Conrad Sebastian Conrad

Kann die Künstliche Intelligenz den Menschen entschlüsseln? – Neue Forderungen zum Datenschutz

Eine datenschutzrechtliche Betrachtung der „Künstlichen Intelligenz“

Aktuelle Studien behaupten, die sogenannte „Künstliche Intelligenz“ (KI) könne inzwischen sogar Krankheiten oder die sexuelle Ausrichtung einer Person erkennen. Gilt der Mensch damit bereits als entschlüsselt? Dieser Beitrag bietet zunächst einen Überblick der gesellschaftlichen Folgen, beschäftigt sich aber auch mit den juristischen Konsequenzen einer derartigen (fiktiven) Zukunftsvision.

1 Einführung

Aktuelle Untersuchungen zum Einsatz der sogenannten „Künstlichen Intelligenz“ (KI) erwecken den Eindruck, der Mensch sei bereits entschlüsselt. Hintergrund ist, dass mit steigender technologischer Entwicklung und rasant zunehmenden Deep Learning Verfahren die KI-basierten Anwendungen das Verhalten des Menschen analysieren. So sollen Medienberichten zur Folge Krankheiten vorhergesagt, eine Lüge nachgewiesen oder sogar die sexuelle Ausrichtung des Menschen erkannt werden können.

Wenn die KI-Prozesse den Menschen jedoch auf derartige Art und Weise vollständig entschlüsseln bzw. nachahmen können, besteht eine erhebliche Gefahr für die Privatsphäre des Einzelnen. Es werden sogar Phantasien über „Menschenklone“ und des Dataismus[1] real, die über den Tod hinaus in der digitalen Welt weiterleben.

1.1 Aktuelle Studien

Wissenschaftliche Studien präsentieren teilweise Ergebnisse, nach denen moderne und KI-basierte Anwendungen auf Grund von Deep Learning Prozessen immer exakter bestimmte Vorgaben erfüllen können. Verkürzte Medienberichte stellen in Aussicht, dass die Programme beispielsweise die sexuelle Ausrichtung eines Menschen,[2] Suizidgedanken,[3] die Straffälligkeit einer Person[4] oder aber dessen Todeszeitpunkt identifizieren bzw. vorhersagen können.[5] Ähnlich soll die Gesichtserkennung anhand biometrischer Daten den Menschen lebenslang erkennen bzw. wiedererkennen[6] und die Verhaltensbiometrie einen Menschen nach wenigen Tastenschlägen identifizieren können.[7] Anhand von Stimme und Gesprächssituation wäre zudem eine psychologische Auswertung ermöglichen, wodurch beispielsweise eine Lüge erkannt werden könnte.[8] Überdies verstehen digitale Assistenten wie Amazon Alexa und Google Home schon heute Befehle per Sprachsteuerung und liefern dem Benutzer mit der Zeit im-

1 Der Historiker Yuval Harari sieht bereits das Ende des Humanismus nahe; Vgl. dazu: http://www.wiwo.de/technologie/digitale-welt/serie-kuenstliche-intelligenz-das-dogma-des-dataismus/19164982-2.html (letzter Aufruf: 15.6.2018).

Conrad Sebastian Conrad

Justiziar – datenschutz nord GmbH

E-Mail: cconrad@datenschutz-nord.de

2 Vgl. https://www.heise.de/newsticker/meldung/KI-erkennt-am-Gesicht-ob-Menschen-schwul-oder-lesbisch-sind-3825449.html (letzter Abruf: 15.6.2018).

3 Vgl. https://www.wired.de/collection/tech/kanadische-kis-suchen-soziale-netzwerke-nach-selbstmordgefaehrdung-ab (letzter Abruf: 15.6.2018).

4 Vgl. https://www.datenschutz-notizen.de/kann-kuenstliche-intelligenz-bald-straftaten-vorhersehen-4316703/ (letzter Abruf: 15.6.2018); auch: https://www.wired.de/collection/tech/kuenstliche-intelligenz-ki-ai-polizei-grossbritannien-hart-university-cambridge (letzter Abruf: 15.6.2018).

5 Vgl. https://www.heise.de/newsticker/meldung/Forschung-Kuenstliche-Intelligenz-sagt-den-Todeszeitpunkt-voraus-3951488.html (letzter Abruf: 15.6.2018) – Studie der Stanford University; https://arxiv.org/pdf/1711.06402.pdf (Letzter Abruf: 15.6.2018).

6 Vgl. *Jandt*, ZRP 2018, S. 16 ff.

7 Vgl. https://www.datenschutz-notizen.de/verhaltensanalyse-beim-online-banking-mit-dem-datenschutz-vereinbar-2018287/ (letzter Abruf: 15.6.2018).

8 So z.B. ein Forschungsprojekt der University of Maryland, https://arxiv.org/pdf/1712.04415.pdf (letzter Abruf: 15.06.2018).

mer passgenauere Inhalte, vermitteln also einen auf den Nutzer zugeschnittenen individuellen Wissenszugang.

1.2 Entschlüsselung des Menschen

Wenn die überlieferten Ergebnisse dieser Untersuchungen zutreffen, stände der Mensch kurz vor seiner (biometrischen) Entschlüsselung. Sein Verhalten und weite Teile seines Lebens ließen sich jederzeit analysieren bzw. kontrollieren, zukünftiges Verhalten vorhersehen, der Mensch wäre in der Konsequenz nur noch ein statistischer Wert.[9] Die damit einhergehenden Folgen wären gravierend und unterstreichen die Gefahren der KI. Nicht ohne Grund warnen bereits Forscher vor düsteren Zukunftsszenarien.[10]

Doch die aktuelle Situation lässt Zweifel an diesen Thesen aufkommen, insbesondere wenn die Fehlerhaftigkeit der KI-basierten Systeme zutage tritt,[11] Gesichter verpixelt sind[12] bzw. nicht korrekt bewertet oder erkannt werden und äußerst niedrige Trefferquoten die grundlegenden Mechanismen infrage stellen.[13] Gleiches gilt bei der Fehlerhäufigkeit von Sprachsteuerung[14] bzw. sprachgesteuerten Systemen oder selbstlernenden Chatbots (Microsoft tay[15]). Diese können sich vielmehr immer nur in dem kleinen vorgegebenen Korridor bewegen. So dass durch ein Training anhand von Fotos zwar die Anwendung zwischen Hund und Katze unterscheiden kann, jedoch nicht einmal weiß, was ein Tier ist. Und der Lernprozess ließe sich noch durch bewusstes falsches Material manipulieren – und wird im Übrigen zumeist nur mit Stereotypen ohne Vielfalt vollzogen.

Viele dieser Studien können daher nicht belegt werden. Sie fußen auf bloßen Wahrscheinlichkeitsberechnungen. Einige Forscher verneinen daher sogar einen Fortschritt im derzeitigen Stadium der KI[16] und bezeichnen die KI als einen „Marketing-Begriff".[17] Auch wird von einigen Wissenschaftlern die Wirtschaftlichkeit der Automatisierung bezweifelt. Hinzu kommt, dass angesichts vermeintlich autonomer Prozesse wie das autonome Fahren im Taxi- und Post-Gewerbe oder im privaten Gebrauch, die Fehler sogar zum Tod eines Menschen führen[18] oder Katastrophen wie z.B. einen Krieg auslösen können.

1.3 (Fiktive) Zukunftsvision der KI

Doch angesichts der rasanten Entwicklung der KI erscheinen die aufgeworfenen Szenarien nicht utopisch. Immerhin können Deep Learning Prozesse dazu führen, dass die Treffergenauigkeit erhöht wird. Je mehr Daten die KI vom Betroffenen erfasst und verarbeitet und je umfangreicher die Berechnungsmethoden durch neuronale Netzwerke unterstützt werden, desto genauer entsteht ein Bild über den Einzelnen. Durch stetige Testdurchläufe und größer werdende vergleichende Analysen, erhöht sich die Genauigkeit der Vorhersage. Diese Daten werden zunehmend miteinander verknüpft. So lässt sich der Einzelne durch sein Verhalten oder seine Biometrie immer treffsicherer identifizieren. Die Genauigkeit von Aussagen über den Betroffenen nimmt durch die KI-basierten Anwendungen daher zu. Im Ergebnis wird der Mensch in seinem Verhalten dadurch nahezu entschlüsselt, was sich der Anwender oder Dritte zu Nutze machen können. Sicherheitskontrollen dürften dadurch effizienter werden, zahlreiche Anwendungsfelder, zum Beispiel im Kundensupport oder bei der automatisierten Berechnung von Wahrscheinlichkeiten (Scoring Daten), wie auch die automatisierte Personalisierung von Inhalten sind denkbar. Dies führt zu den Gefahren und Risiken der KI, wie sie sich beispielsweise in der Preismanipulation, der Ausübung von Überwachungsdruck und der Vorverurteilungen bzw. der Diskriminierungen einzelner Personen äußern können.[19]

Die Fortentwicklung der KI wird aber auch gesellschaftliche, derzeit nicht abzusehende Folgen haben, wenn das Verhalten eines Menschen entschlüsselt und zukünftige Aktivitäten vorherzusagen sind.

2 Datenschutzrechtliche Anforderungen

Bei Betrachtung dieser denkbaren Auswertungsmöglichkeiten eines Menschen bei Einsatz der KI, stellt sich hingegen die Frage, ob das Datenschutzrecht die Rechte und Freiheiten des Einzelnen vor der Verletzung seiner Persönlichkeit überhaupt ausreichend schützen und somit der Entwicklung zur Entschlüsselung des Menschen entgegenwirken kann. Denn für den Einsatz derartiger Verfahren und KI-basierter Anwendungen gilt, den datenschutzrechtlichen Anforderungen gerecht zu werden, die unter anderem die Rechtmäßigkeit der Datenverarbeitung vorsehen sowie geeignete Schutzkonzepte und Maßnahmen zum Schutz des allgemeinen Persönlichkeitsrechts fordern.

2.1 Rechtmäßigkeit der Verarbeitung

Die KI-basierten Anwendungen verarbeiten personenbezogene Daten nach Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO), zum Beispiel das Geschlecht, das Alter, den Standort oder

9 Vgl. hierzu das neue chinesische „Sozialkreditsystem", in dem praktisch jede Bewegung des Einzelnen erfasst und bewertet wird: https://www.tagesschau.de/ausland/ueberwachung-china-101.html (letzter Abruf: 15.6.2018).

10 Vgl. http://www.sueddeutsche.de/digital/technologie-fuehrende-forscher-warnen-vor-kuenstlicher-intelligenz-1.3878669 (letzter Abruf: 15.6.2018), ebenso: https://www.businessinsider.de/stephen-hawking-warnt-vor-den-folgen-kuenstlicher-intelligenz-2017-11 (letzter Abruf: 15.6.2018).

11 Vgl. https://www.tagesspiegel.de/politik/wenn-der-algorithmus-versagt-so-dumm-ist-kuenstliche-intelligenz/20602294.html (letzter Abruf: 15.6.2018).

12 Vgl. https://www.heise.de/newsticker/meldung/Deepfakes-Neuronale-Netzwerke-erschaffen-Fake-Porn-und-Hitler-Parodien-3951035.html (letzter Abruf: 15.6.2018).

13 Vgl. https://www.heise.de/tp/features/Gesichtserkennung-von-Menschenmassen-mit-einer-Fehlerrate-von-92-Prozent-4042982.html (letzter Abruf: 15.6.2018); auch: https://www.spektrum.de/news/die-tuecken-der-gesichtserkennung/1521469 (letzter Abruf: 15.6.2018); und: https://www.heise.de/newsticker/meldung/Kuenstliche-Intelligenz-als-Gefahr-Menschheit-muss-sich-auf-Regeln-einigen-4077950.html (letzter Abruf: 15.6.2018).

14 Vgl. http://www.sueddeutsche.de/digital/amazon-alexa-lachen-1.3897561 (letzter Abruf 15.6.2018).

15 Vgl. https://www.zeit.de/digital/internet/2016-03/microsoft-tay-chatbot-twitter-rassistisch (letzter Abruf: 15.6.2018).

16 Vgl. *Schael*, DuD 2018, S. xx (in diesem Heft)

17 So der Dozent Timo Daum in einer Kolumne; https://www.heise.de/newsticker/meldung/Missing-Link-Ein-Plaedoyer-wider-den-KI-Populismus-4063789.html?seite=2 (letzter Abruf: 15.6.2018).

18 So z.B. durch autonome Fahrzeuge im Straßenverkehr; vgl. https://www.heise.de/newsticker/meldung/Tod-mit-autonomem-Auto-Uber-Fahrerin-schaute-vor-Unfall-nach-unten-4001186.html (letzter Abruf: 21.5.2018); oder aber: http://www.manager-magazin.de/unternehmen/autoindustrie/tesla-autopilot-beschleunigte-tesla-model-x-vor-toedlichem-unfall-a-1211986.html (letzter Abruf: 15.6.2018).

19 Vgl. *Conrad*, DuD 2017, S. 742.

aber das Gewicht. Dies eröffnet den Anwendungsbereich der Datenschutz-Grundverordnung. Irrelevant ist dabei die zeitliche Dauer der Verarbeitung, weswegen auch das Caching bzw. kurzzeitige Speichern oder Umrechnen von Informationen bereits unter dem Begriff der Verarbeitung in der Datenschutz-Grundverordnung fällt.[20] Gegenteilige Auffassungen würden die Anwendbarkeit des Datenschutzrechts von einer zeitlichen Komponente abhängig machen, welches sowohl technisch als auch rechtlich zu Abgrenzungsschwierigkeiten führen und einzelne Prozesse in der Datenverarbeitungskette unterschiedlich werten würde. Darüber hinaus sind jedoch außerdem besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) betroffen, wenn Gesundheitsdaten oder biometrische Daten beispielsweise bei Erfassung oder Auswertung der Stimme sowie des Verhaltens eines Nutzers vorliegen oder eine Gesichtserkennung erfolgt.[21]

Die Rechtmäßigkeit der Verarbeitung erfordert dabei für die Annahme einer die Datenverarbeitung erlaubenden Rechtsgrundlage (Art. 6 DS-GVO) das Vorliegen einer entsprechenden Rechtsvorschrift oder die Einwilligung des Betroffenen (Art 6. Abs. 1 S. 1 lit. a) bzw. Art. 7 DS-GVO). Als Rechtsvorschrift kommt in Betracht die Rechtsgrundlage aus Art. 6 Abs. 1 S. 1 lit. b) DS-GVO, wenn die Verarbeitung zur *„Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich"* ist. Dieses könnte vorliegen, wenn die Gesichtserkennung als Authentifizierung beim Kauf oder Online-Banking dient. In der Regel sind diese sensiblen Angaben des Betroffenen allerdings kein Bestandteil eines Vertrages. Mithin kann die Datenverarbeitung durch die KI-basierte Anwendung aber auch dann zulässig sein, wenn dies nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO *„zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich"* ist, wobei hieran eine Interessensabwägung im Einzelfall anschließt. Sind dabei Kinder betroffen, so soll das berechtigte Interesse des Kindes grundsätzlich überwiegen. Ohnehin dürfte der Schutz des Einzelnen bei der Verarbeitung sensibler Daten überwiegen.

Sodann bleibt zumeist nur die Einwilligung des Betroffenen als Rechtsgrundlage der Datenverarbeitung (Art. 6 Abs. 1 S. lit. a) DS-GVO), deren Nachweis der Verantwortliche jederzeit zu erbringen hat (Art. 7 Abs. 1 DS-GVO). Bei der Verarbeitung biometrischer Daten und sonstiger besonderer Kategorien gelten sogar noch höhere Anforderungen (Art. 9 DS-GVO).[22] Denn soweit biometrische Daten[23] betroffen sind, die zur eindeutigen Identifizierung einer Person Verwendung finden, ist deren Verarbeitung grundsätzlich verboten (Art. 9 Abs. 1 DS-GVO).[24] Eine Ausnahme hiervon bilden die Fälle, in denen der Betroffene ausdrücklich seine Einwilligung in den zuvor festgelegten Zweck erteilt hat (Art. 9 Abs. 2 lit. a) DS-GVO).

Die Einwilligung ist auf Grund ihrer Tragweite an zahlreiche Voraussetzungen geknüpft. Unter anderem ist der Betroffene insbesondere vor Abgabe seiner Zustimmung über Art und Ausmaß der Datenverarbeitung *„in nachvollziehbarer Weise"* zu informieren (Transparenzgebot) sowie über dessen Zweck und den Verantwortlichen aufzuklären (Art. 5 DS-GVO).[25] Die Einwilligung muss auch jederzeit einsehbar und durch die betroffene Person widerrufbar sein (Art. 7 Abs. 3 DS-GVO). Wie Erwägungsgrund 32 zu entnehmen ist, sollte die Einwilligung *„durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist[..]."* Bei der elektronischen Datenverarbeitung wird in der Regel die ausdrückliche Einwilligung zu fordern sein, was ein aktives und freiwilliges Handeln des Betroffenen (Anklicken einer Checkbox) voraussetzt.[26] Die konkludente Einwilligung allein durch Installation der Anwendung oder Kauf einer Hardware durch die betroffene Person wäre demzufolge unzulässig.[27]

Die Freiwilligkeit der Einwilligung lässt sich in der Praxis bezweifeln, wenn die allgegenwärtigen Systeme ein unersetzlicher Bestandteil der EDV geworden und oftmals für die tägliche Kommunikation zwingend erforderlich sind (sog. Lock-in Effekt[28]). Abhilfe könnte eine Wahlfreiheit für datenschutzfreundliche Systemeinstellung und alternative (anonyme) Systeme schaffen, die jedoch der Gesetzgeber oder das Kartellamt erzwingen müsste.[29] Ebenso lässt sich die Freiwilligkeit im Beschäftigungsverhältnis wegen des zumeist bestehenden Abhängigkeitsverhältnisses des Mitarbeiters hinterfragen.

Beim Profiling darf jedoch trotz ausdrücklicher Einwilligung des Betroffenen gem. Art. 22 Abs. 2 DS-GVO die auf eine automatisierte Verarbeitung beruhende „Entscheidung" des Programms nicht auf biometrische Daten zugreifen (Art. 22 Abs. 4 DS-GVO).[30] Dieses würde die KI-Anwendungsfelder drastisch reduzieren,[31] da im Ergebnis bei der Gestaltung des Angebots, wie auch bei dem rechtsgeschäftlichen Handeln der digitalen Assistenten, keine biometrischen Daten verarbeitet werden dürften.[32] Doch gerade dieses ist häufig das Konzept der Anwendung und ermöglicht passgenaue Inhalte bzw. Angebote.

2.2 Zusätzliche Anforderungen

Aus der Datenschutz-Grundverordnung ergeben sich darüber hinaus weitere, allgemeine datenschutzrechtliche Anforderungen an die rechtmäßige Datenverarbeitung. Grundsätzlich ist die Rechtmäßigkeit und Verarbeitung nach Treu und Glauben gem. Art. 5 Abs. 1 lit. a) DS-GVO zu gewährleisten.

Diese muss sich an einem zuvor eindeutig festgelegten und rechtmäßigen Zweck halten (Art 5 Abs. 1 lit. b) DS-GVO). Der Zweck muss auch schon zu diesem Zeitpunkt feststehen,[33] weswegen die weiterentwickelte „Maschine" nicht neue Aufgaben von sich aus kreieren und sogar eigene Schlussfolgerungen tref-

20 Vgl. *Quiel*, PinG 01.18, S. 34; *Schwenke*, NJW 2018, S. 824.
21 Vgl. *Jandt*, ZRP 2018, 16 ff; *Schwenke*, NJW 2018, S. 825.
22 Vgl. Erwägungsgrund 51 der Datenschutz-Grundverordnung.
23 *Ernst*; in: Paal/Pauly, DS-GVO, Art. 4, Rn. 99 ff.
24 *Schiff*, in: Ehmann/Selmayr, DS-GVO, Art. 9, Rn. 22.
25 Vgl. Erwägungsgrund 58 der Datenschutz-Grundverordnung.
26 Vgl. Erwägungsgrund 32 der Datenschutz-Grundverordnung; *Heberlein*; in: Ehmann/Salmayr, DS-GVO, Art. 6, Rn. 11.
27 Vgl. *Albrecht*, CR 2016, S. 91.
28 Vgl. http://www.sueddeutsche.de/digital/streit-ueber-datenschutz-verbraucherschuetzer-gehen-gegen-googles-email-scannen-vor-1.2880644-2 (Abruf: 30.5.2018).
29 Vgl. http://www.handelsblatt.com/politik/deutschland/datenskandal-fdp-und-gruene-drohen-facebook-mit-zerschlagung/21131940.html?ticket=ST-645876-lkwkhap5vr11YhWwUvHA-ap1 (letzter Abruf: 15.6.2018).
30 *Hladjk*, in: Ehmann/Selmayr, DS-GVO, Art. 22, Rn. 16.
31 Vgl. Wojak, DuD 2018, S. 553 (in diesem Heft).
32 Der Betroffene ist ausdrücklich auf das Profiling hinzuweisen, vgl. Erwägungsgrund 60 der Datenschutz-Grundverordnung; Die Regelung des Art. 22 Abs. 1 DS-GVO hat somit mittelbar einen Verbotscharakter – *Schulz*, in: Gola, DS-GVO, Art. 22, Rn. 5.
33 Vgl. S. 6 Erwägungsgrund 39 der Datenschutz-Grundverordnung.

fen darf. Mithin ist dem Grundsatz der Datensparsamkeit und Datenminimierung nach Art. 5 Abs. 1 lit. c) DS-GVO gerecht zu werden. Dieses meint eine Begrenzung der Datenverarbeitung auf das notwendige Maß,[34] was gegen eine unbefristete Speicherung allmöglicher Daten spricht. Mithin müssen die Datensätze auch richtig bzw. ggf. auf dem neuesten Stand sein (Art. 5 Abs. 1 lit. d) DS-GVO).

3 Datenschutzkonforme Umsetzung

An die datenschutzkonforme Umsetzung sind zahlreiche Anforderungen zu stellen. Bereits die Bestimmung des Adressaten dieser Verpflichtung offenbart die Anwendungsschwierigkeiten, wenn hinsichtlich der Datenverarbeitung zwischen dem Entwickler bzw. Hersteller, dem Betreiber, dem „Nutzer" und eben der „KI" als eigene Handlungsform differenziert werden muss, und hier unter Umständen sogar eine Auftragsverarbeitung in Betracht kommt.[35] Ebenso lassen sich Szenarien skizzieren, wenn mehrere KI-Algorithmen bzw. mehrere Verantwortliche (zusammen) agieren.[36] In die Pflicht genommen wird grundsätzlich der „Verantwortliche" im Sinne von Art. 4 Nr. 7 DS-GVO, also wer *„allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet"*. In der Realität wird der vermeintlich Verantwortliche (z. B. die Werbe-Agentur oder die Polizeibehörde[37]), der lediglich ein gekauftes Produkt oder für ihn entwickeltes System einsetzt, spätestens bei Produkten auf dem Massenmarkt keine Kenntnisse der Datenverarbeitung im Hintergrund der Anwendung oder der möglichen Nebeneinsatzfelder der Technologie besitzen und hat folgerichtig nur bedingt Möglichkeiten, tatsächlich die Mittel und Zwecke der eingesetzten Algorithmen zu bestimmen.

Schließlich hat jeweils der Verantwortliche als solcher transparent über die Datenverarbeitung aufzuklären, insbesondere wenn diese auf der Einwilligung des Betroffenen beruht. In den Datenschutzbestimmungen sind ferner die allgemeinen Informationspflichten nach Artt. 12 ff. DS-GVO entsprechend umzusetzen, d. h. der Betroffene muss vom Verantwortlichen bei der Direkterhebung unter anderem über den Namen des Verantwortlichen (Art. 13 Abs. 1 lit. a) DS-GVO), die Zwecke der Datenverarbeitung sowie die Rechtsgrundlage (Art. 13 Abs. 1 lit. c) DS-GVO), den Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (Art. 13 Abs. 1 lit. e) DS-GVO), wie auch die Speicherdauer bzw. Löschkonzepte (Art. 13 Abs. 2 lit a) DS-GVO) und Betroffenenrechte (Art. 13 Abs. 2 lit. b) DS-GVO) umfassend informiert werden. Ebenso könnte ein Profiling gemäß § 22 DS-GVO vorliegen, so dass der Nutzer *„aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person"* (Art. 13 Abs. 2 lit. f) DS-GVO) zu erhalten hat.

Zudem sind die Betroffenenrechte (Artt. 12 ff. DS-GVO) zu wahren, d. h. der Betroffene muss jederzeit die Kontrolle über die Verarbeitung seiner Daten ausüben können. Dies kann die Auskunft (Art. 15 DS-GVO) sein, aber auch der Anspruch auf Berichtigung (Art. 16 DS-GVO), Löschung der Daten (Art. 17 DS-GVO) und Einschränkung der Verarbeitung der ihn betreffenden Daten (Art. 18 DS-GVO).

Sodann sind geeignete Löschroutinen zu entwickeln, darüber hinaus dem Gesichtspunkt des „Rechts auf Vergessenwerden" (Art. 17 DS-GVO) angemessen Rechnung tragen, um eine andauernde Verarbeitung zu verhindern. Es besteht ein offenkundiger Konflikt, wenn die ständige Verarbeitung der Daten gerade Sinn und Zweck des Lernprozesses und somit Folge der KI-basierten Anwendung ist.[38]

Ferner muss eine angemessene Sicherheit der Datenverarbeitung gewährleistet werden, was auf Integrität und Vertraulichkeit der Datenverarbeitung abzielt (Art. 5 Abs. 1 lit. f) DS-GVO). Einen Kern des Datenschutzrechts bilden daher die technisch-organisatorischen Maßnahmen gem. Art. 32 DS-GVO, die der Verantwortliche (und der Auftragsverarbeiter) zum angemessenen Schutze der Datenverarbeitung zu ergreifen hat.[39] Dies sind Zielvorgaben, die einer ständigen Anpassung an den Stand der Technik und einer Risikoabschätzung unterliegen sollten. Von den nicht abschließend aufgezählten Merkmalen sind unter anderem die Verschlüsselung der Datenverarbeitung bzw. Pseudonymisierung der Daten wie auch die Integrität und Belastbarkeit der Systeme zu erwähnen. In der Konsequenz hat der Verantwortliche daher ein IT-Konzept umzusetzen, das nach dem Stand der Technik eine sichere Übertragung und allgemein die geschützte Verarbeitung der ihm zugeordneten personenbezogenen Daten gewährleistet. Die Datenschutz-Grundverordnung fordert sogar ausdrücklich ein Verfahren der regelmäßigen Überprüfung der zu dokumentierenden Maßnahmen und der Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b) DS-GVO), um den Verantwortlichen im Laufe der Zeit zur Vornahme angemessener Anpassungen an den Stand der Technik zu zwingen. So hat dieser *„ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung"* (Art. 32 Abs. 1 lit. d) DS-GVO) zu etablieren und einzuhalten.

Die KI-basierten Anwendungen müssen dementsprechend konzipiert werden, insbesondere sollten die personenbezogenen Daten nur über sichere Übertragungswege übermittelt und vor Zugriffen Dritter geschützt werden. Sofern das Verfahren durch eine App auf dem Smartphone oder IoT-Gerät des Nutzers umgesetzt wird und dadurch besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO, wie bspw. Gesundheitsdaten, verarbeitet werden, gelten diese Vorkehrungen umso stärker, damit nicht Dritte die Daten abfangen oder durch andere Apps eine Schnittstelle zu diesen Informationen des Nutzers aufbauen können. Schließlich sind die Daten nicht nur sicher zu verarbeiten, sondern auch durch Backups zu schützen. Der Verantwortliche hat ferner den Dokumentations- und Nachweispflichten entsprechend der Datenschutz-Grundverordnung nachzukommen.[40]

Des Weiteren gilt es, die neuen Steuerungsmittel von Privacy by Design bzw. Privacy by Default (Art. 25 Abs. 1, Abs. 2 DS-GVO) zu berücksichtigen. Daraus lassen sich präventive, als auch

34 *Frenzel*, in: Paal/Pauly, DS-GVO, Art. 5, Rn. 37.

35 Vgl. *Martini*, in: Paal/Pauly, DS-GVO, Art. 24, Rn. 18.

36 Hierzu näher *Wojak*, DuD 2018, S. 553 (in diesem Heft).

37 Der Einsatz von KI-basierten Anwendungen durch die Polizei wird offenbar von einer Mehrheit begrüßt; https://www.bitkom.org/Presse/Presseinformation/Grosse-Mehrheit-fuer-Kuenstliche-Intelligenz-in-der-Polizeiarbeit.html (letzter Abruf: 15.6.2018).

38 Dazu jedoch: Mitbegründer von Apple, Steve Wozniak, https://www.businessinsider.de/sie-versteht-es-nicht-apple-mitgruender-wozniak-kritisiert-im-interview-merkels-technologie-vorstoss-2018-5 (letzter Abruf: 15.6.2018).

39 *Wennemann*, DuD 2018, S. 174 ff.

40 *Wennemann*, DuD 2018, S. 177.

repressive Vorgaben zum Datenschutz durch Technik ableiten.[41] Jedoch sind diese zu unkonkret und richten sich nicht an den Entwickler bzw. Hersteller der Systeme. Doch gerade der Hersteller, der oftmals gar nicht der Verantwortliche ist,[42] sollte in den Adressatenkreis dieser Vorschrift einbezogen werden.[43] Dies ergibt bereits der Wortlaut der Vorschrift, der die Aufgabe zur datenschutzfreundlichen Grundeinstellung bzw. zum Datenschutz durch Technikgestaltung an den Verantwortlichen adressiert. Und dem Erwägungsgrund 78 der Datenschutz-Grundverordnung ist zu entnehmen, dass die Hersteller nur hierzu „ermutigt" werden sollen. Die Regelungen entfalten daher nur mittelbare Wirkung auf die Entwickler bzw. Hersteller der Systeme, die in der Realität allerdings diejenigen sind, die die KI mit „Leben" füllen und die Bandbreite der Möglichkeiten der Anwendung am ehesten erkennen dürften.

Sodann wird der Verantwortliche häufig nicht in der Lage sein, die KI-Mechanismen zu beschränken oder zu stoppen. Deshalb ist eine konsequente Überwachung der Anwendung zu fordern. In diesem Zusammenhang bestehen Forderungen nach einem „Notschalter",[44] um das System zu deaktivieren. Gleichwohl kann darüber diskutiert werden, ob nicht bereits der Entwickler bzw. Hersteller ein Notfallkonzept zu erstellen hat, um zu verhindern, dass die KI den Code selber weiterschreiben und sich selber modifizieren kann.

Somit sind zusätzlich derartige Schutzmodelle zu entwickeln. Die Kontrolle und Evaluation des Programmcodes ist zwingend erforderlich. Die Ergebnisse sind zuvor durch ein Konzept zu definieren, so dass die KI nur Aussagen über den zuvor definierten Zweck treffen kann, nicht aber nach weiteren vom Konzept nicht definierten Zwecke Daten verarbeitet. Ebenso dürfen diese Daten nicht für andere Anwendungen verwendet oder in zukünftigen Verfahren übermittelt werden.

Angesichts der möglichen Konsequenzen der KI-Anwendungen ist vor der Entwicklung des Verfahrens eine Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) vorzunehmen, die eine konkrete risikobasierte Analyse der Folgen für die Rechte des Betroffenen wie auch Schutzmodelle vorsieht. Immerhin sehen die Anwendungen eine immanente Überwachung vor, wie beispielsweise ein Fitnesstracker durch Verarbeitung der Standort- und Gesundheitsdaten des Nutzers.[45]

Mithin ist der Verantwortliche für die Umsetzung der allgemeinen Datenschutzbestimmungen verantwortlich und trägt den Nachweis für dessen Einhaltung, was sich aus den Rechenschaftspflichten als eine Art der „Beweislastumkehr" ergibt (Art. 5 Abs. 2 DS-GVO). Bei Verstößen drohen dem Verantwortlichen beachtliche Bußgelder (Art. 83 DS-GVO), Schadensersatzansprüche (Art. 82 DS-GVO[46]) und in Deutschland sogar unter Umständen beim gewerbsmäßigen Handeln Freiheitstrafen von bis zu drei Jahren (Art. 84 DS-GVO i. V. m. § 42 Abs. 1 BDSG-neu).

41 *Jandt*, DuD 2017, S. 562.

42 *Hartung*, in: Kühling/Buchner, Art. 25 DS-GVO, Rn. 13.

43 *Rose*, DSRITB 2016, S. 75 (86); Es kann eine „indirekten Wirkung" angenommen werden, *Baumgartner*; in: Ehmann/Selmayr, DS-GVO, Art. 25, Rn. 5.

44 Vgl. https://www.heise.de/newsticker/meldung/Google-Forscher-ruft-nach-Notschalter-fuer-Kuenstliche-Intelligenz-3230045.html (letzter Abruf: 15.6.2018).

45 Vgl. sog. „Blacklist" der Aufsichtsbehörde Baden Württemberg, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf (letzter Abruf: 15.6.2018).

46 Vgl. *Wybitul/Haß/Albrecht*, NJW 2018, S. 113 ff.

4 Neue Forderungen

Die Datenschutz-Grundverordnung bietet ein solides Schutzniveau, weist aber viele Lücken auf. Hier fehlt es vor dem Hintergrund der KI-Bewegung nicht nur an einer deutlichen Trennschärfe, sondern an einer konkreteren Ausgestaltung der in der Datenschutz-Grundverordnung nur grob skizzierten Steuerungsmittel. Die Datenschutz-Grundverordnung verfolgt in erster Linie das Ziel des Individualschutzes des Betroffenen und nicht der Bekämpfung von „Big Data". Angesichts der derzeitigen Regelung[47] zum Privacy by Design bzw. Privacy by Default – Grundsatz bleiben den Entwicklern und Verantwortlichen von KI-basierten Anwendungen weiterhin viele Freiräume.

4.1 Haftungsmodelle

Deshalb könnte sich mit einem Blick auf andere Rechtsgebiete beholfen werden. Schließlich werden derzeit in der rechtwissenschaftlichen Literatur im Hinblick auf die Bewertung von Schadensersatz bei den digitalen Assistenten und KI-basierten Programmen verschiedene zivilrechtliche Haftungsmodelle besprochen und anfänglich entwickelt.[48] Hiermit sollen Rechtslücken und Kausalitätsprobleme überwunden oder sogar eine Haftung des „Roboters" konstruiert werden.

Demnach steht beispielsweise eine Haftung des Betreibers bzw. Verantwortlichen nach § 823 BGB (oder § 43 GmbHG bei Verletzung der Sorgfaltspflichten) im Raume.[49] Allerdings wird der Anspruch in der Regel im Rahmen der Kausalität oder aber des Verschuldens scheitern, zumindest wenn viele Zwischenschritte zwischen Entwicklung und Eintritt des Schadens erfolgten.[50] Diskutiert wird außerdem eine Gefährdungshaftung (analog zu § 7 Abs. 1 StVG[51] oder der Tierhalterhaftung[52]). Neu scheint sich das Modell der Zurechnung des Verhaltens des Roboters oder der KI-Anwendung als solche nach einer Subjektivierung (analog zur Stellvertretung nach § 166 BGB oder der Geschäftsführung ohne Auftrag nach § 687 BGB) zu entwickeln.[53] Vergleichbare Gedanken finden sich auch im Deliktsrecht wieder, wenn unter anderem die Einordnung des Roboters als Verrichtungsgehilfe diskutiert wird.[54] Jüngst tauchten sogar Überlegungen der EU auf, dem Roboter ein eigenes Rechtssubjekt als elektronische Person zuzusprechen.[55] Hierdurch wird deutlich, dass sich die Rechtsprüfung dieser derzeit noch ungreifbaren technologischen Entwicklung immer weiter in die Haftungsfälle verlagern könnte. Analog zu diesen zivilrechtlichen Überlegungen könnten außerdem Anpas-

47 Dies ist vielleicht ein Grund, warum der europäische Gesetzgeber den Gesetzestext der Datenschutz-Grundverordnung knapp einen Monat vor In-Kraft-Treten nochmals sprachlich anpasste und unter anderem im Wortlaut von Art. 25 Abs. 2 S. 1 den Begriff „grundsätzlich" strich und somit den Vorgaben mehr Gewicht verlieh; vgl: http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf (letzter Abruf: 15.6.2018).

48 Vgl. *Kluge/Müller*, InTer 2017, S. 24 ff; *Borges*, NJW 2018, S. 980.

49 Vgl. *Franck/Müller-Peltzer*, DSRITB 2017, S. 254 f.

50 Vgl. *Keßler*, MMR 2017, S. 592 f.

51 Vgl. *Franck/Müller-Peltzer*, DSRITB 2017, S. 255.

52 *Borges*, NJW 2018, S. 981.

53 Vgl. *Kluge/Müller*, InTer 2017, S. 27.

54 Vgl. *Denga*, CR 2018, S. 69; *Keßler*, MMR 2017, S. 593.

55 Entschließung des Europäischen Parlaments vom 16.2.2017, abzurufen unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//DE (letzter Abruf: 15.6.2018); vgl. *Specht/Herold*, MMR 218, S. 43.

sungen des Datenschutzrechts in Betracht gezogen werden, um das bisheriger Sanktionsmodell weiterzuentwickeln und Wertungswidersprüche zu beheben.

4.2 Datenschutz der Zukunft

Eine Umsetzung der datenschutzrechtlichen Anforderungen ist unumgänglich.[56] Es drängen sich zusätzliche Forderungen auf. Was wäre, wenn die KI-basierte Anwendung in Zukunft doch selbstständig wird und damit die Verantwortlichkeit des Entwicklers oder Betreibers ablöst?[57]

Im derzeitigen Stadium der KI, in welchem die Entwickler und Betreiber noch Zweck und Ausmaß der Verarbeitung definieren und (hoffentlich) kontrollieren können,[58] lässt sich der Konflikt über das Datenschutzrecht regeln. Durch die gesetzlich angeordnete Dokumentation und Evaluierung der Verarbeitungsvorgänge wie auch der erforderlichen technischen und organisatorischen Maßnahmen (Art. 32 DS-GVO) bewegt sich die Arbeit in einem datenschutzkonformen Korridor. Dieses wird untermauert durch die vorherige Prüfung der Folgen der Anwendung mit Hilfe der Datenschutz-Folgenabschätzung.[59]

Spätestens ab dem Zeitpunkt, von dem an das Programm oder ein Roboter „in persona" eigene Entscheidungen über Leib und Leben eines Menschen trifft, Personengruppen diskriminiert bzw. bevorzugt und durch das der Technik innewohnende Zusatzwissen möglicherweise über dem Menschen steht, löst sich die Verantwortlichkeit auf. Die Datenschutz-Grundverordnung in der heutigen Fassung liefe ins Leere und es entstünde eine Regelungslücke. Sofern die KI-basierte Anwendung im Ergebnis tatsächlich den Tod eines Menschen verursachen oder die Entwicklung dessen Gesundheit vorhersagen oder anhand von Ton-/Bildaufnahmen des Betroffenen dessen Vorlieben wie auch Gedanken bewerten können, stellen sich nicht nur datenschutzrechtliche, sondern auch zivilrechtliche und strafrechtliche Fragen. Macht sich der Entwickler oder der Roboter möglicherweise strafbar? Die Folgen für die Anwendung, aber auch für die Gesellschaft sind unvorhersehbar.[60] Zu denken wäre an die Konstellation der unterlassenen Hilfeleistung (analog zu § 323c StGB) des Entwicklers oder Anwenders, wenn die Anwendung mit an Gewissheit grenzender Wahrscheinlichkeit eine negative Folge prognostiziert, ohne allerdings Schritte zur Abwehr der Gefahr einzuleiten – zum Beispiel im Falle der Vorhersage einer Straftat oder eines Unglücks, ohne entsprechende Gegenmaßnahmen zu veranlassen. Und auch Maßnahmen gegen den (neuen) Verantwortlichen entfalten keine Wirkung, wenn dies ein Roboter bzw. eine KI-Anwendung ist, die sich weder durch die drohende Abschaltung noch durch Bußgelder abschrecken lässt.[61]

Muss der Mensch letztlich immer die ausführende Handlung selbst vornehmen bzw. das Ergebnis „freigeben" oder wird der Roboter als Rechtsperson eingestuft, um Strafbarkeiten und Haftungsfälle reglementieren zu können? Die Verantwortlichkeiten – auch für spätere Folgeprozesse – sind vorab zu definieren und zu wahren.

Gefordert wird daher unter anderem auch ein „Algorithmen"-TÜV[62] bzw. ein Kontrollmechanismus, um Grenzen festzulegen und künftige Entwicklungen wie auch Entscheidungskompetenzen der KI außerhalb der eigenen Programmierung noch rechtlich einordnen zu können.[63] In diesem Zusammenhang können Risikoszenarien schon bei der Entwicklung der KI-basierten Anwendungen erforderlich sein, damit der „Vater" des Algorithmus in die Haftung einbezogen wird. Die Folgen sind ihm zuzurechnen.

5 Fazit

Es lässt sich konstatieren, dass das derzeitige Datenschutzrecht durch die Datenschutz-Grundverordnung ein solides Konzept entfaltet, jedoch bei weitem nicht die erforderlichen Mittel bereithält, um zukünftige KI-basierte Anwendungen zu erfassen. Die jüngst aufgekommene Kritik, die Datenschutz-Grundverordnung würde Europa bei der technischen Entwicklung im Bereich der „KI" zurückwerfen,[64] ist deshalb nicht nachvollziehbar. Es sind auf globaler Ebene neue Haftungsmodelle zu entwickeln und in das Datenschutzrecht einzubeziehen. Dies setzt neue Regelungen zur Verantwortlichkeit für die Datenverarbeitung voraus. Des Weiteren sind regelmäßige Kontrollmechanismen und „Notfall-Konzepte" zu fordern, die ausdrücklich als Bestandteil der technisch-organisatorischen Maßnahmen auszuformen und umzusetzen sind. Ebenso gilt es globale Strategien und Standards zu definieren, um ungleiche Wettbewerbe zu verhindern, die in naher Zukunft die Wirtschaft beeinflussen dürften.[65]

Die grundlegende Problematik besteht allerdings darin, dass in der gesamten Rechtsdogmatik nur solche Handlungen und Vorgänge reglementiert werden können, die bekannt und vom menschlichen Verhalten für logisch bzw. nachvollziehbar erachtet werden. Diese Logik lässt sich nicht exakt auf eine etwaige KI anwenden, die nicht zwischen „gut" und „böse" differenziert und auch nicht Emotionen wie auch Gefühlen unterworfen wird. Regeln laufen in diesem Bereich immer der technischen Entwicklung hinterher.

56 Vgl. *Conrad*, DuD 2017, S. 742 ff.

57 Siehe bei *Pieper*, DSRITB 2017, S. 568.

58 Vgl. *Schael*, DuD 2018, S. 547 (in diesem Heft).

59 Siehe *Quiel*, PinG 01.18, S. 30ff.

60 Vgl. https://netzpolitik.org/2018/ethische-fragen-bei-kuenstlicher-intelligenz-mit-welchen-herausforderungen-muessen-wir-umgehen/ (letzter Abruf: 15.6.2018).

61 Doch gerade dieses ist Sinn und Zweck der aufsichtsbehördlichen Maßnahmen. Die Bußgelder sollen ausweislich Art. 83 Abs. 1 „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein.

62 Vgl. *Möslein*, ZIP 2018, S. 212.

63 Vgl. *Pieper*, DSRITB 2017, S. 568

64 So bewertete der Investor Thiel die DS-GVO als „dummes Eigentor"; https://www.heise.de/newsticker/meldung/KI-Wettrennen-Europa-hat-sich-mit-der-DSGVO-ins-Knie-geschossen-4075009.html (letzter Abruf: 15.6.2018).

65 Vgl. https://www.zeit.de/digital/datenschutz/2018-07/automatisierung-kuenstliche-intelligenz-bundeskabinett-foerderung (letzter Abruf: 20.07.2018).