Conrad Sebastian Conrad

Künstliche Intelligenz – Die Risiken für den Datenschutz

Immer mehr digitale Assistenten und Anwendungen aus dem Alltag basieren auf der sogenannten „künstlichen Intelligenz" (KI). Dem Einsatz sind kaum Grenzen gesetzt. Bereits die moderne Zahnbürste ist vernetzt und sammelt während ihres Gebrauchs sensible Informationen über den Nutzer. Wie lässt sich diese oftmals täglich genutzte Technik aber mit dem Datenschutz vereinbaren?

1 Einleitung

Der technischen Entwicklung sind kaum Grenzen gesetzt. Roboter übernehmen die Fabrikarbeit, selbstfahrende Autos und digitale Assistenten helfen im Alltag. Den Kern dieser Systeme bildet die „künstliche Intelligenz" (KI), die durch selbstlernende Prozesse bei gleichzeitig stetig wachsender Rechenleistung die Arbeitsweise von IT-Systemen massiv beeinflusst.[1]Trotz der scheinbar häufig positiven Aspekte stellt sich die Frage, ob der technische Fortschritt nicht gleichzeitig eine Gefahr für den Datenschutz des Einzelnen darstellt. Experten im Bereich der Technik sehen zum Teil hierin sogar eine Bedrohung für die Zivilisation,[2] während andere darin eine Chance zur Leistungssteigerung des Menschen sehen.[3] In Deutschland wurde im öffentlichen Fachgespräch des Bundestagsausschusses über die Forderungen neuer rechtlicher Regelungen mit Experten diskutiert[4] und der Bitkom e. V. veröffentlichte in Zusammenarbeit mit dem Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) im Juni 2017 ein erstes Positionspapier.[5] Indes werden auf europäischer Ebene zivilrechtliche Regelungen zum Roboterrecht und der KI besprochen.[5]

Aus datenschutzrechtlicher Sicht stellt sich aber vor allem die Frage, wie soll im Hinblick auf die informationelle Selbstbestimmung der Nutzer dieser alltäglich genutzten Technik, mit der Vielzahl an gesammelten und zum Teil sensiblen Daten umgegangen werden.

1.1 Aktueller Stand der KI

Eine endgültige Definition der „künstlichen Intelligenz" existiert nicht. Dieses ist dem Umstand geschuldet, dass allein der Begriff der „Intelligenz" in den einzelnen Wissenschaften unterschiedlich ausgelegt und bewertet wird.[7] Bereits im Jahre 1955 wurde eine Beschreibung mit folgender Definition versucht: „*Ziel der KI ist es, Maschinen zu entwickeln, die sich verhalten, als verfügten sie über Intelligenz.*" Dabei wird zwischen der „schwachen" und der „starken" KI differenziert. Die starke KI wird angenommen, wenn sie die gleichen intellektuellen Fertigkeiten wie der Mensch hat oder ihn darin sogar übertrifft[8] – oder sogar ein Bewusstsein aufweist. Derzeit befindet sich die technische Entwicklung der KI (noch) im Bereich der Machine Learning / Deep Learning Verfahren und der Mustererkennung, was wohl der „schwachen KI" zuzuordnen sein dürfte.

Die im Folgenden beschriebenen Systeme sind Anwendungen, die im Kern von Prozessen der „schwachen KI" unterstützt werden.

1.2 Aktuelle Anwendungsgebiete

Längst handelt es sich nicht mehr um Pilotprojekte von Forschungsinstituten, sondern um – in unserem Alltag – etablierte Systeme, die auf die KI-basierten Prozesse aufsetzen. Es bietet sich daher inzwischen ein breites und stetig erweiterndes Spektrum an Anwendungen. Einige sollen im Folgenden näher aufgezeigt werden.

1.2.1 Digitaler Assistent

Digitale Assistenten wie Apple Siri, Microsoft Cortana oder Google Bixby steuern Smartphones und private Rechner über Spracheingabe und können verschiedene Aufgaben selbstständig erle-

1 Vgl. http://www.zdnet.de/88288740/kuenstliche-intelligenz-durchdringt-bereits-die-it (Abruf 23.9.2017).

2 Siehe dazu die Aussage von Elon Musk, https://www.heise.de/newsticker/meldung/Das-groesste-Risiko-fuer-unsere-Zivilisation-Elon-Musk-warnt-erneut-vor-KI-3773358.html (Abruf 23.9.2017); dem widerspricht Bill Gates, https://futurezone.at/digital-life/bill-gates-keine-angst-vor-kuenstlicher-intelligenz/288.446.667 (Abruf 28.9.2017).

3 So der Schachgroßmeister Kasparow, http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/kasparow-ueber-ki-wir-haben-alle-diese-aengste-aber-15127820.html (Abruf 23.9.2017).

4 http://www.bundestag.de/dokumente/textarchiv/2017/kw12-pa-digitale-agenda/497340 (Abruf 23.9.2017).

5 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//DE (Abruf 23.9.2017).

Conrad Sebastian Conrad

Justiziar – datenschutz nord GmbH

E-Mail: cconrad@datenschutz-nord.de

6 https://www.bitkom.org/Bitkom/Publikationen/Entscheidungsunterstuetzung-mit-Kuenstlicher-Intelligenz-Wirtschaftliche-Bedeutung-gesellschaftliche-Herausforderungen-menschliche-Verantwortung.html (Abruf 23.9.2017).

7 Vgl. http://www.spektrum.de/lexikon/neurowissenschaft/kuenstliche-intelligenz/6810 (Abruf 23.9.2017).

8 Vgl. Definition von John McCarthy, http://www.informatik.uni-oldenburg.de/~iug08/ki/Grundlagen_Starke_KI_vs._Schwache_KI.html.

digen und proaktiv handeln. Sie erlernen die Interessen bzw. Bedürfnisse und die Sprache des Benutzers, begleiten ihn auf Schritt und Tritt, personalisieren Inhalte, erinnern an Termine, bewerben den neuesten Kinofilm und liefern (passende) Antworten bei stetig verbesserter Verständigung.[9] Amazon Alexa ermöglicht als sprachgesteuerter Lautsprecher sowohl die Musikauswahl als auch den virtuellen und intuitiven Einkauf per Spracheingabe. Oder liest aus Wikipedia vor.

Die jeweiligen Funktionen setzen zumeist ein aktiviertes Mikrofon wie auch eine Internetverbindung und zum Teil GPS-Daten voraus und passen sich ständig dem Benutzer an.

1.2.2 Internet of Things

Unter dem Begriff „Internet of Things" (IoT) wird in der Regel die elektronische Verbindung von Haushaltsgeräten mit dem Internet und digitalen Assistenten verstanden. Dies kann vom Kühlschrank bis zur Zahnbürste[10] reichen. Allen Geräten ist gemein, dass sie durch die zusätzliche Sammlung an Informationen und automatisierte Vorgänge den Komfort des Nutzers verbessern und vielseitige Steuerungsmethoden erlauben, jedoch auch zahlreiche Angriffsstellen und Lücken für Angreifer bieten.[11] Nach einer aktuellen Studie von PWC werden die vernetzen Geräte mit KI noch unterschätzt, bieten jedoch ein hohes wirtschaftliches Potenzial,[12] deren genutzte Anzahl im Alltag weiter zunehmen dürfte.

1.2.3 Bildbearbeitung

Mittlerweile werden der KI zuzuschreibende Prozesse wie das Machine Learning auch in der Bild- und Videobearbeitung eingesetzt. Die Anwendungen können Fotos „aufhübschen"[13] und Gesichter je nach gewählter Einstellung manipulieren, beispielsweise ein Lächeln nachbilden.[14] Außerdem können die KI-Prozesse die „Verpixelung" bestimmter Bilder, die in der Regel zum Schutz der Privatsphäre (z. B. bei Partnerbörsen) geschützt sind, durch Algorithmen rückgängig machen.[15] Hintergrundinformationen wie Meta-Daten können zudem aus den Fotos automatisch ausgelesen werden[16], z. B. um ähnliche Produkte aus Shops zu verlinken.[17]

1.2.4 Gaming

Im Bereich der Computerspiele, der lange Zeit als ein Gradmesser der Leistungsfähigkeit der Computer mit KI-Ansätzen galt, hat sich die KI längst gegenüber der menschlichen Intelligenz durchgesetzt. Die neuesten KI-Systeme sind ausgehend von steigender Rechenleistung und Lernprozessen in der Lage, die besten Schach-Spieler und auch die besten „Go"-Spieler der Welt zu besiegen (Google AlphaGo)[18] oder nie gedachte Highscores[19] zu erzielen.

1.2.5 Autonomes Fahren

Als zukünftig großes Thema gilt das autonome Fahren, das in wenigen Jahren den Straßenverkehr durch selbstfahrende Fahrzeuge verändern dürfte.[20] Auf diese Weise könnte der Computer das Fahrzeug eigenständig steuern, effiziente Routen berechnen und kritische Situationen vermeiden helfen. Offen bleiben ethisch-juristische Fragen bei Schäden und Unfällen.[21]

1.2.6 Videoüberwachung

Die Deep Learning/Machine Learning Technologie wird auch bei der Gesichtserkennungssoftware eingesetzt. Integrierte Lernprozesse analysieren menschliche Bewegungsabläufe, berechnen biometrische Muster von Gesichtern[22] bzw. Körpern und identifizieren Personen zunehmend treffsicherer. Biometrische Muster wie das Alter eines Menschen können sogar in Echtzeit berechnet werden.[23]

Die Verknüpfung von biometrischen Daten bei der automatischen Gesichtserkennung zur sogenannten „intelligenten Videoüberwachung",[24] wie sie unter anderem bei einem Pilotprojekt am Berliner Bahnhof Südkreuz von der Deutschen Bahn in Zusammenarbeit mit dem BKA und der Bundespolizei eingesetzt wird, erleichtert die Profilerstellung.

1.2.7 Bots

Im Bereich des Kundensupports setzen Unternehmen vermehrt auf Chatbots und Social Bots, um durch automatisierte Prozesse jederzeit Antworten zu Bestellungen oder dem Status zu liefern oder dem Kunden individuelle Informationen zukommen zu lassen.[25] Sie können aber außerdem durch Schlagfertigkeit oder Humor für Aufheiterung sorgen. Dies steigert die Kundenzufriedenheit, verknüpft aber auch mehr Informationen zum Kunden. Hingegen ist der erste Versuch von Microsoft fehlgeschlagen, einen Twitter-Bot mittels KI in der Gesellschaft zu etablieren und so „Menschlichkeit" zu erlernen.[26] Dieser Bot nahm im Lernprozess überwiegend die negativen Gedanken und Meinungen der Nutzer in den sozialen Netzwerken auf, was die Risiken der selbstlernenden Algorithmen verdeutlicht.[27]

9 Vgl. http://www.manager-magazin.de/magazin/artikel/kuenstliche-intelligenz-alexa-cortana-home-siri-und-viv-a-1143884.html (Abruf 23.9.2017); http://www.horizont.net/tech/nachrichten/Digitale-Assistenten-Studie-bescheinigt-Alexa-die-groesste-Intelligenz--Schlusslicht-ist-Cortana-158558 (Abruf 23.9.2017).

10 https://www.heise.de/newsticker/meldung/Kolibree-Ara-Startup-zeigt-vernetzte-Zahnbuerste-mit-kuenstlicher-Intelligenz-3635316.html (Abruf 23.9.2017).

11 Vgl. *Klein-Hennig/Schmidt*, DuD 2017, S. 606; *Nürnberger/Bugiel*, DuD 2016, S. 504.

12 http://www.pwc.com/gx/en/industries/communications/assets/pwc-ai-and-iot.pdf (Abruf 23.9.2017).

13 https://www.heise.de/newsticker/meldung/KI-retuschiert-Smartphone-fotos-in-Echtzeit-3792720.html (Abruf 23.9.2017).

14 https://www.heise.de/ct/ausgabe/2017-11-Kuenstliche-Intelligenz-macht-Bildbearbeitung-intuitiv-3705914.html (Abruf 23.9.2017).

15 Vgl. https://www.golem.de/news/google-brain-algorithmus-macht-gesichter-auf-schlechten-bildern-erkennbar-1702-126066.html (Abruf 23.9.2017); https://netzpolitik.org/2016/verpixelung-macht-unsichtbar-oder-doch-nicht (Abruf 23.9.2017).

16 http://t3n.de/news/facebook-ki-bilderkennung-chrome-781194/ (Abruf 23.9.2017).

17 Vgl. https://www.heise.de/newsticker/meldung/eBay-Produkte-mithilfe-von-Fotos-suchen-und-kaufen-3784371.html (Abruf 23.9.2017).

18 http://t3n.de/news/google-ki-schlaegt-go-spieler-825403 (Abruf 23.9.2017).

19 http://winfuture.de/videos/Software/Perfektes-Spiel-bei-Ms.-Pac-Man-Microsoft-KI-setzt-neue-Massstaebe-17963.html (Abruf 23.9.2017).

20 http://www.automobilwoche.de/article/20170315/NACHRICHTEN/170319934/entwicklung-von-eigenem-ki-autocomputer-bosch-investiert--millionen-euro-in-kuenstliche-intelligenz (Abruf 23.9.2017).

21 https://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2017/084-dobrindt-bericht-der-ethik-kommission.html (Abruf 23.9.2017).

22 Vgl. *Drahanský/Goldmann/Spurný*, DuD 2017, S. 417.

23 Vgl. https://www.heise.de/newsticker/meldung/Motorola-plant-Polizei-Bodycams-mit-Gesichtserkennung-in-Echtzeit-3775898.html (Abruf 23.9.2017).

24 Vgl. https://www.datenschutz-notizen.de/datenschutz-bei-der-intelligenten-videoueberwachung-5017416; siehe hierzu *Rose*, DuD 2017, S. 140.

25 https://www.telekom.com/de/blog/konzern/artikel/chatbots-des-kommunikators-kleine-helferlein-494194 (Abruf 23.9.2017).

26 http://www.shz.de/deutschland-welt/netzwelt/wie-kuenstliche-intelligenz-bei-twitter-zum-sexistischen-nazi-wurde-id13140056.html (Abruf 23.9.2017).

27 Vgl. http://www.spiegel.de/wissenschaft/mensch/mark-zuckerberg-und-elon-musk-zukunft-der-kuenstlichen-intelligenz-a-1160095.html (Abruf 23.9.2017).

1.3 Folgen

Insgesamt stellt sich jedoch bei der Vielzahl der aufgezeigten Anwendungen die Frage, was eigentlich die datenschutzrechtlichen Folgen einer derartigen Etablierung der KI-Prozesse in technischen Systemen und Infrastruktur der Gesellschaft bis hin ins Kinderzimmer sind. [28]

1.3.1 Personalisierung

Durch die KI-basierte Auswertung der personenbezogenen Daten entstehen zunehmend personalisierte Angebote und Inhalte. Dies betrifft nicht nur die personalisierte Werbung im Internet. Vielmehr können die gesammelten Informationen dazu genutzt werden, Nachrichten wie auch Dienstleistungen, Versicherungstarife[29] und Preise[30] im Online-Shop an den Einzelnen situationsbedingt anzupassen.

Darüber hinaus filtern diese KI-basierten Algorithmen die Inhalte bei Facebook oder unterbreiten dem Nutzer individuelle Jobvorschläge.[31] Insgesamt stellt dies eine Möglichkeit der Preismanipulation und damit die Gefahr der Beschränkung des freien Marktes wie auch der Beeinflussung von Inhalten und Wissenszugang dar. Auf diese Weise ist es sogar möglich, dass Wahlen beeinflusst werden.

1.3.2 Identifikation

Eine weitere Folge der Nutzung der KI ist der Verlust der Anonymität – sowohl im Internet als auch in der Offline-Welt. Durch die aufgezeigte Foto-Bearbeitung wie auch Gesichtserkennung steigt die Möglichkeit der Personenzuordnung. Hinzu kommen geräteübergreifende Tracking-Methoden.[32]

Banken setzen bereits zum Teil auf die biometrische Verhaltenskontrolle (Verhaltensbiometrie) zur IT-Sicherheit und können so allein nach der Analyse des Benutzerverhaltens in wenigen Sekunden erkennen, ob sich der tatsächliche Kontoinhaber oder ein Fremder in das Konto einzuloggen versucht.[33] Dieses Wissen über den Nutzer wäre für die Werbung und Verbreitung von Dienstleistungen von großem Nutzen und sehr gewinnbringend.

Nicht zuletzt können Geheimdienste und Sicherheitsunternehmen durch die intelligente Videoüberwachung die (staatliche) Überwachung massiv ausweiten und optimieren. Mittels Verhaltens- und Bewegungsanalysen, aber auch ausgehend von der Gesichtserkennung wird der Einzelne zum gläsernen Menschen bei ständigem Überwachungsdruck.[34] Jeder sollte sich vor einer auffälligen Handlung in Acht nehmen. Denn bei entsprechender Anwendung im Diebstahlschutz, wäre es bspw. nicht ausgeschlossen, dass das System Alarm auslöst, wenn eine ältere Person im Supermarkt die Ware vorübergehend zum Tragen in ihrer Tasche aufbewahrt.

1.3.3 Verhaltensanalyse

Anhand von Stimmen- und Bildaufnahmen können KI-basierte Anwendungen unter Implementierung der Lernprozesse immer exakter das Verhalten eines Menschen wie beispielsweise dessen Emotionen bewerten und ausnutzen. Bewegungsabläufe, Tastatureingaben im Chatprogramm[35] oder sogar das Klickverhalten beim Online-Banking lassen anhand von verhaltensbiometrischen Merkmalen eine Personenidentifikation wie psychologische Einschätzungen zu. Die daraus zu ziehenden Erkenntnisse können nicht nur der IT-Sicherheit zum Schutz dienen, sondern sogar das Kaufverhalten des Einzelnen manipulieren. Oder aber die Bewerberauswahl beim Arbeitgeber „erleichtern". Es droht der Kontrollverlust des Menschen über seine Entscheidung wie auch Außenwahrnehmung.

1.3.5 Zukunftsvisionen?

Die Zukunftsvisionen von Maschinen, die Arbeitsplätze und Dienstleistungen des Menschen ersetzen und Antworten auf viele Frage liefern, geben Anlass zur Sorge. Und auch das „predictive policing" ist in vielen Bereichen längst Alltag, wenn Wahrscheinlichkeiten von Einbrüchen oder die Straffälligkeit von Personen durch Mustererkennung berechnet werden.[36] Es drohen Vorverurteilung[37], Fehler und Diskriminierung[38] Vieler. Zudem ist völlig unklar, wie sich die Verantwortlichen der Anwendungen erst verhalten (müssen) werden, sobald diese durch Gesichtserkennung und weitere Analysemethoden Krankheiten oder Suizid-Gedanken[39] erkennen[40] und den Kreditausfall einstufen können.

2 Datenschutzrechtliche Anforderungen

Während derartige Systeme je nach Ausgestaltung zahlreiche Informationen des Benutzers sammeln bzw. benötigen, die vielfältig und damit kaum interpretierbar sind, gewinnen die KI-basierten Anwendungen zunehmend weitergehende Erkenntnisse über den Einzelnen. Diese Daten können zukünftig durch neue Analysen und Möglichkeiten sogar weitergehende Erkenntnisse und Prognosen liefern und so das Persönlichkeitsrecht des Einzelnen, insbesondere seine informationelle Selbstbestimmung verletzen.

2.1 Das Datenschutzrecht

Zu berücksichtigen ist, dass neben den Benutzerinformationen (bspw. Namen, Alter und E-Mail) zumeist auch die Meta- und Hintergrunddaten erfasst werden. Hierzu zählen die Standortdaten, der Suchverlauf und persönliche Vorlieben. Oft sind sogar biometrische Daten betroffen, so z. B. die Stimme, Gesichtsmuster bzw. die Iris, die Körpergestalt, Herkunft oder die Gesundheit. Ebenfalls nicht ausgeschlossen sind Prognosedaten, d. h. Anga-

28 http://www.zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur (Abruf 23.9.2017); vgl. *Wiebusch*, DSRITB 2015, S. 157.

29 https://www.wired.de/collection/tech/eine-japanische-versicherung-ersetzt-mitarbeiter-durch-eine-kuenstliche-intelligenz (Abruf 23.9.2017).

30 https://www.datenschutz-notizen.de/personalisierte-preise-sexy-aber-nicht-bedingungslos-2816074/ (Abruf 23.9.2017).

31 http://www.internetworld.de/social-media/google/google-online-stellenmarkt-aufrollen-1225914.html (Abruf 23.9.2017).

32 *Venzke-Caprarese*, DuD 2017, S. 577.

33 Vgl. https://www.datenschutz-notizen.de/verhaltensanalyse-beim-online-banking-mit-dem-datenschutz-vereinbar-2018287/ (Abruf 23.9.2017).

34 *Rose*, DuD 2017, S. 140.

35 Vgl. http://t3n.de/news/facebook-deeptext-maschinelles-lernen-712349 (Abruf 23.9.2017)

36 Vgl. http://www.polizei-newsletter.de/documents/2017_Artikel_Andre_Schulz.pdf (Abruf 23.9.2017).

37 Z. B. auch hinsichtlich der Sexualität: Sehr bedenklich, vgl. https://www.heise.de/newsticker/meldung/KI-erkennt-am-Gesicht-ob-Menschen-schwul-oder-lesbisch-sind-3825449.html (Abruf 27.9.2017).

38 Vgl. *Kipker*, ZD-Aktuell 2017, 04259; vgl. auch: https://www.heise.de/newsticker/meldung/Diskriminierende-KI-Wissenschaftler-finden-Chatbots-Alexa-und-Co-nicht-divers-genug-3810024.html (Abruf 27.9.2017).

39 Vgl. https://www.moobilux.com/2017/09/kuenstliche-intelligenz-erkennt-suizidgedanken/ (Abruf 27.9.2017).

40 https://www.wired.de/collection/science/diese-ki-erkennt-hautkrebs-so-zuverlaessig-wie-ein-arzt (Abruf 23.9.2017).

ben über in der Zukunft liegende Verhältnisse, die ebenfalls schon Aussagen zu dem Betroffenen ermöglichen können.[41]

Häufig werden diese personenbezogenen Daten direkt beim Betroffenen erhoben und an die Hersteller oder Betreiber als verantwortliche Stelle übermittelt. Schon hier stellt sich die erst Frage nach der datenschutzrechtlichen Rechtmäßigkeit der Übermittlung, da viele dieser Betreiber ihren Sitz außerhalb der EU haben.

Die personenbezogenen Daten werden zudem gespeichert, an weitere Verantwortliche über das Internet oder Cloud-Dienste übermittelt und ständig durch die Verwendung und Verknüpfung mit zusätzlichen Informationen oder Analysen verarbeitet. Es handelt sich demnach um eine Verarbeitung personenbezogener Daten, welche den Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) sowie der Datenschutz-Grundverordnung (DS-GVO) eröffnet.

Doch nicht alle Prozesse der Datenverarbeitung sind definierbar, insbesondere wenn Big Data und lernende Systeme zukünftig neue Erkenntnisse aus den Informationen gewinnen, Interaktionen vorhersehen oder sogar neue personenbezogene Daten wie Gesichtsmuster, Stimmen oder Gesundheitsdaten auswerten, respektive reproduzieren können. Beim Einsatz von KI-Anwendungen sind daher Konzepte zum Datenschutz und der IT-Sicherheit zu fordern, die den technischen Fortschritt, respektive deren Potenzial durch endlose Datensammlung und optimierte Methoden der Analyse durch die KI angemessen Rechnung tragen. Die Rechtsposition des Einzelnen und dessen Kontrolle über seine personenbezogenen Daten darf nicht in der zunehmenden Verkettung von intelligenten Systemen und neuronalen Netzen an Bedeutung verlieren.

2.1.1 Allgemeine Grundsätze

Zunächst gilt es beim Einsatz KI-basierter Anwendungen den allgemeinen Grundsätzen der rechtmäßigen Datenverarbeitung nach Art. 5 Abs 1 DS-GVO zu entsprechen, die von der Rechtmäßigkeit der Verarbeitung, Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO) bis zur etwaigen Anonymisierung personenbezogener Daten, Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DS-GVO) und dem Schutz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DS-GVO) reichen.

Bei der Entwicklung von KI-basierten Methoden sind die Zwecke der Datenverarbeitung daher eindeutig[42] und eng zu definieren und dem Nutzer in verständlicher Weise darzulegen. Die Zweckbindung gilt auch bei der Weiterverarbeitung.[43] Eine Zweckänderung gem. Art. 6 Abs. 4 DS-GVO ist nur unter strengen Voraussetzungen, beispielsweise durch Einwilligung des Betroffenen oder auf Grund einer Rechtsvorschrift denkbar.[44] Weitergehende Systeme oder neue Software müssen sich an die bei der Entwicklung definierten Zwecke halten.

Zum Beispiel darf die aufgezeichnete Stimmeneingabe bei Siri, Alexa und Co. nicht dazu verwendet werden, in Zukunft die Stimme zu analysieren und biometrische Erkenntnisse daraus zu gewinnen – und dieses Wissen darüber hinaus noch zur Preisbestimmung einzusetzen. Und Fitness-Tracker dürfen nicht später als Einkaufsführer oder Apotheken-Shop fungieren.

Zudem sind nach dem Grundsatz der Datenminimierung Löschroutinen gefordert, die in regelmäßigen Abständen greifen und eine endlose Datenbank verhindern sowie dem „Recht auf Vergessenwerden“ (Art. 17 DS-GVO)[45] bei den Betroffenenrechten entsprechen. Die gesammelten Informationen sind auch dann zu löschen, wenn sich dies auf die Resultate der KI-Anwendung oder deren Weiterentwicklung auswirken.

2.1.2 Einwilligung

In der Regel beruht die Rechtmäßigkeit der Datenverarbeitung auf der Einwilligung des Betroffenen (Art. 6 Abs. 1 lit. a) DS-GVO), für deren Vorliegen der Verantwortliche den Nachweis zu erbringen hat (Art. 7 Abs. 1 DS-GVO). Dabei muss der Betroffene insbesondere vor der Inbetriebnahme über Art und Ausmaß der Datenverarbeitung „in nachvollziehbarer Weise“ informiert (Transparenzgebot) sowie über dessen Zweck und den Verantwortlichen aufgeklärt werden (Art. 5 DS-GVO).[46] Es bedarf demnach einer transparenten und verständlichen Aufklärung über die konkreten Prozesse der Datenverarbeitung (Art. 7, Art. 8 DS-GVO). Die Einwilligung muss zudem jederzeit widerrufbar sein (Art. 7 Abs. 3 DS-GVO).

Für die Verarbeitung biometrischer Daten und sonstiger besonderer Kategorien gelten sogar noch höhere Anforderungen (Art. 9 DS-GVO).[47] Denn soweit biometrische Daten[48] wie z. B. bei der Gesichtserkennung betroffen sind, die zur eindeutigen Identifizierung einer Person Verwendung finden, ist deren Verarbeitung grundsätzlich verboten (Art. 9 Abs. 1 DS-GVO).[49] Eine Ausnahme hiervon greift, sofern der Betroffene ausdrücklich seine Einwilligung in den zuvor festgelegten Zweck erteilt (Art. 9 Abs. 2 lit. a) DS-GVO). Führt das Programm durch die automatisierte Verarbeitung der gewonnenen Erkenntnisse zur Erstellung eines Profils des Anwenders, was häufig anzunehmen sein dürfte und gerade die Anwendungsfelder der KI auszeichnet, darf jedoch trotz ausdrücklicher Einwilligung gem. Art. 22 Abs. 2 DS-GVO die „Entscheidung“ des Programms nicht auf biometrische Daten beruhen (Art. 22 Abs. 4 DS-GVO).[50] In Anlehnung an die Rechtsgedanken bedeutet dieses: Wenn die KI verschiedene Entscheidungen im Rechtsverkehr für den einzelnen trifft, beispielsweise Preisvorschläge unterbreitet, dürfen keine biometrischen Daten berücksichtig werden. Dieses würde praktisch die KI-Anwendungsfelder drastisch reduzieren.[51]

Bei der elektronischen Datenverarbeitung wird in vielen Fällen eine ausdrückliche Einwilligung gefordert, was ein aktives und freiwilliges Handeln des Betroffenen (Anklicken einer Checkbox) beinhalten sollte.[52] Die konkludente Einwilligung allein durch Installation der Anwendung oder Kauf ist wie bei bereits angekreuzten Kästchen ungenügend.[53]

Gewiss darf die Freiwilligkeit der Einwilligung bezweifelt werden, wenn die allgegenwärtigen Systeme ein unersetzlicher Bestandteil geworden und oftmals zwingend erforderlich sind für die Grundbedürfnisse (sog. Lock-in Effekt[54]). Es müsste eine echte

41 *Gola*; in: Gola, DS-GVO, Art. 4, Rn. 13.
42 *Heberlein*, in: Ehmann/Selmayr, DS-GVO, Art. 5, Rn. 16.
43 *Frenzel*, in: Paal/Pauly, Art. 5 DS-GVO, Rn. 29.
44 Vgl. *Eichenhofer*, PinG 04.17, S. 139.
45 Vgl. *Kamann/Braun*, DS-GVO, Art. 17, Rn. 19.
46 Vgl. Erwägungsgrund 58 der DS-GVO.
47 Vgl. Erwägungsgrund 51 der DS-GVO.
48 *Ernst*; in: Paal/Pauly, DS-GVO, Art. 4, Rn. 99 ff.
49 *Schiff*, in: Ehmann/Selmayr, DS-GVO, Art. 9, Rn. 22.
50 *Hladjk*, in: Ehmann/Selmayr, DS-GVO, Art. 22, Rn. 16.
51 Mithin ist der Betroffene ausdrücklich auf das Profiling hinzuweisen, Vgl. Erwägungsgrund 60 der DS-GVO.
52 Vgl. Erwägungsgrund 32 der DS-GVO; *Heberlein*; in: Ehmann/Salmayr, DS-GVO, Art. 6, Rn. 11.
53 Vgl. *Albrecht*, CR 2016, S. 91.
54 Vgl. http://www.sueddeutsche.de/digital/streit-ueber-datenschutz-verbraucherschuetzer-gehen-gegen-googles-email-scannen-vor-1.2880644-2 (Abruf 23.9.2017).

Wahlfreiheit für datenschutzfreundliche Systemeinstellung und alternative (anonyme) Systeme bestehen, die der Gesetzgeber beispielsweise durch Forderungen nach alternativen Systemen und Modellen erzwingen könnte.

2.1.3 Privacy by Design & Privacy by Default

Im Hinblick auf die DS-GVO gilt es bereits bei der Konzeption eines Verfahrens die neuen Steuerungsinstrumente bei der automatisierten Datenverarbeitung zu berücksichtigen. Danach soll der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen (Art. 25 Abs. 1 DS-GVO – Privacy by Design). Außerdem müssen geeignete technische und organisatorische Maßnahmen getroffen werden, die sicherstellen, dass bereits durch die Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für die jeweiligen bestimmten Verarbeitungszwecke erforderlich ist, verarbeitet werden (Art. 25 Abs. 2 DS-GVO – Privacy by Default).[55] Insgesamt lassen sich daraus präventive als auch repressive Vorgaben zum Datenschutz durch Technik ableiten.[56] Dabei sollte der Hersteller, der oftmals gar nicht der Verantwortliche ist,[57] in den Adressatenkreis dieser Vorschrift einbezogen werden, was derzeit außer Acht gelassen wird.[58] Der Gesetzgeber will diese ausweislich der Erwägungsgründe nur hierzu „ermutigen".[59]

In der Konsequenz müssten die Geräte beim Kauf eine datenschutzfreundliche Voreinstellung[60] vorsehen und dem Nutzer eine detaillierte Auswahlmöglichkeit bieten, dürften jedoch nicht von der Werkseinstellung an sämtliche datenschutzrechtlich relevanten Prozesse (Tracking des Standortes, Bild- und Tonaufnahme usw.) aktiviert haben. Zudem ist eine individuelle, jederzeit mögliche Einstellung durch den Nutzer schon in der Entwicklung vorzusehen.

2.1.4 Folgenabschätzung

Nach Art. 35 DS-GVO gilt es eine Datenschutz-Folgenabschätzung[61] bei sensiblen Prozessen zu etablieren, ehe diese eingeführt werden. Danach führt der „*Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch*". Der Gesetzgeber hat hiermit eine risikobasierte „Technikfolgenabschätzung" vorgesehen, die dazu dient, die Auswirkung der Verwendung neuer Technologie auf die Gesellschaft und die Umwelt näher zu beleuchten.[62] Insbesondere die Achtung des Privatlebens und der Schutz der personenbezogenen Daten gilt es bei der Einführung neuer Systeme zu berücksichtigen, was eine Risikobewertung für die Rechte und Freiheit der betroffenen Personen einschließt.[63] Bei KI-basierten Systemen stellt sich hingegen durchaus die Frage, ob diese Norm überhaupt umgesetzt werden kann, wenn die selbstlernenden Programme eine neue Stufe erst einmal erreicht haben und sich fortlaufend selbst weiterentwickeln.

55 *Bieker/Hansen*, DuD 2017, S. 285.
56 *Jandt*, DuD 2017, S. 562.
57 *Hartung*, in: Kühling/Buchner, Art. 25 DS-GVO, Rn. 13.
58 *Rose*, DSRITB 2016, S. 75 (86); Es besteht jedoch eine „Indirekte Wirkung", *Baumgartner*; in: Ehmann/Selmayr, DS-GVO, Art. 25, Rn. 5.
59 Vgl. Erwägungsgrund 78 der DS-GVO.
60 *Hartung*, in: Kühling/Buchner, Art. 25 DS-GVO, Rn. 24.
61 *Hansen*, DuD 2017, S. 587.
62 *Martini*, in: Paal/Pauly, Art. 25 DS-GVO, Rn. 2.
63 Vgl. *Jandt*, in: Kühling/Buchner, Art. 35 DS-GVO, Rn. 42.

3 Fazit

Die aufgezeigten Vorschriften bzw. deren Lücken zeigen, dass das Recht sich verstärkt an die wachsende, selbstlernende Technologie anpassen muss. Es muss sichergestellt werden, dass nur solche Daten des Betroffenen erhoben und verarbeitet werden, die im Interesse des Benutzers für die jeweilige Anwendung erforderlich sind. Die Datenschutz-Grundverordnung kann einen ersten Beitrag zum Schutz der Betroffenen leisten, doch bereits jetzt ist absehbar, dass weiteres gesetzgeberisches Handeln auf europäischer Ebene auch in Zukunft angezeigt sein dürfte.

Unter dem Gesichtspunkt der notwendigen Zweckbindung sollte vom Gesetzgeber näher ausgestaltet werden, inwieweit eine zukünftige Verarbeitung der erhobenen Daten mit neuen Methoden wie z. B. zur Erkennung von Krankheiten, Verhaltensanalyse oder Identifikation zu untersagen ist. Betroffenenrechte (z. B. der Widerruf nach Art. 21 Abs. 1 DS-GVO[64]) müssen jederzeit effizient und wirksam (u. a. mit Hilfe automatisierter Verfahren[65]) auch gegenüber den Herstellern und KI-Entwicklern durchsetzbar sein, gleich an welchem Standort sich diese auf der Welt befinden.[66]

Die Anbieter könnten zudem stärker zur Transparenz gezwungen werden, beispielsweise durch Offenlegung des Quellcodes und überprüfbarer Darstellung der KI-Lernprozesse.[67]

Zusätzlich sollte die Pflicht bestehen, die Systeme regelmäßig zu evaluieren, wie es auch für die Sicherheitsmaßnahmen nach Art. 32 DS-GVO gilt. Sodann sind Regeln aufzustellen (wie es bspw. Asimov einst aufzeigte)[68], immerhin könnten sich die KI-Systeme eines Tages so verhalten, dass sie Schäden durch Cyber-Attacken[69] oder Überschreibung anderer Programme selbst anrichten.

Zuletzt kommen Verwertungsverbote in gerichtlichen Verfahren in Betracht, um den Strafverfolgungsbehörden keinen Anreiz weiterer Ausspähung und Datenanalyse zu bieten, wie es offenkundig versucht wurde.[70]

Insgesamt ist für den Einsatz von KI-basierten Systemen ein weltweit rechtsverbindlicher Rechtsrahmen mit eigenen Regeln zu entwickeln, die über die derzeitigen Vorschriften der Datenschutz-Grundverordnung hinausgehen und die ständige Entwicklung der Technik ausreichend berücksichtigen. Es sind daher alternative Modelle zu den vernetzten Systemen zu diskutieren.

Dabei sind die derzeit noch nicht absehbaren Folgen des gesellschaftlichen Wandels durch die Anpassung des Menschen an die virtuelle Welt und den technischen Fortschritt zu berücksichtigen. Hierzu sind wir als Datenschützer gefordert, die Rechte des Einzelnen trotz sinkender Skepsis gegenüber neuer Technologie und undurchsichtiger Prozesse zu schützen.

64 So die „Warnfunktion" beim Profiling, vgl. *Herbst*, in: Kühling/Buchner, Art. 21 DS-GVO, Rn. 13.
65 Zu denken wäre auch an eine Art „Do not Track"-Funktion, vgl. *Schulz*: in: Gola, DS-GVO, Art. 21, Rn. 32.
66 In Anlehnung an das „Marktort-Prinzip"; Vgl. *Schantz*, NJW 2016, 1841, 1842.
67 Ähnliche Forderungen sind im „*Statement on Algorithmic Transparency and Accountability*" von der Association for Computing Machinery US Public Policy Council (USACM) aufgestellt, vgl. https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf (Abruf 23.9.2017).
68 Mehr dazu unter: https://de.wikipedia.org/wiki/Robotergesetze (Abruf 23.9.2017).
69 Vgl. https://futureoflife.org/background/benefits-risks-of-artificial-intelligence (Abruf 23.9.2017).
70 So in einem Mordprozess in den USA: http://www.stern.de/digital/amazons-alexa-hilft-bei-mordermittlung---weil-der-verdaechtige-es-so-will-7357952.html (Abruf 23.9.2017).