Martin Rost

Künstliche Intelligenz

Normative und operative Anforderungen des Datenschutzes

Die normativen und operativen Anforderungen des Datenschutzes, die seit Anfang der 1970er Jahre für IT-Systeme entwickelt werden, haben den Betrieb beherrschbarer KI-Systeme vorbereitet.

„*Für alle Fälle kann es nicht schaden, immer einen Apfel in der Tasche zu haben.*“

(Aleksandra Sowa, 2017: 117)

1 Einleitung

In diesem Artikel werden aktuell kursierende Berichte über Funktionen und Anwendungsszenarien der „Künstlichen Intelligenz“ (KI) anhand der Funktion sowie der sechs Gewährleistungsziele des Datenschutzes analysiert.[1]

Die besonders erfolgreichen KI-Systeme der letzten Jahre basieren auf leistungsfähiger Hardware sowie einer Unmenge an verarbeiteten Daten durch „künstliche neuronale Netze“ (KNN). Im letzten Lernschritt nutzen solche Systeme Trainingsdaten, die sie vielfach in Interaktion mit anderen KI-Systemen einsetzen („deep learning“ der KNN).

Viele der Probleme der KI, die meisten Expertinnen bevorzugen die Rede vom „maschinellen Lernen“ (ML), werden derzeit in Deutschland anhand der Automatisierung des Fahrens von Autos diskutiert: Mangel an verständlichen Erklärungen und Begründungen zu Lernergebnissen gegenüber den Nutzern bzw. Betroffenen; mangelnde Robustheit gegenüber geringfügigen Transformationen von Trainingsdaten, mit dem besonderen Effekt des „katastrophischen Vergessens“ von schon mal korrekt Abgebildetem durch starke Veränderungen von Trainingsdaten (siehe Fraunhofer 2018: 29), großer Aufwand für überwachtes Lernen, keine passablen Ergebnisse bei zu wenigen Trainingsdaten. Es fehlen garantierte Vertrauensniveaus, die es gestatten würden, dass Verantwortliche berechenbare Vertrauens- oder Angreifermodelle bzgl. des KI-Systems formulieren (vgl. Kagermann 2017, Folie 7). Laßmann generalisiert diese Probleme und zieht als Fazit: „*Deep-Learning-Systeme sind also nicht prüfbar, nicht evaluierbar, ändern Ihre Eigenschaften, liefern keinerlei Begründung, sind leicht zu manipulieren, willkürlich aufgebaut und immer ungenau.*“ (Laßmann 2018, Pos. 1304)

Der Computer „deep blue“ schlug 1997 den amtierenden Schachweltweister Kasparov mit einem konventionell geschriebenen Programm, das, nach von Schachexperten eingegebenen Regeln, 200 Mio. Schachstellungen pro Sekunde bewertete. 2011 schlug das KI-System „Watson“ den menschlichen Champion im Begrifferaten von Jeopardy. Seit 2011 können Menschen im Alltagskontext Sprachassistenzsysteme nutzen, die per Internet an die Rechner großer Firmen angeschlossen im Modus einer alltäglich gewordenen „Hintergrunderfüllung“ (Gehlen 1957) agieren. 2017 schlug das Rechnernetzwerk „Alpha Go“ den weltbesten Go-Spieler und das KI-System „Libratus“ gewann ein hoch dotiertes Profi-Pokerturnier.[2]

Diese Systeme zeigen beeindruckende Leistungen bzgl. der automatisierten Lösung komplexer Probleme; zugleich sind sie latent unzuverlässig. Bei Spielen oder der Unterscheidung von Äpfeln und Birnen ist diese Eigenschaft kein Problem, wohl aber bei maschinell errechneten „Entscheidungen“ über Menschen oder im militärischen Einsatz (s. Tegmark 2017: 166f).

Ramge fokussiert drei zivile Gefahren, die durch das von der Industrie weltweit getriebene maschinelle Lernen bestehen: a) Die datengetriebene KI verstärkt die Monopolisierung der Plattform-Ökonomie auf den aktuell wichtigsten Märkten „wie ein Turbo“ (Ramge 2018: 88f). Wenn zudem KI-Systeme nur weniger Hersteller zum Einsatz kommen, und auch die notwendig massenhaften Trainingsdaten nur in den Händen weniger sind, ist eine politisch unabhängige Kontrolle der durch Technik errech-

1 Damit wiederholt dieser Artikel den Ansatz einer Untersuchung zu Cyber-Physical-Systems (vgl. Hansen/Thiel 2012). „Datenvermeidung/-minimierung“ wird hier dem Gewährleistungsziel „Nichtverkettung“ untergeordnet. Zum Thema insgesamt siehe die weiteren Beiträge dieses Schwerpunktheftes DuD 2018, Heft 9.

2 Das sind die aktuell permanent erzählten KI-Erfolgsgeschichten. Die KI-Entwicklung begann 1940, als bereits die ersten KNN-Modellierungen formuliert wurden, während heute offenbar KI-Programme begonnen haben, KI-Programme zu schreiben (Fraunhofer 2018: 9). Aktuelle ML-Produktivsysteme mit Angabe ihres Reifegrads listet eine Studie von Fraunhofer auf (Fraunhofer 2018: 32-37). Ein anschauliches Beispiel zum Einsatz einer aktuellen KI-Software zur Beurteilung von Bewerbern findet sich bei Rövekamp 2018.

Martin Rost

Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

E-Mail:
martin.rost@datenschutzzentrum.de

neten „Entscheidungen" unmöglich. b) Bei von KI gesteuerten persönlichen digitalen Assistenten ist unklar, wie gesichert werden kann, dass diese Systeme den Interessen der Nutzer dienen. c) Als größte Gefahr sieht Ramge den *„staatliche Mißbrauch von schwacher KI für Massenmanipulation, Überwachung und Unterdrückung."* (Ramge 2018: 90).[3]

Ramge schreibt es nicht so deutlich, aber diese Gefahren werden nicht von sich irgendwie verselbständigt habenden, tatsächlich intelligenten Techniken, sondern von Organisationen erzeugt, die diese Techniken für ihre Anliegen entwickeln und betreiben. Technisierung macht soziale Konflikte explizit, das ist spätestens mit der Industrialisierung der Arbeit offensichtlich geworden. Von Organisationen betriebene KI-Assistenzsysteme rücken derzeit ganz nah an die Personen heran und es bricht unabweisbar regelungsbedürftig der Konflikt auf, in welchem Interesse diese Systeme eingesetzt werden.

Beruhigend ist, dass für diese Konflikte im Kontext des „nächsten Schritts der Automatisierung" (Ramge 2018: 13f) und der neuen Qualität maschineller Regelungsintelligenz der Datenschutz teilweise sogar erprobte Lösungen hat. Denn Datenschutz war bereits in den 1970er Jahren im Hinblick auf „Beherrschbarkeit der Maschinerie" (Wilhelm Steinmüller) gestartet, nicht aber, so wie es heute vielfach scheint, um eine „Schneckenhaus-Privatheit" (Paul Müller) zu schützen (vgl. Pohle 2018).[4] Neben Beherrschbarkeit kommt ein weiterer Datenschutz-Aspekt hinzu, wonach eine beliebige Zahl möglicher Zwecke in der Welt auch eine Vielfalt von KI-Techniken bzw. eine „pluralistische KI" (Kappes 2018) erfordert.[5] Handelt es sich um viele einzelne, funktional autonome KI-Systeme oder werden diese zu einer einzigen weltumspannenden „KI-Maschinerie" verkettet, die die lokalen Autonomien bricht und die zudem von nur wenigen Herstellern kontrolliert wird?

Die in Art. 5 der DS-GVO formulierten Grundsätze des Datenschutzes bzw. die sechs elementaren Gewährleistungsziele – Sicherung der Verfügbarkeit, der Integrität, der Vertraulichkeit; Gewährleistung der Transparenz, Nicht-Verkettung und Intervention – bilden das vorläufig letzte Produkt der Evolution operationalisierbarer Grundrechte[6], die in dem EU-Rechtsraum von spezialisierten Aufsichtsbehörden zumindest im Grundsatz kontrolliert und gegenüber Unternehmen sanktioniert werden und vor Gericht einklagbar sind. Datenschutzgrundsätze formulieren die notwendigen funktionalen Voraussetzungen, damit vernünftig, differenziert und effizient kommuniziert werden kann (vgl. Rost 2013). Die Vermutung lautet, dass ohne Umsetzung von Grundrechten zum Schutz von Personen vor notorisch übergriffigen Organisationen eine Technik wie KI im Kontext einer modernen, extrem arbeitsteiligen und disparaten Gesellschaft, deren enorme Effizienz ganz besonders auf Vertrauen angewiesen ist, nicht beherrschbar ist. Der „Datenreichtum", auf den eine KI für den unausweichlich anstehenden nächsten Schritt der Automation angewiesen ist, verlangt nicht nur das Teilen der erhobenen personenbezogenen Daten der Monopolisten mit der Allgemeinheit (vgl. Mayer-Schönberger / Ramge 2017), sondern ebenso, dass die Systeme der Datenverarbeitung auch auf der Ebene der KI und des ML den Grundsätzen der sechs elementaren Gewährleistungsziele des Datenschutzes folgen.

2 Was meint „KI" … „Datenschutz"?

„Maschinelles Lernen bezweckt die Generierung von ‚Wissen' aus ‚Erfahrung', indem Lernalgorithmen aus Beispielen ein komplexes Modell entwickeln. Das Modell, und damit die automatisch erworbene Wissensrepräsentation, kann anschließend auf neue, potenziell unbekannte Daten derselben Art angewendet werden. Immer wenn Prozesse zu kompliziert sind, um sie analytisch zu beschreiben, aber genügend viele Beispieldaten – etwa Sensordaten, Bilder oder Texte – verfügbar sind, bietet sich Maschinelles Lernen an. Mit den gelernten Modellen können Vorhersagen getroffen oder Empfehlungen und Entscheidungen generiert werden – ganz ohne im Vorhinein festgelegte Regeln oder Berechnungsvorschriften." (Fraunhofer 2018: 8).

KI-Systeme können in komplexen Situationen in spezifischen Wissensdomänen bessere Entscheidungen als deren besten menschlichen ExpertInnen treffen. Die KI-Modelle der besonders erfolgreichen Systeme wurden aufwändig anhand von Unmengen an Daten aus der Vergangenheit trainiert.[7] In Bezug auf Beobachtungen menschlicher Interaktionen, Äußerungen und Eigenschaften sammeln die Kommunikationsdienste wie Google, Amazon, Facebook und Baidu genau diese Unmengen an Daten. Ebenso haben Microsoft, IBM, Intel, Alibaba, Tencent, NVIDIA und Tesla oder Unternehmen der klassischen Großindustrien Zugriff auf solche Daten, insbesondere der amerikanische Staat kann auf all diese plus jene der NSA zugreifen. Der chinesische Staat betreibt das Projekt des „social rankings" der Einwohner und auch die EU-Staaten haben Zugriff auf BigData-Quellen. All diesen Organisationen stehen enorme Finanzierungsmöglichkeiten zur Forschung und Entwicklung von KI-Techniken für ihre Interessen zur Verfügung.

Grundrechte und die Grundsätze des Datenschutzes haben sich, ebenso wie ein Bewusstsein von persönlicher Individualität, Freiheit, Privatsphäre und Autonomie, im Kontext der modernen Weltgesellschaft entwickelt. Die Datenschutz-Grundsätze formulieren die aktuell gültigen Anforderungen an eine jede Technik mit Personenbezug, also auch an eine KI, für eine moderne Gesellschaft, mit Märkten, mit Gewaltenteilung und kollektiv bindenden Entscheidungen, die demokratisch erzeugt werden und in der es freie politische, ästhetische, wissenschaftliche und spirituelle Diskurse gibt. Schutzziele sind die Anker der „funktio-

3 Diese Risiken werden ausführlich als „Skalen-, Netzwerk- und Feedback-Effekte" diskutiert (vgl. Meyer-Schönberger et al 2017: 187ff). Spekulativ Dystopisches mit verschiedenen Formen verselbständigter Künstlicher Intelligenzen diskutiert Tegmark 2017: 241ff.

4 Beide Zitate entstammen Videointerviews, die unter https://www.datenschutzzentrum.de/interviews/ zu finden sind (Abruf 18.7.2018).

5 *„Bilderkennung in Berlin wird die Spreewaldgurke gut erkennen, in Baden-Württemberg die Wurstvielfalt und in Italien die Pasta-Vielfalt. Es entsteht eine spanische KI, eine italienische KI, eine deutsche KI."* (Kappes 2018).

6 Die Nutzung von Technik fordert es heraus, angesichts der anhaltenden Vermenschlichung von IT als auch der Technisierung von Menschen, insbesondere durch Braintechnology und Cyborgisierung, attraktive Kandidaten zur vorsichtigen Ergänzung („*to avoid rights inflation*") von Menschenrechten zu diskutieren: „cognitive liberty", „the right to mental privacy", „the right to mental integrity" sowie „the right to psychological continuity" (s. Ienca / Andorno 2017).

7 „'Reine Lernverfahren ohne Weltmodelle funktionieren in der Realität nicht', sagte LeCun. Man könne das Auto nicht Millionen Male von der Klippe stürzen lassen, bis es endlich herausgefunden hat, wie es die Kurve meistern kann. Die meisten Menschen dagegen würden innerhalb von zwanzig Stunden Autofahren lernen, ohne in dieser Zeit einen einzigen Unfall zu verursachen." (https://www.heise.de/newsticker/meldung/Kuenstliche-Intelligenz-Digitale-Dichtung-und-Meinungsmanipulation-4111415.html (Abruf 18.7.2018).

Abbildung 1 | Klassifikation von KI-Systemen (Fraunhofer 2018: 10)

Lernstil	Lernaufgabe	Lernverfahren	Modell
Überwacht	Regression	Lineare Regression	Regressionsgerade
		Klassifikations- und Regressionsbaum-verfahren (CART)	Regressionsbaum
	Klassifikation	Logistische Regression	Trennlinie
		Iterative Dichotomizer (ID3)	Entscheidungsbaum
		Stützvektormaschine (SVM)	Hyperebene
		Bayessche Inferenz	Bayessche Modelle
Unüberwacht	Clustering	K-Means	Clustermittelpunkte
	Dimensionsreduktion	Kernel Principal Component Analysis (PCA)	Zusammengesetzte Merkmale
Bestärkend	Sequentielles Entscheiden	Q-Lernen	Strategien
Verschiedene	Verschiedene	Rückwärtspropagierung	Künstliche Neuronale Netze

nalen Differenzierung“ (s. Luhmann 1997) der modernen Welt in den Organisationen.

Der Zweck des Datenschutzes besteht darin, im Kontext dieser modernen Gesellschaft die Machtasymmetrie zwischen strukturell immer begünstigten Organisationen und natürlichen Personen zu thematisieren, deren normative Regelungen zu beurteilen und technisch und organisatorisch wirksame Schutzmaßnahmen kompensatorisch zugunsten der Betroffenen zu treffen. Die gegenwärtig gültigen Prinzipien und Regelungen zur Gestaltung dieser Beziehung zumindest in Europa finden sind in der EU-Grundrechtecharta sowie in der DS-GVO.[8] Unausweichlich ist dabei, dass „Datenschutz in einer vernetzten Welt eine der zentralen Machtfragen stellt.“ (Nocun 2018: 14). Datenschutz verlangt Organisationen Aktivitäten ab, die betroffenen Personen vor der Datenverarbeitung der Organisation zu schützen, also auch vor den Folgen einer KI-gestützten Datenverarbeitung, entgegen deren strukturellen Interessen an großen Datenmengen, die frei zur zweckungebundenen Verarbeitung sind. Hollywood mag etwas anderes suggerieren, aber es gibt keine autonomen Roboter-Entitäten mit Subjektqualität und Selbstverantwortung, es gibt Expertensysteme, die von Organisationen entwickelt und gesteuert werden und von denen zu verantworten sind.

Technik ist für Datenschutz aus drei Gründen ein relevantes Thema: a) Ohne Datenschutz besteht das Risiko, dass die Nutzung von Informations- und Kommunikationstechnik den ohnehin stattfindenden Grundrechtseingriff der Organisation gegenüber Personen verstärkt. Technikgestützte Herrschaft über Personen kann als materialisierter, alternativloser Sachzwang erscheinen. In Bezug auf KI besteht der Grundrechtseingriff darin, dass die Organisation mit den besonders wirksamen Mitteln der KI als Vollautomation die Autonomie von Personen über die Maßen einschränkt, dabei neue Formen von Manipulationen möglich werden, Fehler passieren und die Verantwortung für Eingriffe und Fehler durch beteiligte Organisationen unsichtbar bzw. abgewälzt werden. b) Die Nutzung von Kommunikations- und Informationstechniken für Datenverarbeitungen ist latent unsicher: Technik kann schlecht konstruiert/ programmiert sein, sie kann kaputtgehen und es können Unbefugte unkontrolliert Technik nutzen und auf Daten zugreifen. Das gilt im vollen Umfang auch für KI-Systeme, diese Themen werden aktuell im Kontext von Haftungsfragen zur KI und Anforderungen an deren IT-Sicherheit diskutiert. c) Eine intelligente (!) Datenschutztechnik kann dafür eingesetzt werden, um die durch intelligente Technik gesteigerten Risiken wiederum ebenso intelligent zu verringern. Mit dem Einsatz von KI wird ein neuer Typ von Datenschutz- und Sicherheits-Schutzmaßnahmen denkbar, wonach Maschinen, im Hinblick auf die Einhaltung bestimmter Eigenschaften und Funktionen, besser als bislang automatisiert sich selbst und andere überwachen und auch bei unvorhergesehenen Situationen durch übergriffige Organisationen erwartungsgemäße, individuelle und/ oder kollektiv wünschbare „Entscheidungen“ treffen können. Eine Datenschutz-KI wäre somit eine wesentliche Schutzmaßnahme zur Sicherung der Resilienz von Verarbeitungstätigkeiten gem. Art. 32 DS-GVO (vgl. Gonscherowski et al. 2018).

Nach Art. 30 DS-GVO sind Eigenschaften zur Erfassung einer Verarbeitung zusammenzustellen, es wird die Zuordnung der Verantwortlichkeit abverlangt. Wenn eine Organisation ein KI-System als Bestandteil einer Verarbeitungstätigkeit mit Personenbezug betreibt, bspw. ein Expertensystem, dann ist die Organisation schlicht für den Betrieb der KI verantwortlich. Die Organisation umschmiegt ein KI-System genauso wie sie auch die Intelligenz der MitarbeiterInnen umschmiegt; ein Fehler der KI oder eine Fehlkonfiguration beim Training im Kontext des ML ist als Fehlentscheidung der Organisation dem Verantwortlichen zuzurechnen.

Wenn eine Person ein KI-System unmittelbar nutzt, bspw. mit dem Kauf eines persönlichen (oder familiär genutzten) KI-Assistenzsystems, das bspw. ein Fahrzeug autonom durch den öffentlichen Verkehr bewegen soll, so bleibt der zuvor genannte Kontext der Verantwortlichkeit erhalten.[9] Der selbstbestimmte Einsatz des Systems durch den Nutzer einer KI bedeutet nicht, dass das System ausschließlich entsprechend dem exklusiven Willen des Besitzes assistiert noch dass das System in Eigenverantwortung und Selbstzwecksetzung agiert. Sowohl der Hersteller der spezifischen KI-Eigenschaften als auch ein Betreiber einer KI-Infrastruktur haben, unter den gegenwärtigen Umständen, einen wesentlichen Einfluss auf die Eigenschaften der KI. Typischerweise bleiben die Daten, die im Kontext einer KI gesammelt und dem ML zugeführt werden, nicht im vom Betroffenen genutzten Assistenzsystem, sondern werden, zumeist durch den KI-Betreiber qualitätsgesichert, auch allen anderen KI- und Assistenz-Systemen zur Verfügung gestellt.[10]

8 Zur Unterscheidung „Prinzipien und Regeln“ und „Schutzzielen als Optimierungsgeboten“ siehe Bock / Robrahn 2018.

9 Laßmann listet die Akteure im Kontext von Asisstenzsystemen (bei ihm mit körperlicher Ausdehnung) auf: a) Entwickler / Hersteller, b) Benutzer / Betreiber, c) Robots, d) Menschen, die mit einem Robot interagieren, e) Menschen, die Roboter beobachten (vgl. Laßmann 2018: Pos. 734f).

10 Zur Gestaltung der unmittelbaren Interaktion Person-KI-System sollten neben den Schutzzielen die Asimovschen Computergesetze berücksichtigt wer-

3 Risikokriterien für KI

Der Betrieb von KI-Systemen für Verarbeitungstätigkeiten mit Personenbezug braucht, wie jede andere Verarbeitung auch, eine Rechtsgrundlage. Aufgrund des hohen Risikos für die Rechte und Freiheiten von Personen – allein durch die Vollautomation von Entscheidungskompetenzen und dem typischerweise stattfindenden Profilieren der unmittelbaren KI-Nutzer – sind Verantwortliche geordert, eine Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DS-GVO durchzuführen.[11]

Es müssen für die Hardware- und Software-Ebene von KI-Systemen, also der „konventionellen" Technikebene unterhalb der technisch-kognitiven Entscheidungsebene, die typischen Schutzmaßnahmen der IT-Sicherheit und des operativen Datenschutzes für zumindest hohen Schutzbedarf getroffen werden. Mit Rückgriff auf KI wird vielfach sehr hoher Schutzbedarf der Nutzer bestehen, weil Fehlfunktionen, wie bspw. beim automatisierten Fahren, Personen existentiell gefährden. Ein (sehr) hoher Schutzbedarf allein für die technische Basis von KI-Systemen erfordert den Einsatz redundanter Systeme, Zertifikatemanagement bzgl. Verschlüsselung und Authentizität aller Beteiligten und Systeme und Interaktions- und Kommunikationskanäle, Umsetzen der Spezifikations-, Dokumentations- und Protokollpflichten, Interventionsmöglichkeiten für Betroffene; Maßnahmen der Pseudonymisierung und Anonymisierung von Daten und gesicherte Trennungen zwischen Datenbeständen, IT-Systemen und Prozessen (siehe SDM V1.1 gem. DSK 2018). Nachfolgend sollen spezifische Probleme und Maßnahmen mit Bezug auf die Intelligenz simulierende kognitive Ebene der automatisierten Entscheidungsgenerierung angesprochen werden.

3.1 Transparenz

Unter Sicherung der Transparenz (s. Art. 5, Art. 25, Art. 32 DS-GVO) versteht man im Datenschutz die Herstellung der Prüfbarkeit – durch den Verantwortlichen, die Betroffenen und Aufsichtsbehörden – der Komponenten von Verarbeitungstätigkeiten mit Personenbezug anhand von Datenschutzerklärungen, Einwilligungen und Verträgen sowie Spezifikationen, Dokumentationen, Logs und Protokolldaten. Die verarbeiteten Daten, die Systeme, die Funktionsweise und die Wirkungen einer Verarbeitung müssen verständlich sein. Datenschutz-ExpertInnen muss man dabei, wie auch ExpertInnen für IT-Sicherheit, ein gegenüber technischen Laien komplexeres Systemverständnis sowie die Fähigkeit, Systeme integer und intelligent prüfen und Korrekturbedarfe konkret formulieren zu können abverlangen.

Bei der Modellierungsebene der Repräsentation des domänenspezifischen Wissens einer KI müssen die Herkunft der Daten, die Form der Veredlung und Anreicherung der Rohdaten zu Modell- oder Trainingsdaten, die Lernstile (überwacht, unüberwacht, bestärkend) und die verwendeten Modelle, die sich aus dem Typ der Lernaufgabe und des Lernverfahren bestimmen lassen, spezifiziert und dokumentiert werden (vgl. Fraunhofer 2018, siehe auch Abb. 1). Fragen wie die Folgenden entstehen im Kontext des Einsatzes von KI und der durch sie verursachten „algorithmische Risiken" (Diakopoulos / Deussen 2017): Wurde eine KI-Komponente eingesetzt? Welcher Typ von Entscheidungsgenerierung kam dabei zum Einsatz? Welcher Art ist die menschliche Beteiligung an der Entscheidungsfindung? Welche Institutionen hatten Kontrolle über die Technik, das Kuratieren der Daten, das Training und der Auswahl der Modelle? Von welcher Qualität sind die verwendeten Trainigsdaten, wie wurden Daten definiert, gesammelt, selektiert, umgewandelt, verifiziert und bearbeitet? Welche unmittelbar personenbezogenen Daten wurden dabei verarbeitet? Wie hoch ist der Grad der Vollständigkeit bzgl. der Repräsentativität der Wissensdomäne? Wie sind historische Änderungen einer Wissensdomäne berücksichtigt (vgl. Diakopoulos / Deussen 2017: 364f zu „Transparenzstandards")? Das Vertrauensniveau für KI-„Entscheidungen", die auf einem methodisch einwandfrei eingesetzten Regressionsverfahren beruhen, ist ungleich integrer einschätzbar als das von KNN. Nicht die Behandlung von Haftungsfragen, sondern die Prüfbarkeit steht im Vordergrund, ob die Intensität des Grundrechtseingriffs in die Autonomie betroffener Personen durch eine KI auf dem geringst möglichen Eingriffsniveau und dem größtmöglichen Nutzen für den Nutzer ausgerichtet ist. Um der Dynamik gerecht werden zu können, müssen die verschiedenen Komponenten einer KI selbstauskunftsfähig werden.

KI läuft darauf hinaus, „Entscheidungskompetenzen an Systeme abzugeben" (Fraunhofer 2018: 40), ohne dass deshalb auch die steuernden Kriterien für maschinelle Entscheidungen und die Verantwortung dafür abgegeben werden. Eine KI sollte nicht einfach empfehlen und „entscheiden", ohne dass nicht auch eine Begründung mitgegeben wird, die im Zusammenhang mit dem Kontext und den Kriterien der maschinellen Entscheidung steht und gegen die dann ggfs. die MitarbeiterInnen einer Organisation, Betroffene oder Aufsichtsbehörden, die stellvertretend für die Gesellschaft stehen, intervenieren können (vgl. Ramge 2018: 26).

Aufgrund der Risiken der KI-Automation und des ML sowie darüber hinaus der Vernetzungen solcher Systeme – man denke an den automatisierten Aktienhandel, an Avatare oder Agents oder an cyber-physical-systems (CPS), dem Internet-of-Things (IoT) oder an verkettete Robots der Industrie 4.0 – müssen wiederum spezielle KI-Systeme zur Beobachtung dieser vernetzten Maschinen unter sicherheitstechnischen und datenschutzrechtlichen Kriterien betrieben werden. Damit hier keine Endlos-Beobachtungsschleife der einander beobachtenden adaptiven Systeme entsteht, sollten die Policies von Prüf-Automaten in automatisiert lesbarer Form formuliert sein und als Referenz genutzt werden.[12] Als Faustregel lässt sich formulieren: Kein Betrieb einer KI ohne eine explizite Datenschutz-Policy auf gesetzlicher Basis mit einer datenschutzgetriebenen Prüf-KI als Bestandteil eines Datenschutz-Managementsystems (siehe Art. 32 Abs. 1d DS-GVO).

den, siehe https://de.wikipedia.org/wiki/Robotergesetze (Abruf 18.7.2018).

11 Eine DSFA soll darauf hinwirken, dass a) ein Verfahren von Vornherein datenschutzgerecht gem. Art. 24 gestaltet ist und dafür die Risiken, die sich im Wesentlichen durch Nichterfüllen der Anforderungen aus Art. 5 ergeben, nicht bearbeitet werden. Außerdem sind b) Organisationen gehalten, sich selbst als Hauptangreifer auf die Betroffenen zu modellieren, weil sie diese Risiken aufgrund der strukturell immer gegenläufigen Interessenslage nicht hinreichend bearbeiten. Außerdem sind weitere Organisationen, wie bspw. Sicherheitsbehörden, Versicherungen oder Forschungsinstitute, mit ihren Interessen in den Blick zu nehmen. Es geht bei einer DSFA im Unterschied zur IT-Sicherheit nicht darum, den Schutz von Geschäftsprozessen vor Hackern in den Hauptfokus zu stellen (vgl. Forum Privatheit 2017).

12 Solche Policies, abgeleitet u. a. aus den Anforderungen der DS-GVO und der IT-Sicherheit nach BSI-Grundschutz, sind als domänenspezifische „Wesensprofile" zur Steuerung von Web-Services im Kontext von XTA2 („Fachunabhängiger Standard für Transportverfahren", https://www.xoev.de) standardisiert worden und stehen vor der Praxiseinführung.

3.2 Nicht-Verkettung

Unter Sicherung der Nicht-Verkettung (s. Art. 5, Art. 17, Art. 22, Art. 25, Art. 32, Art. 40 DS-GVO) wird im Datenschutz die Eigenschaft einer von einem bestimmten Zweck eingeschränkten Verarbeitung bezeichnet, bei der Daten, IT-Systeme und Prozesse von anderen Datenbeständen, IT-Systemen und Prozessen getrennt verarbeitet werden. Dieses Gewährleistungsziel nimmt die Anforderungen nach Datenminimierung sowie insbesondere zur Durchsetzung von Gewaltenteilung, unabhängigen Marktakteuren und Berücksichtigung verschiedener politischer Interessenslagen (verallgemeinert: von Diversität) auf. Ausgangspunkt für eine Operationalisierung dieser Anforderung ist der explizit ausgewiesene Zweck einer Datenverarbeitung.

Dass für die Vollautomation einer Verarbeitung ein KI-System genutzt wird, ändert nichts daran, dass die Zwecksetzung (bzw. Zweckänderung) einer Verarbeitung durch den Verantwortlichen zunächst einmal legitim sein muss. Die Frage nach der Legitimität einer Vollautomation per KI muss sich der Verantwortliche für das KI-System stellen. Aus einer funktionalen Autonomie folgt noch keine Autonomie auch bei der Verantwortung, etwa im Sinne einer Eigenverantwortung einer KI. Ein funktional autonomes KI-System ist, anders als ein funktional autonomer Mensch, kein Zweck an-sich selber, es kann keine eigenen Zwecke setzen und deren Legitimität prüfen. Diese theoretischen Konzepte von Autonomie und Verantwortung geraten allerdings unter zunehmenden Rechtfertigungsdruck insbesondere durch die Hersteller und Betreiber von KNN. Der Umgang mit KNN legt ein Beschränken auf Kalküle bzgl. Blackboxes und Korrelationen nahe, Theorie wird wieder in dogmatisch behavioristischer Manier zur bloßen Spekulation herabgesetzt.[13]

Mag der Zweck einer KI hinreichend eingeschränkt werden, das datenschutzrechtliche Problem insbesondere von KNN besteht darin, dass sehr viele Daten einer Wissensdomäne zu einem Muster korreliert werden, bei denen Menschen mit bestimmten Eigenschaften benachteiligt werden könnten, die selbst dann nicht benachteiligt werden sollen, wenn objektiv messbare Fakten es aus Sicht der Organisation (und selbst vieler Betroffener) rechtfertigen würden. KNN sind sehr gut geeignet, um Diskriminierungen zu verstecken oder als objektiv unumstößlich erscheinen zu lassen. Und das kann auch in solchen Fällen passieren, in denen schon beim Entwurf einer Datenverarbeitung für das maschinelle Lernen nur solche Daten verarbeitet werden, die in einer Wissensdomäne dem Zweck der Verarbeitung theoretisch begründet sehr wahrscheinlich dienlich sind. Es ist genau diese Fähigkeit zur subtilen Unterscheidung und Korrelation im Datenmaterial, die die besondere Leistungsfähigkeit von KNN ausmacht. Dass hier ein offenes Problem liegt, sieht auch die bereits eingangs zitierte Fraunhofer Studie. Es sollen nur solche Trainings erlaubt sein, die bspw. normativ gewünschte, dis-

13 Deswegen sind verwegene Versuche, neben natürlichen und juristischen Personen nun auch noch „elektrische Personen" einzuführen, durchsichtige Manöver der Hersteller und Betreiber von KI-Systemen, die unbeherrschten Risiken von sich abzuwälzen und sich der Verantwortung und vor allem der Übernahme etwaiger Haftungskosten zu entziehen (vgl. Otto 2018).

kriminierungsfreie Modellierungen erzeugen (vgl. Fraunhofer 2018: 31).

Sodann muss der Zweck des KI-Systems so eng wie möglich in einer maschinell zugänglichen Policy beschrieben sein, aus der sich konkrete funktionale Anweisungen bzgl. Funktionen und Schutzmaßnahmen ergeben, um Zweckdehnungen und Zweckverletzungen ebenfalls mit maschineller Unterstützung feststellen, verfolgen und ggfs. ebenfalls automatisiert sanktionieren zu können. Wieder zeigt sich: Es dürfen keine KI-Systeme ohne maschinell zugängliche Policies zu deren unabhängigen Kontrolle betrieben werden. Ganz wesentlich ist dabei die Trennung von solchen Zwecken, die benachbart sind und gerade wegen dieser besonderen Nähe und ihres hohen Effizienzversprechens aus grundrechtlichen Gründen genau nicht verfolgt bzw. trainiert werden sollen. Je spezifischer und eben doch theoriegeleitet die Trainingsdaten sind, desto empfindlicher, selektiver und „erwartungsgemäßer" dürfte das Systemverhalten von KNN sein. Erst dann lassen sich auch Aspekte der horizontalen Zweckbindung innerhalb der Optionenvielfalt der Systeme der Verarbeitung und vertikalen Zweckbindung in Bezug auf die Techniken, die auf den verschiedenen Ebenen eines KI-Systems zum Einsatz kommen, definieren und ausführen. Maßgeblich für eine funktionierende KI ist nicht die möglicherweise beeindruckend umfassende Automationsmöglichkeit, sondern es bleibt der eng auszuführende Zweck.

Um eine möglichst zweckorientierte und somit theoriegestützte Verarbeitung und ein Machine-Learning-Model datenschutzgerecht zu trainieren, müssen Daten aufbereitet werden (vgl. Scheiderer / Meisen 2018: 49). Nur dann ist es möglich:

- die domänenspezifisch relevanten Daten aufzunehmen und zu speichern,
- zutreffende Datenquellen auszuwählen,
- zutreffende Zielgrößen festzulegen
- Daten maschinenverständlich aufzubereiten,
- einen Datenbestand zu komplettieren,
- fehlerhafte Daten zu entfernen,
- Daten zu normalisieren oder zu standardisieren,
- die Dimensionalität der Daten zu reduzieren,
- das Machine-Learning-Model zu trainieren.

Zur Umsetzung des Datenschutzrechts ist eine solche Art der Vorverarbeitung von Trainingsdaten für Klassifikations- oder Regressionsmodelle, die sogenannte „Datenkuration", möglicherweise nicht wirklich geeignet. Aber grundsätzlich ist davon auszugehen, dass das Training von KI-Systemen mit personenbezogenen Daten auf eine ähnliche Weise standardisiert und integritätsgesichert stattfinden muss.

Daten des Nutzers eines Systems sollten ein persönliches KI-Assistenzsystem nicht verlassen. Ob anonymisierte Daten zwecks Verbesserung der KI an einen Betreiber datenschutzgerecht abfließen können, muss noch erforscht werden. Erste Studien zeigen, dass für das Trainieren mit Daten aus unterschiedlichen Quellen die Trennung dieser Quellen im Sinne eines „privacy-preserving machine learning" (ppml) nicht aufgehoben werden muss (vgl. Tian et al., 2016). Es ist zudem eine Überlegung wert, die Nutzung von Trainingsdaten, gerade auch in Bezug auf die Qualität der Daten, deren Domänenspezifik und Vollständigkeit sowie der Anonymisierungsgrad und die Programmier- bzw. Trainingsmethoden, einem Genehmigungsverfahren zu unterwerfen.

3.3 Integrität

Unter Sicherung der Integrität (s. Art. 5, Art. 25, Art. 32, Art. 33 DS-GVO) versteht man im Datenschutz die durch den Zweck bestimmte korrekte Umsetzung von Funktionen bei der Verarbeitung personenbezogener Daten. Abweichungen vom Zweck müssen zumindest erkennbar, beurteilbar und korrigierbar sein.

KI-Systeme bieten im besten Falle problemangemessene Lösungen gerade in unsicheren, bei der Spezifikation nicht vorhergesehenen Entscheidungslagen, was dann als „kreativ" oder „intuitiv" erscheinen mag. Eine KI-Entscheidung ist gültig, wenn sie sich zugleich im Rahmen des Erwartbaren der Nutzer und des normativ Geforderten befindet, beide Erwartungslagen wurden idealerweise im Vorhinein explizit gemacht.[14]

Wesentlich zur Sicherung der Integrität von KI-Systemen und deren ML dürfte die eng am Zweck orientierte Bildung von Einsatzszenarien sein, in denen die Randbedingungen so explizit wie möglich formuliert sind. Dann sind Tests – die im Vorhinein zu spezifizieren, dann zu dokumentieren und die Ergebnisse zu protokollieren sind – zur Modellvalidierung durchzuführen, in denen insbesondere auf adäquate Reaktionen des KI-Systems bei Abweichungen zu prüfen ist. Methodisch sollte Wert darauf gelegt werden, dass auch mit „störsignalbehafteten Daten" (Fraunhofer 2018: 30) trainiert wird. Und es ist auf den Einbau von Sicherheitsspannen in Bezug auf die Sicherung aller Gewährleistungsziele Wert zu legen.

Aus Datenschutzsicht ist anzustreben, dass Organisationen nicht KNN bequemerweise dort einsetzen, wo zwar aufwändiger zu programmierende, aber aufgrund eindeutiger Regeln verlässlichere Regressionsmodelle mit ausweisbarem Vertrauensintervallen programmiert und genutzt werden können.

3.4 Vertraulichkeit

Unter Sicherung der Vertraulichkeit (s. Art. 5, Art. 25, Art. 28, Art. 29, Art. 32 DS-GVO) versteht man eine Verarbeitung[15], die im Sinne des Dataprotection-By-Design gem. Art. 24 DS-GVO so ausgelegt ist, dass nur Befugte auf deren Daten, IT-Systeme und Prozesse zugreifen können.

Bei KI-Systemen stellt sich somit die Frage, welche Instanzen befugt und welche nicht befugt sind, in Bezug auf den ausgewiesenen Zweck

- die Daten für ein KI-System zu sammeln und zu kuratieren,
- das dafür angemessene Lernmodell zu bestimmen und es zu programmieren oder zu trainieren,
- die Einsatzszenarien für den befugten Zugriff festzulegen und mit deren relevanten Dimensionen auszuformulieren,
- die Integrität des Verhaltens der KI in Bezug zum als befugt ausgewiesenen Nutzer zu testen und die Ergebnisse zu beurteilen,
- dieses System und deren Entscheidungen für einen automatisierten Betrieb dann zu nutzen.

Eine KI wird gerade durch die permanente Interaktion mit der befugten Nutzerin immer nützlicher und effektiver, wobei die Mensch-Maschine-Interaktionen vermutlich so charakteristisch wie ein biometrisches Datum sind. Genau an solchen Daten wer-

14 Wobei sich erst im Nachhinein herausstellen kann, dass eine Lösung im erwartbaren Rahmen lag. Sowohl bei Alpha-Go als auch Libratus haben ExpertInnen von den per KI generierten Lösungen gelernt.

15 Zur langen Definition von „Verarbeitung" siehe Art. 4 Abs. 1 DS-GVO.

den die Hersteller oder Betreiber von KI-Systems besonders interessiert sein, weil sie dadurch die Nutzer und Nutzerinnen wiederum besonders effektiv auf ihre Interessen hin steuern oder auch eine falsche Anwendung der KI nachweisen können. In Gesetzen, Verträgen und Einwilligungserklärungen werden sich Organisationen eine Nutzungsberechtigung der Personenprofile zum ML und Training von KI-Systemen einräumen. Neben den KI-Herstellern und Betreibern werden insbesondere Sicherheitsbehörden, Versicherungen, Forschungsinstitute und zunehmend auch politische Vereinigungen zwecks Verbesserung komplexer gesellschaftlicher Planungen die Berechtigung ihrer Zugriffe geltend machen.[16] Eine Gretchenfrage wird sein, ob eine KI, mit deren Assistenz Ordnungswidrigkeiten oder Straftaten werden, diese als solche zumindest „bemerkt" und dann vielleicht nicht unmittelbar an die Sicherheitsbehörden meldet wohl aber anhand von Protokolldaten durch Betreiber und Hersteller bemerkt werden können? Wenn ein solches System funktioniert werden Innenminister darauf zugreifen wollen. Das andere Problem, ob eine KI das entsprechend den Nutzerkriterien tatsächlich beste Produkt vorschlägt und es ggfs. für den geringsten Preis bestellt, wird qua spezialisierter Beratungsdienstleistungen lösbar sein.

Die Sicherung des Zugriffs durch Befugte auf Assistenzsysteme ist ein Problem der IT-Sicherheit, die Sicherung der Exklusivität der inhaltlich orientierten Steuerung und Nutzung der KI durch die Nutzer sowie Nutzerinnen und inwieweit die Entscheidungen oder die Kriterien für die Entscheidungen der KI ausschließlich durch die NutzerInnen festgelegt werden, hingegen eines des Datenschutzes.

3.5 Intervenierbarkeit

Unter Sicherung der Intervenierbarkeit (s. Art. 5, Art. 13 bis Art. 18, Art. 20, Art. 21, Art. 25, Art. 32 DS-GVO) versteht man im Datenschutz, dass eine personenbezogene Verarbeitung mit ihren technischen Komponenten verändert und auch gestoppt werden kann.

Bei KI stellt sich die Gretchenfrage einer jeden Vollautomation: Toppt in Konfliktsituationen der Pilot die Maschine oder die Maschine den Piloten? Die generelle Antwort des Datenschutzes lautet: Ein Mensch muss eine Maschine, zumindest sofern diese in ihren Folgen allein ihm assistiert, toppen können. Zwecks Risikominimierung optimal sind offenbar „Hybridsysteme" einer möglichst intelligenten Interaktion von Mensch und Maschine (vgl. Wahlster 2017). Für die Gestaltung unmittelbar wirksamer Interaktionen zwischen Personen und Maschinen lassen sich zudem Anforderungen aus der Arbeitssicherheit übertragen, die in Bezug zur KI vermutlich um die drei „Asimovschen Gesetze" anzureichern sind.[17]

Die Möglichkeiten zum Eingriff, zum Stoppen oder zur manuellen Steuerung müssen bei einer KI-Assistenz klar gestaltet sein, Korrekturen müssen im gesamten System durchsetzbar sein. Denkbar wäre die Nutzung besonders vertrauenswürdiger persönlicher KI-Assistenzsysteme, die tatsächlich autonom von anderen KI-Systemen agierend Interventionen veranlassen und deren Ausführungen beständig überwachen und ggfs. weitergehende Korrekturen anfordern.

Mit der Übernahme einer manuellen Steuerung einer KI ändert sich die Haftung für ein System. Es ist damit zu rechnen, dass Hersteller und Versicherungen von der eigenbestimmten Steuerung durch Nutzer, für deren maschinelle Beobachtung dann aus Sicht der Nutzer kein Anlass mehr besteht, dadurch entmutigen, dass diese die Haftungskosten besonders hochtreiben.

3.6 Verfügbarkeit

Unter einer gesicherten Verfügbarkeit (s. Art. 5, Art. 13, Art. 15, Art. 20, Art. 25, Art. 32 DS-GVO) einer Verarbeitung versteht man zusätzliche Maßnahmen, mit denen erwartete Funktionen in Bezug auf Daten, IT-Systeme und Prozesse innerhalb einer definierten Qualität erbracht werden können.

Es muss definiert sein, ob der Nutzer eines persönlichen KI-Assistenten bei Ausfall des Systems die Steuerung übernehmen kann (wie bei einem Sprach-Assistenten) oder nicht (wie beim Fahr-Assistenten ohne Führerschein des Nutzers) oder diese zumindest teilweise übernehmen kann (Nutzer als Assistent des KI-Systems). Ist ein Nutzer auf einen KI-Vollautomaten angewiesen könnte eine Lösung darin bestehen, dass ein anderes KI-System, das zentral als Dienstleistung betrieben wird, die Funktionen für die Zeit des Ausfalls übernimmt. Probleme der Sicherung der Verfügbarkeit von KI-System stehen traditionell nicht so sehr im Fokus des Datenschutzes, sie werden gegenwärtig insbesondere mit Bezug zur Übernahme von Haftungskosten besonders intensiv bearbeitet. Ein besonderes Problem in Bezug auf von KNN gesteuerten Systemen besteht offenbar darin, dass es weder auf der Hardware-Ebene noch der kognitiven Ebene eine perfekte Kopie eines solchen Systems geben kann (Laßmann 2018: Pos. 543).

4 Fazit

Eines wird ohne jeden Zweifel auch weiterhin gelten: Ein Hundehalter kann sich nicht damit herausreden, nicht wissen zu können, was der Hund so dachte, als dieser zubiss. Die Datenschutz-Schutzziele empfehlen sich als generelle Design-Imperative zwecks Beherrschung intelligenter Automationstechniken. Es hat sich an vielen Stellen der Untersuchung gezeigt, dass KI-Systeme zudem wiederum durch andere KI-Systeme beobachtet und gesteuert werden sollten. Das setzt voraus, dass diese Systeme unabhängig voneinander, mit klarer Explikation des Zwecks, der Auftrags- und der Interessenslage, hergestellt und betrieben werden können. Die Machtfrage, die Datenschutz speziell in Bezug zur KI aufwirft, ist die, wer über die Ausgestaltung von KI-Techniken herrscht und dadurch über Unbestimmtheit, Vielfalt und kontingente Aktivitäten in einer modernen Gesellschaft entscheidet.

16 In diesem Kontext ist an Cybersyn zu erinnern, einem chilenischen Projekt aus den 1970er Jahren, in dem mit Hilfe modernster Informations- und Kommunikationstechnik wirtschaftspolitische Entscheidungen offenbar erfolgreich vorbereitet wurden (vgl. Sowa 2017: 99f; Mayer-Schönberger et al. 2017: 206f).

17 Im Kontext eines Simulationsmodells zur Umsetzung der Asimovschen Gesetze (vgl. Laßmann 2018: Pos. 314f) zeigte sich, dass die zur Operationalisierung notwendigen Explikationen auf die Gewährleistungsziele des SDM (vgl. DSK 2018), die auch diesen Artikel strukturieren, hinauslaufen. Das stärkt die Vermutung, dass im vollständigen Durchgang durch die Gewährleistungsziele des Datenschutzes weitere nützliche Explikationen für die Asimovschen Gesetze zu finden wären.

5 Literatur

Bock, Kirsten / Robrahn, Rasmus, 2018: Schutzziele als Optimierungsgebote; in: DuD – Datenschutz und Datensicherheit, 42. Jahrgang, Heft 1: 7-12.

Diakopoulos, Nicholas / Deussen, Oliver, 2017: Brauchen wir eine Rechenschaftspflicht für algorithmische Entscheidungen? in: Informatik-Spektrum, Ausgabe 4: 362-366.

DSK 2018: Handbuch zur SDM-Methodik, V1.1, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf (Abruf 18.7.2018).

Forum Privatheit: „Whitepaper ‚Datenschutzfolgenabschätzung'", V3.0, https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf (Abruf 18.7.2018).

Fraunhofer 2018: Maschinelles Lernen – Eine Analyse zu Kompetenzen, Forschung und Anwendung; https://www.bigdata.fraunhofer.de/de/big-data/kuenstliche-intelligenz-und-maschinelles-lernen/ml-studie.html (Abruf 18.7.2018).

Gehlen, Arnold, 1956: Urmensch und Spätkultur, Bonn, Athenäum.

Gonscherowski, Susan / Hansen, Marit / Rost, Martin, 2018: Resilienz – eine neue Anforderung aus der Datenschutz-Grundverordnung; in: DuD – Datenschutz und Datensicherheit, 42. Jahrgang, Heft 7: 43-48.

Hansen, Marit / Thiel, Christian, 2012: Cyber-Physical-Systems und Privatsphärenschutz; DuD – Datenschutz und Datensicherheit, 36. Jahrgang, Heft 1: 26-30.

Ienca, Marcello / Andorno, Roberto, 2017: Towards new human rights in the age of neuroscience and neurotechnology; in: Life Sciences, Society and Policy, https://doi.org/10.1186/s40504-017-0050-1 (Abruf 18.7.2018).

Kappes, Christoph, 2018: „Anmerkungen zur KI-Strategie Europas" im Rahmen eines Gutachterkommentars „EU-Strategie zur Künstlichen Intelligenz", http://christophkappes.de/ (Abruf 18.7.2018).

Laßmann, Günter, 2018: Asimovs Robotergesetze – Was leisten sie wirklich? Telepolis.

Luhmann, Niklas, 1997: Die Gesellschaft der Gesellschaft, 1. Aufl., Frankfurt am Main, Suhrkamp.

Mayer-Schönberger, Viktor / Ramge, Thomas, 2017: Das Digital – Markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus, 1. Aufl., Berlin, Econ.

Nocun, Katharina, 2018: Die Daten die ich rief – Wie wir unsere Freiheit an Großkonzerne verkaufen, 1. Aufl., Köln, Lübbe.

Otto, Claudia, 2018: Das dritte Ich – Ist die ‚Schizophrenie' künstlich intelligenter Systeme behandelbar? In: Recht innovativ, Ausgabe 2: 68-88, https://rechtinnovativ.online/assets/recht-innovativ-(ri)-02218.pdf (Abruf 18.7.2018).

Pohle, Jörg, 2017: Geschichte und Theorie des Datenschutzes, https://edoc.hu-berlin.de/handle/18452/19886 (Abruf 18.7.2018).

Ramge, Thomas, 2018: Mensch und Maschine – Wie künstliche Intelligenz und Roboter unser Leben verändern, 2. Aufl., Stuttgart, Reclam.

Rövekamp, Marie, 2018: „Der Algorithmus kann 42 Dimensionen einer Persönlichkeit messen"; in: Der Tagesspiegel, 02.07.2018, https://www.tagesspiegel.de/wirtschaft/kuenstliche-intelligenz-der-algorithmus-kann-42-dimensionen-einer-persoenlichkeit-messen/22756300.html (Abruf 18.7.2018).

Rost, Martin, 2013: Soziologie des Datenschutzes; DuD – Datenschutz und Datensicherheit, Heft 2: 85-91.

Rost, Martin, 2018: Ordnung der Schutzziele; in: DuD – Datenschutz und Datensicherheit, Heft 1: 13-18.

Scheiderer, Christian / Maisen, Tobias, 2018: Auf eigenen Füßen – Machinen-Learning in der Industrie; in: iX-Special 2018, Internet Of Things: 48-50.

Sowa, Aleksandra, 2017: Digital Politics – So verändert das Netz Demokratie, 1. Aufl., Bonn, Dietz.

Tegmark, Max, 2017: Leben 3.0 – Mensch sein im Zeitalter Künstlicher Intelligenz, 2. Aufl., Berlin, Ullstein.

Tian, Lu / Jayaraman, Bargav / Gu, Quanquan / Evans, David, 2016: Aggregating Private Sparse Learning Models Using Multi-Party Computation; in: Workshop on Private Multi-Party Machine Learning (NIPS 2016), Barcelona, Spain, http://oblivc.org/docs/pmpml.pdf (Abruf 18.7.2018).

Wahlster, Wolfgang, 2017: Künstliche Intelligenz als Grundlage autonomer Systeme, https://www.stiftung-jgsp.uni-mainz.de/Bilder_allgemein/Beitrag_Autonome_Systeme-Informatik-Spektrum-Wahlster.pdf (Abruf 18.7.2018).