DSGVO vs. Künstliche Intelligenz

Chance oder Hindernis für den Einsatz von KI?

Simone Rosenthal, Rechtsanwältin; Partnerin, Schürmann Rosenthal Dreyer

16. Oktober 2018

LR 2018, Seiten 173 bis 178 (insgesamt 6 Seiten)

Künstliche Intelligenz (KI) ist in unserem Alltag angekommen. Sie gilt als die Schlüsseltechnologie der Zukunft, die Aufgaben in Industrie, Gesellschaft und Wissenschaft erleichtern wird. Bereits heute kommen KI-Anwendungen im IT-Bereich, Kundenservice, Vertrieb, Fertigung und Betriebsabläufen zum Einsatz. Immer mehr Unternehmen setzen auf KI und Machine Learning, um Prozesse zu optimieren, Prognosen zu generieren oder für autonome Diagnoseverfahren. Bei allen Vorteilen, die sich durch den Einsatz von KI-Anwendungen ergeben, muss sich dennoch die Frage nach der rechtlichen Handhabung dieser vielversprechenden Technologie stellen. Insbesondere der rasante technische Fortschritt generiert in immer kürzeren Zeiträumen neue rechtliche Fragestellungen, wie z. B. nach der Haftung und dem Datenschutz. Letzteres wird zentraler Gegenstand dieses Beitrags sein, mit speziellem Fokus auf das Verhältnis von KI zur neuen Datenschutz-Grundverordnung (DSGVO), die seit dem 25.05.2018 europaweit gilt. Im Zentrum steht dabei das Problem der Vereinbarkeit automatisierter Entscheidungen mit den Rechten der von der Datenverarbeitung betroffenen Personen. 1

Werden die strengen Anforderungen der DSGVO den Einsatz und die Entwicklung von KI bremsen oder bietet das neue Regelwerk gar Chancen für den Anwender?

I. Der technische Hintergrund

Das Herzstück einer jeden KI-Anwendung ist ein Algorithmus. Einfach gesagt handelt es sich dabei um eine Handlungsvorschrift zur Lösung eines Problems. Auf einen bestimmten eingegebenen Wert folgt die Ausgabe eines Ergebnisses. Diesen immer gleichen Ablauf übernimmt in der digitalen Welt ein Computerprogramm.[1] Im Bereich der KI soll der Algorithmus die Fähigkeit erreichen, menschliches Handeln zu simulieren, wobei künstliche „neuronale Netze“ geschaffen werden, die der Struktur des menschlichen Gehirns entsprechen. Ein besonders relevantes Teilgebiet ist das sogenannte Deep Learning, bei dem es einer Maschine möglich ist, selbstständig, d. h. ohne menschlichen Einfluss, neues 2

[1] Zur Definition von Algorithmen DFK BitKom, künstliche Intelligenz, Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, Berlin, 2017, S. 67.

Wissen und Erkenntnisse aus Erfahrung zu generieren. Hierfür wird das System mit großen Datenmengen (Big Data) gefüttert, anhand derer es Zusammenhänge und Strukturen erkennt und sich für zukünftige Ergebnisse verbessert, indem es selbstständig immer neue Algorithmen schreibt.[2] Hierbei entsteht ein, insbesondere für die rechtliche Auseinandersetzung, folgenreiches Problem: Aufgrund der Selbstständigkeit des Programms ist im Nachhinein der Entstehungsprozess der Datenverarbeitung von außen betrachtet nicht mehr nachvollziehbar.[3] Hier kommt die DSGVO ins Spiel, die in Art. 22 DSGVO den betroffenen Personen grundsätzlich das Recht zuspricht, gerade nicht einer solchen automatisierten Entscheidung unterworfen zu werden. Die mit Art. 22 DSGVO verbundenen Art. 13-15 DSGVO beinhalten bestimmte Informationspflichten für datenverarbeitende Unternehmen sowie das Auskunftsrecht der betroffenen Personen. Hierbei stellt sich die Frage, inwieweit über eine Datenverarbeitung Auskunft erteilt werden kann, die für den Verantwortlichen selbst nicht (mehr) nachvollziehbar ist.

II. Das Verbot automatisierter Entscheidungen

Gemäß Art. 22 Abs. 1 DSGVO dürfen Betroffene „nicht einer ausschließlich auf einer automatisierten Verarbeitung [...] beruhenden Entscheidung unterworfen werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt." Darunter versteht sich ein Verfahren, welches vom Erfassen der Daten bis hin zur Ausgabe der Entscheidung ohne menschliches Eingreifen erfolgt.[4] Bei dem der KI zugrunde liegenden Deep Learning ist dies naturgemäß der Fall und zwar auch dann, wenn ein Mensch das von der KI erzeugte Ergebnis letztlich noch bestätigt, ohne dabei Einfluss auf den Inhalt der Entscheidung zu nehmen (z. B. Drücken eines OK-Buttons).[5] Hintergrund des Art. 22 DSGVO sind die grundrechtlich geschützten Rechte auf Handlungsfreiheit und informationelle Selbstbestimmung.[6] Allerdings ist das Verbot automatisierter Entscheidungen durch Art. 22 Abs. 2 DSGVO abdingbar. Hierfür müssen Unternehmen, die personenbezogene Daten für die KI verwenden möchten, entweder die Einwilligung der Betroffenen einholen, oder Verträge abschließen, die die Analyse der Daten legitimieren. 3

Ist das Problem KI vs. DSGVO damit gelöst? Im Gegenteil. Durch die Legitimierung automatisierter Datenverarbeitung ist der volle Anwendungsbereich der Betroffenenrechte eröffnet. Insbesondere die Handhabung der Informationspflichten und des Auskunftsrechts sind hierbei problematisch und teilweise umstritten.

[2] *J. Schmidhuber*, Deep learning in neural networks: An overview, Neural Networks 61, 2015, 85 (86).
[3] *O. Stiemerling*, Künstliche Intelligenz – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge, CR 2015, 762 (764).
[4] Erwägungsgrund 71 zur DSGVO
[5] *Hoeren/Niehoff*, KI und Datenschutz - Begründungserfordernisse automatisierter Entscheidungen, RW 2018 S. 47 (53).
[6] (Fn. 5).

III. Informationspflichten und Auskunftsrecht

Das Auskunftsrecht der Betroffenen und die Informationspflichten der Verantwortlichen sind in den Art. 13-15 DSGVO geregelt. Bezogen auf automatisierte Entscheidungen begründen die Art. 13 Abs. 2 lit. f) und Art. 14 Abs. 2 lit. g) DSGVO eine Informationspflicht der (für die Datenverarbeitung) Verantwortlichen gegenüber den Betroffenen. Diese Pflicht besteht zum Zeitpunkt der Datenerhebung. Den Betroffenen wiederum wird mit Art. 15 DSGVO ein Auskunftsrecht gewährt, welches bei Bestehen einer automatisierten Entscheidungsfindung auch Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen für die betroffene Person umfasst. Gemäß Art. 12 DSGVO müssen die Informationen in transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitgestellt werden. Wie bereits angedeutet, ist es im Zusammenhang mit KI allerdings häufig nicht möglich, vollständige Informationen zur Datenverarbeitung zum maßgeblichen Zeitpunkt zu übermitteln, da KI-basierte Systeme häufig selbst Analysen durchführen und Daten selbstständig weiterentwickeln, sodass dem Betreiber im Vorfeld gar nicht möglich sein kann zu erfassen, welche Daten in welcher Weise verarbeitet werden. Es stellt sich daher die Frage, was genau Verantwortliche bei automatisierten Entscheidungen eigentlich über die „involvierte Logik" mitteilen müssen. Hierfür müssen Rechtsprechung und Unternehmen praktikable Lösungen entwickeln. 4

IV. Sonderproblem: Offenlegung des Algorithmus

Eine viel diskutierte Möglichkeit über die *„involvierte Logik"* zu informieren, wäre die Offenlegung des Algorithmus, der sich hinter der Verarbeitung verbirgt. Dieser könnte aussagekräftige Informationen darüber liefern, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und zudem Tragweite und die angestrebten Auswirkungen der Verarbeitung offenbaren. 5

Dagegen spricht jedoch der Erwägungsgrund 63 S. 5 zur DSGVO, wonach die Auskunft Geschäftsgeheimnisse anderer Personen nicht beeinträchtigen darf. Eine solche Beeinträchtigung ist durchaus denkbar, da es sich bei einem Algorithmus in der Regel um schutzwürdiges geistiges Eigentum handeln dürfte. Dennoch darf gemäß Erwägungsgrund 63 S. 6 nicht jede Auskunft mit einem pauschalen Verweis auf das Geschäftsgeheimnis verwehrt werden. Stattdessen muss eine Abwägung der Interessen der Geschäftsgeheimnisse der Verantwortlichen gegenüber den Auskunftsinteressen der Betroffenen vorgenommen werden. Eine Abwägung dieser Art ist einzelfallabhängig und kann meist abschließend erst durch Gerichtsentscheidungen geklärt werden.[7] 6

Auch wenn die Interessenabwägung im Einzelfall zugunsten des Auskunftssuchenden ausfallen sollte, besteht weiterhin das Problem der fehlenden Einsicht des Verantwortli- 7

[7] Noch zum BDSG-alt SCHUFA-Urteil, BGHZ 200, 38.

chen in den Entscheidungsprozess des Systems. Da die KI-Anwendung selbstständig immer neue Algorithmen schreibt, ist es wahrscheinlich, dass der „Ur"-Algorithmus nicht mehr mit der automatisierten Entscheidung in Verbindung steht. Hier wird offensichtlich, dass die Verfasser der DSGVO undurchsichtige, selbstlernende Prozesse im Regelwerk nicht berücksichtigt haben.[8]

Zudem sei darauf hingewiesen, dass es sich bei Algorithmen für den Laien um komplizierte mathematisch-technische Prozesse handelt, die nur sehr schwer in leicht verständlicher Sprache zu erklären sein dürften. 8

Im Ergebnis wird die Einhaltung der strengen Anforderungen des Art. 12 Abs. 1 S. 1 DSGVO nur durch eine Beschreibung der zugrundeliegenden Prozesse gelingen. Dabei sollte es ausreichen, in verständlicher Form zu erläutern, wie die Technologie rund um den Algorithmus und dessen Entscheidungsfindung funktioniert. 9

V. DSGVO und KI: Weitere Problemfelder

- **Recht auf Datenübertragbarkeit** 10
  Die DSGVO stärkt entsprechend einem ihrer Primärziele die Rechte des Betroffenen. Als gänzlich neues Recht führt die DSGVO dabei das Recht auf Datenübertragbarkeit ein. Dieses Recht ermöglicht es Betroffenen, von Unternehmen die vollständige Übertragung ihrer personenbezogenen Daten auf ein anderes Unternehmen zu verlangen. Es stellt sich die Frage wie dieses Recht etwa im Falle von Machine Learning umgesetzt werden kann. So können von selbstlernenden Apps etwa nicht ohne weiteres vorher verwendete Daten vollständig „übertragen" werden, da die Daten bereits Grundlage der selbstlernenden Vorgänge der Apps wurden und selbst bei Übertragung der Ausgangsdaten noch im System vorhanden sind. Hier ist es sowohl an Unternehmen, technische Möglichkeiten für eine solche vollständige Übertragung zu entwickeln, als auch an der Rechtsprechung konkrete Leitlinien für die Umsetzung dieses Rechts vorzugeben. Diese Leitlinien müssen das (von der DSGVO geschützte) wirtschaftliche Interesse von Unternehmen an der Verarbeitung personenbezogener Daten, das Recht des Betroffenen auf Informationelle Selbstbestimmung sowie die Grundsätze der Datensparsamkeit und Transparenz einem fairen Ausgleich zuführen.

- **Recht auf Löschung** 11
  Dasselbe Problem stellt sich darüber hinaus bezüglich des Rechts auf Löschung. Auch hier kann es für Unternehmen insbesondere im Bereich des Machine Learning schwer werden, das Recht auf Löschung umzusetzen. Vor allem in Zusammenhang mit Smart Cars (Berechnung von Unfallwahrscheinlichkeiten, Stauumgehungen durch Auswertung des bevorstehenden Andrangs von Fahrzeugen) und Smart

[8] DFK Bitkom, künstliche Intelligenz, (Fn. 1), S. 20: „Die Europäische Datenschutz-Grundverordnung hatte KI nicht im Blick.".

Home (Energieersparnis) stellt sich zudem die Frage, ob das Recht auf Vergessenwerden ausnahmsweise nicht besteht, weil gemäß Art. 17 Abs. 3 lit. c DSGVO ggf. ein öffentliches Interesse an der Datenverarbeitung und Sammlung besteht. Sollte das Recht auf Vergessenwerden jedoch auch hier greifen, ohne dass eine Ausnahmeregelung greift, so wäre der Verstoß gegen dieses Betroffenenrecht, wie bei allen Betroffenenrechten, bußgeldbewehrt.

- **Datenschutz-Folgenabschätzung** 12
  Mit der Datenschutz-Folgenabschätzung, ebenfalls eine Anforderung aus der DSGVO, führt der Verordnungsgeber ein Instrument für unternehmerische Risikoanalysen ein, die bereits in der frühen Planungsphase eines Projekts den Blick auf Schwachstellen lenken, die sonst erst in der späteren und vor allem kostenintensiveren Implementierungsphase berücksichtigt würden. So können z.B. Softwareentwickler frühzeitig auf mögliche Datenschutzrisiken hingewiesen werden, die Entwicklern möglicherweise zunächst nicht als kritisch erscheinen. Der weitere Entwicklungsprozess kann besser abgestimmt und im gegenseitigen Austausch erfolgen. Gerade beim Machine Learning ist es wichtig, dass der Input, die Prozesse und das Ergebnis der Datenverarbeitung durch autonome Maschinen kritisch und aus datenschutzrechtlicher Sicht geprüft werden.
  Allerdings stehen die Verantwortlichen auch hier wieder vor dem Problem der fehlenden Vorhersehbarkeit selbstlernender Prozesse in neuronalen Netzwerken.[9]

VI. Die DSGVO als Chance für den Einsatz von KI

Neben allen Herausforderungen bietet die DSGVO auch Chancen für den Einsatz von KI. 13
Die von der DSGVO verlangte Datenschutz-Folgenabschätzung kann eine Möglichkeit darstellen, um die datenschutzrechtlichen aber auch ökonomischen Risiken beim Einsatz von KI bereits während der Planungsphase (etwa der Software-Entwicklung) abzuschätzen und Bußgelder zu vermeiden. Zudem lässt die Datenschutz-Folgenabschätzung Risiken erkennen, die aus dem Design und den technischen Voreinstellungen von Produkten oder Anwendungen resultieren. Damit lassen sich die Vorgaben der DSGVO an Privacy by Design und Privacy by Default, also datenschutzfreundliches Design und datenschutzfreundliche technische Voreinstellungen, ebenfalls erkennen und Bußgelder können vermieden werden.

Die zunehmenden Datenskandale um NSA, Facebook und Cambridge Analytica zeigen, 14
dass das Vertrauen der Nutzer in KI in kürzester Zeit schwinden und damit die zur Verfügung stehende Datenmenge abnehmen kann. Gerade das Vertrauen in den sicheren Umgang mit personenbezogenen Bürgerdaten auf Grundlage der DSGVO kann zukünftig also einen erheblichen Wettbewerbsvorteil darstellen. Auf diese Weise kann insbesondere der Vorsprung Chinas und der USA bezüglich der zur Verfügung stehenden Datenmenge

[9] *C.S. Conrad,* Künstliche Intelligenz – Die Risiken für den Datenschutz, DuD 2017, 744.

dadurch ausgeglichen werden, dass wegen der größeren Sicherheit qualitativ hochwertigere Daten im deutschen und europäischen Markt zunehmen.

VII. Fazit

Die Anforderungen der DSGVO sind streng. Dies wiegt umso schwerer, wenn man bedenkt, dass die Verfasser der DSGVO an selbstlernende, undurchsichtige Prozesse wie das Deep Learning bei der Gestaltung des Regelwerks nicht gedacht haben. Die bestehenden Vorschriften müssen nun so ausgelegt werden, dass deren Einhaltung für die Verantwortlichen nach dem heutigen Stand der Technik möglich ist. Dies ist auch mit Blick auf den technologischen Fortschritt zu befürworten. Einer innovativen Technologie wie der KI und deren Entwicklung sollte nicht durch Überregulierung der Riegel vorgeschoben werden. 15

Der gerechte Ausgleich von Datensicherheit und Förderung der Innovation neuer KI-Technologien stellt eine der großen Aufgaben der Zukunft dar. Gelingt es Unternehmen und Rechtsprechung, zeitnah KI-orientierte Mechanismen für die Einhaltung der Datenschutzgesetze zu entwickeln, werden sich die Bemühungen für den deutschen und europäischen Markt auf lange Sicht auszahlen.