentlichen Bereich wird die Einwilligung nicht als praktikabel angesehen. Hier kann sich eine Rechtfertigung wohl nur aus Art. 6 Abs. 1 S. 1 lit. f) DSGVO ergeben. Innerhalb der hier gebotenen Interessenabwägung stellt sich die Frage, ob ein Interesse Betroffener an nicht-personalisierter Werbung anzunehmen ist, ähnlich dem Recht auf Anonymität.

Daneben stellt sich eine weitere Frage, die in der datenschutzrechtlichen Diskussion bisher kaum erörtert wird: die Zulässigkeit der Konfrontation mit der Werbebotschaft. Dieser Aspekt wurde am Beispiel der Werbung per Brief intensiv diskutiert. Dort hat sich als Interessenausgleich herausgestellt, dass der Werbende grundsätzlich ein Recht hat, seine Werbebotschaft mitzuteilen, aber das (durch einen Hinweis auf dem Briefkasten kundgemachte) Veto des Adressaten, nicht beworben werden zu wollen, zu beachten hat.[177]

Diese Frage stellt sich hier ebenso, freilich unter ganz anderen faktischen Vorzeichen. Neben der Zulässigkeit der Konfrontation mit der Werbebotschaft, kommt bei Werbung auf Monitoren im öffentlichen Bereich eine Frage hinzu, die bei der Werbung im Internet, die der Nutzer häufig allein wahrnimmt, weniger stark von Bedeutung ist: die Zulässigkeit der Mitteilung der Werbebotschaft an Dritte, die sich im räumlichen Umfeld des Werbeadressaten befinden (dazu unten II.5).

Die personalisierte Werbung wirft Fragen auf, die über das klassische Datenschutzrecht deutlich hinausgehen. Insbesondere können bei personalisierter Werbung auch Aspekte der Wissensüberlegenheit und der Manipulation von Bedeutung sein, die zu Recht im Entwurf des KI-Gesetzes adressiert werden. So wird in der Literatur befürchtet, dass durch den zumindest potenziell beeinflussenden und intransparenten Charakter personalisierter Werbung die Entscheidungsfreiheit beschränkt oder gar ausgehebelt werden könne.[178]

Nicht zuletzt ist von Interesse, ob in Bezug auf personalisierte Werbung Transparenzgebote eingreifen sollten.

Diese können sich de lege lata etwa aus Wettbewerbsrecht ergeben, de lege ferenda könnte ggf. das KI-Gesetz im Rahmen der dort geregelten Transparenzgebote eingreifen.

### 2. ERSCHEINUNGSFORMEN UND RECHTSFRAGEN INDIVIDUELLER PREISE

Seit einigen Jahren wird unter dem Stichwort des algorithmic pricing die automatisierte Bepreisung

175 Luke Dormehl, Japanese taxis will use facial recognition to target you with ads as you ride, 24.4.2019, Blog-Beitrag, abrubbar unter https://www.digitaltrends.com/cool-tech/facial-recognition-taxi-japan/; Annie Palmer, Privayy fears a Toyo taxis use facila recognition amrears to guess riders's age and gender for targeted advertisements, DailyMail Online, 23.4.2019, abrufbar unter https://www.dailymail.co.uk/science-tech/article-6951727/Tokyo-taxis-use-facial-recognition-guess-riders-age-gender-targeted-advertisements.html

176 EuGH, Urt. v. 1.10.2019, Rs. C-673/17 - Planet 49

177 BGH, Urt. v. 20.12.1988, VI ZR 182/88, NJW 1989, 902, 903.

178 Micklitz/Namyslowska/Jablonowska, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, § 6 Rn. 10.

von Dienstleistungen oder Gütern diskutiert.[179] Mit dem Begriff des algorithmic pricing wird die automatisierte Bepreisung von Dienstleistungen oder Waren durch Software bezeichnet.[180] Alternative Bezeichnungen sind etwa digital pricing oder dynamic pricing, in der deutschen Sprache auch individuelle Bepreisung.

Aus rechtlicher Sicht kann man zwischen einer dynamischen Bepreisung anhand objektiver Marktgegebenheiten, wie bspw. Angebot und Nachfrage oder Wettbewerbsumfeld, und einer individuellen Bepreisung anhand von Merkmalen des Nachfragenden, i.d.R. eines Konsumenten, unterscheiden.[181]

Die Dynamisierung im Sinne der Anpassung an die Marktlage ist ein unverzichtbares Grundelement der Bepreisung in der Marktwirtschaft. Auch die individuelle Bepreisung in dem Sinne, dass für dieselbe Leistung unterschiedliche Preise verlangt oder vorgeschlagen werden je nach den Verhältnissen des Nachfragers, ist seit jeher eine wichtige Strategie der Bepreisung. Indes bestehen gegenüber der individuellen Bepreisung auch erhebliche Vorbehalte, die vor allem auf der Erwartung des Verbrauchers, teils auch auf der rechtlichen Pflicht, dass für dieselbe Leistung derselbe Preis verlangt wird, beruhen.

Die Automatisierung der Dynamisierung und der Individualisierung von Preis(angebot)en werfen jeweils spezifische Rechtsfragen auf, teils legen sie den Finger in die Wunde bereits vorhandener, aber nicht geklärter Fragen. Aspekte des algorithmic pricing werden nicht zuletzt im Kartellrecht diskutiert. Dabei ist eine Reihe von Fragen von Bedeutung. So wird etwa diskutiert, unter welchen Voraussetzungen Preisbildungsalgorithmen zu einer kartellrechtlich unzulässigen Absprache zwischen Unternehmen über Preise führen.[182]

Bei der individuellen Preisfindung anhand von Merkmalen der nachfragenden Person sind Fragen des Diskriminierungsschutzes, des Wettbewerbsrechts, des Datenschutzrechts und des Persönlichkeitsschutzes angesprochen.

## II. SPEZIFIKA DER INDIVIDUELLEN KOMMUNIKATION DURCH KI-SYSTEME

### 1. DIE AUTOMATISIERTE EINSCHÄTZUNG EINER PERSON ALS KERNELEMENT DER INDIVIDUELLEN KOMMUNIKATION

Individuelle Werbung und individuelle Bepreisung weisen wichtige Gemeinsamkeiten auf: Im Zentrum steht jeweils die Beurteilung einer Person, des Werbeadressaten beziehungsweise des Nachfragers, durch den Anbieter der Werbung oder des nachgefragten Gutes. Soweit also die Information automatisiert, also durch Einsatz von Software oder eines KI-Systems, erfolgt, steht im Zentrum der Fragestellung die schon erörterte Frage einer Beurteilung einer Person durch eine Maschine.

Diese Beurteilung ist bei der Information im Fall der Werbung oder einer Preisangabe eingebettet in einen kommunikativen Gesamtvorgang, in dem vier Phasen unterschieden werden können: (1) die Datenerfassung durch technische Geräte, z.B. eine Kamera, (2) die automatisierte Verarbeitung dieser Information, im Kern die hier interessierende Einschätzung oder Beurteilung des menschlichen Kommunikationspartners in Bezug auf dessen Interessen (Werbung) oder Zahlungsbereitschaft (Bepreisung), (3) die automatisierte Schlussfolgerung, konkret die Entscheidung über die anzuzeigende Werbung oder Preisangabe, und (4) die automatisierte Mitteilung einer Information, d.h. der Werbenachricht oder der Preisangabe sowie der zugrundeliegenden Einschätzung.

Jede dieser Phasen wirft, wie die kurze Zusammenfassung der Diskussion zu individualisierter Werbung und Preise gezeigt, unterschiedliche Rechtsfragen auf und betrifft verschiedene Rechtsgebiete. Als Spezifikum der KI-Anwendung ist hier der Aspekt der automatisierten Individualisierung von Interesse, die durch KI ermöglicht wird. Da diese mit einer Einschätzung von Menschen einhergeht, sollen hier, in Ergänzung zu den Ausführungen zur Beurteilung (oben E), die Rechtsfragen der Einschätzung in den verschiedenen Phasen der

179 Vgl. Paal, GRUR 2019, 43, 43; Paschke, in: Hamburger Kommentar – Gesamtes Medienrecht, 4. Auflage 2021, 13. Abschn. Rn. 22 f.; Ylinen, NZKart 2018, 19, 19.
180 Vgl. Paal, GRUR 2019, 43, 43; Paschke, in: Hamburger Kommentar – Gesamtes Medienrecht, 4. Auflage 2021, 13. Abschn. Rn. 22 f.; Ylinen, NZKart 2018, 19, 19.
181 Vgl. Hofmann, WRP 2016, 1074, 1075; Paala, GRUR 2019, 43, 44; Zander-Hayat/Reisch/Steffen, VuR, 2016, 403, 404.
182 Dazu etwa König, § 17 Rn 40 m.w.N.; Ylinen, NZKat 2018, 19 ff.

automatisierten Kommunikation im Vordergrund stehen.

Dabei sind vor allem zwei Aspekte von Interesse: die materielle Zulässigkeit des Vorgangs zum einen, Anforderungen an die Transparenz der Automatisierung oder der Nutzung von KI-Systemen zum anderen.

## 2. DATENERFASSUNG DURCH KI-SYSTEME

Die Erfassung von Merkmalen einer Person betrifft den Kern des Datenschutzrechts. In der Diskussion stellt sich jeweils die Frage, ob und inwieweit personenbezogene Daten vorliegen. Diese Frage, die für Cookies intensiv diskutiert und hier am Beispiel der Gesichtserkennung erörtert wurde, betrifft nicht die Spezifika des Einsatzes von KI und soll daher nicht vertieft werden.

In Bezug auf die Rechtfertigung der Datenerfassung wurden Besonderheiten der Informationsgewinnung (oben B. III.) ausführlich erörtert; darauf kann im Wesentlichen verwiesen werden. Bei der personalisierten Werbung und individuellen Preisen ist die Rechtfertigung der Datenerhebung, insbesondere soweit sie auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO beruht, im Hinblick auf die Individualisierung, der der Datenerhebung dient, zu beurteilen. Diese wird nachfolgend (unten II.4) näher erörtert.

## 3. AUTOMATISIERTE EINSCHÄTZUNG NATÜRLICHER PERSONEN

Die Frage nach der materiellen Zulässigkeit der automatisierten Einschätzung wurde im Hinblick auf das Verbot der automatisierten Entscheidung nach Art. 22 DSGVO bereits erörtert (oben E.III); darauf kann verwiesen werden. Die Untersuchung des Art. 22 DSGVO hat deutlich gemacht, dass diese Norm die Rechtsfragen der automatisierten Einschätzung oder Beurteilung von Personen nicht einmal ansatzweise vollständig adressiert. So ist Art. 22 DSGVO nach h.M. auf eine bloße Einschätzung nicht anwendbar (Vgl. E.III.2.b), sodass die Norm für die hier interessierende Frage getrost außer Betracht bleiben kann.

Die Frage nach rechtlichen Grenzen der Einschätzung von Personen als solcher ist schwierig. Soweit Menschen eine solche Einschätzung vornehmen, handelt es sich um einen Vorgang in der inneren Gedankenwelt des Einschätzenden, der schon faktisch einer rechtlichen Regelung kaum zugänglich ist, solange er nicht zumindest in einer Dokumentation oder einer Meinungsäußerung des Einschätzenden zutage tritt. Im Übrigen gehört die Einschätzung als Meinungsbildung zum inneren Kern der grundrechtlich geschützten Meinungsfreiheit, der aus gutem Grund nicht einzuschränken ist.

Es handelt sich also um eine durchaus neuartige Frage, da erst die KI komplexere Einschätzungen von Menschen durch eine Maschine ermöglicht. Diese Frage kann im Rahmen dieser Untersuchung nicht ausgelotet werden. Sie soll daher auf den Aspekt fokussiert werden, ob und in welchen Fällen dem Datenschutzrecht insoweit Einschränkungen zu entnehmen sind.

Als ein bekanntes Beispiel für die datenschutzrechtliche Diskussion zu Einschätzungen natürlicher Personen ist das Kreditscoring zu erwähnen, das in Deutschland seit vielen Jahren Gegenstand intensiver datenschutzrechtlicher Debatte ist.[183]

Das Datenschutzrecht ist auf die Bildung einer Einschätzung anwendbar, soweit personenbezogene Daten verarbeitet werden. In diesem Fall bedarf sie der datenschutzrechtlichen Rechtfertigung. Insoweit ist anerkannt, dass die Erstellung einer Einschätzung datenschutzrechtlich zulässig ist. Der datenschutzrechtlichen Kontrolle unterliegt aber die Frage, welche Daten in die Einschätzung eingehen dürfen. Soweit sich die Rechtfertigung aus Art. 6 Abs. 1 S. 1 lit. f) DSGVO ergeben soll, muss ein legitimes Interesse an der Verarbeitung bestehen, und weiterhin muss die Verarbeitung erforderlich sein. Bei Einschätzungen wird insoweit geprüft, ob die Einbeziehung der betreffenden Daten erforderlich ist. Dieser Aspekt ist bei der Einschätzung der Kreditwürdigkeit bedeutsam. Hier ist sehr umstritten, welche Daten in die Einschätzung der Kreditwürdigkeit einfließen dürfen.[184] Als Leitlinie gilt insoweit, dass nur solche Daten verwendet werden dürfen, die für die Kreditwürdigkeit nachweisbar von Bedeutung sind.

Ob der Debatte zum Kreditscoring ein allgemeiner datenschutzrechtlicher Grundsatz des Inhalts zu entnehmen ist, dass in eine automatisierte Einschätzung nur solche Daten eingehen dürfen,

183 Siehe monographisch etwa Rohrmoser; zu den Grundlagen des Scoring im interdisziplinären und internationalen Überblick siehe etwa Schröder/Taeger.

184 Siehe dazu etwa Assion/Hauck, ZD-Beilage 12/2020, S. 1 ff.

die für die Einschätzung nachweislich von Bedeutung sind, ist offen. Ebenso ist ungeklärt, welche Einschränkungen sich hieraus für personalisierte Werbung ergeben.

## 4. AUTOMATISIERTE SCHLUSSFOLGERUNGEN AUS INDIVIDUELLER EINSCHÄTZUNG

Die Frage, ob und in welchen Grenzen automatisierte Schlussfolgerungen aus einer individuellen Einschätzung einer Person gezogen werden dürfen, entzieht sich offensichtlich einer generalisierenden Betrachtungsweise, da hier die Art der Schlussfolgerung im Vordergrund steht.

Die Frage hat zwei Aspekte, die im Ausgangspunkt durchaus zutreffend sind: zum einen die Frage, ob und unter welchen Voraussetzungen überhaupt Schlussfolgerungen aus einer automatisierten Einschätzung getroffen werden dürfen, und zum anderen die Frage der Automatisierung der Schlussfolgerung. So adressiert etwa Art. 22 DSGVO ausdrücklich die Automatisierung der Schlussfolgerung, soweit diese als „Entscheidung" zu qualifizieren ist (dazu oben III.2). Andere Aspekte, wie etwa ein Recht auf Gleichbehandlung in Bezug auf Werbung oder Bepreisung, sind von der Automatisierung letztlich unabhängig, erhalten durch diese aber besondere praktische Relevanz. Bei der hier interessierenden Fallgruppe der Echtzeitverarbeitung von Daten geht es vor allem um die situationsbedingte Überlegenheit, die nachfolgend am Beispiel der personalisierten Werbung und der individuellen Preise diskutiert werden soll.

Im Beispiel der personalisierten Werbung geht es um die Frage, welche Werbung einem konkreten Kunden angezeigt wird. Dabei sind, wie bereits angesprochen, zwei Aspekte zu unterscheiden: die Anzeige der Werbung als solcher und die damit implizit verbundene Mitteilung der Einschätzung zum anderen (dazu unten 3.).

Soweit es um den Inhalt der Werbung als solcher geht, handelt es sich nicht um KI-spezifische Fragen im engeren Sinne, sondern Aspekte der Informationsüberlegenheit, deren praktische Relevanz aber in der durch KI-Systeme ermöglichten Datenauswertung in Echtzeit dramatisch gesteigert wird. Rechtliche Grenzen für Werbung aufgrund ihres Inhalts sind anerkannt. So gelten Einschränkungen insbesondere durch Jugendschutz. Am Beispiel der Schockwerbung, die anhand von Werbekampagnen der Firma Benetton diskutiert wurde, hat die Rechtsprechung darüber hinaus Einschränkungen entwickelt.[185]

Während bisher die Frage, ob eine bestimmte Werbung rechtswidrig ist, in Bezug auf den hypothetischen Adressaten der Werbung diskutiert wurde, so im Fall der Benetton-Werbung, stellt sich in Bezug auf personalisierte Werbung die bisher kaum diskutierte Frage, ob auf die Befindlichkeiten des konkreten Werbeadressaten Rücksicht zu nehmen ist. Ist es einem ungewollt Kinderlosen zumutbar, Werbung zu glücklichen Familien präsentiert zu bekommen? Sollten alte Menschen Werbung sehen, die für junge Menschen bestimmt ist, oder schlimmer, Werbung, die alte Menschen adressiert? Die wichtigere Frage geht zweifellos dahin, ob ein Anspruch auf kommunikative Gleichbehandlung besteht, ob es also ein Recht des Einzelnen gibt, nicht mit einer personalisierten Werbung konfrontiert zu werden.

Ein solches Recht wird bisher nicht angenommen, ja kaum einmal angesprochen. Tatsächlich geht das deutsche Recht zutreffend davon aus, dass das Recht des Werbenden auf Gestaltung seiner Ansprache überwiegt. Diese Position wird möglicherweise zu überdenken sein. Einen interessanten Anhaltspunkt liefert die gegenwärtige Diskussion in Japan, wo individuelle Werbung durch automatisierte Anzeigen weitaus stärker verbreitet ist. Hier erhielt das Designprojekt „Unlabeled" jüngst mehrere Designpreise für ein Camouflage-Design, das automatisierte individuelle Werbung vermeiden soll.[186] In dem Projekt, das sich ausdrücklich gegen exzessive Überwachung und Beobachtung richtet[187] und von mehreren Forschungsinstituten sowie einem KI-Kunstwerke produzierenden Unternehmen getragen wurde, wurde durch Techniken des maschinellen Lernens ein Design entwickelt, das Fehlklassifikation der Gesichtserkennungs-Software auslöst.[188]

185 Siehe etwa BVerfG, Urt. v. 12.12.2000, 1 BvR 1762,95, 1 BvR 1787/95, BVerfGE 102, 347 – Schockwerbung I; BVerfG, Urt. v. 11.3.2003, 1 BvR 426/02, BVerfGE 107, 275 – Schockwerbung II; BGH, Urt. v. 6.7.1995, I ZR 293/93, BGHZ 130, 196; BGH, Urt. v. 6.7.1995, I ZF 180/94; Urt. v. 6.7.1995, I ZR 110/93, BGH, Urt. v. 6.12.2001, I ZR 284/00, BGH, Urt. v.27.10.2014, AnwZ (Brfg) 67/13.

186 Siehe dazu die Website der Gruppe, abrufbar unter https://unlabeled.jp/en/about.

187 Vgl. Amano/Hirata/Nakajima /Sai, Unlabeled – Camouflage against the machines, abrufbar unter https://cclab.sfc.keio.ac.jp/en/projects/unlabeled-en/.

188 Siehe eine anschauliche Beschreibung durch das beteiligte Unternehmen Quosmo unter https://qosmo.jp/en/projects/unlabeled-2/. sowie bei Vgl. Amano/Hirata/Nakajima /Sai, Unlabeled – Camouflage against the machines, abrufbar unter https://cclab.sfc.keio.ac.jp/en/projects/unlabeled-en/.

Die Frage ist komplex und geht über klassisches Datenschutzrecht weit hinaus. De lege lata wird man einen Anspruch auf nicht-individuelle Kommunikation auch für den Fall der automatisierten Werbung schwerlich begründen können. Auch der europäische Gesetzgeber hat mit dem Entwurf des KI-Gesetzes insoweit keine Maßnahmen vorgesehen, sondern beschränkt sich auf das Verbot der Manipulation.

Im Zusammenhang mit individuellen Preisen wird die Frage nach Gleichbehandlung auch im deutschen Recht aufgeworfen, bisher allerdings recht verhalten. Hintergrund ist wohl der Umstand, dass die zugrunde liegende Frage nach der Zulässigkeit von Preisdifferenzierung unabhängig von der Automatisierung bereits seit langem Gegenstand sehr differenzierter Regelungen ist. Als Grundsatz gilt freilich weiterhin, dass die Preisdifferenzierung zulässig ist.

Ob dieser Grundsatz weiterhin gelten kann, wenn Preise durch KI-Systeme so auf den Einzelnen zugeschnitten werden, dass seine situations- und rollenbedingte Unterlegenheit ausgenutzt wird, ist zweifelhaft. Wäre es wirklich unbedenklich, wenn sich der Benzinpreis an einer Tankstelle immer dann erhöht, wenn der Autofahrer die Straße verlassen, sich in die Warteschlange eingereiht hat und schließlich vor der Zapfsäule steht, um sich dann, nachdem sich der Kunde auf den erhöhten Preis eingelassen hat, wieder zu senken, um den nächsten Kunden anzulocken? Ist es wirklich unproblematisch, wenn der auf einer Website angebotene Flugpreis immer dann höher wird, wenn ein Interessierter zum zweiten Mal denselben Flug aufruft?

Die Beispiele sprechen durchaus verschiedene Aspekte, insbesondere die Ausnutzung von Transaktionskosten sowie der Wissensüberlegenheit an. Bei der individuellen Vereinbarung von Preisen wird die Verhandlungsmacht auf die jeweilige Situation der konkreten Parteien bezogen, deren individueller Wissensstand und Transaktionskosten maßgeblich werden. Durch die einseitige Automatisierung verschieben sich etwa die Transaktionskosten in der Preisverhandlung dramatisch zulasten des manuell agierenden Nachfragers.

Der Kern der Problematik liegt freilich weniger bei einem etwaigen materiellrechtlichen Anspruch auf einen gleichen Preis, sondern eher im Aspekt der Transparenz. So wird etwa in Bezug auf das Wettbewerbsrecht die Ansicht vertreten, der Verbraucher erwarte gleiche Preise mit der Folge, dass eine individuelle Preisangabe irreführend sei, soweit dieser Umstand nicht deutlich gemacht werde.[189]

Diese These ist überaus interessant und verdient Beachtung. Leider geht die Diskussion auf diesen Aspekt, der de lege lata von der Rechtsprechung geklärt werden könnte, nicht ein. Die Frage ist wohl so grundlegender Art, dass der Gesetzgeber die Antwort nicht der Rechtsprechung überlassen sollte. Abhilfe scheint bisher nicht in Sicht. Der Entwurf des KI-Gesetzes enthält im Art. 52 Transparenzvorschriften für KI-Systeme, geht aber auf individuelle Preise nicht ein.

## 5. MITTEILUNG EINER EINSCHÄTZUNG

Im Zusammenhang mit individualisierter Werbung wird die Frage relevant, ob und welchen rechtlichen Einschränkungen die Mitteilung einer automatisierten Einschätzung an den Betroffenen oder Dritte unterliegt. Dabei geht es hier um den Tatbestand der Mitteilung als solche.

Die Frage, die zu Recht vor allem bei der Mitteilung von Kreditwürdigkeitseinschätzung etc. diskutiert wird, mag bei einer personalisierten Werbung überraschen. Im Fall der Werbung erfolgt keine unmittelbare Mitteilung einer solchen Einschätzung. Mittelbar lässt sich diese aber durchaus entnehmen. Wenn etwa Werbung für Damenkleidung angezeigt wird, kann das als implizite Aussage verstanden werden, dass das System den betreffenden Kunden als Frau eingestuft hat. Und wenn der Monitor Werbung für Medikamente zu typischen Altersbeschwerden anzeigt, liegt dem offensichtlich eine entsprechende Alterseinschätzung zugrunde.

Das Beispiel der Werbung ist interessant, weil die Bedeutung einer solchen Einschätzung wesentlich geringer ist als eine über Prüfungsergebnisse, Kreditwürdigkeit, Verkehrseignung oder gar etwaiges strafbares Verhalten.

### a. Mitteilung an den Betroffenen

Die Mitteilung von Einschätzungen an den Betroffenen scheint bisher keinen Einschränkungen zu unterliegen. Im Zusammenhang mit der Diskussion um „Lookism“ wird aber zu Recht die Frage aufge-

189 Zander-Hayat/Reisch/Steffen, VuR 2016, 403 (407).

worfen, ob sich der Bürger ständig mit Einschätzungen zu seiner Person konfrontieren lassen muss.

Wer möchte, plakativ gesagt, schon ständig mit der Aussage konfrontiert werden, dass man alt und krank aussehe? Es ist offensichtlich, dass hier ein Aspekt der privacy oder der negativen Meinungsfreiheit angesprochen ist. In der bisherigen rechtlichen Diskussion stand dem Recht auf negative Meinungsäußerung oder privacy meist ein Recht auf Meinungsäußerung gegenüber, so dass eine Konfrontation im öffentlichen Bereich als zulässig angesehen wurde. In der einseitig automatisierten Kommunikation aber ist diese Frage ganz anders zu diskutieren. Dabei sind zwei Aspekte zu unterscheiden: Zunächst besteht hier kein Gleichgewicht der Kommunikationspartner. Vielmehr steht der menschliche Empfänger einer Übermacht an Kommunikationspartnern gegenüber, die zu sehr geringen Grenzkosten kommunizieren können. Der zweite Aspekt, der ebenfalls unter dem Gesichtspunkt des Persönlichkeitsrechts zu diskutieren ist, betrifft den Aspekt der Einschätzung als solcher. Es mag sein, dass man sich im öffentlichen Raum der Kommunikation nicht entziehen kann, aber muss man sich deswegen Einschätzungen zur eigenen Person anhören? Die Frage ist, soweit es nur die Mitteilung an den Betroffenen angeht, nicht einfach zu beantworten und wird überlagert von dem Aspekt der Öffentlichkeit, der die Möglichkeit der Kenntnisnahme der Einschätzung durch Dritte einschließt.

Ob das Datenschutzrecht insoweit anwendbar ist, ist zweifelhaft, da der Personenbezug nur für den Betroffenen selbst herzustellen ist. Geht man von der Anwendbarkeit aus, ist eine Rechtfertigung der Datenverarbeitung meist nur im Wege der Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO möglich. Das legitime Interesse des Werbenden an der Mitteilung ist zu bejahen, so dass alles auf die Frage hinausläuft, ob es ein entgegenstehendes Interesse des Betroffenen gibt.

In der Diskussion um personalisierte Werbung im Internet wird seit jeher vorgetragen, dass nach Umfragen eine Mehrheit der Internetnutzer ein Interesse an personalisierter Werbung hat. Ob dieser Befund, der für personalisierte Werbung auf Webseiten gilt, sich auch auf die Werbung auf Monitoren im öffentlichen Raum übertragen lässt, darf bezweifelt werden. Das Interesse, nicht automatisiert mit einer personenbezogenen Einschätzung konfrontiert zu werden, selbst wenn diese zutreffend sein sollte, betrifft den Kern der Persönlichkeit als Schutz der Selbstachtung des Einzelnen, der um diese ringen mag.

Die Frage nach der Interessenabwägung kann hier nicht abschließend beantwortet werden. Es ist aber ein entgegenstehendes Interesse anzuerkennen, in der Öffentlichkeit nicht mit automatisierten Einschätzungen konfrontiert zu werden. Ein absolutes Hindernis gegenüber personalisierter Werbung lässt sich daraus sicher nicht herleiten. In der differenziert vorzunehmenden Interessenabwägung wird es nicht zuletzt darauf ankommen, welchen Inhalt die Einschätzung hat. So macht es einen Unterschied, ob eine Einschätzung in Bezug auf Alter oder Geschlecht oder über den Gesundheitszustand implizit mitgeteilt wird.

### b. Mitteilung einer impliziten Einschätzung an die Öffentlichkeit

Das zentrale Problem der Mitteilung einer Einschätzung ist seit jeher die Mitteilung an Dritte, die traditionell zu Recht im Fokus der Diskussion steht. Die Mitteilung über Kreditwürdigkeit, Prüfungsergebnisse, Gesundheitszustand, kriminelle oder ordnungsrechtliche Vergangenheit an Dritte unterliegt, etwa im Datenschutzrecht, scharfen Einschränkungen und ist im Grundsatz nur mit Einwilligung des Betroffenen zulässig.

Bei der individuellen Werbung durch Monitore im öffentlichen Raum ist die implizite Einschätzung des Betroffenen häufig nicht nur für diesen selbst, sondern auch für andere Personen in der unmittelbaren Umgebung des Betroffenen, insbesondere dessen Begleitung, ersichtlich. Die Einschätzung wird also stets auch an dessen Umgebung mitgeteilt. Dies kann aus Sicht des Betroffenen in besonderer Weise unerwünscht sein. In dieser Frage kommt dem Datenschutzrecht entscheidende Bedeutung zu. Im Fall der automatisierten Mitteilung einer Einschätzung durch Monitore liegt eine Verarbeitung personenbezogener Daten vor, weil jedenfalls Personen in der Umgebung des Betroffenen diese dem Betroffenen zuordnen können. Soweit sich aus der Werbung Rückschlüsse auf Gesundheitsdaten ziehen lassen, etwa bei einer Werbung für Medikamente, greifen die Einschränkungen des Art. 9 DSGVO.

Im Rahmen der Rechtfertigung nach Art. 6 DSGVO kommt es wiederum auf entgegenstehende Interessen des Betroffenen an. Besondere Bedeutung kommt dem Interesse des Betroffenen zu, nicht

durch negative Einschätzung gegenüber seinem Umfeld bloßgestellt zu werden. Die automatisierte Einschätzung kann insoweit besonders belastend sein, weil sie als „objektive" Drittmeinung verstanden werden kann.

Da es kaum eine Produktwerbung gibt, der man nicht je nach dem Kontext eine implizite negative Aussage über den Adressaten zuschreiben kann – warum soll sich der Adressat für Shampoo oder Deodorant interessieren, warum der Herr oder die Dame im Anzug oder im Jogginganzug für Putzmittel etc. –, ist das entgegenstehende Interesse des Betroffenen von Gewicht.

Ob damit ein abschließendes Urteil über personalisierte Werbung im öffentlichen Raum gesprochen ist, kann hier nicht abschließend untersucht werden. Aus Sicht des Verfassers ist die Welt eine angenehmere, wenn der Einzelne nicht damit rechnen muss, das automatisierte Einschätzungen über ihn auf Monitoren seiner Umgebung mitgeteilt werden, selbst wenn es um scheinbar harmlose Merkmale wie Geschlecht und Alter geht.

Unabhängig davon, welche Ansicht man hier in den angesprochenen Aspekten vertritt, zeigen die Überlegungen, dass sich durch Datenschutzrecht erhebliche Einschränkungen für personalisierte Werbung im öffentlichen Raum ergeben.

### c. Transparenzanforderungen

Unter dem Gesichtspunkt der Transparenz ist zu fragen, ob und ggf. in welchen Fällen über die Personalisierung der Werbung zu informieren ist. Der Entwurf des KI-Gesetzes enthält in seinem Artikel 52 Bestimmungen zur Transparenz über den Einsatz von KI-Systemen in der Kommunikation. Danach soll insbesondere über den Einsatz von Chatbots informiert werden. Individuelle Werbung durch Anzeigen auf Monitoren oder individuelle Preise sind von Art. 52 jedoch nicht erfasst.

Ob das Datenschutzrecht de lege lata im Fall der personalisierten Werbung durch KI-Systeme eine Pflicht zur Transparenz enthält, ist unklar. Art. 13 Abs. 2 lit. f) DSGVO und Art. 14 Abs. 2 lit. g) DSGVO enthalten eine Pflicht zum Hinweis auf eine automatisierte Entscheidung i.S. des Art. 22 DSGVO.

Allerdings fehlt es hier an der von Artt. 13 und 14 DSGVO vorausgesetzten Erhebung personenbezogener Daten, so dass die Informationspflichten unabhängig davon, ob hier eine automatisierte Entscheidung vorliegt, nicht anwendbar sind.

## III. FAZIT

Versucht man ein Fazit, so lassen sich aus den Überlegungen zu personalisierter Werbung und individuellen Preisen einige Erkenntnisse ableiten, die für das Verhältnis von KI und Datenschutz von Bedeutung sind und zugleich über das Datenschutzrecht deutlich hinausgehen.

So lässt sich anhand der personalisierten Werbung belegen, dass dem Datenschutzrecht de lege lata erhebliche Bedeutung in Bezug auf die Erstellung und Verwendung automatisierter Einschätzungen zu natürlichen Personen zukommt. Das Schutzrecht enthält mit dem Erfordernis der Rechtfertigung und der Interessenabwägung ein flexibles Instrumentarium, das hochdifferenzierte Ergebnisse ermöglicht und insoweit den vom Recht erstrebten Interessenausgleich auch im Einzelfall orientiert herzustellen. Der Preis hierfür ist indes ein ungeheures Maß an Rechtsunsicherheit, das der Entwicklung neuer Technologien abträglich ist. Diese Rechtsunsicherheit ist dem Gesetzgeber anzulasten, soweit es den Erlass unnötig unklar formulierter Rechtsnormen betrifft, wie im Fall des Art. 22 und der daran anknüpfenden Informationspflicht.

Unabhängig davon bewährt sich das Datenschutzrecht im Fall der personalisierten Werbung. Hier können zentrale Fragen, etwa die Mitteilung von Einschätzungen an die Öffentlichkeit, de lege lata beantwortet werden. Soweit Rechtsunsicherheit besteht, liegt das Problem nicht im Datenschutzrecht, sondern in der Schwierigkeit, die Bedeutung automatisierter Einschätzungen und der Interessen daran verlässlich abschätzen zu können. Soweit sich in Europa, ähnlich wie etwa in Japan, eine Praxis der personalisierten Werbung im öffentlichen Raum entwickeln sollte, wird sich insoweit voraussichtlich eine intensive Diskussion entwickeln.

In anderen Fällen gerät das Datenschutzrecht an Grenzen, wie sich etwa am Beispiel der individualisierten Preise zeigt. Dies ist kein Manko des Datenschutzrechts, sondern weist lediglich darauf hin, dass das Datenschutzrecht ein Teil der Rechts-

ordnung mit spezifischen Aufgaben und damit ein Baustein im zu erreichenden Rechtsrahmen für KI-Systeme ist.

**Kapitel G**

# LEISTUNGSFÄHIGKEIT DES DATENSCHUTZRECHTS UND REGELUNGSBEDARF ZUM SCHUTZ VON PERSÖNLICHKEITSRECHTEN GEGEN RISIKEN DURCH KÜNSTLICHE INTELLIGENZ

Der zentrale Gegenstand dieser dem facettenreichen Spannungsverhältnis von künstlicher Intelligenz und Datenschutz gewidmeten Untersuchung betrifft die Leistungsfähigkeit des derzeitigen Datenschutzrechts und die Frage, ob das Datenschutzrecht die Nutzung der Potenziale der künstlichen Intelligenz eher stärkt oder aber schwächt.

Die Antwort fällt, wenig überraschend, differenzierend aus. Das geltende Datenschutzrecht ist auch gegenüber Risiken aus der Datenverarbeitung durch KI-Systeme, auf die es umfassend anwendbar ist, durchaus leistungsfähig. Die Sammlung von Daten und die Erzeugung von Informationen über natürliche Personen durch KI-Systeme wird von den klassischen Regeln des Datenschutzrechts, wie sich am Beispiel der Gesichtserkennung gezeigt hat, erfasst und kann danach interessengerechten Lösungen zugeführt werden.

Sehr stark ist das Datenschutzrecht auch in Bezug auf die Verwendung zutreffender personenbezogener Daten durch KI-Systeme, die durch starke Schutzmechanismen sowohl im Bereich der materiellen Wertung als auch hinsichtlich der Durchsetzung geschützt wird.

Die bekannten Schwächen des geltenden Datenschutzrechts, insbesondere die auch in vielen grundlegenden Aspekten bestehende Rechtsunklarheit, haben erhebliche nachteilige Auswirkungen auf Forschung und Nutzung von KI-Systemen. Besonders problematisch ist der schier uferlose und zudem höchst unklare Anwendungsbereich der DSGVO, der zu dem absurden Ergebnis führt, dass jedwede Daten in der Praxis oft als im Zweifel personenbezogen geführt werden. Rechtsunklarheit besteht auch in Bezug auf die Forschung als Rechtfertigung zur Verarbeitung personenbezogener Daten.

Eine Wirkung des Datenschutzes derart, dass „KI made in Europe“ aufgrund des derzeitigen Datenschutzrechts besondere Chancen hat, kann daher nicht festgestellt werden. Dagegen erscheint die plausible Vermutung, dass Datenschutz als Bestandteil des Rechtsrahmens eine wesentliche Grundlage des Vertrauens in neue Technologien einschließlich der künstlichen Intelligenz darstellt, zutreffend.

Die Grenzen des Datenschutzrechts zeigen sich in besonderer Weise bei Entscheidungen von KI-Systemen, insbesondere bei Bewertungen. Das Verbot automatisierter Entscheidungen nach Art. 22 DSGVO, dessen praktische Bedeutung ohnehin minimal ist, ist schon konzeptionell nicht überzeugend und sollte im Sinne des Gebots angemessener Beteiligung eines menschlichen Entscheidungsträgers fortentwickelt werden.

Das Datenschutzrecht ist auf die inhaltliche Überprüfung automatisierter Entscheidungen nicht zugeschnitten und – nach hiesiger Auffassung – auch nicht anwendbar. Der auf menschliche Entscheidungen zugeschnittene rechtliche Rahmen von Bewertungen ist für maschinelle Entscheidungen nicht geeignet, da sich die maschinelle Entscheidungsfindung von der menschlichen grundlegend unterscheidet. Nicht zuletzt bestehen bei maschinellen Entscheidungen aufgrund der Reproduzierbarkeit der Entscheidung Möglichkeiten der Überprüfung, die bei menschlichen Entscheidungen fehlen. Hierauf geht der bisherige Rechtsrahmen – verständlicherweise – nicht ein.

Es bedarf dringlich eines spezifischen Rechtsrahmens für sog. algorithmische Entscheidungen, der den Besonderheiten maschineller Entscheidungsfindung gerecht wird. Der Entwurf des KI-Gesetzes, der ein Risikomanagement für Hochrisiko-KI-Sys-

teme verlangt, liefert hierzu einen Baustein, dem freilich weitere hinzuzufügen sind. Einen durchaus wichtigen Baustein im Rechtsrahmen für algorithmische Entscheidungen kann wiederum das Datenschutzrecht beisteuern, das schon derzeit auf die Übermittlung von Bewertungen zu natürlichen Personen anwendbar ist und hier Grenzen setzt.

Eine zentrale unterstützende Wirkung kann das Datenschutzrecht nicht zuletzt bei Verstößen gegen das – noch zu schaffende – materielle Recht automatisierter Entscheidungsfindung ausüben, da es solcherart rechtswidrige Verarbeitung personenbezogener Daten mit seinem gesamten, überaus kraftvollen Instrumentarium abwehren kann.

Das Datenschutzrecht wird daher voraussichtlich eine wichtige Rolle im künftigen Rechtsrahmen für die Nutzung von künstlicher Intelligenz spielen.

# LITERATURVERZEICHNIS

*Arzt, Clemens: Nutzung von Satellitendaten in der Umweltüberwachung, DuD 2000, 204-208;*

*Assion, Simon / Hauck, Daniel: Datenschutzrechtliche Zulässigkeit geschlossener Branchenpools, ZD Beilage 12/2020, 1–8;*

*Auernhammer, hrsg. von Martin Eßer, Philipp Kramer, Kai von Lewinski, DSGVO, BDSG, 7. Aufl. 2020 (zit.: Auernhammer-Bearbeiter);*

*Auer-Reinsdorff, Astrid / Conrad, Isabell (Hrsg.): Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019 (zit.: Auer-Reinsdorff/Conrad-Bearbeiter);*

*Beck'scher Online-Kommentar Datenschutzrecht, hrsg. von Stefan Brink und Heinrich Amadeus Wolff, 37. Edition, Stand: 01.08.2021 (zit.: BeckOK DatenschutzR-Bearbeiter);*

*Beck'scher Online-Kommentar Grundgesetz, hrsg. von Volker Epping und Christian Hillgruber, 48. Edition, Stand: 15.08.2021 (zit.: BeckOK GG-Bearbeiter);*

*Beck'scher Online-Kommentar IT-Recht, hrsg. von Georg Borges und Marc Hilber, 4. Edition, Stand: 01.05.2021 (zit.: BeckOK IT-Recht-Bearbeiter);*

*Begleitforschung PAiCE, iit-Institut für Innovation und Technik in der VDI / VDE Innovation + Technik GmbH: Potenziale der Künstlichen Intelligenz im produzierendem Gewerbe in Deutschland, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi), 2018, potenziale-kuenstlichen-intelligenz-im-produzierenden-gewerbe-in-deutschland.pdf (bmwi.de), zuletzt abgerufen am 28.11.2021 (zit.: Begleitforschung PAiCE);*

*Bitkom e. V. / DFKI (Hrsg.): Künstliche Intelligenz, Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, 2017 (zit.: Bitkom/DFKI, Künstliche Intelligenz);*

*Borges, Georg: A legal Framework for Autonomous Systems, in: Georg Borges/ Christoph Sorge (Hrsg.), Law and technology in a global digital society. Autonomous systems, big data, IT security and legal tech, Springer, im Erscheinen 2022;*

*Dammann, Ulrich: Erfolge und Defizite der EU-Datenschutzgrundverordnung, Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307–314;*

*Datenethikkommission der Bundesregierung: Gutachten, Oktober 2019, abrufbar unter:* Gutachten der Datenethikkommission (bund.de)*;*

*Drechsler, Jörg / Jentzsch, Nicola: Synthetische Daten: Innovationspotential und gesellschaftliche Herausforderungen, 2018, abrufbar unter https://www.stiftung-nv.de/sites/default/files/synthetische_daten.pdf (zit.: Drechsler/Jentzsch);*

*Dressel, Julia / Farid, Hany: The accuracy, fairness, and limits of predicting recidivism, Science Advances 2018 (Vol 4), No. 1;*

*Ebers, Martin / Heinze, Christian / Krügel, Tina / Steinrötter, Björn: Künstliche Intelligenz und Robotik, Rechtshandbuch, 2020 (zit.: EHKS-Bearbeiter);*

*Ebert, Andreas / Spiecker gen. Döhmann, Indra: Der Kommissionsentwurf für eine KI-Verordnung der EU, Die EU als Trendsetter weltweiter KI-Regulierung, NVwZ 2021, 1188–1193;*

*Ehmann, Eugen / Selmayr, Martin (Hrsg.): DS-GVO, 2. Aufl. 2018 (zit.: Ehmann/Selmayr-Bearbeiter);*

*Eifert, Martin (Hrsg.): Digitale Disruption und Recht, Workshop zu Ehren des 80. Geburtstags von Wolfgang Hoffmann-Riem, 2020 (zit.: Bearbeiter in Eifert, Digitale Disruption und Recht, 2020);*

*Enquete-Kommission Künstliche Intelligenz: Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale, Bericht, BT-Drs. 19/23700 (zit.: Bericht Enquete-Kommission KI);*

*Flores, Anthony W. / Lowenkamp, Christopher T. / Bechtel, Kristin: False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks.", Federal Probation, 2016 (Vol 80), No. 2, pp. 38–46, abrufbar unter: 80_2_6_0.pdf (uscourts.gov);*

*Franzen, Martin / Gallner, Inken / Oetker, Hartmut (Hrsg.) Kommentar zum europäischen Arbeitsrecht, 4. Aufl.2022 (zit.: Franzen/Inken/Oekter-Bearbeiter);*

*Gesellschaft für Informatik e.V. (Hrsg.): Abschlussbericht ExamAI – KI Testing und Auditing Herausforderungen, Lösungsansätze und Handlungsempfehlungen für das Testen, Auditieren und Zertifizieren von KI, 2021, abrufbar unter https://gi.de/fileadmin/PR/Testing-AI/Abschlussbericht_ExamAI_-_KI_Testing_und_Auditing.pdf;*

*Gesellschaft für Informatik (Hrsg.): Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Gutachten der Fachgruppe Rechtsinformatik der Gesellschaft für Informatik e.V. im Auftrag des Sachverständigenrats für Verbraucherfragen (Hrsg.), 2018, abrufbar unter https://adm.gi.de/fileadmin/GI/Allgemein/PDF/GI_Studie_Algorithmenregulierung.pdf (zit.: GI-Studie);*

*Ehmann, Eugen / Selmayr, Martin (Hrsg.): DS-GVO, 2. Aufl. 2018; zit.: Ehmann/Selmayr-Bearbeiter;*

*Gola, Peter (Hrsg.): DS-GVO, Kommentar, 2. Aufl. 2018 (zit.: Gola-Bearbeiter);*

*Hauer, Marc / Adler, Rasmus / Zweig, Katharina: Assuring Fairness of Algorithmic Decision Making, 2021 IEEE International Conference on Software Testing, Verification and Validation Workshops, abrufbar unter https://ieeexplore.ieee.org/abstract/document/9440188;*

*Heinemeyer, Dennis: Datenverarbeitungs-Crashtests ohne Daten-Dummys, CR 2019, 147–151;*

*Hennemann, Moritz / Kumkar, Lea Katharina: Robo Advice und automatisierte Entscheidungen im Einzelfall, in: Linardatos (Hrsg.). Rechtshandbuch Robo-Advice, 2019, § 13, S. 324–338 (zit.: Hennemann/Kumkar, in Linardatos, § 13);*

*Horner, Susanne / Kaulartz, Markus: Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7–14;*

*Hornung, Gerrit / Wagner, Bernd: Anonymisierung als datenschutzrelevante Verarbeitung?, ZD 2020, 223–228;*

*Krämer, Hannes: Die bußgeldbewehrte „Dash-Cam", NZV 2018, 146;*

*Krumm, Stephan / Dwertmann, Anne: Perspektiven der KI in der Medizin, in: Volker Wittpahl (Hrsg.), Künstliche Intelligenz, 2019, S. 161–175.*

*Kühling, Jürgen: Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, 1–26;*

*Kühling, Jürgen / Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung, BDSG, 3. Aufl. 2020 (zit.: Kühling/Buchner-Bearbeiter);*

*Kühling, Jürgen / Sackmann, Florian / Schneider, Hilmar: Datenschutzrechtliche Dimensionen Datentreuhänder, Kurzexpertise im Auftrag des Bundesministerium für Arbeit und Soziales, IZA Research Report No. 104, 2020, abrufbar unter https://ftp.iza.org/report_pdfs/iza_report_104.pdf (zit.: Kühling/Sackmann/Schneider);*

*Kumkar, Lea Katharina / Roth-Isigkeit, David: Erklärungspflichten bei automatisierten Datenverarbeitungen nach der DSGVO, JZ 2020, 277–286;*

*Langer, Markus / Oster, Daniel / Speith, Timo et al., What do we want from Explainable Artificial Intelligence (XAI)? – A stakeholder perspective on XAI and a conceptual model guiding interdisciplinary XAI research, AI 296 (2021), 103473;*

*Lapuschkin, Sebastian / Wäldchen, Stephan / Binder, Alexander / Montavon, Grégoire / Samek, Wojciech / Müller, Klaus-Robert: Unmasking Clever Hans predictors and assessing what machines really learn, Nature Communications 10, 1096 (2019), abrufbar unter https://www.nature.com/articles/s41467-019-08987-4.pdf;*

*Linardatos, Dimitrios: Autonome und vernetzte Aktanten im Zivilrecht, 2021;*

*Lutz, Lennart: Datenschutzrechtliche Herausforderungen auf dem Weg zum automatisierten Fahren. Verarbeitung von Daten aus dem öffentlichen Verkehrsraum zur Algorithmenentwicklung, ZD 2020, 450—454;*

*Marsch, Nikolaus: KI und das europäische Datenschutzgrundrecht – Spielräume für technologische Innovation und innovativen Schutz, in: Veronika Fischer / Peter J. Hoppen / Jörg Wimmers (Hrsg.). DGRI Jahrbuch 2018, 2019, S.175–198.*

*Martini, Mario: Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, 2019; zit.: Martini Blackbox Algorithmus;*

*Martini, Mario / Nink, David: Wenn Maschinen entscheiden … Persönlichkeitsschutz in vollautomatisierten Verwaltungsverfahren, NVwZ 2017, 681–682;*

*Meents, Jan Geert: Datenschutz durch KI, in: Markus Kaulartz / Tom Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 8.8, S. 445 – 461;*

*Meyer, Julia: Identität und virtuelle Identität natürlicher Personen im Internet, 2011;*

*Moos, Flemming / Rothkegel, Tobis: Nutzung von Scoring-Diensten im Online-Versandhandel, ZD 2016, 561 – 568;*

*Paal, Boris: Spannungsverhältnis von KI und Datenschutzrecht, in: Markus Kaulartz / Tom Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 8.7, S. 427 – 444;*

*Paal, Boris / Pauly, Daniel (Hrsg.): Datenschutz-Grundversordnung, Bundesdatenschutzgesetz, 3. Auf. 2021 (zit.: Paal/Pauly-Bearbeiter);*

*Piltz, Carlo: BDSG. Praxiskommentar für die Wirtschaft, 2018;*

*Plath, Kai-Uwe (Hrsg.): Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, 3. Aufl. 2018 (zit.: Plath-Bearbeiter);*

*Raji, Behrang: Rechtliche Bewertung synthetischer Daten für KI-Systeme, DuD 2021, 303–309;*

*Rohrmoser, Raphael: Die Auswirkungen des neuen BDSG und der DSGVO auf das Verbraucherschutzniveau bei der Datenerhebung und dem Scoringverfahren der SCHUFA, 2020;*

*Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen, Digitalisierung für Gesundheit. Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems, Gutachten 2021, abrufbar unter https://www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021.pdf. (zit.: SVR Gesundheitswesen, Gutachten 2021);*

*Samek, Wojciech / Binder, Alexander / Montavon, Grégoire / Lapuschkin, Sebastian / Müller, Klaus-Robert: Evaluating the Visualization of What a Deep Neural Network Has Learned, IEEE Transactions on Neural Networks and Learning Systems 28 (2017), pp. 2660–2673, abrufbar unter https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7552539;*

*Schmidt, Hubert: Kamera ab! Dashcam läuft: Kein Beweisverwertungsverbot trotz rechtswidrig beschafften Beweismaterials, JA 2018, 869–872;*

*Schröder, Michael / Taeger, Jürgen (Hrsg.): Scoring im Fokus: Ökonomische Bedeutung und rechtliche Rahmenbedingungen im internationalen Vergleich, 2014;*

*Schröder, Meinhard: Datenschutz beim Kameraeinsatz im Automobil, ZD 2021, 302–307;*

*Schwartmann, Rolf / Jaspers, Andreas / Thüsing, Gregor / Kugelmann, Dieter (Hrsg.): DVSGO/BDSG, 2. Aufl. 2020 (zit.: Schwartmann/Jaspers/Thüsing/Kugelmann-Bearbeiter);*

*Simitis, Spiros / Hornung, Gerrit / Spiecker genannt Döhmann, Indra (Hrsg.): Datenschutzrecht, DSGVO mit BDSG, 2019 (zit.: Simitis/Hornung/Spieker-Bearbeiter);*

*Specht-Riemenschneider, Louisa / Blankertz, Akine / Sierek, Pascal / Schneider, Ruben / Knapp, Jakob / Henne, Theresa: Die Datentreuhand, Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, MMR-Beilage 2021, 25–48;*

*Spindler, Gerald: Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E), Ansatz, Instrumente, Qualität und Kontext, CR 2021, 361–374;*

*Spindler, Gerald / Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 4. Aufl. 2019 (zit.: Spindler/Schuster-Bearbeiter);*

*Stevens, Jeremy: Datenqualität bei algorithmischen Entscheidungen, Überlegungen aus Anlass des Gutachtens der Datenethikkommission, CR 2020, 73–79;*

*Strauß, Samuel: Dashcam und Datenschutz, Eine kritische Gegenüberstellung von alter und neuer Rechtslage, NZV 2018, 554–559;*

*Sydow, Gernot (Hrsg.): Europäische Datenschutzgrundverordnung, 2. Aufl. 2018 (zit.: Sydow-Bearbeiter);*

*Taeger, Jürgen / Gabel, Detlev: DSGVO, BDSG, Kommentar, 3. Aufl. 2019 (zit.: Taeger/Gabel-Bearbeiter);*

*Valera, Isabel: Discrimination in Algorithmic Decision Making, in Ulla Weber (Hrsg.), Fundamental Questions, Gender Dimensions in Max Planck Research Projects, 2021, S. 15–26 (zit.: Valera);*

*Valkanova, Monika: Trainieren von KI-Modellen, in: Markus Kaulartz / Tom Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 8.1, S. 336 – 351;*

*Valta, Matthias / Vasel, Johann Justus: Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz, Mit viel Bürokratie und wenig Risiko zum KI-Standort, ZRP 2021, 142–145;*

*v. Mangoldt/Klein/Starck, GG, Kommentar, begründet von Hermann v. Mangold, fortgeführt von Friedrich Klein und Christian Starck, herausgegeben von Peter M. Huber und Andreas Voßkuhle, Band 1, 7. Aufl. 2018 (zit.: Mangoldt/Klein/Starck-Bearbeiter);*

*Wegner, Susan: Synthetische Daten, in: Andreas Leupold / Andreas Wiebe / Silke Glossner (Hrsg.): IT-Recht. Rech, Wirtschaft und Technik der digitalen Transformation, 4. Aufl. 2021 Teil 6.5, S. 572 – 586 (zit.: Leupold/Wiebe/Glossner-Wegner);*

*Weichert, Thilo: Datenverarbeitung und Datenschutz bei Tesla-Fahrzeugen. Kfz-Automation und informationelle Selbstbestimmung, 2020, abrufbar unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020tesla.pdf; zit: Weichert, Tesla-Gutachten;*

*Zech, Herbert: Künstliche Intelligenz und Haftungsfragen, ZfPW 2019, 198–219;*

*Zweig, Katharina / Hauer, Marc / Raudonat, Franziska: Anwendungsszenarien KI-Systeme im Personal- und Talentmanagement, 2020, abrufbar unter https://testing-ai.gi.de/fileadmin/PR/Testing-AI/ExamAI_Publikation_Anwendungsszenarien_KI_HR.pdf.*

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

gestiftet von der Bundesrepublik Deutschland
vertreten durch den Vorstand Frederick Richter

Die Arbeit der Stiftung Datenschutz wird aus dem Bundeshaushalt gefördert (Einzelplan des BMI).

Bundesministerium des Innern, für Bau und Heimat

Bildnachweis Titel: https://thispersondoesnotexist.com/