

MACHT OHNE MORAL

Algorithmen sind ein Werkzeug:
Ob sie Gutes oder Schlechtes tun, hängt davon ab,
wie wir sie einsetzen. Lässt sich der
Risikofaktor Mensch beherrschen?

TEXT: CHRISTIAN SCHWÄGERL



ÜBERWACHUNG

Mit der Gesichtserkennung »Face++« der Firma Megvii identifizieren Smartphones ihre Besitzer oder Banken ihre Kundinnen. Die chinesische Regierung überwacht damit die Bevölkerung auf Schritt und Tritt. Als am Bahnhof Berlin Südkreuz 2017 ein ähnliches System getestet wurde, protestierten Gegner und Gegnerinnen öffentlichkeitswirksam gegen die Überwachung des öffentlichen Raums durch KI.

Regierungen, die ihre Bürgerinnen und Bürger rund um die Uhr mithilfe künstlicher Intelligenz (KI) überwachen: Bis vor wenigen Jahren war das der Stoff dystopischer Zukunftsvisionen. Doch in China werden die Schreckensszenarien von einst gerade Realität.

»Sobald ich aus dem Haus gehe, werde ich von einer Kamera erfasst«, berichtete der investigative Journalist Hu Liu im Mai der BBC. Die Kamera filmt ihn nicht bloß. Vielmehr erkennt ein Algorithmus sein Gesicht und ordnet die Aufnahmen seinem persönlichen Profil in den staatlichen Datenbanken zu. »Wenn ich ein Taxi nehme, leitet die Taxifirma meine Daten an die Regierung weiter. Wenn ich Freunde in einem Café treffe, dann wissen das die Behörden – wegen der Kamera im Café«, sagt Hu Liu. Jede Bewegung, jede Zusammenkunft wird analysiert. Er bekomme immer wieder Anrufe von Staatsbediensteten, die ihm vorschreiben, mit wem er sich besser nicht treffen solle. »Der künstlichen Intelligenz wegen können wir uns nirgendwo mehr verstecken«, sagt Hu Liu.

»Der Einsatz von KI im Bereich der öffentlichen Sicherheit hat in China explosionsartig zugenom-

men, getrieben durch das Bemühen, sie zur Massenüberwachung einzusetzen«, warnt das Mercator-Institut für China-Studien in einem Bericht aus dem Mai dieses Jahres. Das autoritär regierte Land besitzt beispielsweise eine Datenbank namens »Police Cloud«, in der Überwachungsvideos bestimmter Personen unter anderem mit deren Wohnort, IP-Adresse, Profilen in sozialen Medien, Hotelaufenthalten, Einkaufsgewohnheiten in Supermärkten, biometrischen Daten und Behördenanträgen zusammengeführt werden. Ziel ist es, abweichende Verhaltensmuster aufzuspüren.

Ein technisches Großprojekt: Daten werden nicht nur erfasst und gespeichert, sondern in Echtzeit ausgewertet. Die Entwickler und Entwicklerinnen der KI haben ihren Systemen beigebracht, die Gesichtszüge der Menschen zu vermessen und live mit Bildern etwa von Ausweisdokumenten abzugleichen. Die Algorithmen lernen eigenständig dazu. Schon heute kann es in China passieren, dass jemand plötzlich keine Zug- oder Flugtickets mehr buchen kann. Dann hat ein KI-System den Behörden zu viele Regelverstöße gemeldet und »Sozialpunkte« abgezogen. In der Provinz Xinjiang wird Gesichtserkennung durch KI speziell dazu einge-

setzt, die ethnische Minderheit der Uiguren, aus deren Reihen Hunderttausende in »Umerziehungslagern« interniert werden, lückenlos zu überwachen.

Die Entwicklung in China alarmiert selbst die größten Verfechter der Technologie – etwa den Informatiker Antonio Krüger, Chef des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI). Unter seiner Führung entwickeln 1200 Wissenschaftlerinnen und Wissenschaftler in 24 bundesweit verteilten Forschungsbereichen neue digitale Verfahren. Wenn KI-Systeme in Echtzeit die gesamte Bevölkerung überwachen, Individuen erkennen und ihr Verhalten analysieren, sei das »mit unserer Vorstellung von Menschenwürde nicht gut vereinbar«, sagt Krüger.

Der Wissenschaftler Krüger glaubt aber fest an den Nutzen von KI, etwa in der Medizin. Er selbst forscht an persönlichen digitalen Assistenten, die den Alltag erleichtern, das Lernen beschleunigen und die Gesundheit verbessern sollen. Doch bei manchen Entwicklungen ist ihm zunehmend mulmig zumute. »Vor fünf oder zehn Jahren hätte ich gesagt, lasst die Kirche mal im Dorf, gucken wir doch erst mal, in welche Richtung sich die künstliche Intelligenz entwickelt«, sagt er. »Das ist jetzt anders.«

Die digitale Massenüberwachung durch eine Diktatur ist dabei nur das offensichtlichste Risiko künstlicher Intelligenz. Auch in westlichen Ländern verleihen die neuen digitalen Möglichkeiten einzelnen Akteuren ungeahnte Macht. Nicht nur Kriminelle, auch Firmen, gewählte Regierungen und Interessengruppen können KI für hochproblematische Ziele nutzen. »Es gibt die Befürchtung, dass ein breiter Einsatz von KI auch bei uns Grundrechte verletzen und Minderheiten diskriminieren könnte«, sagt Kilian Gross, Abteilungsleiter in der EU-Kommission für die weitere Entwicklung künstlicher Intelligenz.

Wie schnell sich KI-Systeme ausbreiten, überrascht selbst Fachleute. Allerdings geriet in den 1990er-Jahren die Entwicklung der Elektronenhirne ins Stocken, weil Datenmengen zu groß und zu ambivalent wurden. Damals setzte die Zunft auf Expertensysteme, die händisch mit strukturiertem Wissen gefüttert wurden. Das verursachte beispielsweise bei der Bild- und Spracherkennung Probleme, die man auf diese Art nicht mehr lösen konnte. Der Durchbruch gelang dann erst einige Zeit später dank maschinellem Lernen: einer Methode, bei der Programme darauf trainiert werden, eigenständig Schlüsse zu ziehen. Die Algorithmen sind so konstruiert, dass sie ihrem Ziel in immer neuen Feedbackschleifen Schritt für Schritt näher kommen – und schließlich selbstständig dazulernen. Oft kommen beim maschinellen Lernen neuronale Netze zum Einsatz, deren Aufbau sich grob an der Verschaltung von



P.M. Wissen

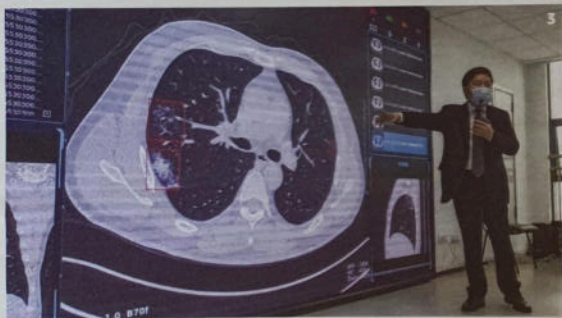
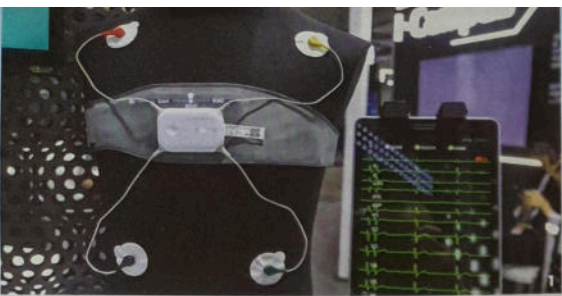
KI im TV

P.M. Wissen hat autonomen Robotern, schlaun Maschinen und lernenden Systemen eine Sonder-sendung gewidmet. Zu sehen ist sie unter pm-wissen.com/ki-spezial

PANDEMIE

Um die Covid-19-Infektionen einzudämmen, greift China auf sein engmaschiges Überwachungssystem zurück. Dieser Helfer misst händisch die Temperatur; andernorts erledigen das Infrarotkameras aus mehreren Metern Distanz. Apps verfolgen Kontakte; die Gesichtserkennung lernt, Menschen trotz Schutzmaske zu erkennen.





Einkauf vom ersten Klick an, gibt personalisierte Empfehlungen und sagt sogar die Mode der nächsten Saison voraus.

Aus den gesammelten Kaufentscheidungen können KI-Systeme weitreichende Schlüsse über eine Person ziehen – über ihren Wohlstand, ihre Neigungen und Interessen, ihre Krankheiten und vieles mehr. Algorithmen erkennen in den Daten unzähliger Nutzerinnen und Nutzer versteckte Muster und destillieren daraus Persönlichkeitsprofile. Die Erkenntnisse nutzen Firmen beispielsweise dazu, Menschen zum Kaufen zu bewegen – oder ihre Meinung zu einem Thema zu ändern. »Jedem wird das angezeigt, was er oder sie schon immer haben wollte. Doch die Kehrseite ist, dass die Vorschläge individuell manipulativ wirken, weil die Website für jeden Nutzer, jede Nutzerin anders aussieht«, sagt KI-Forscher Krüger.

In der Hand von Regierungen – auch demokratisch gewählt – kann die wachsende Datenmacht außerdem dazu führen, dass Menschen maschinell abgestempelt werden. So hat Österreich 2018 seine Arbeitsämter mit einem digitalen Assistenten ausgestattet, der aus den verfügbaren Daten errechnet, wie sinnvoll es ist, Arbeitssuchende mit Fördermitteln zu unterstützen. Am Ende landet jeder Fall in einer von drei Kategorien: hohe Chancen auf eine neue Arbeitsstelle, mittlere Chancen, niedrige Chancen. Auch künftig sollen die menschlichen Angestellten der Agentur die finale Entscheidung treffen. Doch das Verfahren macht aus Bürgerinnen und Bürgern, die zum Amt gehen, Datenpunkte in einer Wahrscheinlichkeitsrechnung. »Social Scoring« heißt das Verfahren, das sich beliebig ausdehnen ließe – etwa auf die Bildungschancen von Kindern.

Eine spezifische Anwendung von KI ist besonders umstritten: die Echtzeit-Gesichtserkennung. Die Sorge geht um, dass auch bei uns KI-Systeme zur lückenlosen Überwachung und Kontrolle eingesetzt werden könnten. So erprobte die Bundesregierung bereits 2017/18 am Bahnhof Südkreuz in Berlin die Echtzeit-Gesichtserkennung, wie sie aus China bekannt ist. Das Innenministerium jubelte: Testpersonen seien in 80 Prozent der Fälle erkannt worden, selbst dann, wenn sie einen Teil ihres Gesichts mit einer Brille oder einem Schal verdeckten. In nur 0,1 Prozent der Fälle habe das System fälschlicherweise Alarm geschlagen: Von 1000 unbeteiligten Passantinnen und Passanten brandmarkten die Algorithmen im Schnitt eine Person als verdächtig.

Das Max-Planck-Institut für Bildungsforschung geißelte die entsprechende Pressemitteilung als »Unstatistik des Monats«. Erstens sei die Trefferquote von 80 Prozent durch technische und rechnerische Kniffe sowie eine selektive Datenauswahl zustande gekommen. Zweitens würden bei 11,9 Millionen Fahrgästen pro Tag im Schnitt 11 900 Menschen von der Software fälschlicherweise als terrorverdächtige »Gefährder« eingestuft – zumindest für den Fall, dass alle deutschen Bahnhöfe mit einer entsprechenden Gesichtserkennung ausgestattet würden.

Das Bundesinnenministerium verkündete dennoch: »Die Systeme haben sich in beeindruckender Weise bewährt, sodass eine breite Einführung möglich ist.« Zwar werden die Spezialkameras an Bahnsteigen derzeit nur eingesetzt, um Gefahrensituationen zu erkennen. Doch die Versuchung ist groß. »Wir haben Angst, dass KI einen Überwachungsstaat ganz anderer Qualität ermöglichen könnte«, sagt EU-Abteilungsleiter Kilian Gross – und meint explizit auch Europa.

Verstärkt werden diese Sorgen durch ein weiteres Potenzial der Gesichtserkennung: das Aufspüren von Eigenschaften. »Eines der großen, sehr relevanten Felder in der KI-Entwicklung ist es, mit Wahrscheinlichkeitsverfahren aus unauffälligen Datenquellen weitreichende Folgerungen zu ziehen, etwa aus einem Gesicht die



Antonio Krüger

ist Geschäftsführer des Deutschen Forschungszentrums für Künstliche Intelligenz. Als Leiter des Forschungsbereichs Kognitive Assistenzsysteme entwickelt er außerdem Wege, wie Menschen mittels Sprache, Gestik, Mimik oder Berührungen mit smarten Algorithmen interagieren können.

sexuelle Orientierung herauszulesen«, sagt Thilo Hagendorff, KI-Ethiker an der Universität Tübingen (siehe Kasten Seite 28). »Einen solchen Einsatz fände ich sehr riskant.« Derartige Gesichtsanalysetools könnten beispielsweise zur Erpressung von Menschen eingesetzt werden, die sich nicht als homosexuell outen wollen – oder Regierungen helfen, sexuelle Minderheiten zu verfolgen.

Auf die Spitze getrieben wird der KI-Missbrauch von Gesichtsdaten durch sogenannte Deepfakes (P.M. 09/2020). Es gibt heute schon simple Apps dafür, Menschen Sätze in den Mund zu legen, ihre Gesichter in Filmszenen einzufügen oder sogar in Sexvideos zu montieren. Doch bisher war meist leicht zu erkennen, dass es sich um eine Fälschung handelte. Was aber, wenn KI-Systeme die Bewegungen und die Aussprache eines Politikers, einer Politikerin so perfekt imitieren können, dass glaubhafte Videos entstehen – etwa von einer Kriegserklärung oder einer angeblichen Sex-Eskapade? Und wenn die für die Fälschung Verantwortlichen ebenfalls dank maschinellem Lernen in den Lage sind, ihre digitalen Spuren zu verwischen? Anfang 2021 kurstierte im Internet ein Deepfake-Video, das den Schauspieler Tom Cruise überzeugend echt zeigte – und sich als komplettes KI-Werk entpuppte.

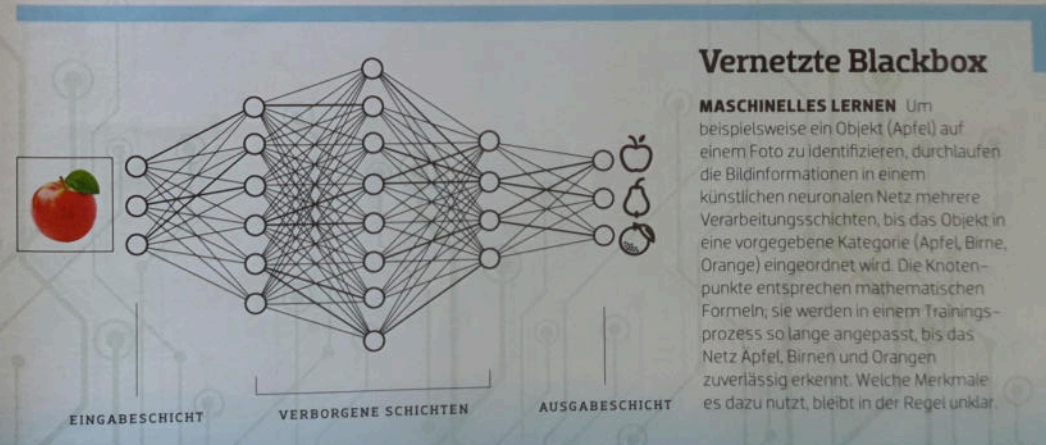
»KI verschärft die Bedrohung durch Cyberangriffe und Desinformationskampagnen, die Russland, China und andere staatliche und nicht-staatliche Akteure nutzen«, heißt es in einem »

MEDIZIN

- 1 Mit »CardioCloud« lässt sich daheim ein Elektrokardiogramm aufzeichnen. Algorithmen suchen in den Kurven der Herzaktivität nach Mustern, die auf Erkrankungen hindeuten.
- 2 Das Projekt »Ophthalmic-AI« hat zum Ziel, bei Augenleiden die individuell beste Therapie zu finden. Ärztin und Algorithmus sind dabei ein Team.
- 3 Eine KI identifiziert auf CT-Scans Läsionen der Lunge, verursacht durch Covid-19-Infektionen.

Nervenzellen im Gehirn orientiert. Eine immer schnellere Datenverarbeitung und enorm gewachsene Speicherkapazitäten befähigen die künstliche Intelligenz nun zu neuen Höchstleistungen.

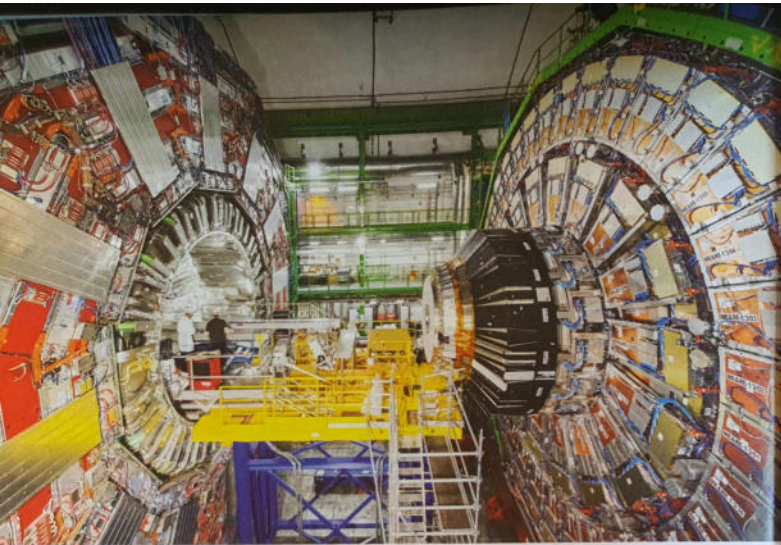
Die Fähigkeit von KIs, enorme Datenmengen zu sammeln, zusammenzuführen und auszuwerten, verschafft einigen wenigen Akteuren einen enormen Wissensvorsprung. Es mag sich harmlos anfühlen, am Rechner zu sitzen und auf der Website eines Onlinehändlers nach Kleidung zu suchen. Doch durch die Summe aller Klicks entstehen Profile – von Individuen, Gruppen, Gesellschaften. Im Onlinehandel »ist KI entlang der gesamten Lieferkette im Spiel«, sagt DFKI-Direktor Antonio Krüger. Sie analysiert das Verhalten beim



Vernetzte Blackbox

MASCHINELLES LERNEN Um beispielsweise ein Objekt (Apfel) auf einem Foto zu identifizieren, durchlaufen die Bildinformationen in einem künstlichen neuronalen Netz mehrere Verarbeitungsschichten, bis das Objekt in eine vorgegebene Kategorie (Apfel, Birne, Orange) eingeordnet wird. Die Knotenpunkte entsprechen mathematischen Formeln; sie werden in einem Trainingsprozess so lange angepasst, bis das Netz Äpfel, Birnen und Orangen zuverlässig erkennt. Welche Merkmale es dazu nutzt, bleibt in der Regel unklar.

FOTOS: GETTY IMAGES (2); HEIDE LEBERG ENGINEERING GMBH/DFKI (1); DFKI/SHUTTERSTOCK



FORSCHUNG

In vielen Bereichen der Wissenschaft ist die Datenflut händisch nicht zu bewältigen. Im Teilchenbeschleuniger LHC etwa kollidieren bis zu eine Milliarde Protonen pro Sekunde. Innerhalb von einer Mikrosekunde entscheidet eine Software, welche Ereignisse weiter untersucht werden sollten. Steigt die Zahl der Kollisionen wie geplant auf fünf bis sieben Milliarden, könnten superschnelle, selbstlernende neuronale Netze die interessantesten Zusammenstöße auswählen.

FLUGSICHERUNG

Verhüllen tief hängende Wolken den Tower des Flughafens London Heathrow, sehen die Lotsinnen und Lotsen die Landebahnen nicht. Dann prüfen sie per Radar, ob ein Runway frei ist, und fertigen aus Sicherheitsgründen weniger Flieger ab. Das kostet Kapazitäten und führt zu Verspätungen. Die britische Flugsicherung testet derzeit ein KI-System, das Abhilfe schaffen soll. Kameras filmen das Rollfeld, Algorithmen werten die Bilder in Echtzeit aus und verfolgen jede Maschine bis zum Gate.

FOTOS: KEITH WILSON/GETTY IMAGES



VISIONEN | KÜNSTLICHE INTELLIGENZ

Spezialreport der Nationalen Sicherheitskommission der Vereinigten Staaten. Die Angst geht um, dass ein perfekt gemachter und zum strategisch richtigen Zeitpunkt veröffentlichter Deepfake sogar einen Krieg auslösen könnte.

Die Risiken künstlicher Intelligenz sind groß – doch ebenso groß ist ihr Potenzial, Gutes zu tun. »KI kann die Medizin revolutionieren, wenn wir zum Beispiel Tumordiagnosen besser stellen und Therapien besser planen können«, sagt Antonio Krüger. KI-Verfahren seien auch für den Übergang zu umweltfreundlicher Energieerzeugung entscheidend, um die Schwankungen von Wind- und Solarstrom in den Stromnetzen auszugleichen. »85 Prozent der derzeitigen Anwendungen künstlicher Intelligenz sind nach unserer Einschätzung unproblematisch, und wir glauben an ihr enormes positives Potenzial«, sagt EU-Abteilungsleiter Kilian Gross. Als Beispiel nennt er den Corona-Impfstoff, der nur dank KI-Verfahren so schnell habe entwickelt werden können. Der Pharmakonzern Johnson & Johnson machte beispielsweise mithilfe eines mathematischen Modells Orte ausfindig, an denen hohe Infektionszahlen zu erwarten waren – und führte dort klinische Studien zu seinem Vakzin durch.

Doch diese Erfolge könnten in der öffentlichen Wahrnehmung schnell in den Hintergrund rücken, wenn klar wird, dass Persönlichkeitsprofile oder Gesichtserkennung nicht bloß fehlerhaft sind, sondern eine ganze Gesellschaft zum Negativen verändern können. Deshalb suchen Expertinnen und Experten nach Wegen, die Risiken der KI zu bändigen. Den derzeit wichtigsten Versuch unternimmt die Europäische Union. Sie hat als erster globaler Machtblock konkrete Regeln erarbeitet, die für alle 27 Mitgliedsstaaten gelten sollen. »Es ist positiv, dass die EU hier weltweit vorangeht«, sagt Leonie Beining, KI-Expertin der Stiftung Neue Verantwortung in Berlin.

Ängste in der Bevölkerung »können dem weiteren Einsatz der Technologie sehr schaden«, warnt Kilian Gross. Er arbeitet als Jurist in der Generaldirektion Kommunikationsnetze und Technologien und ist zuständig dafür, wie sich künstliche Intelligenz im größten Wirtschaftsraum der Welt entwickelt – für die Förderung ebenso wie für die Regeln. Mit seinem 13-köpfigen Team hat Gross in den vergangenen zwei Jahren das Regelwerk für künstliche Intelligenz geschrieben. Während die chinesische Regierung KI zum Machterhalt einsetzt und die neuen Technologien in den USA weitgehend unreguliert dem Profit dienen, sollen in Europa

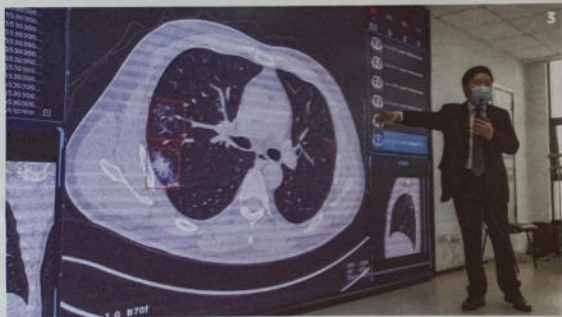
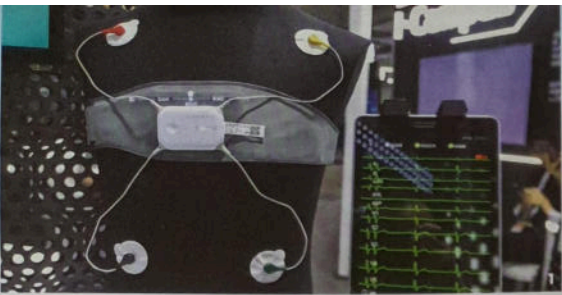
Werte wie die Gleichberechtigung aller Menschen und Prinzipien wie Transparenz verankert sein, sagt er: »Wir wollen sicherstellen, dass die Entwicklung wertebasiert verläuft und es Grenzen gibt.« KIs ermöglichen »Dinge, die wir in Europa gar nicht oder nicht in dieser Form haben wollen. Dinge, die wir innerhalb von Demokratien nicht akzeptabel finden«.

Nachdem 52 Expertinnen und Experten über zwei Jahre hinweg immer wieder getagelt hatten und mehr als 1200 Fragebögen und mehrere Hundert Stellungnahmen aus der Gesellschaft ausgewertet worden waren, schlug die EU-Kommission Ende April 2021 vor,

- dass Produkte mit künstlicher Intelligenz, die ein hohes Risiko für den Nutzer bergen, grundsätzlich einer Überprüfung unterzogen werden müssen, bevor sie auf den Markt kommen;
- KI-Systeme zu verbieten, die menschliches Verhalten manipulieren oder Behörden wie beim »Social Scoring« eine Bewertung der Bürgerinnen und Bürger ermöglichen;
- Gesichtserkennung in Echtzeit, wie sie in China praktiziert wird, mit eng umrissenen Ausnahmen zu untersagen.

Auch die Praxis in Österreich, Arbeitslose mit statistischen Verfahren zu klassifizieren, könnte ein Ende haben. Es dürfe nicht so weit kommen, »dass staatliche Leistungen oder Zulassungen an ein bewertendes Punktesystem geknüpft werden, das mit einer KI betrieben wird«, sagt Gross.

Vorgaben will die EU-Kommission auch für die Daten machen, mit denen KI-Systeme trainiert werden. Das sind zum Beispiel Umfragen von Fotos, die aus sozialen Medien stammen, oder statistische Datensätze, die Firmen einkaufen können. Die EU warnt, dass eine falsche Auswahl von Daten zu Diskriminierung führen könnte, etwa wenn eine medizinische Diagnose für Frauen erstellt wird, obwohl die Daten zum Training der Software nur von Männern stammen. Die Antidiskriminierungsstelle der Bundesregierung hat 47 problematische Fälle zusammengetragen, hauptsächlich aus den USA. So sollen Frauen bei der Vergabe von Jobs systematisch benachteiligt worden sein, weil Algorithmen hauptsächlich mit Daten von Männern trainiert worden waren. Systeme zur Gesichtserkennung, die den Zugang zu geschützten Bereichen kontrollierten, versagten bei Schwarzen, weil beim Maschinenlernen hauptsächlich Bilder Weißer zum Einsatz kamen. »



Einkauf vom ersten Klick an, gibt personalisierte Empfehlungen und sagt sogar die Mode der nächsten Saison voraus.

Aus den gesammelten Kaufentscheidungen können KI-Systeme weitreichende Schlüsse über eine Person ziehen – über ihren Wohlstand, ihre Neigungen und Interessen, ihre Krankheiten und vieles mehr. Algorithmen erkennen in den Daten unzähliger Nutzerinnen und Nutzer versteckte Muster und destillieren daraus Persönlichkeitsprofile. Die Erkenntnisse nutzen Firmen beispielsweise dazu, Menschen zum Kaufen zu bewegen – oder ihre Meinung zu einem Thema zu ändern. »Jedem wird das angezeigt, was er oder sie schon immer haben wollte. Doch die Kehrseite ist, dass die Vorschläge individuell manipulativ wirken, weil die Website für jeden Nutzer, jede Nutzerin anders aussieht«, sagt KI-Forscher Krüger.

In der Hand von Regierungen – auch demokratisch gewählt – kann die wachsende Datenmacht außerdem dazu führen, dass Menschen maschinell abgestempelt werden. So hat Österreich 2018 seine Arbeitsämter mit einem digitalen Assistenten ausgestattet, der aus den verfügbaren Daten errechnet, wie sinnvoll es ist, Arbeitssuchende mit Fördermitteln zu unterstützen. Am Ende landet jeder Fall in einer von drei Kategorien: hohe Chancen auf eine neue Arbeitsstelle, mittlere Chancen, niedrige Chancen. Auch künftig sollen die menschlichen Angestellten der Agentur die finale Entscheidung treffen. Doch das Verfahren macht aus Bürgerinnen und Bürgern, die zum Amt gehen, Datenpunkte in einer Wahrscheinlichkeitsrechnung. »Social Scoring« heißt das Verfahren, das sich beliebig ausdehnen ließe – etwa auf die Bildungschancen von Kindern.

Eine spezifische Anwendung von KI ist besonders umstritten: die Echtzeit-Gesichtserkennung. Die Sorge geht um, dass auch bei uns KI-Systeme zur lückenlosen Überwachung und Kontrolle eingesetzt werden könnten. So erprobte die Bundesregierung bereits 2017/18 am Bahnhof Südkreuz in Berlin die Echtzeit-Gesichtserkennung, wie sie aus China bekannt ist. Das Innenministerium jubelte: Testpersonen seien in 80 Prozent der Fälle erkannt worden, selbst dann, wenn sie einen Teil ihres Gesichts mit einer Brille oder einem Schal verdeckten. In nur 0,1 Prozent der Fälle habe das System fälschlicherweise Alarm geschlagen: Von 1000 unbeteiligten Passantinnen und Passanten brandmarkten die Algorithmen im Schnitt eine Person als verdächtig.

Das Max-Planck-Institut für Bildungsforschung geißelte die entsprechende Pressemitteilung als »Unstatistik des Monats«. Erstens sei die Trefferquote von 80 Prozent durch technische und rechnerische Kniffe sowie eine selektive Datenauswahl zustande gekommen. Zweitens würden bei 11,9 Millionen Fahrgästen pro Tag im Schnitt 11 900 Menschen von der Software fälschlicherweise als terrorverdächtige »Gefährder« eingestuft – zumindest für den Fall, dass alle deutschen Bahnhöfe mit einer entsprechenden Gesichtserkennung ausgestattet würden.

Das Bundesinnenministerium verkündete dennoch: »Die Systeme haben sich in beeindruckender Weise bewährt, sodass eine breite Einführung möglich ist.« Zwar werden die Spezialkameras an Bahnsteigen derzeit nur eingesetzt, um Gefahrensituationen zu erkennen. Doch die Versuchung ist groß. »Wir haben Angst, dass KI einen Überwachungsstaat ganz anderer Qualität ermöglichen könnte«, sagt EU-Abteilungsleiter Kilian Gross – und meint explizit auch Europa.

Verstärkt werden diese Sorgen durch ein weiteres Potenzial der Gesichtserkennung: das Aufspüren von Eigenschaften. »Eines der großen, sehr relevanten Felder in der KI-Entwicklung ist es, mit Wahrscheinlichkeitsverfahren aus unauffälligen Datenquellen weitreichende Folgerungen zu ziehen, etwa aus einem Gesicht die



Antonio Krüger

ist Geschäftsführer des Deutschen Forschungszentrums für Künstliche Intelligenz. Als Leiter des Forschungsbereichs Kognitive Assistenzsysteme entwickelt er außerdem Wege, wie Menschen mittels Sprache, Gestik, Mimik oder Berührungen mit smarten Algorithmen interagieren können.

sexuelle Orientierung herauszulesen«, sagt Thilo Hagendorff, KI-Ethiker an der Universität Tübingen (siehe Kasten Seite 28). »Einen solchen Einsatz fände ich sehr riskant.« Derartige Gesichtsanalysetools könnten beispielsweise zur Erpressung von Menschen eingesetzt werden, die sich nicht als homosexuell outen wollen – oder Regierungen helfen, sexuelle Minderheiten zu verfolgen.

Auf die Spitze getrieben wird der KI-Missbrauch von Gesichtsdaten durch sogenannte Deepfakes (P.M. 09/2020). Es gibt heute schon simple Apps dafür, Menschen Sätze in den Mund zu legen, ihre Gesichter in Filmszenen einzufügen oder sogar in Sexvideos zu montieren. Doch bisher war meist leicht zu erkennen, dass es sich um eine Fälschung handelte. Was aber, wenn KI-Systeme die Bewegungen und die Aussprache eines Politikers, einer Politikerin so perfekt imitieren können, dass glaubhafte Videos entstehen – etwa von einer Kriegserklärung oder einer angeblichen Sex-Eskapade? Und wenn die für die Fälschung Verantwortlichen ebenfalls dank maschinellem Lernen in den Lage sind, ihre digitalen Spuren zu verwischen? Anfang 2021 kursierte im Internet ein Deepfake-Video, das den Schauspieler Tom Cruise überzeugend echt zeigte – und sich als komplettes KI-Werk entpuppte.

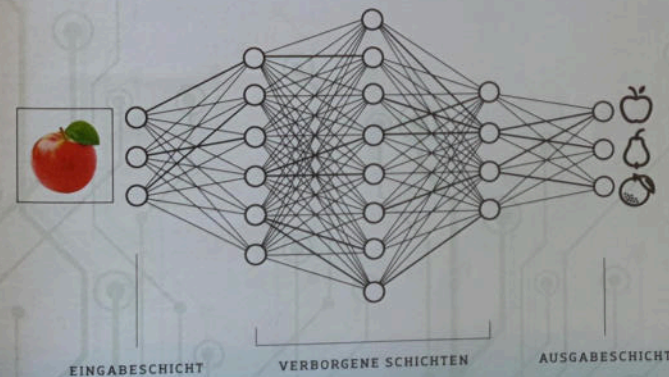
»KI verschärft die Bedrohung durch Cyberangriffe und Desinformationskampagnen, die Russland, China und andere staatliche und nicht-staatliche Akteure nutzen«, heißt es in einem »

MEDIZIN

- 1 Mit »CardioCloud« lässt sich daheim ein Elektrokardiogramm aufzeichnen. Algorithmen suchen in den Kurven der Herzaktivität nach Mustern, die auf Erkrankungen hindeuten.
- 2 Das Projekt »Ophthalmic-AI« hat zum Ziel, bei Augenleiden die individuell beste Therapie zu finden. Ärztin und Algorithmus sind dabei ein Team.
- 3 Eine KI identifiziert auf CT-Scans Läsionen der Lunge, verursacht durch Covid-19-Infektionen.

Nervenzellen im Gehirn orientiert. Eine immer schnellere Datenverarbeitung und enorm gewachsene Speicherkapazitäten befähigen die künstliche Intelligenz nun zu neuen Höchstleistungen.

Die Fähigkeit von KIs, enorme Datenmengen zu sammeln, zusammenzuführen und auszuwerten, verschafft einigen wenigen Akteuren einen enormen Wissensvorsprung. Es mag sich harmlos anfühlen, am Rechner zu sitzen und auf der Website eines Onlinehändlers nach Kleidung zu suchen. Doch durch die Summe aller Klicks entstehen Profile – von Individuen, Gruppen, Gesellschaften. Im Onlinehandel »ist KI entlang der gesamten Lieferkette im Spiel«, sagt DFKI-Direktor Antonio Krüger. Sie analysiert das Verhalten beim



Vernetzte Blackbox

MASCHINELLES LERNEN Um beispielsweise ein Objekt (Apfel) auf einem Foto zu identifizieren, durchlaufen die Bildinformationen in einem künstlichen neuronalen Netz mehrere Verarbeitungsschichten, bis das Objekt in eine vorgegebene Kategorie (Apfel, Birne, Orange) eingeordnet wird. Die Knotenpunkte entsprechen mathematischen Formeln; sie werden in einem Trainingsprozess so lange angepasst, bis das Netz Äpfel, Birnen und Orangen zuverlässig erkennt. Welche Merkmale es dazu nutzt, bleibt in der Regel unklar.