7
AI: Science over Fiction

Vertrauenswürdige Künstliche Intelligenz durch Privatsphäre wahrende Technologie

Faktenpapier

Aus der Serie: AI: Science over Fiction

www.bitkom.org

Digitaltag 2020 | bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Verantwortliches Bitkom-Gremium

AK Artificial Intelligence

Projektleitung

Dr. Nabil Alsabah | Bitkom e. V.

Autor

Prof. Dr. Michael Huth | Imperial College London & CTO XAIN AG

Lektorat

Monika Ilves | Bitkom e. V.

Satz & Layout

Katrin Krause | Bitkom e. V.

Titelbild

© Lisa H. | unsplash.com

1 Was wir unter KI verstehen liegt im Auge des Betrachters

Die meisten von uns haben schon von Künstlicher Intelligenz (KI) gehört. Oft taucht dieser Begriff in Berichten auf, die vielversprechende Möglichkeiten aber auch eventuelle Bedrohungen der Digitalisierung aufzeigen wollen. Aber was meinen wir eigentlich, wenn wir über Künstliche Intelligenz sprechen?

Eine einheitliche Definition zu KI gibt es nicht. Je nachdem, wen man fragt, erhält man unterschiedliche Antworten. Auch in der Wissenschaft gibt es unterschiedliche Definitionen dessen, was KI eigentlich ist. Zur Veranschaulichung führen wir hier einige der geläufigsten Definitionsversuche auf:

1. KI schließt die Fähigkeit von Maschinen ein, intelligente Tätigkeiten auszuführen, die normalerweise von Menschen durchgeführt werden, sodass der Mensch sich auf andere Dinge konzentrieren kann.

2. KI bedeutet mit Hilfe von Daten und statistischen Algorithmen Muster zu erkennen, die dabei helfen, wichtige Entscheidungen zu treffen.

3. KI bezeichnet das Imitieren kognitiver Funktionen eines Menschen, wie z.B. das Sehen, Hören oder die Problemlösungskompetenz.

4. KI benennt eine Weiterführung menschlicher Intelligenz, so dass künstlich intelligente Systeme anders und weitaus erfolgreicher »denken« können als Menschen dies jemals vermögen.

»Durch KI können wir menschliche Fähigkeiten erweitern. KI wird den Menschen nicht ersetzen, sondern ihn unterstützen. KI hat auch das Potenzial, Routineaufgaben zu übernehmen.«

Diese Definitionen decken eine große Spannweite an möglichen Interpretationen zu KI ab. So suggeriert zum Beispiel die letztgenannte Definition, dass KI eine potentielle Bedrohung für uns Menschen darstellen könne; wohingegen man die ersten drei Ausführungen so deuten kann, dass KI geschaffen wird, um das Leben von uns allen zu verbessern.

2 KI ist eine Schlüsseltechnologie, die menschliche Werte maßgeblich beinhalten wird

Bei der Betrachtung von KI geht es also nicht nur um ihr innovatives Potential, sondern auch darum, mit was für einem Werteverständnis KI in Wirtschaft, Gesellschaft sowie den staatlichen Organen und Diensten eingesetzt werden soll. Die Bundesländer, die Bundesrepublik und die Europäische Union – aber auch Verbände wie Bitkom e.V. – leisten hier wichtige Arbeit. Diese Mühen zielen darauf ab, dass wir die erheblichen Vorteile, die in der Weiterentwicklung der Künstlichen Intelligenz stecken, auch voll nutzen können – ohne dabei die Werte unserer Gesellschaft und ihrer Bürger und Bürgerinnen zu gefährden.

Wir erinnern uns an eine Anwendung der KI, über die breit in den Medien berichtet wurde: Ein Computer hatte mit dem sogenannten Deep Reinforcement Learning (deutsch: tiefgehendes bestärkendes Lernen) maschinell »gelernt«, das Brettspiel Go auf so einem hohen Niveau zu spielen, dass der Computer einen Go-Weltmeister besiegte. Dies war ein symbolischer und großer Schritt in der KI-Entwicklung. Es zeigt außerdem auf, wie menschliche Fähigkeiten durch KI erweitert werden können. Zum Beispiel kann solch ein Computer Spielzüge in Go »erfinden«, deren Nutzen den allerbesten menschlichen Gegnern erst in einer späteren Spielphase deutlich werden.

Zentral in der Nutzung solcher erweiterten Fähigkeiten ist aber, dass der Mensch – und unser Werteverständnis des Menschseins – im Mittelpunkt dieser neuen Möglichkeiten steht! Die sehr gute Nachricht ist hierbei, dass sowohl die Wissenschaft als auch die Wirtschaft und die Politik hier an einem Strang ziehen. Die Wissenschaft hat zum Beispiel große Fortschritte bei den Selektionskriterien für die Datenauswahl gemacht. So werden mittlerweile die Datenmengen, die für das maschinelle Lernen benötigt werden, derart gestaltet und verarbeitet, dass die daraus gewonnenen Erkenntnisse soweit möglich frei von Verzerrungen sind. Dadurch können sie dabei unterstützen, ausgewogene und faire Entscheidungen zu treffen – und so zum Beispiel systematische Diskriminierungen vermeiden helfen. Ein Anwendungsbeispiel für KI ist die Kreditvergabe von Banken. Hier kann die KI unterstützen, dass Kredite nach objektiven Kriterien vergeben werden – und subjektive (und häufig auch unreflektierte) Vorurteile von Bearbeitern (z.B. gegenüber Minderheiten) außen vor bleiben.

»Wissenschaft, Wirtschaft und Politik ziehen an einem Strang: Eine KI, die unsere Werte widerspiegelt, ist ein gemeinsames Ziel. Dabei machen wir große Fortschritte.«

Sowohl die Politik also auch die Wirtschaft haben ein großes Interesse an der Umsetzung von derart fairer und transparenter KI. Die KI-Forschung hat hierbei bereits große Fortschritte gemacht. Die neu gewonnenen Erkenntnisse und ihre Anwendung in der Praxis haben sogar das Potenzial, existierende soziale oder wirtschaftliche Missstände zu beheben.

Wir wollen dieses Potenzial nun anhand eines Beispiels erläutern, bei dem der Wert der Privatsphäre im Mittelpunkt steht.

3 Intelligente Suchmaschinen werden ein zentrales Vehikel unserer digitalen Erfahrung

Das Internet hat die Welt erobert. Mehr als **4 Milliarden Menschen weltweit** surfen mittlerweile im Netz – und nutzen dabei Suchmaschinen, um Informationen zu finden. Nicht umsonst ist **Google die meistbesuchte Website** weltweit; allein im Februar 2020 bearbeitete die Seite **11,13 Milliarden Suchanfragen**.

Die Suchanfragen werden dabei entweder in Form von konkreten Suchbegriffen – wie zum Beispiel »Westfälischer Friede« – oder in Form von kompletten, eigentlichen Fragen – wie zum Beispiel »Ab welchem Alter kann mein Kind alleine in die Schule gehen?« – gestellt. Bei der

Suchanfrage »Westfälischer Friede« erwarten wir relevante Informationen über den Westfälischen Frieden zu erhalten. Eine Suchmaschine wird in der Regel mit einer Liste von Webseiten, die Informationen zu diesem historischen Ereignis beinhalten, antworten.

Bei der eigentlichen Frage, ab wann man Kinder alleine in die Schule gehen lassen kann, erwartet man hingegen nicht einfach nur eine Liste von Webseiten, sondern eher eine qualifizierte und – wenn erforderlich – differenzierte Antwort. Die Antwort könnte zum Beispiel im rechtlichen Sinne in verschiedenen Ländern anders ausfallen oder könnte Gegenfragen zur Risikoabschätzung anregen, wie beispielsweise »Sind alle Straßenüberquerungen des Schulweges durch Ampeln gesichert?«.

Es dürfte einleuchten, dass KI hier sehr nützlich sein kann, um die Qualität bei der Suche nach Informationen zu erhöhen. Das trifft auch auf allgemein erscheinende Suchanfragen wie »Westfälischer Friede« zu: Jemand, der gerade Hausaufgaben für den Geschichtsunterricht macht, erwartet vielleicht eine andere Aufbereitung solcher Informationen als jemand, der als Diplomat aktiv in Friedens- oder Waffenstillstandsverhandlungen beteiligt ist.

»Für den Nutzer ist KI am nützlichsten, wenn sie Apps ermöglicht, sich an die situativen Bedürfnisse der Anwender anzupassen.«

KI kann solch eine höhere Qualität der Antworten auf Suchanfragen, die auch persönlichen Umständen Rechnung trägt, durch den Einsatz einer Reihe von komplementären Methoden erreichen. Wir erwähnen hier

- das Berechnen und Stellen von Gegenfragen, um die Suche zu optimieren,
- die Fähigkeit, das Suchen den Wünschen und Anforderungen einer Person anzupassen (Stichwort *Personalisierung*),
- sowie die Nutzung von Antworten auf Gegenfragen, um Sucherfahrungen zu verbessern.

Zum Beispiel kann die von der Suchmaschine gestellte Gegenfrage »Sind alle Straßenüberquerungen des Schulweges durch Ampeln gesichert?« von dem Elternteil mit »Mein Kind kann mit dem Bus fahren und muss nur einen Zebrastreifen überqueren.« beantwortet werden. Die KI könnte diese Information dann benutzen, um die Risikobewertung zu verfeinern und entsprechende Empfehlungen zu geben. Es ist wohl selbstverständlich, sollte aber hier unbedingt gesagt werden, dass KI in solchen Fällen selbst keinerlei Entscheidungen treffen sollte. Vielmehr soll die KI die Suche nach Informationen verbessern, um den Prozess der Entscheidungsfindung zu unterstützen und idealerweise zu verbessern. Die Entscheidung, ob ein Kind alleine in die Schule gehen soll, muss natürlich von den Eltern gemacht werden und das Kind in den Entscheidungsprozess mit einbeziehen.

Eine genauere, individuellere und dadurch relevantere Sucherfahrung im Internet ist also ein gutes Beispiel dafür, wie KI das Leben von uns allen sehr positiv beeinflussen kann. Um dieses Potenzial voll und werteerhaltend auszuschöpfen, müssen wir aber sicherstellen, dass solche Lösungen die Privatsphäre derer wahren, die solche Suchbegriffe eingeben – also von uns allen!

Das mag bei Suchbegriffen wie »Westfälischer Friede« als unproblematisch erscheinen. Aber selbst die Eingaben allgemein erscheinender Suchbegriffe sagen in ihrer Gesamtheit und ihrem räumlichen und zeitlichen Kontext sehr viel über die nach Informationen suchende Person aus. Die jeweiligen Anfragen nach einer Zugverbindung Berlin-Hamburg, nach einem Blumengeschäft in Hamburg und nach dem deutschen Fürsorgerecht mögen im Strom der Suchanfragen zwar auf den ersten Blick wenig Brisanz haben. Aber das Wissen, dass all diese Anfragen von derselben Person am selben Tag gestellt wurden und dass diese Person zum Beispiel sehr selten Fahrten nach Hamburg online bucht, gewährt unter Umständen tiefe, wenn auch spekulative Einblicke in ihr Privatleben.

Eine Privatsphäre wahrende Suche ist also nicht nur bei Suchbegriffen welche intimere Aspekte unseres Privatlebens, wie gesundheitliche Probleme, abfragen erstrebenswert.

Wir wollen nun aufzeigen, wie wissenschaftliche Fortschritte dies in der Tat ermöglichen.

4 Suchmaschinen werden in Zukunft intelligent werden und die Privatsphäre wahren

Kann man überhaupt intelligente Suchmaschinen bauen, die sich den Bedürfnissen und Interessen von Einzelpersonen anpassen, aber gleichzeitig die Privatsphäre ihrer Nutzer wahren? Ja, das kann man – und man kann die Privatsphäre auch in anderen Anwendungen der KI wahren.

Warum dies möglich ist, ist auch ein Beispiel dafür, wie unterschiedliche Gebiete der Wissenschaft sich gegenseitig befruchten können, um innovative Lösungen zu erschließen. In diesem konkreten Falle der Suchmaschinen ist das eine Verbindung von Lösungsansätzen aus dem maschinellen Lernen, der Kryptographie und dem Gebiet der Verteilten Systeme. Wir wollen uns hier natürlich nicht in die technischen Details vertiefen. Vielmehr wollen wir aufzeigen, welche Prinzipien solche Lösungen leiten, um Privatsphäre wahrende KI zu ermöglichen.

»KI-Systeme bringen unterschiedliche Teile der Informatik zusammen. So integrieren Suchmaschinen z.B. Lösungsansätze aus den Bereichen des maschinellen Lernens, der Kryptographie und der verteilten Systeme.«

Eins dieser Prinzipien lässt sich kurz und prägnant mit dem Ausruf zusammenfassen: »Meine Daten gehören mir!«

Eine sachlichere und dennoch allgemein verständliche Version dessen findet sich zum Beispiel bei Wikipedia: »Das **Recht auf informationelle Selbstbestimmung** ist im Recht Deutschlands das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.«

Wie man dieser Beschreibung entnehmen kann, geht es vor allem darum, dass wir die Kontrolle darüber behalten, was mit unseren persönlichen Daten geschieht. Wenn wir aber im Internet unterwegs sind, geben wir oft eine Einverständniserklärung ab, durch die wir anderen Parteien erlauben, unsere persönlichen Daten zu verwalten, zu verarbeiten oder gar an Dritte weiterzugeben.

Die Datenschutz-Grundverordnung (DSGVO) schreibt hier deshalb aus gutem Grunde vor, dass

- solch ein Einverständnis nur erbeten werden kann, wenn verständlich ist, zu was genau zugestimmt wird, und dass
- einmal gegebene Einverständnisse auch in der Zukunft widerrufen werden können.

Dies stellt uns momentan bei der Online-Suche wohl vor ein Dilemma, das die Privatsphäre wahrende KI aufzulösen vermag. Derzeit haben wir anscheinend nur zwei Möglichkeiten:

- Zum einen können wir solche Einverständniserklärungen abgeben, um es den marktführenden Suchmaschinenanbietern zu ermöglichen, uns bessere Suchergebnisse zu liefern. Hier ist aber das potenzielle Problem inbegriffen, dass solche Firmen dann ein unglaubliches Wissen über uns aufbauen können, was zumindest auf der emotionalen Ebene nicht im Einklang mit dem Wahren unserer Privatsphäre zu stehen scheint.
- Zum andern können wir den Service von einigen Startups nutzen, die unsere Suchanfragen für uns anonymisieren, so dass das Berechnen der Suchresultate – was von den großen Marktführern erledigt wird – nicht mehr in unsere Privatsphäre eindringen kann. Das ist an und für sich natürlich erstrebenswert, hat aber den entschiedenen Nachteil, dass die Suchergebnisse keinerlei persönliche Aspekte berücksichtigen können und so oft ungenau oder für uns nicht zufriedenstellend sind.

Dieses Dilemma lässt sich aber durch den Einsatz Privatsphäre wahrender KI prinzipiell wie folgt lösen: KI, in der Form des maschinellen Lernens, kann ein ganz persönliches Modell berechnen und kontinuierlich aktualisieren. Dieses Modell kann in unserem Smartphone, auf unserem Laptop oder Tablet errechnet und gespeichert werden. Dadurch behalten wir als Nutzer die komplette Kontrolle über dieses Modell. Sowohl die persönlichen Daten, die zur Errechnung oder Aktualisierung des Modelles benutzt werden, als auch das Modell selbst bleiben dabei stets auf den Endgeräten. Wir können also den Leitspruch von oben zu »Meine Daten und meine KI-Modelle gehören mir!« verfeinern. Methoden aus der Kryptographie, wie zum Beispiel die so genannte homomorphe Verschlüsselung, erlauben es dann unterschiedliche persönliche Modelle miteinander zu aggregieren ohne dass persönliche Daten von uns in dieses aggregierte Modell einfließen oder daraus herleitbar sind.

»KI kann ein ganz persönliches Modell berechnen und kontinuierlich aktualisieren. Dieses Modell kann in unserem Smartphone, auf unserem Laptop oder Tablet errechnet und gespeichert werden.«

Dieses aggregierte Gesamtmodell können wir als die Gesamtheit der Vorlieben und Interessen aller Nutzer verstehen. Dieses kollektive Wissen kann dann mit unserem eigenen persönlichen Modell auf unserem Smartphone interagieren, um sehr genaue, effektive und persönlich zugeschnittene Suchergebnisse zu ermöglichen und ohne persönliche Daten in der Berechnung der Suchergebnisse preiszugeben.

Solche Lösungen der KI stecken zwar noch in den Kinderschuhen. Aber sie sind als Konzepte schon ziemlich ausgereift und so entworfen, dass sie den Anforderungen des Datenschutzes

gerecht werden (Stichwort *Privacy By Design*). Diese Produkte werden auch so angelegt sein, dass sie den Nutzer in ihren Mittelpunkt stellen und sie so zusätzlich einen hohen Grad an Transparenz (Stichwort *Open-Source Code*) schaffen werden.

Zum Abschluss zeigen wir noch einige Anwendungsbeispiele dieser Zukunftstechnologie auf.

5 Personalisierbare und Privatsphäre wahrende Suchmaschinen werden breite Verwendung finden

Covid-19 hat uns gezeigt, wie wichtig eine beschleunigte und in alle Teile des Lebens reichende Digitalisierung ist. Dies trifft auch auf Behörden und deren Dienstleistungen zu. Zum Beispiel können in Zukunft die Angestellten und das operative Personal einer Großstadt einen personalisierten Sprachassistenten auf ihrem Smartphone oder Desktop-Browser haben, der es Ihnen ermöglicht, schnell sehr relevante interne Dokumente oder Arbeitsvorgänge zu finden und zu bearbeiten. Solch eine personalisierte KI kann im Prinzip auch auf Kalendereinträge oder per Email erhaltene Arbeitsanweisungen reagieren, um zum Beispiel automatisch Links für Dokumente zu präsentieren, die der Nutzer – nach Einschätzung der KI – aufgrund dieser Einträge oder Anweisungen lesen oder bearbeiten will.

Ein anderer interessanter Anwendungsbereich findet sich in der Werbung. Viele von uns haben schon erlebt, dass wir wegen unserer Suchanfragen »passgenaue« Werbung auf weiteren Webseiten erhalten. Dies kann unter Umständen sogar recht bizarre Ausmaße annehmen und dem Nutzer unheimlich erscheinen. Außerdem wird die Privatsphäre hier gleich in zweierlei Hinsicht verletzt: Zum einen können werbende Firmen ein sehr detailliertes Wissen über uns, unsere Präferenzen und Bedürfnisse aufbauen. Zum anderen kann die eingeblendete Werbung unbeteiligten Dritten z.B. im Büro tiefe – und unerwünschte – Einblicke in unser Privatleben geben. Werbung ist aber ein wichtiger Bestandteil unseres wirtschaftlichen Lebens. Privatsphäre wahrende KI kann hier konstruktive und wertschöpfende Lösungen bieten.

»Privatsphäre wahrende KI kann konstruktive und wertschöpfende Lösungen bieten. Solche Lösungen werden in Zukunft zunehmend an Bedeutung gewinnen.«

Zum Beispiel gibt es schon Browser-Plattformen, in denen Nutzer dafür bezahlt werden, sich Werbung anzuschauen. Die werbende Partei erfährt dabei nicht, welche Person sich die Werbung anschaut. Der Nutzer erhält so einen monetären Anreiz, sich Werbung anzuschauen, während er oder sie gleichzeitig weiß, dass dies anonym geschieht. Die Partei, welche die Webseiten bereitstellt (z.B. eine national erscheinende Tageszeitung), kann dafür im Gegenzug ihren eigenen werbenden Parteien aufzeigen, wie viele Nutzer auf welche Arten, wie lange welche Werbung anschauen. So kann auch die Vergütung dementsprechend und zielgenau angepasst werden. Die KI und ihre Personalisierung kann hier entscheidend helfen sicherzustellen, dass eine Nutzerin für sie hoch relevante Werbung eingeblendet bekommt, ohne dass dabei ihre Privatsphäre verletzt wird.

6 Fazit

Die Zukunft wird uns also vertrauenswürdige, Privatsphäre wahrende KI bieten. So genutzt kann uns KI dabei helfen, unsere Gesellschaft und ihre Werte zu stärken und wertschöpfende Impulse für die deutsche und europäische Wirtschaft im digitalen Zeitalter zu geben!

Autor

Professor Michael Huth
↗Professor Michael Huth (Ph.D.) ist Mitgründer sowie CTO der ↗XAIN AG und lehrt seit 2001 Computer Science am Imperial College London. Seine Spezialgebiete sind u.a. Cybersecurity sowie Sicherheit und Datenschutz beim Machine Learning. Er agierte als Technischer Leiter des Projekts »Harnessing Economic Value« beim britischen PETRAS IoT Cybersecurity Research Hub. Gemeinsam mit Leif-Nissen Lundbæk und Felix Hahmann gründete er 2017 XAIN. Das Berliner Unternehmen entwickelt eine eigene Plattform und Anwendungen für datenschutzkonforme KI-Lösungen. XAIN gewann den ersten Porsche Innovation Contest und arbeitete bereits erfolgreich mit der Porsche, Daimler, Deutsche Bahn und Siemens zusammen.

Professor Huth studierte Mathematik an der TU Darmstadt und erhielt seinen Ph.D. an der Tulane University, New Orleans. Anschließend forschte und lehrte er u.a. an der TU Darmstadt, der Kansas State University und verbrachte einen Forschungsaufenthalt an der University of Oxford. Huth verfasste zahlreiche wissenschaftliche Publikationen und tritt international als Redner auf.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

Digitaltag 2020 | bitkom