2021/28 dschungel

https://www.jungle.world/artikel/2021/28/maskerade-vor-der-kamera

Ein Gespräch mit Roland Meyer über Diskriminierung durch die Praxis der digitalen Gesichtserkennung

»Maskerade vor der Kamera«

Interview Von **Till Schmidt**

Automatisierte Verfahren zur Gesichtserkennung begünstigen Diskriminierung. Der Medientheoretiker Roland Meyer warnt vor der Voreingenommenheit des Algorithmus und fordert, den Einsatz biometrischer Identifizierung einzuschränken.

Digitale Techniken der Gesichtserkennung haben eine Vorgeschichte, die bis in die Physiognomik im 18. Jahrhundert zurückreicht. Oft ging es darum, vom Äußeren eines Menschen Hinweise auf Neigungen zu kriminellem Verhalten abzulesen. Seit wann wurde die Gesichtserkennung automatisiert?

Die ersten Versuche hierzu sind schon sehr alt. So wurde bereits 1970 bei der Weltausstellung in Osaka erstmals etwas gezeigt, was der automatisierten Gesichtserkennung ähnelt. Damals wurde versucht, auf dem Rechner einzelne Gesichtsmerkmale zu vergleichen: Augenabstände, Mundwinkel und so weiter. Um 1990 - begann man dann, nicht mehr Gesichtszüge zu vermessen, sondern Helligkeitsverteilungen im gesamten Gesicht zu erfassen. Damit wurden nicht mehr anatomische Merkmale von Gesichtern verglichen, sondern visuelle Eigenschaften von Bildern. Das hat sich als recht erfolgreich erwiesen: In den neunziger Jahren begannen kommerzielle Unternehmen damit, diese Technologie erstmals für die Polizei, Casinos und sogar Privatleute anzubieten. Nach 9/11 witterten diese Firmen dann das enorme Marktpotential und versuchten, automatisierte Gesichtserkennung mit massiver staatlicher Unterstützung an Flughäfen und Grenzübergängen durchzusetzen.

Der Gesichtserkennung liegt immer eine bestimmte Vorstellung zugrunde, was ein Gesicht ist, woraus es besteht und was man daran messen kann. Kann eine solche Normierung gesellschaftliche Vielfalt überhaupt angemessen berücksichtigen?

Lange Zeit war Gesichtserkennung auf standardisierte Bilder angewiesen, auf denen das Gesicht frontal in die Kamera schaut. Doch heutige Verfahren sind immer besser in der Lage, Gesichter zu erkennen, die in the wild, also unter beliebigen, unkontrollierten

Alltagsbedingungen aufgenommen wurden. Dafür werden künstliche neuronale Netze an riesigen Bildermengen aus dem Internet trainiert, an denen sie selbständig lernen sollen, ein und dasselbe Gesicht in unterschiedlichen Posen und Perspektiven wiederzuerkennen.

> »Insgesamt birgt Gesichtserkennung ein enormes Gefahrenpotential – wenn sie funktioniert, aber mehr noch, wenn sie nur schlecht und fehlerhaft funktioniert. Die Bewegung Reclaim Your Face setzt sich daher europaweit für ein Verbot der Technologie ein.«

Doch dabei erkennen sie nie alle Gesichter gleich gut – Männer werden in der Regel besser erkannt als Frauen, weiße Gesichter besser als die von people of color, junge besser als ältere. Das allerdings war von Anfang an so. Schon die ersten Versuche in den siebziger Jahren setzten eine bestimmte Art von Gesicht voraus und scheiterten an Gesichtern, die nicht dieser Norm entsprachen. Daran hat sich, trotz aller Entwicklung der Technologie, im Prinzip nichts geändert.

Können Sie das genauer erläutern?

Bei den neueren Verfahren, die auf machine learning basieren, wird zwar nicht mehr, wie noch in den Anfängen, ein vermeintliches Normalgesicht in die Software einprogrammiert, sondern die Software bestimmt die Kriterien, an denen sie ein Gesicht erkennt, auf Basis der beim Training verwendeten Bilder. Doch viele dieser Trainingsdatensätze bestanden noch bis vor kurzem ganz überwiegend aus Bildern weißer Männer, und das führt zu entsprechenden Diskriminierungen.
Wäre dieser algorithmic bias, also die algorithmische Voreingenommenheit, allein ein Produkt der Bilddatensätze, ließe er sich verhältnismäßig einfach beseitigen – aber das scheint nicht der Fall zu sein. Der algorithmic bias erweist sich vielmehr als sehr hartnäckiges Problem. Ein Grund dafür mag darin liegen, dass maschinelles Lernen kein vollständig automatisierter Prozess ist. Es sind Menschen, die in den Computerlaboren die Technologien entwickeln und deren Normalitätsvorstellungen sich dabei in die Software einschreiben – und ganz überwiegend sind das junge, männliche, entweder weiße oder asiatische Programmierer.

Was sind die Folgen?

Für die USA sind inzwischen mehrere Fälle dokumentiert, in denen Schwarze irrtümlicherweise verhaftet wurden – aufgrund einer falschen Identifizierung durch Gesichtserkennungssoftware. Mir stellt sich dabei vor allem die Frage, wie im Zuge polizeilicher Ermittlungen mit den Unzulänglichkeiten der Software umgegangen wird. Nicht selten, so scheint mir, werden deren diskriminierende Effekte in der polizeilichen Anwendung noch verschärft – und umgekehrt wird polizeiliche Diskriminierung durch die Software technisch objektiviert und unsichtbar gemacht. Das ist allerdings kaum empirisch erforscht, und insbesondere für den deutschen Kontext gibt es meines Wissens keine Untersuchung darüber, wie und mit welchen Effekten Gesichtserkennungssoftware im Polizeialltag eingesetzt wird.

Welche Verzerrungen ergeben sich in Bezug auf das Geschlecht?

Fast alle diese Programme bestimmen auch das Geschlecht einer Person – und obwohl sie dabei mit Wahrscheinlichkeiten operieren, steht am Ende immer eine binäre Zuweisung: weiblich oder männlich. Damit sind alle nichtbinären Optionen ausgeschlossen, was notwendigerweise zu misgendering führt. Zudem erkennt die Software Weiblichkeit häufig an stereotypen Mustern, die sie aus den Bildern ableitet, mit denen sie trainiert wurde, die aber nichts über die Geschlechtsidentität einer Person aussagen. So interpretiert die Software ein Gesicht, das stärker lächelt, eher als weiblich. Im Umkehrschluss kann das unter bestimmten Umständen einen Druck erzeugen, sich nach diesen Mustern zu richten und sich mimisch entsprechend zu verhalten. Vor der Kamera wird dann buchstäblich »Weiblichkeit als Maskerade« performt.

In automatisierten Auswertungen von Online-Bewerbungsgesprächen etwa wird die Gesichtsanalyse inzwischen eingesetzt, um Persönlichkeitsprofile zu erstellen. Ebenso dienen solche Programme dazu, um bei Online-Prüfungen Studierende vom Schummeln abzuhalten. Abgesehen von den mehr als fragwürdigen Vorannahmen, die dabei gemacht werden, lässt sich nachweisen, dass insbesondere women of color von diesen Systemen erheblich benachteiligt werden und großen Aufwand betreiben müssen, damit ihr Gesicht überhaupt von der Software erkannt wird. Und auch hier ist zu beobachten, wie die Einschreibung von kulturellen Normen in solche Technologien das mimische Verhalten standardisiert. In Korea zum Beispiel gibt es schon Kurse für die Vorbereitung auf Online-Bewerbungsgespräche, um vor der Maschine möglichst vertrauenerweckend zu wirken.

Ein weitere Gefahr ist der Einsatz der Technologie zur Repression gegen politisch Missliebige.

Insgesamt birgt Gesichtserkennung ein enormes Gefahrenpotential – wenn sie funktioniert, aber mehr noch, wenn sie nur schlecht und fehlerhaft funktioniert. Die Bewegung Reclaim Your Face setzt sich daher europaweit für ein Verbot der Technologie ein. Insgesamt lässt sich ein wachsendes politisches Bewusstsein für die aus der Gesichtserkennung resultierenden Gefahren feststellen. Das wird auch ablesbar am aktuellen Vorschlag der EU-Kommission zur Regulierung von künstlicher Intelligenz. Der sieht zwar eine Reihe von Ausnahmeregelungen vor, will aber zumindest die besonders fehler- und missbrauchsanfällige Echtzeitgesichtserkennung im öffentlichen Raum einschränken. Und je mehr öffentlicher Druck entsteht, umso mehr ist die Politik gezwungen, nicht alles, was möglich wäre, auch zu erlauben. Die Entwicklungen in Russland, wo Demonstrationen mit Hilfe von Gesichtserkennung unterdrückt werden, oder China, wo sie eingesetzt wird, um die uigurische Minderheit zu verfolgen, könnten dabei als abschreckendes Beispiel dienen.

Welche Anzeichen für einen kritischeren Umgang mit Überwachungstechnologien sehen Sie?

Es gab 2018 einen Pilotversuch mit Echtzeitgesichtserkennung am Südkreuz in Berlin, der nach Aussage des Bundesinnenministers ein Riesenerfolg, nach Prüfung des Chaos Computer Clubs ein ziemlicher Fehlschlag war. Bemerkenswert finde ich, dass seither in Deutschland kein weiterer Vorstoß in diese Richtung unternommen wurde – wohl auch, um die allgemeine Akzeptanz von Videoüberwachung nicht zu gefährden. In Bezug auf den

nachträglichen Einsatz von Gesichtserkennung, wie das etwa bei Ermittlungen wegen der Proteste gegen den G20-Gipfel in Hamburg geschehen ist, gibt es aber wenig Regulierungsbemühungen.

Es handelt sich schlicht um eine Hochrisikotechnologie. Daher plädiere ich auch für ein Verbot oder zumindest ein Moratorium, damit wir erst mal eine Debatte führen können: Was kann diese Technologie, was sind ihre Risiken? Bislang wird Gesichtserkennung als Black Box behandelt, über deren Funktionsweise und Verwendung man fast nichts weiß. Es darf nicht sein, dass sie auf so vielen Ebenen schleichend implementiert wird – ohne gesellschaftliche Kontrolle.

Die Polizei ist in Deutschland primär Sache der Bundesländer. Was kann hier getan werden?

Es ist ermutigend zu sehen, dass es in den USA gerade die lokale Gesetzgebung ist, die voranschreitet. Auf Bundesebene gibt da noch keine Regulierung, trotz starker Stimmen, die das fordern. Aber ausgerechnet in der Tech-Metropole San Francisco gibt es ein Verbot des Einsatzes von Gesichtserkennung durch Polizei und öffentliche Behörden. Und in Deutschland ermittelt jetzt der Landesdatenschutzbeauftragte von Baden-Württemberg gegen Clearview AI und Pim Eyes, zwei global agierende Unternehmen, die massenhaft Bilder aus sozialen Medien zur Gesichtserkennung nutzen, ohne dass die Betroffen eingewilligt hätten. Da zeigt sich, dass lokale Initiativen durchaus etwas bewegen können.

Roland Meyer: Gesichtserkennung. Wagenbach-Verlag, Berlin 2021, 80 Seiten, 10 Euro