Kommunikation & Recht

K&R 12/2018

Justiziar Conrad S. Conrad, Hamburg*

Künstliche Intelligenz und die DSGVO – Ausgewählte Problemstellungen

Die EU-Kommission stellte im April 2018 ein Konzept zur „künstlichen Intelligenz" (KI) vor, das sowohl Forderungen nach Investitionen in Höhe von rund 20 Milliarden vorsieht als auch ethische Leitlinien für den Umgang mit den Programmen etablieren soll. Auch die Bundesregierung präsentierte ein Strategiepapier. Hierin wurde festgestellt, die DSGVO bilde „einen verlässlichen gesetzlichen Rahmen für innovative Technologien und Anwendungen auch im Bereich der KI". Ein Expertengremium hat das Thema seither auf der Agenda. Viele juristische Fragen, insbesondere aus dem Datenschutzrecht sind indes weiterhin ungeklärt.

I. Stand der KI

Die mit „künstliche Intelligenz" bezeichnete technische Entwicklung von lernfähigen Algorithmen bis hin zu Theorien des „selbstdenkenden" Computerprogramms feiert seit einigen Jahren eine Renaissance.[1] Dabei bereitet die Begriffsbestimmung den Experten Schwierigkeiten, die nach einem gängigen Modell zwischen einer „starken" und „schwachen" Künstlichen Intelligenz unterscheiden.[2] Erstere, die selbstdenkende Maschine, erscheint für viele Wissenschaftler noch in weiter Ferne.[3]

Im Wesentlichen werden derzeit Prozesse angewandt, in denen „deep Learning"-Verfahren vorgegebene Routinen durchlaufen und dadurch die Wahrscheinlichkeit bzw. Treffgenauigkeit verbessern. So lernt die Anwendung durch vorgelegte Fotos anhand bestimmter Merkmale zwischen einer Katze und einem Hund zu unterscheiden und steigert mit Zunahme an Daten die korrekte Zuordnung, würde aber vermutlich ein Bild eines geschminkten Kindes ebenso einer dieser Kategorien zuweisen. Das System kann sogar durch bewusst verfälschtes Material manipuliert werden.[4] Diese Begrenzung und Fehleranfälligkeit lassen auch nach jahrelanger Forschung mit stets gestiegener Rechenleistung Zweifel am Erfolg dieser Technologie aufkommen.

Trotzdem wird behauptet, die KI könne Krankheiten und Suizidgedanken anhand von Bildern diagnostizieren, ebenso die sexuelle Ausrichtung[5] oder aber die Straffälligkeit der Person vorhersagen.

II. Risikoszenarien

Noch sind die Folgen der Einführung von KI-basierten Systemen nur grob vorhersehbar. Erste Erkenntnisse sollten aber als Risikoszenario einer Betrachtung unterzogen werden:[6]

Videokameras mit KI-basierter Gesichtserkennung, die u. a. Verhaltens- und Bewegungsmuster auswerten, ermöglichen eine effiziente Personenidentifikation. Werden dabei biometrische Daten verarbeitet, entstehen einzigartige Hashwerte. Selbst bei optischen oder dem Altersprozess unterliegenden Veränderungen kann der Mensch anhand des Hashwertes mit sehr hoher Wahrscheinlichkeit wiedererkannt werden. Im Internet findet durch Verhaltensanalyse und stets optimierten Tracking-Methoden (z. B. fingerprinting) vergleichbar eine Personenidentifikation statt. Mit wenigen Mausbewegungen und Klicks kann eine Person mittlerweile geräteübergreifend identifiziert werden.

Die KI lernt anhand des Verhaltens des Nutzers, personalisierte Inhalte anbieten zu können. Dem Benutzer sollen nach dessen Vorlieben Nachrichten, passende Dienstleistungen oder Produkte angezeigt werden. Soziale Netzwerke wählen bereits Inhalte (Nachrichten und Werbung) nach Algorithmen individuell für den Nutzer aus und beeinflussen den Wissenszugang. Können KI-Systeme Krankheiten oder eine Lüge diagnostizieren, stellt sich die Frage, inwiefern diese Erkenntnisse auch auf das Verhalten eines Menschen rückwirken. Droht das normgerechte Verhalten des Individuums?

Auch Unternehmen machen sich die Technologie zu Nutze: Anhand von Verhaltensanalysen werden dem Kunden neben passgenauen Inhalten auch persönliche Preise angeboten. Somit besteht das Risiko der Preismanipulation, welches zur Einschränkung des freien Marktes führt.[7]

Deep Learning Prozesse erfordern Informationen und Daten. Diese werden als Input vorab geliefert, zum Teil auch automatisiert aus der Masse der Gesellschaft herausgezogen, wobei demografische Informationen berücksichtigt werden. So lernen die KI-Systeme anhand regionaler Besonderheiten (z. B. der Herkunft) und unterliegen Vorverurteilungen und Diskriminierungen. Bei der Polizeiarbeit mittels predictive policing droht eine Diskriminierung bestimmter Personengruppen.[8] Durch die Automatisierung

---

* Mehr über den Autor erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 19. 11. 2018.

1 *Herberger*, NJW 2018, 2825; *Pieper*, DSRITB 2017, 555.

2 Diese Differenzierung fehlt aber im KI-Strategiepapier der Bundesregierung, https://www.bmbf.de/files/180718 %20EckpunkteKI-Strategie%20final%20Layout.pdf.

3 https://www.spektrum.de/lexikon/neurowissenschaft/kuenstliche-intelligenz/6810; *Schael*, DuD 2017, 547, 548.

4 https://www.zdf.de/nachrichten/heute/selbstfahrendes-uber-auto-ueber-faehrt-passantin-100.html; https://www.zeit.de/digital/internet/2016-03/microsoft-tay-chatbot-twitter-rassistisch.

5 https://www.heise.de/newsticker/meldung/KI-erkennt-am-Gesicht-ob-Menschen-schwul-oder-lesbisch-sind-3825449.html.

6 *Conrad*, DuD 2017, 740, 742.

7 *Schmidt*, DSRITB 2018, 1007, 1008; *Ebers*, MMR 2018, 423, 435.

8 *Kipker*, ZD-Aktuell 2017, 04259; Vgl. https://www.heise.de/news-ticker/meldung/Diskriminierende-KI-Wissenschaftler-finden-Chatbots-Alexa-und-Co-nicht-divers-genug-3810024.html.

von Fahrzeugen bzw. der Infrastruktur wird sich die Gesellschaft verändern,[9] die ausgehend vom Kontrollverlust an Eigenständigkeit und Denkvermögen des Einzelnen verlieren dürfte. Das autonome Fahrzeug ist hierbei nur ein Teilaspekt. Der Arbeitsmarkt wird sich durch die Automatisierung von Kundensupport oder Dienstleistungen verändern.[10] Und selbst autonome Waffen und Drohnen, die emotionslos handeln und Kriege mangels Beteiligung menschlicher Soldaten verharmlosen, sind keine Fiktion mehr.[11]

III. Anforderungen nach dem derzeitigen Datenschutzrecht

Die aufgeworfenen Szenarien spiegeln noch nicht die Realität wider. Angesichts der systemimmanenten wie auch von der Politik geförderten Entwicklung[12] der KI könnte sich dieses zeitnah ändern. Deshalb gilt es bereits heute die denkbaren Folgen im Rahmen der Risikoeinschätzung bei der rechtlichen Bewertung zu berücksichtigen.

1. Rechtmäßigkeit der Datenverarbeitung

Die KI verarbeitet mithilfe von Hard- und Software personenbezogene Daten nach Art. 4 Nr. 1 DSGVO, wie z. B. das Alter, das Geschlecht oder aber den Standort des Nutzers. Darüber hinaus können auch besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) vorliegen, wenn Gesundheitsdaten oder biometrische Daten im Sinne von Art. 4 Nr. 14 DSGVO durch die Gesichtserkennung oder Verhaltensauswertung verarbeitet werden.[13] Vor allem die Verhaltensbiometrie, also die Erstellung nahezu einzigartiger Muster einer Person zu dessen Identifikation anhand von individuellen Körperbewegungen, Reaktionen oder Tastaturschlägen dürfte in Zukunft weiter zunehmen.[14] Nahezu jeder technische Vorgang stellt eine Verarbeitung nach Art. 4 Nr. 2 DSGVO dar.[15] Dabei darf die zeitliche Komponente des einzelnen Vorgangs keine Rolle spielen, weswegen auch das Caching bzw. kurzzeitige Speichern von Informationen in KI-Anwendungen oder Betriebssystemen bereits in den Anwendungsbereich der DSGVO fällt.[16]

Die Rechtmäßigkeit der Datenverarbeitung setzt eine gültige Rechtsgrundlage der Verarbeitung voraus (Art. 6 DSGVO), die sich aus einer Rechtsvorschrift oder aber der Einwilligung des Betroffenen (Art 6. Abs. 1 S. 1 lit. a, Art. 7 DSGVO) ergeben kann.

Dieses wird durch Grundsätze flankiert.[17] Zuerst ist der Zweck der Datenverarbeitung als solcher eindeutig festzulegen (Art 5 Abs. 1 lit. b DSGVO). Die Zweckbindung gilt auch selbst im Privatrechtsverkehr,[18] der üblicherweise von der Privatautonomie ausgeht, und soll auch den unkontrollierten Einsatz von Big Data Systemen möglichst eingrenzen.[19] Die Definition eines eindeutigen Zwecks verhält sich konträr zum freien Anwendungsfeld der KI, die sich weiterentwickeln und möglicherweise in der Zukunft eigene Entscheidungen treffen oder Handlungen vornehmen soll. Je enger der Zweck definiert wird, desto eingeschränkter wäre das Potenzial der Technologie. Weitere Grenzen bilden die Grundsätze der Datensparsamkeit und Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO, die auf eine Begrenzung der Datenverarbeitung auf das notwendige Maß[20] abzielen und in einem Spannungsverhältnis zur fortlaufenden KI stehen.

a) Rechtsvorschrift

Die zentralen Rechtsgrundlagen finden sich in Art. 6 Abs. 1 DSGVO wieder. Eine wesentliche Rolle spielt Art. 6 Abs. 1 S. 1 lit. b DSGVO, wonach die Datenverarbeitung rechtmäßig ist, wenn diese zur „Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich" ist.[21] Hierfür sollte ein Vertragsverhältnis aus einem mindestens zweiseitigem Rechtsgeschäft bestehen.[22] Es wird jedoch darüber hinaus ein unmittelbarer Zusammenhang mit dem konkreten Zweck des Vertragsverhältnisses gefordert.[23] Im Hinblick auf KI-Anwendungen bestehen Zweifel bei der Annahme eines Vertrages. Oft ist die Verarbeitung derartig sensibler Daten über den Nutzer kein erforderlicher Bestandteil eines etwaigen allgemeinen Nutzungsvertrages des Dienstes. Die sprachgesteuerte Bestellung mittels digitaler Assistenten (z. B. Alexa) oder Chatbots setzt keine Sprach- und Verhaltensanalyse voraus, auch wenn derartiges ein Bestandteil des Systems sein mag. Auch für die Nutzung eines sozialen Netzwerks, eines Smartphones oder aber einer Überwachungskamera ist die Verarbeitung personenbezogener Daten bis hin zur Stimme oder Gesundheit nicht erforderlich. Anders wäre es lediglich bei Authentifizierungssystemen (z. B. beim Online-Banking) oder Firewalls.[24]

Im Bereich der Daseinsfürsorge lässt sich die Datenverarbeitung auf Art. 6 Abs. 1 S. 1 lit. d bzw. Art. 9 Abs. 2 lit. c, lit. h DSGVO stützen, wenn sie für die Zwecke der Gesundheitsvorsorge bzw. Behandlung oder zum Schutze lebenswichtiger Interessen erforderlich ist. Dieses wäre bei KI-Anwendungen in Krankenhäusern oder beim Arzt anzunehmen, die Krankheiten diagnostizieren, Patienten überwachen oder Behandlungen vornehmen.

Auch könnte die Verarbeitung durch die KI bei typischen Anwendungsfeldern in der Privatwirtschaft für zulässig erachtet werden, wenn sie nach Art. 6 Abs. 1 S. 1 lit. f DSGVO „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" ist, worunter ausweislich des ErwG. 47 auch die Kundenbindung oder „Direktwerbung" zu fassen wäre.[25] Personalisierte Angebote ausgehend vom Verhalten (z. B. Husten,[26] Bewegungsabläufe, Interessen) des Betroffenen wären denkbar, wenn dieses klar erkennbar und mit der werbenden Ansprache zu rechnen ist. Dies kann sich aus einer Kundenbeziehung ergeben. Dabei gilt es aber die Interessen der

9 *Borges*, NJW 2018, 977.
10 Mehr dazu: *Specht/Herold*, MMR 2018, 40, 41; Zu den Anforderungen im Gesellschaftsrecht: *Möslein*, ZIP 2018, 204, 212.
11 https://www.heise.de/tr/artikel/Militaerroboter-Schwierige-Entscheidungen-4141591.html.
12 https://www.heise.de/newsticker/meldung/Bundesregierung-will-KI-und-autonome-Systeme-in-die-Flaeche-bringen-4155863.html.
13 Vgl. *Jandt*, ZRP 2018, 16, 17; *Schwenke*, NJW 2018, 823, 825.
14 https://www.datenschutz-notizen.de/verhaltensanalyse-beim-online-banking-mit-dem-datenschutz-vereinbar-2018287.
15 *Sydow*, DSGVO, 2. Aufl. 2018, Art. 4 Rn. 47; Dies folgt aus der „Technologieneutralität" aus ErwG. 15.
16 Vgl. *Quiel*, PinG 1.18, 31, 34; *Schwenke*, NJW 2018, 823, 824.
17 *Piltz*, K&R 2016, 557, 558, *Rossnagel*, ZD 2018, 339, 340.
18 Vgl. *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 25.
19 *Culik/Döpke*, ZD 2017, 230.
20 *Frenzel*, in: Paal/Pauly (Fn. 18), Art. 5 Rn. 37.
21 *Schulz*, in: Gola, DSGVO, 2. Aufl. 2018, Art. 6 Rn. 27.
22 *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 6 Rn. 13.
23 *Schulz*, in: Gola, (Fn. 21), Art. 6 Rn. 38.
24 Hemker, DuD 2018, 629, 630.
25 *Schulz*, in: Gola, (Fn. 21), Art. 6 Rn. 77.
26 Vgl. https://www.heise.de/newsticker/meldung/Alexa-hoert-dich-husten-Amazon-erhaelt-Patent-auf-Werbeangebote-fuer-Kranke-4190512.html.

Beteiligten miteinander abzuwägen,[27] weshalb eine unbegrenzte Verhaltensanalyse bis hin zur Auswertung von Aktivitäten, Emotionen und Gesundheitsdaten zu hinterfragen ist. Ohnehin dürften die Grundrechte des Betroffenen aus Art. 7 und 8 GRCh und das Interesse am Schutze seiner sensiblen Daten gegenüber dem Interesse des agierenden Unternehmens überwiegen.[28] Sind von der Datenverarbeitung Kinder unter 16 Jahren betroffen, soll das berechtigte Interesse des Kindes grundsätzlich überwiegen (Art. 6 Abs. 1 S. 1 lit. f DSGVO).[29]

b) Einwilligung

Als Ausweg bleibt bei KI-Systemen zumeist nur die Annahme der Einwilligung des Betroffenen als Rechtsgrundlage der Datenverarbeitung (Art. 6 Abs. 1 S. 1 lit. a DSGVO).[30]

Zunächst ist der Betroffene insbesondere vor Abgabe der Einwilligung über Art und Ausmaß der Datenverarbeitung „in nachvollziehbarer Weise" zu informieren, aber auch über den Verantwortlichen und den Zweck der Datenverarbeitung aufzuklären (Art. 5 DSGVO).[31] Im Sinne des von der DSGVO getragenen Transparenzgedankens hat der Verantwortliche diese Mitteilungen sogar leicht zugänglich und in verständlicher und klarer und einfacher Sprache darzustellen.[32]

Fraglich ist die Ausgestaltung der Einwilligung. Die DSGVO schafft mit dem ErwG. 32 Klarheit, wonach die Einwilligung „durch eine eindeutige bestätigende Handlung" erfolgen muss. Bei der elektronischen Datenverarbeitung ist die ausdrückliche Einwilligung gefordert, was ein aktives und freiwilliges Handeln des Betroffenen voraussetzt.[33] Eine stillschweigende oder konkludente Einwilligung durch bloßen Gebrauch einer Anwendung oder Kauf eines KI-Gerätes würde indes nicht ausreichen.[34] Werden personenbezogene Daten besonderer Kategorien nach Art. 9 DSGVO verarbeitet, wie es bei KI-Systemen üblich sein dürfte, wird vom Betroffenen die Erteilung seiner ausdrücklichen Einwilligung in den zuvor festgelegten Zweck gefordert (Art. 9 Abs. 2 lit. a DSGVO).[35] Es ist wegen der Sensitivität dieser Daten eine ausdrückliche Erklärung durch den Betroffenen zu verlangen, die durch eine Einholung einer schriftlichen Einwilligung oder protokollierte Textform umzusetzen ist.[36]

Dabei wird die Freiwilligkeit der Abgabe der Einwilligung vorausgesetzt, an der aber häufig Zweifel bestehen.[37] So wird in ErwG. 42, S. 5 der DSGVO erläutert, dass eine Freiwilligkeit nur dann anzunehmen ist, „wenn sie [die Person] eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden." Sind die erwähnten Verfahren jedoch elementarer Bestandteil einer Gesellschaft, wie es beispielsweise längst durch eine marktbeherrschende Stellung von Google, Amazon oder Facebook anzunehmen sein dürfte, besteht der sog. Lock-in-Effekt.[38] Eine echte Wahlfreiheit des Nutzers ist folglich mangels alternativer Systeme anzuzweifeln.[39] Diese Abhängigkeit droht somit nicht nur im Beschäftigungsverhältnis[40] bzw. bei der Bewerberauswahl durch KI-basierte Bewerbertools,[41] sondern ist allgegenwärtig in der heutigen Informationsgesellschaft, weswegen vor diesem Hintergrund erhöhte Anforderungen an die tatsächliche Entscheidungsfreiheit des Einzelnen in die Datenverarbeitung zu stellen sind.[42] Immerhin werden KI-Anwendungen immer mehr in Betriebssystemen als zwingende Funktion verankert und finden Einzug in automatisierte Systeme (von „connected car" bis hin zu Berechnungsformeln in der Versicherungsbranche[43] bzw. im Social Scoring). Daher werden in jüngster Zeit Forderungen nach kartellrechtlichen Konsequenzen laut.[44] Ferner hat der Verantwortliche jederzeit den Nachweis der Einwilligung zu erbringen (Art. 7 Abs. 1 DSGVO). Zudem muss die Einwilligung in der KI-Anwendung auch jederzeit einsehbar und widerrufbar sein (Art. 7 Abs. 3 DSGVO). Bei Kindern unter 16 Jahren ist die Einwilligung nur wirksam, wenn sie durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird (Art. 8 Abs. 1 S. 2 DSGVO). Dieses würde in letzter Konsequenz zu einer vorgelagerten Altersabfrage im KI-Produkt oder Betriebssystem führen.[45]

Eine Besonderheit bildet die automatisierte Entscheidung im Einzelfall (Profiling), bei der nur mit ausdrücklicher Einwilligung des Betroffenen nach Art. 22 Abs. 2 DSGVO die auf eine automatisierte Verarbeitung beruhende „Entscheidung" auf biometrische Daten gestützt werden darf (Art. 22 Abs. 4 DSGVO).[46] Aber entspricht es gerade nicht dem Geschäftsmodell der KI-Anwendungen, solche Daten bei der Dienstleistung zu verarbeiten? Zu denken ist an den sprach- und verhaltensgesteuerten Einkauf über einen digitalen Assistenten oder dessen Filterung/Vorauswahl, was hiernach zumeist unzulässig wäre.

2. Verantwortlichkeiten

Die DSGVO zeichnet sich dadurch aus, dass die Verantwortlichkeit und somit der Adressat der Anforderungen eindeutig und konsequent zu bestimmen ist. Bereits diese Aufgabe offenbart die Umsetzungsschwierigkeiten bei der KI, wenn im Hinblick auf die Datenverarbeitung zwischen den einzelnen Akteuren (Entwickler, Betreiber, Nutzer und die KI als eigene Rechtsfigur) differenziert werden muss. Erschwert wird diese Rollenverteilung durch Konstellationen, in denen eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit im Raum steht.

In die Pflicht genommen wird der „Verantwortliche" im Sinne von Art. 4 Nr. 7 DSGVO, also wer „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Anknüpfungspunkt sind einerseits die Idee bzw. Zielvorgabensetzung der Verarbeitung, andererseits aber auch die

27 *Gierschmann*, MMR 2018, 7, 10.
28 Vgl. *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 6 Rn. 171.
29 Vgl. Erwägungsgrund 38.
30 *Heckmann/Paschke*, in: Ehrmann/Selmayr (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 7 Rn. 1.
31 ErwG. 58 der DSGVO.
32 ErwG. 39 der DSGVO.
33 ErwG. 32 der DSGVO; *Heberlein*; in: Ehmann/Selmayr (Fn. 30), Art. 6 Rn. 11.
34 *Albrecht*, CR 2016, S. 91.
35 Kritisch hierzu: *Jandt*, ZRP 2018, 16, 18.
36 *Weichert*, in: Kühling/Buchner (Fn. 28), Art. 9 Rn. 47.
37 *Frenzel*, in: Paal/Pauly (Fn. 18), Art. 7 Rn. 18; *Veil*, NVwZ 2018, 686, 688; *Tinnefeld/Conrad*, ZD 2018, 391, 392.
38 Zum Wettbewerbsrecht beim Datenschutz*: Paal/Hermann*, NJW 2017, 1697, 1698.
39 Vgl. *Ernst*, ZD 2017, 110, 113; *Schneider*, ZD 2017, 303, 305.
40 *Pauly*, in: Paal/Pauly (Fn. 18), Art. 88 Rn. 9; *Tinnefeld/Conrad*, ZD 2018, 391, 392.
41 *Wojak*, DuD 2018, 553, 554.
42 *Weichert*, in: Kühling/Buchner (Fn. 28), Art. 9 Rn. 51.
43 http://www.manager-magazin.de/finanzen/versicherungen/kuenstliche-intelligenz-versicherungen-ruesten-gegen-betrug-auf-a-1217651.html.
44 https://www.heise.de/newsticker/meldung/Effektiveres-Wettbewerbsrecht-soll-Marktmissbrauch-von-Internetriesen-verhindern-4154823.html.
45 *Schulz*, in: Gola (Fn. 21), Art. 8 Rn. 21.
46 *Hladjk*, in: Ehmann/Selmayr (Fn. 30), Art. 22 Rn. 16.

Einflussnahme hierauf. Die Annahme der Verantwortlichkeit wirkt sich maßgeblich auf die Haftung und Umsetzung zahlreicher Pflichten aus der DSGVO aus und sollte durch entsprechende vertragliche Regelungen festgelegt sein. Häufig drängt sich eine Auftragsverarbeitung mit einem solchen Vertrag nach Art. 28 DSGVO auf, sofern beide Unternehmen ihren Sitz in Europa haben. Bei diversen Anbietern wie Amazon oder Google dürfte die Datenverarbeitung außerhalb des Anwendungsbereichs der DSGVO liegen. Vor diesem Hintergrund ist zu prüfen, ob diese in einen unsicheren Drittstaat erfolgt und deshalb BCRs oder Verträge nach den EU-Standardvertragsklauseln heranzuziehen wären.

In nicht seltenen Fällen liegt eine gemeinsame Verantwortlichkeit im Sinne von Art. 26 DSGVO vor, wie es jüngst auch in der Entscheidung[47] des EuGH zu den Facebook Fanpages von den Richtern angenommen wurde, die das soziale Netzwerk wie auch die darin aktiven Unternehmen vor neue Herausforderungen stellt. In der Zukunft dürften sich weitere Konstellationen entwickeln lassen, wann mehrere Verantwortliche zusammenwirken,[48] da die KI-Anwendung nur ein Produkt im Massenmarkt ist oder sogar lokal auf der Anwendung des Nutzers eigenständig agiert. Zumeist dürften den Kunden dieser Software aber das Verständnis und insbesondere die technischen Möglichkeiten fehlen, die konkreten Mittel und Zwecke der eingesetzten Algorithmen zu bestimmen oder diese zu begrenzen. Der Kunde der Software erhält keinen Zugriff auf Datenbanken oder Quellcode der KI-Anwendung und könnte daher den ihn treffenden Pflichten gar nicht nachkommen.

3. Informationspflichten

Einen Kern der DSGVO bilden die Informationspflichten aus Art. 12 ff. DSGVO. Getragen von dem Transparenzgedanken hat der Verantwortliche den Betroffenen alle Informationen zur Datenverarbeitung „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln" (Art. 12 Abs. 1 DSGVO). Mehrere Verantwortliche sollten die Aufgabenverteilung untereinander vertraglich festlegen.[49] In der Praxis werden die Informationen häufig unzureichend in elektronischer Textform den Betroffenen in einer Datenschutzerklärung dargestellt. Dies müsste aber in der KI-Anwendung erfolgen; gleichwohl sollte ein Medienbruch vermieden werden.[50]

Bei der Direkterhebung der Daten muss der Betroffene gem. Art. 13 Abs. 1 und 2 DSGVO unter anderem über den Verantwortlichen, die Zwecke der Datenverarbeitung sowie die Rechtsgrundlage wie auch die Speicherdauer bzw. Löschroutinen umfassend informiert werden. Erhält der Verantwortliche die Daten vom Dritten, müsste er nach Art. 14 DSGVO den Betroffenen zusätzlich auch darüber informieren „aus welcher Quelle die personenbezogenen Daten" stammen. Zu denken ist an die KI, die sich aus dem Internet oder fremden Apps/Anbietern eigenständig bedient oder vielschichtige Informationen bei sich zusammenführt und deshalb diese Informationspflichten ständig neu (bei jedem Import) auslösen würde. Im Übrigen ist auch bei einer Zweckänderung, wenn die KI-Anwendung durch ihren Fortschritt neue Ziele definiert oder ursprünglich nicht bedachte Zwecke erreicht (z. B. Gesundheitsdiagnostik) eine erneute Information aus Art. 13 DSGVO geboten.[51]

Beim Profiling gem. Art. 22 DSGVO hat 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 DSGVO) zu erhalten. Unklar ist, ob damit auch die Logik des Systems und der KI-Algorithmus erfasst werden,[52] oder dies dem Geschäftsgeheimnis unterliegt, wie es wohl bei systemimmanenten Assistenten in einem Betriebssystem (wie bixby, Siri, Cortana) anzunehmen wäre. Dennoch müsste dargestellt werden, auf Grundlage welcher Daten(-quelle) und Entschlüsse der KI ein personalisiertes Angebot oder eine Handlung vorgenommen wird.

4. Betroffenenrechte

Mithin sind die Betroffenenrechte der DSGVO zu wahren, d. h. der Betroffene muss jederzeit die Kontrolle über die Verarbeitung seiner Daten effektiv ausüben können.[53] Dies setzt natürlich Kenntnis über die tatsächliche Datenverarbeitung voraus, die bei „Big Data"-Auswertungen und KI-Systemen häufig nicht besteht.[54] Hinzu kommt der Umstand, dass immer mehr Dienstleistungen automatisiert werden und Bots und KI-Systeme menschliche Vorgänge vornehmen, ohne dass dieses erkennbar ist. Der Betroffene erkennt gar nicht den Verantwortlichen in der Datenverarbeitungskette der KI-Systeme.

Zudem herrscht Uneinigkeit über den konkreten Umfang des Auskunftsrechts. So ist dem Betroffenen eine „Kopie" (Art. 15 Abs. 3 DSGVO) der personenbezogenen Daten (z. B. als Download) zur Verfügung zu stellen, die Gegenstand der Verarbeitung sind. Meta-Daten sollen dabei nicht von Art. 15 DSGVO erfasst sein. Individuelle Berechnungsgrundlagen der KI dürften nicht in den Regelungsgehalt dieser Norm fallen, auch wenn sich daraus ein Personenbezug herstellen lässt. Die begehrte Löschung von Daten dürfte ausgeschlossen und damit das Betroffenenrecht eingeschränkt sein, wenn diese elementarer Bestandteil der KI sind. Und unter Annahme der Verantwortlichkeit für die Datenverarbeitung, müsste die KI selber über die Umsetzung der Betroffenenanfrage entscheiden und diese dokumentieren – ohne menschliche Kontrollinstanz.

5. Technisch-organisatorische Maßnahmen

Nach der DSGVO gilt es eine angemessene Sicherheit der Datenverarbeitung zu gewährleisten. Dies setzt bei der Integrität und Vertraulichkeit der Datenverarbeitung (Art. 5 Abs. 1 lit. f DSGVO) an und wird durch die technisch-organisatorischen Maßnahmen gem. Art. 32 DSGVO ausgeformt, die der Verantwortliche zum Schutz der Datenverarbeitung zu ergreifen hat.[55] Es ist daher ein IT-Konzept des KI-Systems zu entwickeln, das der Verantwortliche und ggfs. der Auftragsverarbeiter (zusammen) stets zu kontrollieren und anzupassen haben. Nur die regelmäßige Evaluation der Maßnahmen würden zu einer nachhaltigen Datensicherheit führen.[56]

47 EuGH, 5. 6. 2018 – C-210/16; *Härting/Gössling*, NJW 2018, 2523, 2524.
48 *Wojak*, DuD 2018, 553, 554.
49 *Bäcker*, in: Kühling/Buchner (Fn. 28), Art. 13 Rn. 18.
50 Artikel-29-Datenschutzgruppe, WP 260, Guidelines on transparency under the Regulation 2016/679.
51 *Bäcker*, in: Kühling/Buchner (Fn. 28), Art. 13 Rn. 78.
52 Vgl. BGH, 28. 1. 2014 – VI ZR 156/13, K&R 2014, 269.
53 *Piltz*, K&R 2016, 558, 559.
54 *Rossnagel*, ZD 2018, 339, 344.
55 *Wennemann*, DuD 2018, 174, 175.
56 *Martini*, in: Paal/Pauly (Fn. 18), Art. 32 Rn. 43.

Die getroffenen Maßnahmen unterliegen einer ständigen Anpassung an den Stand der Technik und einer agilen Risikoabschätzung. Dies wird noch verstärkt durch die ausdrückliche Forderung nach einem Verfahren der regelmäßigen Überprüfung der zu dokumentierenden Maßnahmen wie auch der Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO). Es gilt „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 DSGVO) zu etablieren, das in der KI verankert oder durch Updates vom Hersteller eingespielt werden müsste.

Als konkrete Maßnahmen werden die Verschlüsselung der Datenverarbeitung bzw. Pseudonymisierung[57] in Art. 32 DSGVO genannt, weitere spezifische technische Kriterien sind abhängig vom konkreten Prozess. Neben der typischen Absicherung von Systemen durch Rollenkonzepte, Passwort-Parameter, Firewalls, regelmäßigen Updates und redundanten Netzwerken sollte ein Augenmerk auf die Spezifika der KI-Anwendungen gelegt werden: Werden diese in naher Zukunft auf Betriebssystemen, Smartphones oder „IoT"-Geräten installiert und mit einem riesigen weltweit agierenden Netzwerk verknüpft, ist bereits die Steuerungsmöglichkeit des Nutzer fraglich. Der Betroffene verwendet die Anwendung tagtäglich, ohne sich der Analyse durch das System bewusst zu sein bzw. sich dieser entziehen zu können, muss sich aber gleichzeitig um Updates und Kontrollen bemühen. Involvierte Unternehmen oder Entwickler haben allenfalls mittelbar, nur auf Teilbereiche der KI ihrerseits Zugriff oder können lediglich auf bereits erfolgte Schritte reagieren, nicht jedoch die möglicherweise sich fortschreitende Formel des Programms nachvollziehen oder abändern. Auch sind Zugriffe durch Dritte auf entsprechende Apps zu den KI-Verfahren oder deren Datenübertragung an das dahinterstehende Rechennetzwerk zu verhindern. Sofern sogar besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet werden, sind noch stärkere Vorkehrungen geboten.

Es sind effiziente Löschroutinen zu installieren, die dem „Recht auf Vergessenwerden" (Art. 17 DSGVO) angemessen Rechnung tragen, um eine andauernde Verarbeitung zu verhindern. Konflikte bestehen, wenn die anzunehmende Rechtsgrundlage eine zweckmäßige, andauernde Verarbeitung der personenbezogenen Daten des Betroffenen begründet. Demnach wäre eine Verarbeitung für die Dauer der aktiven Nutzung eines Accounts bzw. einer Software denkbar, die angesichts der Monopolstellung von Apple, Samsung, Microsoft und Co. langwierig sein kann. Das Amazon-, Gmail- oder Apple-Konto ist mittlerweile auf Lebzeiten angelegt und ersetzt sogar bei vielen Dienstleistern eigene Benutzerkonten. Ist die ständige Verarbeitung der Kundendaten gerade Sinn und Zweck des Lernprozesses der KI, gilt es die Betroffenenrechte durch neue Kontrollmechanismen zu stärken.

6. Privacy by Design und Privacy by Default

Hervorzuheben sind die Steuerungsmittel der DSGVO, die sich in Privacy by Design und Privacy by Default (Art. 25 DSGVO) wiederfinden. Hieraus lassen sich präventive und repressive Vorgaben zum Datenschutz ableiten.[58] So hat der Verantwortliche danach eine gewisse Datenschutzkonformität durch die Gestaltung der Technik und datenschutzfreundlichen Voreinstellungen zu erreichen. Das KI-System muss in seiner Grundeinstellung möglichst datensparsam und transparent arbeiten und sollte dem Nutzer jederzeit die Kontrolle über seine Daten ermöglichen.[59] In vielen Branchen wurden bereits Datenschutz-Frameworks entwickelt,[60] für die KI-Branche existieren noch keine Richtlinien. Die Daten sollten pseudonymisiert und nur zeitlich begrenzt verarbeitet werden.

Diese Forderungen verhalten sich jedoch konträr zur Datenverarbeitung beim Machine Learning (KI), das durch Begrenzungen und Kontrollmechanismen in der Funktionsweise gefährdet wäre. Die Deaktivierung bestimmter Sensoren (Stimm-, Gesichtserkennung oder GPS-Tracking) könnte sogar zum Systemausfall der KI führen.

Außerdem ist Art. 25 DSGVO zu unkonkret und erlaubt eine eigene Interpretation bzw. Festlegung des Grads der Umsetzung durch den Verantwortlichen. Zudem ist der angesprochene Adressatenkreis der Regelung lückenhaft, denn diese richtet sich ausweislich des Wortlauts nur an den Verantwortlichen für die Datenverarbeitung.[61] In der Realität sind es die Hersteller, Entwickler der KI-Systeme oder zukünftig die KI selbst als lokal ausgeführtes System, die die Form der Datenverarbeitung sowie dessen denkbare Ausmaße bestimmen (kontrollieren), jedoch häufig hierfür nicht verantwortlich sind.[62] Eine mittelbare Wirkung von Art. 25 DSGVO auf die Entwickler bzw. Hersteller der Systeme wird aber diskutiert.[63] Die unglückliche Gestaltung der Norm wird durch den ErwG. 78 der DSGVO noch abgerundet, wonach die Hersteller zum Datenschutz lediglich „ermutigt" werden sollen.

7. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) zwingt den Verantwortlichen zu einer vorab vorzunehmenden „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten." Damit soll eine risikobasierte „Technikfolgenabschätzung" erreicht werden, um die Auswirkung der Verwendung neuer Technologie auf die Gesellschaft und die Umwelt näher zu beleuchten.[64] Die Achtung des Privatlebens und der Schutz der personenbezogenen Daten sollen bei der Einführung neuer Systeme berücksichtigt werden.

Wann eine Datenschutz-Folgenabschätzung angezeigt ist, lässt sich der DSGVO dagegen nicht entnehmen. Die Aufsichtsbehörden hierzulande haben jedoch bereits sog. „Blacklist" veröffentlicht,[65] die einige Anwendungsfelder (z. B. das GPS-Tracking von Mitarbeitern, das Scoring oder Big-Data-Analysen von Kunden) benennen.[66] In Anbetracht dieser Empfehlungen dürfte ein KI-basiertes Verfahren, das mithilfe eines Smartphones oder IoT-Geräts direkt mit dem Nutzer agiert und diesen auf Schritt und Tritt analysiert, auch in den Anwendungsbereich dieser Norm

57 Mehr hierzu: *Rossnagel*, ZD 2018, 246.
58 *Jandt*, DuD 2017, 562.
59 Vgl. *Brockmeyer*, ZD 2018, 258, 261; *Mantz*, in: Sydow (Fn. 15), Art. 25 Rn. 54.
60 *Mantz*, in: Sydow (Fn. 15), Art. 25 Rn. 61; Art. 29-Datenschutzgruppe, WP 163.
61 Vgl. *Baumgartner*, in: Ehmann/Selmayr (Fn. 30), Art. 25 Rn. 5.
62 *Hartung*, in: Kühling/Buchner (Fn. 28), Art. 25 Rn. 13.
63 *Rose*, DSRITB 2016, 75, 86; Zur „indirekten Wirkung", *Baumgartner*, in: Ehmann/Selmayr (Fn. 30), Art. 25 Rn. 5.
64 *Martini*, in: Paal/Pauly (Fn. 18), Art. 25 Rn. 2.
65 Zur Übersicht: https://www.datenschutz-notizen.de/deutsche-aufsichtsbehoerden-legen-blacklist-vor-0920586.
66 DSFA – Liste Deutschland – nicht-öffentlicher Bereich, Version 1, DSK, https://datenschutz-hamburg.de/assets/pdf/DSFA_Muss-Liste_f%C3%BCr_den_nicht-oeffentlichen_Bereich-Version_1.0-Stand_10.7.2018_(002).pdf.

fallen. Viele Funktionen wären daher nur unter strengen Vorgaben zulässig und müssten offengelegt werden.

IV. Datenschutzrechtliche Sanktionen

Bei Verstößen gegen die DSGVO drohen dem Verantwortlichen Bußgelder (Art. 83 DSGVO), Schadensersatzansprüche (Art. 82 DSGVO[67]) und weitere Maßnahmen der Aufsichtsbehörde. Die Bußgelder können sogar bis zu vier Prozent des weltweit erzielten Jahresumsatzes einnehmen, womit die „Global Player" mit Umsätzen von vielen Milliarden Euro nun neben dem Wettbewerbsrecht auch das Datenschutzrecht beachten sollten. Schließlich soll die Verhängung von Geldbußen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein (Art. 83 Abs. 1 DSGVO).

Zurzeit scheinen die Aufsichtsbehörden (noch) davon abzusehen, Bußgelder nach Art. 83 DSGVO zu verhängen. Grund hierfür könnte sein, dass die relevanten Vorschriften der DSGVO zu unbestimmt sind und Anordnungen womöglich einer Überprüfung durch ein deutsches VG nicht standhalten würden.[68] Dieses dürfte umso mehr für undurchsichtige oder weltweit verknüpfte KI-Systeme gelten, wenn bereits die Zuständigkeit der Aufsicht ungeklärt ist.

V. Weitere Haftung

Während sich aufsichtsbehördliche Maßnahmen nach der DSGVO grds. an den Verantwortlichen richten, können durch zivilrechtliche Ansprüche auch weitere Akteure, also Entwickler und Hersteller der Systeme angesprochen werden. So kommt die Haftung nach § 823 BGB und § 43 GmbHG bei Verletzung der Sorgfaltspflichten in Betracht.[69] Wegen offenkundiger Kausalitätsprobleme des Nachweises eines (verschuldensabhängigen) Handelns zur Geltendmachung des Anspruchs könnte auf eine Gefährdungshaftung (gem. § 7 Abs. 1 StVG[70] oder der Tierhalterhaftung nach § 833 BGB analog[71]) ausgewichen werden. Auch die Zurechnung des Verhaltens einer KI-Anwendung mittels Subjektivierung (gem. § 166 BGB oder § 687 BGB analog) und im Deliktsrecht[72] wird diskutiert.[73] Die EU plant dem Roboter ein eigenes Rechtssubjekt als elektronische Person zuzusprechen,[74] so dass eine eigene Haftung des lokal auf dem Gerät des Nutzers ausgeführten KI-Systems ohne Steuerung durch Entwickler oder Hersteller denkbar wäre, im Ergebnis jedoch die Haftung ins Leere laufen ließe. Der Roboter lässt sich nicht durch Bußgelder, Schadensersatz oder Maßnahmen „abschrecken". Anders wäre es bei einer (fiktiven) uns Menschen bekannten Emotionen unterliegenden starken KI, die Angst um eigene Datenbestände, Funktionen oder ihr Dasein hätte.

Angesichts dessen erscheinen Anpassungen des bisherigen Sanktionsmodells der DSGVO die logische Konsequenz, um Wertungswidersprüche und fehlende Verantwortlichkeiten beim Einsatz von KI zu verhindern und das Datenschutzrecht effizient umzusetzen.[75]

VI. Fazit

Die DSGVO ist im Hinblick auf die KI zu unbestimmt und weist Regelungslücken auf. Der Adressatenkreis der Pflichten ist um KI-Entwickler und Hersteller zu erweitern, damit die Zurechnungskette der Verantwortlichkeit nicht abreißt. Wenn die KI „eigene" Entscheidungen trifft, das Verhalten des Nutzers beeinflusst und sogar über Leben und Tod eines Menschen urteilen kann, sind interdisziplinäre Haftungsmodelle zu entwickeln. Neue Kontrollmechanismen sind zu fordern, um jederzeit eine Überprüfung von Zweck bzw. Zielvorgabe wie auch Sicherheit des Systems zu gewährleisten. Die Transparenz bei Logik und Tragweite des KI-Systems ist zu erzwingen und darf nicht vom Schutz des Geschäftsgeheimnisses verdrängt werden. Die Informationspflichten wie auch Betroffenenrechte müssen in der KI-Anwendung effizient umgesetzt werden.

Es gilt einen „Framework" zu entwickeln, damit eine eigenständig agierende KI sich nicht Kontrollmechanismen (z. B. des Datenschutzbeauftragten) entziehen und Zwecke und Mittel eigenständig und losgelöst von Grundrechten definieren kann – und dadurch zum Richter über sich selbst wird.

67 Zum Schadensersatzanspruch: *Wybitul/Haß/Albrecht*, NJW 2018, 113, 114.
68 *Rossnagel*, ZD 2018, 339, 344.
69 Vgl. *Keßler*, MMR 2017, 592 f.; *Franck/Müller-Peltzer*, DSRITB 2017, 241, 254.
70 *Franck/Müller-Peltzer*, DSRITB 2017, 241, 255.
71 *Borges*, NJW 2018, 977, 981.
72 *Keßler*, MMR 2017, 589, 593; *Denga*, CR 2018, 69.
73 *Kluge/Müller*, InTeR 2017, 24, 27.
74 Entschließung des Europäischen Parlaments v. 16. 2. 2017.
75 *Conrad*, DuD 2018, 541, 546.

RA Felix Krupar und Laurenz Strassemeyer, Hamburg*

Distributed Ledger Technologien und Datenschutz

Widerspruch oder Evolution?

Distributed Ledger Technologien gelten als eine der revolutionärsten Technologien des 21. Jahrhunderts, sowohl für die Wirtschaft als auch für den Datenschutz selbst. Zeitgleich soll die DSGVO die wichtigste Errungenschaft des letzten Jahrzehnts für Verbraucher sein. Beide Konstruktionen scheinen jedoch auf den ersten Blick nur schwerlich auf einen Nenner zu bringen. Der Beitrag versucht daher ein wenig Licht ins Dunkle hinsichtlich der datenschutzrechtlichen Einordnung der noch jungen Technologie zu bringen und zu untersuchen, ob und wie das

* Der Beitrag basiert auf einem Vortrag, gehalten auf der DSRI-Herbstakademie 2018, erschienen im Tagungsband der Herbstakademie 2018: *Krupar/Strassemeyer*, Datenschutz auf der Blockchain – Die Innovationsfeindlichkeit der DSGVO, in: Taeger (Hrsg.), Rechtsfragen Digitaler Transformationen – Gestaltung digitaler Veränderungsprozesse durch Recht, 2018, S. 343 ff. Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 12. 11. 2018.