Daniel Leisegang

Biometrische Videoüberwachung: Die neue Hochrisikotechnologie

Mitte Januar deckte die „New York Times“ auf, dass mehrere hundert Ermittlungsbehörden und Privatunternehmen weltweit eine Software namens *Clearview* nutzen. Diese erlaubt es, Fotos von Personen innerhalb weniger Sekunden zu identifizieren. Mit wenigen Klicks lassen sich die Namen der Gesuchten, ihre Anschrift und berufliche Tätigkeit sowie ihr Freundeskreis ermitteln.[1]

Zwei Aspekte machen die Enthüllungen besonders brisant: Zum einen greift Clearview für die Identifikation auf eine eigene Datenbank mit mehr als drei Mrd. privater Fotos zu. Zum Vergleich: Die Fotodatenbank des FBI umfasst „nur“ gut 640 Mio. Fotos. Die Bilder hat das Unternehmen *Clearview AI* ohne Wissen der Betroffenen aus frei zugänglichen Quellen im Internet abgesaugt – von Facebook, YouTube, Twitter, aber auch von Nachrichten- und Firmenwebseiten. Zum anderen ist nicht bekannt, welche Behörden genau Clearview verwenden: Bislang erfolgt der Einsatz der Software fernab politischer und juristischer Kontrolle.

Fest steht: Würde das Programm in den App Stores von Android und Apple auftauchen, könnten Nutzer mit Hilfe ihrer Smartphones potentiell jede beliebige Person identifizieren – in der U-Bahn, auf der Straße oder auf einer Demonstration. Damit aber stellt Clearview nicht nur für Bürgerinnen und Bürger, sondern insbesondere auch für politische Aktivisten eine immense Gefahr dar. Es ist daher auch kein Zufall, dass Clearview AI sein Produkt schon 2017 ausgerechnet Paul Nehlen als Werkzeug für „außergewöhnliche Oppositionsrecherchen“ anpries. Nehlen gilt als einer der berüchtigsten *White Nationalists* in den USA, der immer wieder auch zu Gewalt gegenüber Minderheiten aufruft.

Wegen solcher Missbrauchsrisiken schreckten selbst Technologiekonzerne wie Google bereits vor Jahren davor zurück, eine ähnliche Applikation anzubieten. Clearview AI hingegen arbeitet offenbar bereits an einer Datenbrille, mit der sich die Ausspähung noch unauffälliger ausüben ließe.

Die Schockwellen der „Times“-Enthüllungen reichten bis nach Berlin – und machten Bundesinnenminister Horst Seehofer einen gehörigen Strich durch die Rechnung. Denn sein Haus plante, wie gleich zu Jahresbeginn bekannt wurde, die bundesweite Einführung biometrischer Gesichtserkennung plant. Auf 135 Bahnhöfen und 14 Flughäfen sollte die Technologie installiert werden und dort die automatische Fahndung „nach Terroristen und Schwerkriminellen“ ermöglichen. 130 Mio. Euro wollte das Ministerium dafür bereitstellen; der Entwurf für ein entsprechend angepasstes Bundespolizeigesetz lag bereits vor.

Doch daraus wird vorerst nichts. Zwar betonten deutsche Geheimdienste und Behörden umgehend, Clearview nicht für die eigene Arbeit zu verwenden. Gleichzeitig aber rückte der Bericht der „New York Times“ schlagartig die Risiken der biometrischen Überwachung in den Fokus auch der deutschen Debatte. Horst Seehofer hatte

1 Vgl. Kashmir Hill, The Secretive Company That Might End Privacy as We Know It, www.nytimes.com, 18.1.2020.

keine andere Wahl, als seine Pläne auf Eis zu legen. Zu viele Fragen seien derzeit noch offen, hieß es aus dem Innenministerium.

Dem ist in der Tat so, und zwar sowohl in technischer als auch in grundrechtlicher Hinsicht. Bislang funktionieren die biometrischen Systeme alles andere als zuverlässig, weshalb immer wieder Unschuldige ins Visier der Ermittler geraten. Gleichzeitig aber ist die Technologie, selbst wenn sie fehlerfrei arbeiten würde, keinesfalls unbedenklich. Denn die biometrischen Systeme heben die staatliche Überwachung auf eine gänzlich neue Stufe und bedeuten letztlich nicht weniger als das Ende der Anonymität im öffentlichen Raum.

Der maschinenlesbare Mensch

Naturgemäß nehmen die Sicherheitsbehörden eine diametral andere Position ein: Sie betrachten die biometrische Videoüberwachung als Quantensprung in der Strafverfolgung, mit deren Hilfe sich ihre mühsame Fahndungsarbeit an Algorithmen delegieren ließe. Möglich macht dies die jüngste Weiterentwicklung von Systemen künstlicher Intelligenz, die eigenständig Muster identifizieren können. Schneller und genauer als je zuvor sind künstliche neuronale Netze heute in der Lage, Menschen zu „lesen", also deren Körperdaten zu erfassen und mit Datenbanken abzugleichen – und zwar ohne, dass die Betroffenen den Scanvorgang bemerken. Die biometrische Videoüberwachung im öffentlichen Raum funktioniert damit wie eine anlasslose, stille Rasterfahndung, der sich niemand entziehen kann.

Der Traum von der automatisierten Fahndung hat jedoch – neben den massiven rechtsstaatlichen Problemen – einen gewaltigen technischen Haken: Denn die biometrische Videoüberwachung funktioniert längst nicht so gut, wie es die Behörden glauben machen wollen. Um den Einsatz der Überwachungstechnologie dennoch zu legitimieren, rechnen sie immer wieder die Erkennungsquote schön.

So auch das Bundesinnenministerium: Bereits im Sommer 2017 hatte es die automatisierte Gesichtserkennung am Berliner Bahnhof Südkreuz für die Dauer eines Jahres getestet. Aus Sicht des Ministeriums war der Probelauf ein voller Erfolg: Die Technologie habe im Durchschnitt 80 Prozent der teilnehmenden Freiwilligen richtig erkannt. Sie sei damit bereit für den flächendeckenden Praxiseinsatz, so das offizielle Ergebnis.

Experten zweifeln jedoch die Wissenschaftlichkeit des Testlaufs an. Sie stellten fest, dass das durchschnittliche Ergebnis für das beste der insgesamt drei getesteten Systeme tatsächlich bei gerade einmal 68,5 Prozent gelegen habe.[2] Doch selbst wenn man die angegebenen 80 Prozent vom Ministerium zugrundelegt, würden bei täglich rund 90 000 Reisenden am Berliner Südkreuz noch immer 18 000 Menschen falsch identifiziert. Derweil die Polizei also von automatisierter Fahndungsarbeit träumt, vermitteln die biometrischen Systeme aus Sicht des Deutschen Anwaltsvereins nurmehr eine „trügerische Sicherheit".

In Großbritannien finden derzeit ganz ähnliche Zahlenspiele statt. Die Londoner Polizei gab Ende Januar bekannt, dass sie die Kameras der Stadt – im Großraum London gibt es bereits rund eine halbe Million davon – mit einer Gesichtserkennungssoftware und einer Polizeidatenbank verknüpfen will. Entdeckt das System jemanden, der nicht in der Datenbank enthalten ist, löscht es die Informationen innerhalb von Sekunden wieder. Schlägt es jedoch Alarm, weil eine gesuchte Person erkannt wird, werden die Beamten aktiv. Dabei werden laut Polizei in nur einem von 1000 Fällen Menschen fälschlicherweise als gesucht markiert.

2 Vgl. Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, www.ccc.de, 13.10.2018.

Professor Pete Fussey von der Universität Essex, der als Experte für Überwachungssysteme eigens von der Londoner Polizei damit beauftragt worden war, deren Testläufe zu bewerten, widerspricht jedoch: Ihm zufolge arbeite die biometrische Videoüberwachung in gerade einmal 19 Prozent der Fälle korrekt.[3]

USA: Rassismus als Systemfehler

Diese Zahlen sprechen eindeutig gegen die Praxistauglichkeit der biometrischen Videoüberwachung. Dennoch halten die Behörden an deren Einsatz fest, offenbar in der Hoffnung, dass die Technologie im Alltag zur rechtmäßigen Einsatzfähigkeit „reifen" werde.

Wie überaus fahrlässig eine solche Strategie ist, zeigt sich in den USA. Dort setzen die Ermittlungsbehörden bereits seit Jahrzehnten biometrische Systeme ein – neuerdings nicht nur Clearview, sondern auch *Rekognition*, eine Gesichtserkennungstechnologie von Amazon. Dem Konzern zufolge soll es die Software ermöglichen, ganze Städte in Echtzeit zu überwachen.

Technisch ausgereift ist jedoch auch dieses System nicht: Im Juli 2018 testete die Bürgerrechtsorganisation ACLU Rekognition und glich dafür Bilder von 535 US-Kongressabgeordneten mit 25 000 Häftlingsfotos der Polizei ab. 28 der Abgeordneten markierte die Software daraufhin fälschlicherweise als Kriminelle. Unter ihnen seien auffällig viele nicht-weiße Politiker gewesen, so die ACLU, etwa der schwarze Bürgerrechtler John Lewis.

KI-Experten weisen schon lange darauf hin, dass Gesichtserkennungssysteme vor allem bei Menschen mit dunkler Hautfarbe gehäuft Fehler machen.[4] Die fatalen Folgen eines solchen Fehlalarms in der Praxis lassen sich leicht ausmalen: Immer wieder werden vor allem schwarze Menschen zu Unrecht krimineller Handlungen verdächtigt, von der US-Polizei drangsaliert und überdurchschnittlich häufig erschossen. „Eine Identifizierung […] könnte Menschen ihre Freiheit oder sogar ihr Leben kosten", mahnt daher auch die ACLU.

Dennoch ist die biometrische Videoüberwachung gerade in den Vereinigten Staaten weiter auf dem Vormarsch – und zwar bis tief in die amerikanischen Vororte hinein. Amazons Überwachungsfirma „Ring" bietet bereits seit einigen Jahren Gegensprechanlagen mit WLAN und Videokameras an. Millionen dieser Geräte hat der Konzern bereits verkauft; einmal installiert können die Bewohner mittels Smartphone aus der Ferne den Eingangsbereich ihrer Häuser überwachen.

Und nicht nur sie: Mehr als 770 Polizeidienststellen im ganzen Land greifen gemäß einer Übereinkunft mit Amazon ebenfalls auf die Videoaufzeichnungen zu – mit Zustimmung der Nutzer, jedoch ohne dass dafür eine richterliche Verfügung erforderlich wäre. Noch fehlt Ring die Funktion der Gesichtserkennung, an der Amazon nach eigenen Angaben aber bereits arbeitet. Damit könnte das System künftig Alarm schlagen, wenn sich „Verdächtige" einem Haus nähern.[5] Auf diese Weise lassen sich dann ganze Communities virtuell observieren und faktisch auch technisch abriegeln.

Was passiert, wenn man das Überwachungsnetz mit Hilfe der biometrischen Videoüberwachung noch dichter spannt, lässt sich heute bereits in China beobachten. Im Reich der Mitte ist die automatisierte Gesichtserkennung aus dem Alltag nicht mehr wegzudenken: Vielerorts zahlen Menschen per Gesichtsscan, verschaffen sich so Zugang zu U-Bahn-Eingängen und ihren

3 Vgl. Vikram Dodd, Met police to begin using live facial recognition cameras in London, www.theguardian.com, 24.1.2020.

4 Vgl. Facial Recognition Technology (FRT), www.nist.gov, 6.2.2020.

5 Rani Molla, How Amazon's Ring is creating a surveillance network with video doorbells, www.vox.com, 28.1.2020.

privaten Wohnhäusern. Gleichzeitig aber nutzen die chinesischen Behörden biometrische Systeme auch dazu, um ethnische Minderheiten zu überwachen und zu kontrollieren.

Vor knapp einem Jahr wurde bekannt, dass chinesische Behörden in Gefangenenlagern die Gesichter von mehr als einer Million Menschen vermessen haben. Mit den Daten werden Algorithmen von Gesichtserkennungssystemen auf die äußerlichen Merkmale der muslimischen Minderheit der Uiguren trainiert. Vor allem in der ostchinesischen Region Xinjiang suchen Kameras gezielt nach deren Angehörigen, etwa um Ansammlungen von Uiguren frühzeitig zu erkennen. Zudem kann die Polizei so eine bestimmte Person als potentielle Bedrohung markieren. Versucht diese dann, einen bestimmten öffentlichen Ort zu betreten, wird umgehend ein Alarm ausgelöst.[6]

Der hohe Preis der Sicherheit

Gewiss, ein Schreckensszenario wie in China ist hierzulande derzeit nicht zu befürchten. Zugleich aber zeigt der Blick in andere Länder, dass die anlasslose biometrische Videoüberwachung auch und gerade für Demokratien eine gesellschaftliche Hochrisikotechnologie darstellt. Denn mit ihr verfügt der Staat über ein überaus machtvolles Überwachungsinstrument, das die Anonymität im öffentlichen Raum auf einen Schlag zerstören kann. Damit aber zahlen die Bürgerinnen und Bürger einen gewaltigen Preis für ein wenig mehr an versprochener Sicherheit.

Der Bundesdatenschutzbeauftragte Ulrich Kelber bezweifelt daher auch, dass die biometrische Videoüberwachung überhaupt mit dem Grundgesetz vereinbar ist. Gerade in Demokratien würde das ständige Gefühl, überwacht zu werden, Freiheitsrechte, individuelle Entfaltung und politische Teilhabe in Mitleidenschaft ziehen: „Wer zum Beispiel bei Demonstrationen befürchten muss, trotz gesetzestreuen Auftretens identifiziert und gespeichert zu werden, der ändert möglicherweise sein Verhalten und geht nicht mehr demonstrieren."[7]

Offenbar aus derlei grundrechtlichen Überlegungen hatte die EU-Kommission auch ein zeitweises Verbot der biometrischen Videoüberwachung erwogen. Im vergangenen Dezember wurde ihr Entwurf für ein „Weißbuch" bekannt, das Teil eines Maßnahmenpakets zur Bewältigung der Herausforderungen der KI ist. Demzufolge sollte die Gesichtserkennung im öffentlichen Raum für drei bis fünf Jahre verboten werden, um zunächst die gesellschaftlichen Folgen dieser Technologie genauer abschätzen zu können.

Dies wäre auf europäischer Ebene einer erstaunlichen Kehrtwende gleichgekommen: Noch im April 2019 hatte das EU-Parlament für die Einrichtung des *Common Identity Repository* (CIR) gestimmt – eine gigantische biometrische Datenbank, die Grenzkontroll-, Migrations- und Strafverfolgungsdatensysteme zusammenführt. Sie soll am Ende die Einträge von mehr als 350 Mio. EU-Bürgern enthalten und wäre damit eine der weltweit größten Datenbanken zur Personenverfolgung, direkt hinter den Systemen der chinesischen und der indischen Regierung.

Leider aber überlegte es sich die EU-Kommission noch einmal anders – und stützt damit letztlich auch Horst Seehofers Pläne: In der am 19. Februar veröffentlichten Endfassung des Maßnahmenpakets ist von einem Moratorium nicht länger die Rede. Für den Schutz unserer Grundrechte ist dies ein fatales Signal.

6 Vgl. Paul Mozur, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, www.nytimes.com, 14.4.2019 sowie Chris Buckley and Paul Mozur, How China Uses High-Tech Surveillance to Subdue Minorities, www.nytimes.com, 22.5.2019.

7 Wie viel Gesichtserkennung dürfen wir zulassen?, www.deutschlandfunk.de, 22.1.2020.