DIGITALE WIRTSCHAFT – DIGITALE ETHIK

Vertrauen in Algorithmen

KI kann Fahrzeuge steuern oder selbstständig Fehler in der Produktion aufdecken. Doch wie verlässlich die Ergebnisse sind, ist schwierig zu beurteilen. Tech-Firmen und Forschungsinstitute wollen das ändern.

VON MARKUS STREHLITZ

Künstliche Intelligenz oder KI sorgt für viel Wirbel. Viele erwarten sich davon Veränderungen in nahezu allen Bereichen des Lebens. Doch die Intelligenz der Systeme, die aktuell so erfolgreich sind, ist eher begrenzt. In Wirklichkeit handelt es sich vor allem um selbstlernende Verfahren, die auf genau eine Aufgabe ausgerichtet sind.

Das Besondere: Sie werden nicht wie klassische Software programmiert, sondern trainiert – auf der Basis von einer großen Menge an Daten. Je größer diese ist, desto besser kann das System seinen Job erledigen. Und während es diesen ausübt, lernt es ständig hinzu.

Unternehmen nutzen solche Verfahren zum Beispiel bei der Suche nach Stellenkandidaten. Banken arbeiten mit KI-Software, um die Vergabe von Krediten effizienter zu gestalten. Und auch in Fertigungsprozessen kommt entsprechende Software zum Einsatz. Firmen kontrollieren damit etwa die Qualität ihrer Produkte. Kameras – ausgerüstet mit KI – überprüfen die Bilder von Kotflügeln oder Elektronikbauteilen nach Fehlern. Selbstlernende Systeme werten Daten aus den Produktionsabläufen aus, um diese zu optimieren. Auch Roboter, die mit Menschen zusammenarbeiten, werden mit künstlicher Intelligenz ausgestattet.

Die Tatsache, dass die Software trainiert statt programmiert wird, bringt Vorteile. Die Systeme passen sich schnell an verschiedene Aufgaben an. Und sie liefern neue, unerwartete Erkenntnisse.

Doch das führt auch zu einem Problem. Wie die KI zu ihrem Resultat kommt, lässt sich kaum nachvollziehen. „Das ist so, als ob man eine physiologische Untersuchung eines menschlichen Gehirns durchführt und daraus herleiten möchte, ob dieser Mensch etwas Falsches tut“, erklärt Professor Mario Trapp, geschäftsführender Leiter des Fraunhofer-Instituts für Kognitive Systeme (IKS). „Man kann zwar die einzelnen Synapsen prüfen, aber erhält trotzdem keine Aussage darüber, warum jemand etwas Bestimmtes tut.“ Hinzu kommt: Im realen Einsatz können KI-Systeme aufgrund äußerer Einflüsse auch verzerrte Ergebnisse liefern.

VERZERRTE ERGEBNISSE

Nach Meinung von Trapp wiegt das Problem bei Themen wie etwa dem autonomen Fahren schwerer als in der Produktion. In diesem Umfeld sei die KI „noch wesentlicher leichter abzusichern, weil der Kontext eingeschränkter ist“, so Trapp. Will heißen: Eine Kamera, die zur Qualitätskontrolle auf ein Produkt ausgerichtet ist, arbeitet meist unter sehr ähnlichen Bedingungen – mit quasi unveränderlichen Lichtverhältnissen und Perspektiven. Im Gegensatz dazu kann ein Fahrzeug in Situationen geraten, die nicht vorhersehbar sind.

Anders kann es dagegen aussehen, wenn Menschen mit Robotern zusammenarbeiten. Hier ist der Kontext nicht mehr ganz so eingegrenzt. Und in diesen Fällen drohen nicht nur wirtschaftliche Schäden, wenn die KI nicht funktioniert. Auch der Mitarbeiter kann dann in Gefahr geraten.

Unabhängig davon, wo die künstliche Intelligenz zum Einsatz kommt – Personen und Firmen wollen sich auf die Ergebnisse, die sie liefert, verlassen können. Andrea Martin sieht dabei die Anbieter der Technologien in der Pflicht. Die IBM-Managerin ist Mitglied der KI-Kommission des deutschen Bundestages. „Wir brauchen proaktive Verfahren, die bereits während der Entwicklung von KI-Systemen sicherstellen, dass diese nachvollziehbare Entscheidungen treffen“, so Martin.

Sie berichtet, dass IT-Werkzeuge, die Verzerrungen in der KI erkennen und abschwächen, zur Zeit entwickelt würden oder sogar schon auf dem Markt seien. Dazu zählt sie ein System von IBM, das die Ergebnisse von KI-Modellen misst und dafür sorgen soll, dass diese erklärbar sind.

Auch die Forscher des Fraunhofer IKS arbeiten daran, künstliche Intelligenz abzusichern. Sie konzentrieren sich dabei ebenfalls auf deren Ergebnisse. „Wir nutzen klassische Algorithmen, um den Vorschlag der KI zu plausibilisieren“, erklärt Trapp. „So versuchen wir, beide Welten miteinander in Einklang zu bringen. Wir nutzen die Kreativität der KI, können diese aber trotzdem noch mal überprüfen.“

Einem ähnlichen Ansatz folgt auch das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI). Die Wissenschaftler wollen in einem Projekt sogenannte Deep-Learning-Verfahren verlässlicher machen – eine spezielle Form von selbstlernenden Methoden. Dabei arbeiten sie mit Problemstellungen, die sowohl mit Deep Learning als auch mit einem herkömmlichen Verfahren gelöst werden können. Das Resultat der KI wird dann von dem klassischen System geprüft und gegebenenfalls korrigiert.

Der Ansatz wird an Robotern getestet – zum einen an kleinen Transportsystemen, die selbstständig ihren Weg finden müssen. Zum anderen versucht das DFKI-Team mit der Methode, einem Industrieroboter mit zwei Armen das Jonglieren beizubringen. Der Roboter soll sowohl allein als auch zusammen mit einem Menschen jonglieren, indem er die berechneten Bewegungsabläufe kennt und dank künstlicher Intelligenz schnell über die nächste Armbewegung entscheiden kann.

Die Wissenschaft versucht seit vielen Jahren, den komplexen menschlichen Geist künstlich nachzubauen. Foto: peshkov/Adobe Stock

» impressum

Produktion: STZW Sonderthemen
Anzeigen: Jürgen Maukner

Was ist wo über mich gespeichert und warum? Jeder hat das Recht, das zu erfahren. Foto: Patrick Pleul/dpa-tmn

Fragen stellen und sich schützen

Privatsphäre im digitalen Zeitalter – das bedeutet nicht mehr den Rückzug in die heimischen vier Wände, sondern die Hoheit über die eigenen Daten.

VON MARKUS STREHLITZ

Daten = Macht = Verantwortung – so laute die Digitalisierungsgleichung, sagt Philipp Otto, Direktor des Thinktanks iRights.Lab. Wer Daten über Personen besitzt, kann diese vielfältig nutzen. Er kann damit politische Entscheidungen beeinflussen – was das Beispiel Facebook und der US-Wahlkampf zeigt. Er kann diese an Wirtschaftsunternehmen verkaufen und darauf sein Geschäftsmodell aufbauen. Digitale Informationen geben aber auch darüber Aufschluss, ob eine Person kreditwürdig oder der passende Kandidat für eine Arbeitsstelle ist. Wer etwa seine Privatsphäre preisgibt und Bilder von ausschweifenden Partys auf seinem Social-Media-Account veröffentlicht, muss damit rechnen, dass diese im Bewerbungsgespräch zum Thema werden.

Schon aus vergleichsweise harmlosen Daten lassen sich tiefe Einblicke ins Privatleben gewinnen – zum Beispiel in spezielle Vorlieben oder die gesundheitliche Verfassung von Menschen.

Das gilt etwa für das Zeitprotokoll, das Google Maps von jedem einzelnen Nutzer anlegt, der diese Funktion nicht deaktiviert hat. Wer diese Daten einsieht, der weiß nicht nur, wo der Maps-Nutzer seinen Urlaub verbracht hat. Es lässt sich auch erkennen, in welchem Krankenhaus dieser eventuell gelegen hat und wie lange dies der Fall war.

Auf einem Kongress des Chaos Computer Clubs vor ein paar Jahren zeigte Datenspezialist David Kriesel, wie sich schon aus öffentlich verfügbaren Daten Rückschlüsse auf intime Angelegenheiten ziehen lassen. Er erfasste über einen bestimmten Zeitraum hinweg die Metadaten zu Artikeln auf „Spiegel Online“ – wie etwa Autor, Erscheinungsdatum und -uhrzeit sowie Ressort. Indem er diese miteinander verknüpfte, konnte er zum Beispiel erkennen, welche Redakteure untereinander aller Wahrscheinlichkeit nach eine Beziehung haben.

„Privatsphäre bedeutet heute nicht mehr Rückzug in die analogen vier Wände, sondern die Herrschaft über die eigenen Daten in einer immerwährenden Öffentlichkeit“, erklärt Otto. Moderner Datenschutz als Bestandteil dieser Privatsphäre sei ein „harmonisches Zusammenspiel aus gesetzgeberischer Rahmensetzung, unternehmerischer Verantwortung und der Fähigkeit zu eigenverantwortlichem Handeln digitalkompetenter Verbraucherinnen und Verbraucher“.

Jeder Nutzer ist also auch selbst gefordert, seinen Teil zum Erhalt seiner Privatsphäre beizutragen. Tim Mackey, Sicherheitsexperte beim IT-Anbieter Synopsys, schlägt vor, „in die Offensive zu gehen“. Das heiße, „die Menschen, Unternehmen und Institutionen, die Daten über uns erheben, stärker in die Verantwortung zu nehmen.“ Verbraucher hätten das Recht, die Art und Weise zu beeinflussen, wie und an wen ihre Daten weitergegeben werden. „Der einfachste Weg, hier Klarheit zu schaffen, besteht darin, Fragen zu stellen“, so Mackey.

Dazu zählen nicht nur Fragen nach dem Weitergeben von Informationen, sondern auch: Wie werden diese erhoben, gesichert, wie lange aufbewahrt? Oder: Wie stellt das Unternehmen beziehungsweise die Institution fest, wenn jemand ohne die entsprechende Berechtigung auf die Daten zugegriffen hat?

Wenn mehr Menschen dazu übergehen würden, diese Fragen zu stellen, glaubt Mackey, „sind wir so weit, dass Verbraucher nicht länger dazu verdammt sind, passive Empfänger von Meldungen über neue Datenschutzverletzungen zu sein“.

» INFO

Auf seiner Website hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) umfangreiche Informationen zusammengestellt, wie Bürgerinnen und Bürger ihre Privatsphäre im elektronischen Zeitalter schützen können.
Dazu zählt etwa, wie sich „digitaler Verbraucherschutz“ umsetzen lässt:
https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/digitaler_Verbraucherschutz/digitaler_Verbraucherschutz_node.html
Aufgeführt werden auch einige Maßnahmen für den Schutz der digitalen Identität:
www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Schutzmassnahmen/id-dieb_schutz_node.html
Ein Video zum Vortrag von David Kriesel auf dem Kongress des Chaos Computer Clubs ist hier verfügbar:
https://www.youtube.com/watch?v=-YpwsdRKt8Q Markus Strehlitz