2018/33 Networld

https://jungle.world/artikel/2018/33/die-im-dunkeln-sieht-man-doch

Gesichtserkennungsprogramme sind keineswegs zuverlässig, aber auch nicht immer problematisch

Die im Dunkeln sieht man doch

Von **Enno Park**

Der Präsident und Justiziar von Microsoft, Brad Smith, warnte in einem bemerkenswerten Aufruf vor der automatischen Gesichtserkennung. Diese gefährde Grundrechte und müsse reguliert werden. Von Staaten ist eher Gegenteiliges zu erwarten.

Langsam ist die Gesichtserkennung im Alltag angekommen. Facebook hat sein seit Jahren existierendes entsprechendes Feature auch für europäische Nutzer freigeschaltet. Das derzeit neueste iPhone wird nicht mehr durch Fingerabdruck entsperrt, sondern per Blick aufs Display. Bei den olympischen Spielen 2020 in Tokio soll ein entsprechendes System benutzt werden, um Athleten, Presseleute und Mitarbeiter zu identifizieren, die bestimmte Bereiche betreten dürfen. Das Medienunternehmen Live Nation, zu dem auch der Dienstleister Ticketmaster gehört, kaufte das auf Gesichtserkennung spezialisierte Unternehmen Blink Identity, um Konzertbesucher künftig beim Einlass anhand ihres Gesichts zu kontrollieren, statt mit Hilfe eines vorgezeigten Tickets.

Begehrlichkeiten weckt diese Technologie schon lange auch bei Ermittlungsbehörden zahlreicher Länder. So benutzte die US-Polizei nach dem Amoklauf in der Redaktion der *Capital Gazette* in Annapolis, Maryland, im Juni Gesichtserkennungssoftware, um den Todesschützen zu identifizieren. Das FBI soll Fotos von 117 Millionen US-Amerikanern gespeichert haben.

In China verwenden Polizisten Datenbrillen, um gesuchte Personen zu erkennen und aus der Menge zu fischen. Auch in Deutschland wird automatische Gesichtserkennung eingesetzt: **Die Hamburger Polizei benutzte sie, um nach dem G20-Gipfel** mögliche Straftäter auf vorliegendem Bild- und Videomaterial zu identifizieren. **Am Berliner Bahnhof Südkreuz** wurde monatelang ein System zur **Gesichtserkennung** getestet. Das Argument für die Totalüberwachung lautet meistens: Attentäter wie Anis Amri sollen sich nicht mehr unerkannt in der Öffentlichkeit bewegen können.

> Zur Gesichtserkennung soll die Verhaltenskontrolle hinzukommen. Daran wird 2009-2014 im EU-Forschungsprojekt Indect gearbeitet.

Da scheint der **Aufruf von Brad Smith, Präsident und oberster Jurist von Microsoft,** zum richtigen Zeitpunkt zu kommen. Mitte Juli wandte er sich auf dem offiziellen Microsoft-Blog an die Öffentlichkeit, IT-Unternehmen und den US-Kongress und forderte gesetzliche Regelungen für die Gesichtserkennung. Unternehmen, die solche Software entwickeln oder nutzen, hätten eine besondere Verantwortung, dies nur im ethisch vertretbaren Rahmen zu tun, schrieb Smith, der sich technische Mindeststandards wünscht. Nur Systeme, die mindestens eine bestimmte, noch festzusetzende Erkennungsrate leisten, sollten zugelassen werden. Außerdem müsse sichergestellt werden, dass diese Technologie nicht zum Zwecke von racial profiling eingesetzt werde. Explizit erwähnt Smith die US-Behörde United States Immigration und Custom Enforcement (ICE), die unter anderem dafür zuständig ist, illegale Einwanderer zu überwachen und auszuweisen. **Als die ICE im Juni kritisiert wurde**, weil sie Eltern und Kinder illegaler Einwanderer voneinander getrennt hatte, traf das auch Microsoft, weil der Konzern die ICE mit Software beliefert – allerdings nur mit Standard-Software für den Büroeinsatz, wie Smith betonte.

Bereits die ausführliche Erwähnung der ICE zeigt, dass es in Smiths Brandbrief nicht alleine um die Sorge wegen der gesellschaftlichen Folgen automatischer Gesichtserkennung geht, sondern auch um Marketing. Seine Botschaft lautete: Es gibt gute und böse Einsatzzwecke und bei den bösen mache Microsoft nicht mit. Er transportiert damit eine Botschaft an potentielle Kunden: Gesichtserkennung funktioniert und bei uns könnt ihr sie guten Gewissens kaufen.

Dabei ist fraglich, wie gut sie denn tatsächlich funktioniert. Gearbeitet wird an dieser Technik bereits seit über 30 Jahren. Die ersten lauffähigen Systeme wurden Anfang der neunziger Jahre vorgestellt. Sie taugten allerdings nur als Prototypen zur weiteren Forschung, weil ihre Erkennungsraten miserabel waren. Den Durchbruch brachte die sogenannte künstliche Intelligenz, ein missverständlicher Begriff, der Laien suggeriert, der Computer könne wie ein Mensch denken. Tatsächlich handelt es sich um komplexe Algorithmen, die teilweise menschliche Hirnstrukturen simulieren und nach längerem Training in der Lage sind, Muster in Bildern zu erkennen – wie eben Gesichter. Dabei kommt das System nie zu eindeutigen Ergebnissen, sondern erreicht einen Wahrscheinlichkeitswert. Problematisch am Einsatz solcher Systeme ist, dass abgewägt werden muss, ab welchem Wahrscheinlichkeitswert sie Alarm schlagen sollen. Eine Person auf einem Foto ist mit einer Wahrscheinlichkeit von drei, 50 oder 97 Prozent mit einer gesuchten Person identisch: Wird der Schwellenwert zu niedrig gesetzt, verwechselt das System zu viele Personen miteinander. Wird der Wert zu streng gesetzt, gehen dem System zu viele gesuchte Personen durch die Lappen.

Was mit dieser Technologie praktikabel ist, hängt vom Einsatzzweck ab. Es macht einen großen Unterschied, ob per Gesichtserkennung ein Telefon entsperrt werden soll oder ob im öffentlichen Raum massenhaft Menschen überwacht werden.

Wichtig für die Bewertung der Software sind zwei Kennzahlen: Wie viele Personen werden korrekt erkannt und wie viele fälschlich? Beim kürzlich zu Ende gegangen Testlauf am Berliner Bahnhof Südkreuz lag die Erkennungsrate nach Angaben des Bundesinnenministeriums bei 70 Prozent. Das heißt, von zehn gesuchten Personen, die den Bahnhof passieren, werden sieben erkannt und drei nicht. Drei von zehn potentiellen Terroristen und Bombenlegern, mit denen

Politiker gerne den Einsatz solchen Überwachungssysteme rechtfertigen, würden also unbemerkt durchkommen.

Problematisch wird dieses Ergebnis vor allem im Hinblick auf die Anzahl der irrtümlich identifizierten Personen. Beim Berliner Experiment wird sie mit 0,3 Prozent beziffert. Das klingt wenig, ist aber viel. Bei täglich 89 000 Fahrgästen und Besuchern würde das bedeuten, dass es jeden Tag zu mehr als 250 Fehlalarmen käme – einer alle fünf Minuten. Wie die Polizei damit umgehen will, ist völlig schleierhaft.

Probleme mit der korrekten Erkennung gibt es nicht nur am Südkreuz. So hat die US-amerikanische Bürgerrechtsorganisation **American Civil Liberties Union** (ACLU) »Rekognition«, das Gesichtserkennungssystem von Amazon, mit den Fotos der 535 Abgeordneten des US-Kongresses gefüttert und mit mugshots verglichen – Polizeifotos von 25 000 Menschen, die in den USA festgenommen worden waren. Ergebnis: 28 Abgeordnete wurden vom System für eine der inhaftierten Personen gehalten.

Besonders peinlich war, dass die Software afroamerikanische Abgeordnete fast doppelt so häufig mit Verdächtigen verwechselte wie Abgeordnete mit weißer Hautfarbe. Das Experiment der ACLU wird zwar vielfach kritisiert, weil die Datenbasis – 535 Abgeordnete und 25 000 Polizeifotos – viel zu klein sei. Ganz unrealistisch ist es allerdings nicht, schließlich soll die Polizei auf Verbrecherjagd die Videoschnappschüsse vieler Tausend Menschen mit einer überschaubaren Datenbank von Fotos gesuchter Personen vergleichen.

Nun ließe sich argumentieren, Videoüberwachung und Gesichtserkennung könnten zumindest helfen, Straftaten nachträglich aufzuklären. Allerdings ist das nicht das einzige Ziel solcher Systeme. Zur Gesichtserkennung soll die Verhaltenskontrolle hinzukommen. Daran wird 2009-2014 im EU-Forschungsprojekt Indect gearbeitet. Verhält sich eine Person auffällig? Bewegt sie sich anders als die Mehrzahl der Menschen in der Menge? Liegt, sitzt oder steht sie verdächtig irgendwo herum?

Irgendwann soll die Polizei in der Lage sein, eine Person festzunehmen oder wegzuschicken, bevor es zu einer kriminellen Tat kommt. Das würde grundlegende rechtsstaatliche Prinzipien auf den Kopf stellen. Eine solche Verhaltenskontrolle ist explizit für die zweite Phase des Südkreuz-Experimentes geplant, die im September beginnen soll.

Brad Smith hat also recht: Gesichtserkennung hat ein gefährliches Potential. Allerdings zeigt es sich weniger bei den iPhones oder bei Facebook, wo sie sich sogar als praktisch herausstellen kann, ohne Personen konkret zu gefährden – etwa wenn User unberechtigt Fotos von Dritten ins Netz stellen. Die Gefahren liegen eher in der Nutzung durch Staaten, die ihre Bürger per Überwachung unter Generalverdacht stellen. In Kombination mit den neuen Polizeigesetzen der Bundesländer beispielsweise könnte die automatisierte Gesichtserkennung erst ihr dystopisches Potential entfalten.

Vom deutschen Staat ist derzeit eher nicht zu erwarten, dass er dem Aufruf von Brad Smith folgt und sich selbst strenger reguliert. **Die kürzlich wirksam gewordene EU-Datenschutzgrund-verordnung** etwa sieht Ausnahmen beim Schutz biometrischer Daten bei »erheblichem öffentlichen Interesse« ausdrücklich vor.

In einer früheren Version dieses Artikel hieß es fälschlich, das EU-Forschungsprojekt liefe seit 2005. Geändert am 27. August