RUBIKON

Samstag, 28. Mai 2022, 15:57 Uhr
~11 Minuten Lesezeit

Albtraum „Künstliche Intelligenz“

KI-gestützte Systeme werden als Lösung aller gesellschaftlichen Probleme angepriesen, doch sie dürften uns unfreier machen denn je. Teil 1/2.

von Simone Hörrlein
Foto: cigdem/Shutterstock.com

Manche Menschen sind der Meinung, Künstliche Intelligenz (KI) werde unser aller Leben verbessern. Selbstfahrende Autos würden schon bald die Sicherheit im Straßenverkehr erhöhen, Logistik würde sicherer, schneller und verlässlicher, und auch der Traum von intelligenten Städten könne Realität werden. Andere dagegen sind fest davon überzeugt, dass KI sämtliche Arbeitsplätze Schritt für Schritt wegrationalisieren und uns alle zu Bittstellern eines wie auch immer gearteten Grundeinkommens machen wird. Wieder

andere glauben, KI sei Zukunftsmusik, eine Technologie, die noch lange nicht marktreif sei und sie deshalb nicht beträfe. Während die ersten beiden Gruppen zumindest im Ansatz recht haben, liegt die dritte leider voll daneben. Die KI, die für die meisten Menschen eine Blackbox ist und dies auch für immer bleiben wird, ist nicht nur längst unter uns, sie wird auch immer übergriffiger und ist deshalb brandgefährlich: für unsere Freiheitsrechte, unsere Privatsphäre, unsere körperliche Integrität und letztlich sogar für unser physisches Leben.

Nur wer versteht, was KI ist und wie sie eingesetzt werden soll, ist in der Lage, sich gegen die geplanten Übergriffe durch diese Art von Technologie zu wehren. Was also ist KI? Es gibt unterschiedliche Definitionen, aber immer geht es darum, etwas zu programmieren, zu konstruieren und zu bauen, das „intelligent" reagiert oder sich wie „ein Mensch" verhält.

Und genau hier liegt der Denkfehler: Denn egal wie raffiniert ein Algorithmus auch sein mag, er wird sich niemals wie ein Mensch verhalten können. Selbst anspruchsvolle KIs, die auf neuronalen Netzen basieren oder visuelle Reize ähnlich wie Hirnzellen verarbeiten sollen, werden niemals menschlich handeln können.

Denn Menschen sind keine rationalen Wesen, sie besitzen zwar einen logischen Verstand, werden aber unbewusst von Gefühlen und Emotionen gesteuert. Daniel Kahnemann, der 2002 für seine Arbeiten zur Psychologie des Urteilsvermögens und der Entscheidungsfindung sowie zur Verhaltensökonomie mit dem Nobelpreis für Wirtschaftswissenschaften ausgezeichnet wurde, hat

die Mähr vom *Homo oeconomicus*, also dem rein rational entscheidenden Individuum, ein für alle Mal ad acta gelegt.

Der Mensch entscheidet nicht rein rational, wie KI dies tut, er agiert und reagiert fast ausschließlich emotional. Nichts durchdringt die Pforten der Wahrnehmung, was nicht zuvor die limbischen Strukturen passiert hat, um dort emotional aufgeladen zu werden. Und nur das, was als emotional relevant angesehen wird, schafft es schließlich in unsere Aufmerksamkeit. Die Tatsache, dass Entscheidungen im Gehirn weitgehend unbewusst und immer emotional fallen, werden heute bereits im Neuromarketing erfolgreich genutzt.

> ***Dass KI den Menschen ersetzen kann, ist also ausgemachter Blödsinn, eine perfide Manipulation, die dazu genutzt wird, uns glauben zu machen, KI wäre uns überlegen.***

Wer dies glaubt, kann allzu leicht dazu gebracht werden, die Kontrolle an eine scheinbar „allwissende“ KI abzugeben, was angesichts der aktuellen Entwicklungen fatal wäre. Denn in einer Welt, in der Maschinen als allwissend und dem Menschen überlegen eingestuft werden, sterben das eigene Denken, die Skepsis und jede Art von freier Entscheidung.

Patentierter Datendiebstahl

Leider wird allzu oft verschwiegen, dass es KI ohne riesige Mengen von Daten nicht gäbe und dass sie mit dem, was wir unter Intelligenz verstehen, rein gar nichts zu tun hat. KI benötigt *Big Data* und wie ein Artikel auf der Website ***Biometric Update*** (https://www.biometricupdate.com/202203/clearview-ai-makes-face-biometrics-service-available-to-ukraine-ministry-of-defense) zeigt, bemächtigen sich KI-Technologien bereits — ohne

Konsequenzen fürchten zu müssen — privater Daten. Der Artikel „Clearview AI makes face biometrics service available to Ukraine Ministry of Defense“ (deutsch: Clearview AI stellt dem ukrainischen Verteidigungsministerium einen biometrischen Gesichtserkennungsdienst zur Verfügung) zeigt das wahre Ausmaß der illegalen Datensammelwut.

Im Artikel kündigt die Firma **Clearview AI** (https://www.clearview.ai) (Clearview) an, ihre biometrische App, der eine Datenbank mit Milliarden Fotos von Internetnutzern zugrunde liegt, dem ukrainischen Verteidigungsministerium kostenlos zur Verfügung zu stellen. Mehr als zwei Milliarden der über 10 Milliarden Fotos von Internetnutzern sollen dabei von der russischen Social-Media-Website VK*ontakte* stammen.

Dass die Menschen, die im Netz so sorglos ihre Bilder teilen, Clearview die Genehmigung erteilt haben, diese in einer riesigen Datenbank zu speichern und sie wahllos an jedermann zu verteilen, bezweifle ich stark. Was ich aber nicht bezweifle, ist, dass das US-Unternehmen wohl auch sämtlich Fotos aus den europäischen Sozialen Medien rechtswidrig in seiner Datenbank abgelegt hat und von seiner KI verwalten lässt.

Der Mitbegründer der Firma, Hoan Ton-That, ein autodidaktischer Software-Programmierer vietnamesischer und australischer Abstammung, schlug zudem vor, dass die App auch zur Identifizierung russischer Agenten genutzt werden könne. Das ist schon deshalb höchstgefährlich, weil in einem Krieg jeder wie auch immer geartete Gegner zu einem Agenten degradiert werden kann. Wer zu den Guten und wer zu den Bösen zählt, entscheiden einige wenige. Und was mit denjenigen geschieht, die sie als Böse erkannt haben wollen, ist aus der Historie hinlänglich bekannt.

Wer glaubt, KI wäre nur dazu da, unser Leben einfacher und besser zu gestalten, der wird spätestens jetzt eines Besseren belehrt.

> ***Eine Technologie, die es ermöglicht, private Daten eines Menschen — ohne dessen Wissen — in Datenbanken zu speichern und Menschen bei Bedarf willkürlich als Feinde zu definieren, ist nicht nur unverantwortlich, sie ist auch in höchstem Maße gefährlich.***

Die zivilgesellschaftliche Gruppe *Surveillance Technology Oversight Project* weist in obigem Artikel darauf hin, dass auf dem Schlachtfeld eingesetzte Technologien missbraucht werden können. Ich gehe sogar noch einen Schritt weiter und sage, dass die Kriegspropaganda sie mit an Sicherheit grenzender Wahrscheinlichkeit missbrauchen wird.

Weshalb die Gründer dieses Unternehmens nicht längst hinter Schloss und Riegel sitzen, ihr Laden geschlossen und ihre illegalen Datenbanken gelöscht wurden, ist ein Rätsel. Schließlich sieht sich Clearview schon länger mit Vorwürfen der Massenüberwachung und der Verletzung der Geschäftsbedingungen von sozialen Netzwerken wie Twitter sowie der Privatsphäre der Nutzer konfrontiert.

Trotz dieser Vorwürfe wurden die Datendiebe von Clearview am 15. Februar 2022 sogar noch mit dem **Patent** (https://www.freepatentsonline.com/11250266.pdf) für „Methods for Providing Information About a Person Based on Facial Recognition“ (deutsch: Verfahren zur Bereitstellung von Informationen über eine Person auf der Grundlage von Gesichtserkennung) belohnt.

Und das, obwohl das Patent ein System zur Anwendung von Gesichtserkennung beschreibt, dessen Informationen aus dem öffentlichen Internet stammen. Die US-Firma nutzt persönliche Daten von Menschen, ohne deren Einwilligung eingeholt zu haben, und verkauft diese, ebenfalls ohne Einwilligung, an Strafverfolgungsbehörden und andere Institutionen. Es ist ein

Skandal, dass ein derartiges Produkt auch noch patentiert wird.

Der Kommentar des Geschäftsführers Hoan Ton-That ist eine Farce: „Diese Auszeichnung ist mehr als ein Schutz des geistigen Eigentums; sie ist eine klare Anerkennung der technologischen Innovation von Clearview AI in der Branche der künstlichen Intelligenz."

Eine KI, die die Welt verändert

Doch Clearviews Projekt erscheint noch harmlos im Vergleich zu der autonomen KI des in Israel beheimateten Unternehmens **Cortica** (https://www.cortica.com). Der Geschäftsführer Igal Raichelgauz begann seine Karriere in einer Eliteeinheit des Nachrichtendienstes der *Israel Defence Forces* (IDF), weshalb es auch nicht verwunderlich ist, dass sich unter Corticas Mitarbeitern, neben führenden KI-Forschern, auch *zahlreiche Veteranen der israelischen Eliteeinheiten des Militärgeheimdienstes* befinden.

Der KI, die die Welt verändern soll, liegen viele Jahre firmeneigener Forschung an Teilen eines Rattenhirns zugrunde. Denn die KI, so das Unternehmen, sei der Neuronenaktivität und den Lernmechanismen des Säugergehirns nachempfunden. Die Überlegenheit der KI beruhe darauf, dass sie zur visuellen Datenverarbeitung nicht die Konzepte bisheriger *Deep Learning Systeme* nutze, sondern den gleichen Prozess wie das menschliche Gehirn. Aus diesem Grunde könne die KI, die durch 200 Patente abgesichert ist, nicht nur Konzepte und Kontexte verstehen, sondern daraus auch Schlussfolgerungen ziehen.

Bisher wurde die KI vor allem für die Steuerung autonomer Autos oder für die Vorhersage von komplexen Systemen wie dem Wetter beworben, doch in der „*Neuen Normalität*" soll sie auch in der

Videoüberwachung zum Einsatz kommen. Das erste Projekt dieser Art läuft seit 2017 in Indien. In einer Partnerschaft mit der **Best Group** (https://www.digitaltrends.com/cool-tech/could-ai-based-surveillance-predict-crime-before-it-happens/) analysiert die Cortica-KI die Daten sämtlicher CCTV-Kameras im öffentlichen Raum. Im Jahr 2018 gab Cortica öffentlich bekannt, seine KI könne — ganz im Stil des Science Fiction Streifens *Minority* Report — Verbrechen vereiteln, noch bevor diese verübt würden.

Dieser im Fachjargon als *Predictive Crime* bezeichnete Ansatz wird weltweit zwar schon länger in diversen Pilotprojekten getestet, doch Corticas Technologie ist ausgefeilter, weil sie sich auf den Menschen an sich fokussiert. So will die KI potenzielle Verbrecher durch sogenannte Verhaltensanomalien in der Mikromimik ausfindig machen.

Die verräterischen Zeichen, die darauf *hindeuten könnten*, dass eine Person im Begriff sei, ein Gewaltverbrechen zu begehen, sind so winzig, dass sie nur vom unbestechlichen Auge einer KI erkannt werden können, erklärt das Unternehmen. Die Software soll aber nicht nur Verhaltensunterschiede zwischen gesetzestreuen Bürgern und möglichen Kriminellen erkennen, sie soll auch zwischen einem friedlichen, überfüllten Markt und einer politischen Demonstration, die gewalttätig zu werden droht, unterscheiden können.

Wohin führen uns derartige Ansätze?

> ***Wollen wir die Überwachung des öffentlichen Raumes tatsächlich einer Software überlassen, deren Programmierung wir nicht kennen und deren Lernprozesse und Entscheidungen wir nicht nachvollziehen können?***

Wollen wir die Absichten eines komplexen Wesens wie dem Menschen von einem, im Vergleich zu uns, primitiven Algorithmus

einschätzen lassen? Und wie wollen wir uns gegen mögliche Anschuldigungen wehren, wenn eine KI erst einmal als allwissend und unfehlbar eingestuft wurde?

Was, wenn ein totalitäres Regime ein solches System missbraucht, um abweichende Meinungen zu unterdrücken und Menschen zu verhaften, bevor diese überhaupt die Möglichkeit hatten, einen Protest zu organisieren?

Wem derart dystopische Aussichten nicht schon gruselig genug erscheinen, für den hat Cortica noch ein weiteres Anwendungsbeispiel parat: Die KI könnte in Zukunft in autonomen Taxen das Verhalten von Fahrgästen überwachen, um potenziell gefährliche Situation zu erkennen und die Strafverfolgung einzusetzen, bevor Menschenleben verloren gingen.

Sie hatten einen schlechten Tag, sind wütend auf ihren Partner oder ihren Boss? In diesem Fall begeben sie sich in Zukunft besser nicht in den öffentlichen Raum, vermeiden sie die Nutzung eines Taxis oder verbergen sie zumindest ihr Gesicht vor dem allsehenden Auge der KI. Denn die kleinste Muskelzuckung in ihrem Gesicht, die etwa Wut, Ärger oder vielleicht sogar Hass ausdrückt, könnte dazu führen, dass sie als Gefahr für die Allgemeinheit identifiziert und präventiv festgenommen werden.

Eine KI für das Maskenzeitalter

Wie weit KI auf Abwege geraten kann, zeigt das Beispiel **Corsight AI** (https://www.corsight.ai/) (Corsight). Das 2019 in Tel Aviv gegründete Privatunternehmen ist eine Tochtergesellschaft der Firma Cortica. Im **Beirat des Unternehmens** (https://ist-security.com/ist-wp/wp-content/uploads/2020/10/Corsight-Deck-2020Rev1.pdf) sitzen der ehemalige CIA-Direktor James

Woolsey und der ehemalige stellvertretende FBI-Direktor Oliver Revell.

Die ebenfalls auf Gesichtserkennung spezialisierte autonome **KI Fortify** (https://www.corsight.ai/product-fortify/) zeichnet sich dadurch aus, dass sie auch unter schwierigen Verhältnissen valide Ergebnisse liefern soll. Menschenmengen, schlechte Lichtverhältnisse und teilweise verdeckte Gesichter sollen für Fortify keine Probleme darstellen.

Aus diesem Grunde bewirbt das Unternehmen das Werkzeug auch explizit zur Überwachung von Pandemiemaßnahmen:

„*Wir leben in einer beispiellosen Zeit mit neuen sozialen Normen und Herausforderungen. Da Gesichtsmasken allgegenwärtig werden, sind neuartige Lösungen erforderlich, um Sicherheitsstandards aufrechtzuerhalten.*“

Um diese Sicherheitsstandards — ein Euphemismus für totale Kontrolle — aufrechtzuerhalten, soll Fortify die Einhaltung aller Quarantäneanordnungen überwachen. Dazu prüft die Software, ob Menschen Maske tragen, in Bereichen, in denen dies gefordert ist; sie stellt fest, ob Menschen Fieber haben; überwacht berührungslose Zugangskontrollen in bestimmten Einrichtungen, die Einhaltung von Abstandsregelungen sowie die Rückverfolgung von Kontakten zur Sicherung von Arbeitsplätzen und zur Verhinderung der Verbreitung von Infektionen. Würde beispielsweise eine die Sicherheit bedrohende Person erkannt, die die Maske nicht korrekt trägt, könne Fortify eine Warnmeldung in Echtzeit ausgeben.

Das „DNA to Face“-Projekt

Doch bei konventioneller Gesichtserkennung soll es nicht bleiben. Wie aus einer Präsentation für die ***Imperial Capital Investors Conference 2021*** (http://imperialcapital-sic.com/2021/) hervorgeht, arbeitet das Unternehmen an einem Projekt, das es als „*DNA to Face*“ bezeichnet. Wie der ***MIT Technology Review*** (https://www.technologyreview.com/2022/01/31/1044576/corsight-face-recognition-from-dna/) berichtete, wird bei diesem Ansatz nicht das Gesicht eines Menschen zur Identifizierung herangezogen, sondern sein Erbmaterial, seine DNA.

Anhand der individuellen DNA soll ein Modell des Gesichts erstellt werden, welches anschließend mit einer Gesichtserkennungssoftware auf KI-Basis das physische Pendant aus einer Datenbank herausfiltert. Zusätzlich zu „DNA to Face“ umfasst die **Produkt-Roadmap** (https://www.renovisionfund.com/uncategorized/this-company-says-its-developing-a-system-that-can-recognize-your-face-from-just-your-dna/) auch noch die Gangbiometrie sowie auf Stimmerkennung basierende Gesichtsmerkmale, welche die Gesichtserkennungsfähigkeiten der KI noch erweitern sollen.

Nach aktuellem Wissensstand ist eine zweifelsfreie Gesichtserkennung über die individuelle DNA zwar noch nicht möglich, denn die verschiedenen Verfahren zur Phänotypisierung — die Untersuchung der Gene, die für die äußeren Merkmale eines Individuums verantwortlich sind- lassen bisher nur auf Abstammung und Geschlecht schließen und können mit einer bestimmten Wahrscheinlichkeit Augen-, Haar- und Hautfarbe ermitteln.

Ob eine valide Gesichtsrekonstruktion anhand des Erbgutes jemals möglich sein wird, steht in den Sternen, doch es wird mit Hochdruck an der Realisierung dieser Idee gearbeitet. Der Bürgerrechtsanwalt und Geschäftsführer des *Surveillance Technology Oversight Project* (STOP), Albert Fox Cahn, bezeichnet

die Idee als „Pseudowissenschaft." Doch wie die Coronakrise gezeigt hat, sollte dies kein Grund sein, uns diese Technik – wenn nötig – als absolut seriöse Wissenschaft zu verkaufen.

Derartige Verfahren sollen in Zukunft weitreichend genutzt werden. Dafür spricht auch, dass in Deutschland relevante Gesetze zu diesem Thema bereits geändert wurden. Die DNA-Phänotypisierung war bis Ende 2019 in Deutschland aufgrund rechtlicher Beschränkungen in der Strafprozessordnung (StPO) verboten. Im Jahr 2018 wurde die forensische DNA-Analyse durch den **Koalitionsvertrag** (https://archiv.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1) erweitert: „Die DNA-Analyse wird im Strafverfahren auf äußerliche Merkmale (Haar, Augen, Hautfarbe) sowie Alter ausgeweitet (Paragraf 81e StPO)." Am 15. November 2019 vom Bundestag verabschiedet, trat die Änderung am 12. Dezember 2019 in Kraft.

Der **Paragraf 81e StPO Absatz 2, Satz 2** (https://www.gesetze-im-%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20internet.de/stpo/__81e.html) lautet nun wie folgt:

„Ist unbekannt, von welcher Person das Spurenmaterial stammt, dürfen zusätzlich Feststellungen über die Augen-, Haar- und Hautfarbe sowie das Alter der Person getroffen werden."

In Bayern ist sogar erlaubt, mittels Phänotypisierung die biogeografische Herkunft zu ermitteln.

Es wurden also gerade zur rechten Zeit die notwendigen Gesetze geändert, um eine Gesichtserkennung mittels DNA später auch Schritt für Schritt auf unbescholtene Bürger auszuweiten. Denn wer ein potenzieller Straftäter sein könnte, entscheidet vielleicht schon

bald nicht mehr ein Mensch, sondern ein „selbstlernender“ Algorithmus.

Redaktionelle Anmerkung: Dieser Text erschien am 23. Mai 2022 unter dem Titel „**Albtraum ‚Künstliche Intelligenz‘ — Teil 1** (https://www.nomonoma.de/albtraum-kuenstliche-intelligenz-teil-1/)“ im Blog ***NomoNoma*** (https://www.nomonoma.de/).

Simone Hörrlein ist Lebensmittelchemikerin und Wissenschaftsjournalistin. Nach ihrem Studium an der **TU München** war sie mehrere Jahre in der medizinischen Forschung tätig und arbeitete zuletzt in der Wissenschaftskommunikation des **Kompetenzzentrums für Ernährung**. Neben den Naturwissenschaften interessiert sie sich für Finanz- und Geopolitik. Aktuell lebt sie in Kanada.