KULTUR NEU ENTDECKEN

SWR2

SWR2 Wissen

Überwachtes Leben – Gesichtserkennung und Tracking

Von Cäcilia und Thomas Kruchem

Sendung vom: Dienstag, 24. Mai 2022, 8.30 Uhr
Redaktion: Dirk Asendorpf
Autorenproduktion
Produktion: SWR 2022

Immer mehr Menschen werden automatisch auf den Bildern von Überwachungskameras identifiziert - eine Gefahr für die Freiheitsrechte.

MANUSKRIPT

Atmo 1:
Krawalle 07.07.2017 in Hamburg

Sprecher:
Hamburg, 7. Juli 2017: Während eines Treffens der G20-Staatschefs kommt es zu den vielleicht größten Krawallen in der Geschichte der Bundesrepublik. Vermummte werfen Gullideckel auf Polizisten, Supermärkte werden geplündert, Autos gehen in Flammen auf. In den folgenden Monaten ermittelte die Polizei mit einer zuvor kaum genutzten Technik – berichtet Hamburgs Datenschutzbeauftragter Thomas Fuchs:

O-Ton 1 Thomas Fuchs:
Die Polizei hatte damals umfangreiches Bildmaterial gesammelt – also aus Überwachungskameras, Handyaufnahmen und Ähnliches. Insgesamt fast hundert Terabytes Bild- und Videomaterial. Und hat dann, um diese unfassbaren Mengen von Materialien auszuwerten, eine Gesichtserkennungssoftware eingesetzt.

Ansage:
Überwachtes Leben – Gesichtserkennung und Tracking. Von Cäcilia und Thomas Kruchem.

Sprecher:
Gesichter in Video-Bergen zu suchen und mit Datenbanken von Bildern abzugleichen, ähnelt der Suche nach der Nadel im Heuhaufen. Sicherheitsbehörden jedoch wollen diese Nadel unbedingt finden, um den Bürger noch besser zu schützen – vor Gewaltverbrechen, Terror, Kindesmissbrauch. Eine Lösung bietet so genannte künstliche Intelligenz, die in den letzten Jahren dramatisch verbessert wurde. Ein Aktionsfeld künstlicher Intelligenz ist die Biometrie: Menschen werden anhand ihrer DNA, Handvenen oder Iris, anhand ihrer Stimme oder ihrer Bewegungsmuster erkannt.

Atmo 2:
Englische Erklärung von Webseite der Firma DSIRF

Sprecher:
Als eleganteste Methode der Biometrie gilt die Gesichtserkennung durch Foto- und Videoanalyse: Sie kommt ohne Berührung aus; der Betroffene merkt gar nicht, dass sein Gesicht untersucht wird. Bis zu 2.000 Datenpunkte vermesse ein Algorithmus, ein Programm der Gesichtserkennung, heißt es auf der Webseite des Wiener Softwareentwicklers DSIRF. Der Abstand zwischen Augen und Nase wird vermessen, der zwischen Stirn und Ohren, die Struktur der Hautoberfläche, die Form der Lippen. Je mehr Datenpunkte dann auf zwei Bildern übereinstimmen, desto wahrscheinlicher ist es, dass es sich um dieselbe Person handelt.

Jeder Einsatz von Gesichtserkennung und Biometrie jedoch berührt den Kern unserer Identität und unser Recht auf Anonymität im öffentlichen Raum – erklärt Francesco Ragazzi, Professor für Politikwissenschaft an der Universität Leiden und Autor einer Studie zum Thema für das Europäische Parlament.

O-Ton 2 Francesco Ragazzi (englisch), darüber Übersetzung:
Der erste Einsatzzweck von Gesichtserkennungstechnologie ist die Authentifizierung: Sind Sie tatsächlich die Person, die Sie behaupten zu sein? – Dies per Gerichtserkennung zu prüfen, halten wir für rechtlich eher unproblematisch. In der Regel haben ja Sie zugestimmt, mit ihrem Gesicht Ihr Smartphone zu entsperren oder, zum Beispiel, Zutritt zu einem Firmengebäude zu erhalten: Ja, ich bin es, Thomas Kruchem, der Zugang zu diesem Telefon oder Gebäude erhalten möchte.

Sprecher:
Die Prüfung unserer Identität durch Gesichtserkennung wird zunehmend auch bei Grenzkontrollen und beim Einchecken am Flughafen eingesetzt: Unser Gesicht wird mit unserem Passbild oder einem den Behörden vorliegenden Bild verglichen. Problematischer ist das zweite Einsatzfeld der Gesichtserkennung:

O-Ton 3 Francesco Ragazzi, darüber Übersetzung:
Sucht dieses System eine einzelne Person, indem es die Gesichter von zahllosen Passanten scannt? Oder sucht das System die Person, indem es Videoaufnahmen aus einem Bahnhof oder einem Einkaufszentrum untersucht? In solchen Fällen haben wir es mit Eingriffen ins Privatleben und die Menschenrechte zu tun; mit biometrischer Massenüberwachung. Und die ist laut Datenschutz-Grundverordnung prinzipiell verboten in der EU, wenn nicht alle Betroffenen zustimmen.

Sprecher:
Die Datenschutz-Grundverordnung der EU sagt: Ich selbst entscheide, wer was über mich weiß. Auch im öffentlichen Raum muss ich mir meiner Anonymität sicher sein können. Nur so sind meine Grundrechte auf freie Entfaltung der Persönlichkeit und Versammlungsfreiheit garantiert. In diese Rechte eingreifen darf der Staat nur aus einem Grund, der per Gesetz explizit definiert ist.

Atmo 3:
Krawalle 07.07.2017 in Hamburg

Sprecher:
Nach den Krawallen in Hamburg 2017 griff die Polizei in die Grundrechte unzähliger Bürger ein, als sie Zehntausende Stunden an Videomaterial mit Gesichtserkennungssoftware durchforstete. Mit frappierendem Erfolg – resümiert in der Tagesschau vom 7. Juli 2020 Sandra Levgrün, Sprecherin der Hamburger Polizei:

O-Ton 4 Sandra Levgrün:
Aus diesem Videomaterial haben sich über 430 Öffentlichkeitsfahndungen ergeben, von denen wir inzwischen 135 Tatverdächtige identifizieren können, so dass man summa summarum sagen muss, dass die Ermittlungen wirklich sehr erfolgreich gelaufen sind.

Sprecher:
2018, zwei Jahre zuvor, hatte Hamburgs Datenschutzbehörde die Ermittlungen mittels Gesichtserkennung noch untersagt. Für den Eingriff in die Grundrechte zahlloser Menschen gebe es keine explizite Erlaubnis im Hamburger Polizeigesetz,

erklärt der Datenschutzbeauftragte Thomas Fuchs. Es gebe nur eine vage polizeiliche Generalklausel.

O-Ton 5 Thomas Fuchs:
Die Polizei hat, auf Grundlage der polizeilichen Generalklausel, sinngemäß argumentiert: Das ist ja nichts anderes, als wenn Polizisten händisch Bilder miteinander vergleichen, halt nur so ein bisschen schneller mit Software-Unterstützung. Aber eigentlich war dieser Anwendungsbereich weder erlaubt noch verboten; und da muss man als Datenschutzbehörde dann sagen: Wenn ihr keine Legitimation dafür habt, dann dürft ihr das so auch nicht tun.

Sprecher:
Die Polizei zog gegen das Verbot vor Gericht und siegte in erster Instanz. Über die Berufung, die die Datenschutzbehörde einlegte, wurde noch nicht entschieden. Der massive Einsatz von Gesichtserkennung in Hamburg ist bis heute ein Einzelfall in der EU. Unter dem Radar der Öffentlichkeit jedoch identifiziert die Polizei Deutschlands längst routinemäßig Straftäter, vor allem Kleinkriminelle. Die Videoaufnahme zum Beispiel eines Randalierers am Bahnhof wird abgeglichen mit Bildern, über die der Staat verfügt. Parallel werde auch die Technologie der Live-Gesichtserkennung intensiv erprobt, monieren Kritiker; und die Logistik für ihren Einsatz werde ausgebaut: Am Berliner Bahnhof Südkreuz, zum Beispiel, testete das Bundesinnenministerium 2017 Massenüberwachung per Gesichtserkennung. Auf den Videos hochauflösender Kameras identifizierten die Behörden live Freiwillige, aus denen man eine Suchliste zusammengestellt hatte. Messdaten ahnungsloser Passanten wurden in den Abgleich einbezogen, unmittelbar danach jedoch gelöscht. Derweil werden in vielen Großstädten immer neue Überwachungskameras installiert.

Atmo 4:
Big Ben

Sprecher:
London. Die Stadt mit der höchsten Dichte an Überwachungskameras in Europa. Und: Schauplatz des…

Atmo 5:
Nottinghill Carnivall

Sprecher:
…Nottinghill Carnival. Alljährlich im August feiern ethnische Minderheiten aus der Karibik und Afrika das größte Straßenfest Europas. 2016 begann Londons Polizei auf dem Nottinghill Carnival mit bis heute andauernden Tests der Live-Gesichtserkennung: Vom Dach eines Vans aus filmten hochauflösende Kameras die tanzende Menge; im Innern des Vans glich Erkennungssoftware die Bilder mit einer watchlist ab, einer Liste gesuchter Personen. Immer wieder wurden feiernde Menschen überprüft.

Professor Pete Fussey, Soziologe an der Universität von Essex, hat – eingeladen von der Polizei – eine Studie zu den Tests erarbeitet. **(1)** Die watchlist habe zunächst 2.000 Personen umfasst, berichtet Fussey am Küchentisch seines Reihenhauses in East London. Inzwischen umfasse die Liste 10.000 Personen: Schwerverbrecher,

aber auch Opfer von Verbrechen, potenzielle Zeugen und Leute, die versehentlich auf der Liste gelandet sind.

O-Ton 7 Pete Fussey (englisch), darüber Übersetzung:
In den sechs Tagen, die ich im Überwachungswagen saß, hatten wir 42 sogenannte matches. 16 wurden von Polizisten, die die Bilder verglichen, gleich aussortiert; vier Personen gingen in der Menschenmenge verloren. 22 wurden schließlich angehalten und überprüft. 14 davon hatte man falsch identifiziert; nur acht Personen waren tatsächlich von Interesse für die Polizei.

Sprecher:
Viel Aufwand mit geringem Ertrag – auf zudem juristisch dünnem Eis. Denn auch in Großbritannien gilt, übernommen von der EU, die Datenschutz-Grundverordnung.

Erstens, sagt Professor Fussey, werde die vorgeschriebene Zustimmung betroffener Passanten häufig nicht eingeholt. Im Gegenteil: Zeitweise überprüfte die Polizei gezielt Leute, die der Kamera auswichen.

Zweitens hat der Algorithmus der Gesichtserkennung zwar eine hohe Trefferquote von über 99 Prozent. Werden aber zehntausende Gesichter gescannt, müssen auch bei kleinster Fehlerquote hunderte Menschen eine Überprüfung über sich ergehen lassen.

Drittens hat die Technologie Probleme, ältere und sehr junge Menschen, Frauen und Angehörige nicht-weißer ethnischer Minderheiten zu erkennen. Die werden deshalb von der Polizei besonders häufig überprüft und damit diskriminiert.

Viertens fehlt für die Überwachungsmaßnahmen, wie im deutschen Hamburg, die explizite gesetzliche Grundlage. Das kritisierte zum Beispiel am 11. August 2020 der oberste Gerichtshof von England und Wales in einem Verfahren gegen die Polizei von South Wales. Die testet bis heute ebenfalls Gesichtserkennung an belebten Plätzen. Zu deren Verbot konnte sich der Gerichtshof nicht durchringen.

Ein fünftes, besonders schwerwiegendes Rechtsproblem schließlich sei in die Massenüberwachung per Gesichtserkennung quasi eingebaut, erklärt Professor Fussey.

O-Ton 8 Pete Fussey, darüber Übersetzung:
Will die Polizei, zum Beispiel, den Internetverkehr einer Person überwachen, muss sie eine richterliche Anordnung beantragen. Und sie muss dem Richter Anhaltspunkte für einen dringenden Verdacht auf eine Straftat präsentieren. Nur dann ist die Überwachung des Internetverkehrs zulässig. Ganz anders läuft Massenüberwachung durch Gesichtserkennung: Da gelten, ohne Mitwirkung eines Richters, zunächst mal wir alle als verdächtig und müssen im Zweifelsfall unsere Unschuld beweisen.

Sprecher:
Die Londoner Polizei lehnte eine Stellungnahme gegenüber SWR2 Wissen ab**.** Doch nicht nur die Polizei betreibt in Großbritannien Gesichtserkennung, sondern auch private Unternehmen wie die Supermarkt-Kette Southern Co-op. **(2)** Bilder von

Kunden, die einen ihrer Läden betreten, werden abgeglichen mit einer watchlist registrierter Ladendiebe und Randalierer.

Atmo 6:
Verkehr an der Grays Inn Road

Sprecher:
Über dem Co-op-Laden in der Londoner Grays Inn Road etwa hängen zwei Kameras, die auch den öffentlichen Gehweg erfassen. Ein Aushang sagt, Co-op überwache den Laden und reiche Aufnahmen an die Polizei weiter. Wie sehen das zufällig angesprochene Kunden?

O-Ton 10 Lehrer, darüber Übersetzung:
Ich halte das für keine gute Sache. Unser Land ist zu sehr von Sicherheit besessen. Ich will einfach im Supermarkt einkaufen, was ich brauche, und nicht darüber nachdenken, dass man mich fotografiert.

O-Ton 11 – Mann eritreischer Herkunft:
Mir persönlich ist schon passiert, dass die gedacht haben, dass es ich bin. Die haben sogar Fotos gehabt, dass sie hundert Prozent sicher waren, dass ich es war, Ich musste das beweisen, dass ich nicht war. Das war in Holborn; ich glaube, Tesco war das.

Sprecher:
Eine weitere Supermarktkette, die ihre Läden mit Gesichtserkennung überwacht. Weder Tesco noch Southern Co-op beantworteten Bitten um eine Stellungnahme.

Atmo 7:
Park

Sprecher:
Treffen in einem Park mit Ioannis Kouvakas. Der junge Rechtsanwalt arbeitet für die Datenschutzorganisation privacy international. Private Gesichtserkennung sei legal, wenn der Kunde sie als Bedingung, ein Geschäft zu betreten, akzeptiert, sagt Kouvakas. Dessen ungeachtet sieht er Indizien für Amtsanmaßung – auch bei den Lieferanten von Gesichtserkennungssoftware. Zu den größten in Großbritannien zählt das Unternehmen Facewatch, das sowohl die Polizei als auch private Kunden beliefert.

O-Ton 12 Ioannis Kouvakas (englisch), darüber Übersetzung:
Der Chef des Unternehmens Facewatch hat öffentlich gesagt, er tausche watchlist-Daten mit der Polizei aus; die Polizei überlasse Facewatch-Bilder verdächtiger Personen. Und diese Informationen würden das Unternehmen und seine Kunden nutzen, um Betroffenen den Zugang zu Geschäften zu verwehren. Ich sehe hier einen höchst gefährlichen Präzedenzfall: Die Polizei nutzt private Unternehmen für Massenüberwachung, die sie selbst aus Datenschutzgründen nicht betreiben darf.

Atmo 8:
Verkehr New York mit Polizeisirene

Sprecher:
Sprung über den Atlantik – in die USA, wo es keine Datenschutz-Grundverordnung gibt. In New York hat 2017 der junge Australier Hoan Ton-That das Startup Clearview.ai gegründet **(3)**. Das Unternehmen füttert seinen Algorithmus der Gesichtserkennung mit Bildern aus dem Internet, aus sozialen Medien wie Facebook und Instagram vor allem. Bis Ende April 2022 hatte das Unternehmen, nach eigenen Angaben, 20 Milliarden Fotos zusammengerafft, ohne Betroffene zu fragen. Ende 2022 sollten es hundert Milliarden sein. Clearviews Algorithmus habe eine beeindruckend hohe Trefferquote, bestätigen Experten. Entsprechend groß ist die Nachfrage bei der Polizei: Rund 3.000 Polizeibehörden in den USA nutzen die Clearview-Software; Polizeibehörden in Kanada, Schweden, Neuseeland und Australien nutzten sie zeitweise. Tausende Verdächtige seien bereits identifiziert worden, sagt das Unternehmen – darunter Dutzende Teilnehmer des Sturms auf das Kapitol am 6. Januar 2021. Im März 2022 stellte Clearview seinen Algorithmus kostenlos dem Verteidigungsministerium der Ukraine zur Verfügung **(4)**.

Atmo 9:
Hoan Ton-That auf News Nation 1

Sprecher:
Mit der Software sollen die Ukrainer russische Gefallene identifizieren und über deren Profile in sozialen Medien Angehörige informieren, sagt der Clearview-Chef am 18. April 2022 im US-Fernsehsender News Nation.

Atmo 10:
Hoan Ton-That auf News Nation 2

Sprecher:
Auch die Identifizierung von Kriegsverbrechern, Saboteuren und Plünderern begrüßt Hoan Ton-That. Ein Ziel seiner App sei es, von Verbrechen und Kriegsverbrechen abzuschrecken.

Der demokratische US-Senator Ron Wyden jedoch befürchtet, dass Clearviews Super-Algorithmus die Anonymität des Einzelnen im öffentlichen Raum unwiderruflich zertrümmern könnte. Die Regierungen von Kanada, Australien, Schweden, Großbritannien und Italien haben derweil Clearviews Selbstbedienung im Internet für illegal erklärt. Auch Hamburgs Datenschutzbeauftragter Thomas Fuchs hat sich, nach der Beschwerde eines Bürgers, mit dem Startup auseinandergesetzt:

O-Ton 13 Thomas Fuchs:
Das Grundproblem ist, dass Clearview sagt: „Wir sind ein amerikanisches Unternehmen, und europäisches Datenschutzrecht interessiert uns überhaupt nicht.“ Die grundsätzliche Frage, dass nämlich das ganze Geschäftsmodell von Clearview mit europäischem Datenschutzrecht überhaupt nicht vereinbar ist – da kommen wir mit unseren auf Europa begrenzten verwaltungsrechtlichen Möglichkeiten nicht ran. Und da, muss man auch sagen, ist Clearview strukturell unerreichbar.

Sprecher:
Eine E-Mail mit der Bitte um ein Interview hat Clearview nicht beantwortet.

Kaitlin Jackson, eine New Yorker Anwältin, arbeitet für die Bronx Public Defenders, die jährlich fast 30.000 Strafverfolgte kostenlos verteidigen. Die Anwältin erzählt von einem Fall, in dem der polizeiliche Einsatz von Gesichtserkennungstechnologie eine verhängnisvolle Rolle spielte: Eine Überwachungskamera hatte einen Ladendieb gefilmt, der, als ihn ein Sicherheitsmann ansprach, ein Teppichmesser zückte und davonrannte. Die Polizei verglich dann, mittels Gesichtserkennung, das Video mit ihrer Datenbank von Verdächtigen und Straftätern. Aus den Männern, die dem Ladendieb ähnlich sahen, sortierten Polizisten per Hand den ihrer Meinung nach richtigen heraus.

O-Ton 14 Kaitlin Jackson (englisch), darüber Übersetzung:
Die Polizei mailte dem Wachmann das Foto und fragte ihn: „Ist das der Mann, den sie gesehen haben?“ Und natürlich sagte der Wachmann „ja“ – so, wie es ihm die Polizisten suggeriert hatten. Man habe den Mann mit Gesichtserkennungstechnologie schon identifiziert, hatten die dem Zeugen gesagt. Er müsse das nur noch bestätigen. Ein ganz anderes Vorgehen als früher: Da stellte man sechs Personen in eine Reihe; und der Zeuge musste die richtige heraussuchen. Jetzt sieht er nur ein Foto, das – mit angeblich fast hundertprozentiger Sicherheit – den Täter zeigt. Und das kann natürlich die Erinnerung des Zeugen beeinflussen.

Sprecher:
Der Verdächtige, ein Mandant Kaitlin Jacksons, saß sechs Monate in Untersuchungshaft. Jackson wollte dann zumindest die Bilder der anderen Männer sehen, die dem Verbrecher auf dem Überwachungsvideo ähnelten. „Nein“, habe die Polizei gesagt, „das behindere die Ermittlungen und gefährde Geschäftsgeheimnisse des Software-Produzenten.“

O-Ton 15 Kaitlin Jackson, darüber Übersetzung:
Die New Yorker Polizei wehrte sich mit allem, was ihre Anwälte an juristischer Munition aufbieten konnten. Auf gar keinen Fall wollten sie uns andere Bilder zeigen. Und schließlich machte der Staatsanwalt ein, wie er sagte, großzügiges Angebot: Mein Mandant sollte sich schuldig bekennen; dann sei seine Strafe mit der U-Haft abgegolten. Tatsächlich hatte mein Mandant ein Alibi: Er war am Tag des Raubs Vater geworden und hatte diesen Tag im Krankenhaus verbracht. Trotzdem stand er vor der Frage: Bekenne ich mich schuldig und bin frei? Oder sitze ich bis zum Prozess noch monatelang im Knast?

Sprecher:
Auch immer mehr autoritäre Regierungen weltweit nutzen heute Gesichtserkennung –zur Massenüberwachung: In China, dem Land mit der höchsten Dichte an Überwachungskameras, kann das System SkyNet beliebige Großstadtbewohner binnen Sekunden identifizieren. Mit SharpEyes, dem Überwachungsprogramm für Kleinstädte und Dörfer, können Bürger Bilder der Überwachungskameras auf ihrem Smartphone betrachten – und so Blockwart spielen.

In den USA und Australien verbreitet sich vor allem kommerzielle Massenüberwachung: In Einkaufszentren, Casinos, Stadien und Konzerthallen werden Leute mit Hausverbot automatisch abgewiesen; Journalisten und VIPs

erhalten Zutritt zu speziellen Bereichen. Ein beliebtes Einsatzfeld sind auch höchst sensible Institutionen: Schulen und Universitäten. **(6)**

Atmo 11:
Verhaltensanweisung US-Schule im Fall einer Schießerei

Sprecher:
Fliehen, sich verstecken, notfalls kämpfen. In dramatischen Szenen zeigt ein Video des amerikanischen Schuldistrikts Oak Hills bei Cincinnati, wie sich Schüler bei einer Schießerei auf ihrem Campus verhalten sollen. Jahr für Jahr kommt es an Dutzenden US-Schulen zu Schießereien. Ein Grund dafür, dass Tausende Schulen flächendeckend mit Kameras und Gesichtserkennung überwacht werden, berichtet Neil Selwyn, Professor für Erziehungswissenschaften an der australischen Monash University.

O-Ton 16 Neil Selwyn (englisch), darüber Übersetzung:
Mithilfe von Gesichtserkennung versuchen die Schulen, nicht autorisierte Personen von ihrem Campus fernzuhalten. Dies bedeutet aber auch, dass die Schüler ununterbrochen überwacht werden. Eine Untersuchung in einem Bezirk in Texas zum Beispiel zeigt, dass es unter den 5.000 Schülern dort 164.000 Erkennungen binnen einer Woche gab. Ein Schüler wurde sogar 220-mal erkannt.

Sprecher:
An australischen Schulen gebe es kaum Schießereien, erzählt Selwyn, aber ähnlich viele Kameras mit Gesichtserkennung. Die wichtigsten Gründe hier: effizienter Schulbetrieb und Kontrolle der Schüler. Vielerorts wird das Kantinenessen per Gesichtserkennung abgerechnet. Und:

O-Ton 17 Neil Selwyn, darüber Übersetzung:
Während der Pandemie sind vielerorts Systeme der Fernüberwachung entstanden: Schüler und Studenten absolvieren Prüfungen jetzt daheim am Laptop. Online-Systeme identifizieren sie und stellen sicher, dass sie nicht schummeln. Kurz: Alles, was früher die Aufsicht im Prüfungsraum machte, erledigt jetzt die Kamera.

Sprecher:
Sorgen bereitet dem Pädagogen Selwyn das hinter dem Gesichtserkennungs-Boom stehende Schüler- und Menschenbild: Der ideale Schüler verhält sich möglichst unauffällig; er lernt nicht im kritischen Dialog und mit viel Experimentierfreude, sondern speichert passiv Wissen. Er wird erzogen zum braven Bürger in einer tendenziell autoritären Gesellschaft. Für fast alle australischen und amerikanischen Eltern jedoch ist das kein Problem: Sie wollten – zitiert Selwyn Umfragen – vor allem Sicherheit, Effizienz und Komfort an den Schulen ihrer Kinder.

In der EU und Großbritannien verbietet die Datenschutz-Grundverordnung Gesichtserkennung an Schulen, es sei denn, alle Eltern haben zugestimmt. Insgesamt aber stünden auch Europäer der Gesichtserkennung eher positiv gegenüber – wenn sie das Leben erleichtert, meint der in Leiden lehrende Politik-Professor Francesco Ragazzi. **(6)**

O-Ton 17 Francesco Ragazzi (englisch), darüber Übersetzung:

Wenn wir die Leute fragen, ob sie für Massenüberwachung sind, sagen sie natürlich „Nein“. Ganz anders, wenn wir sie fragen: „Haben Sie ein Facebook- oder Gmail-Konto? Würden sie sich mit ihrem Gesicht ausweisen, um schneller in der Metro oder am Flughafen voranzukommen? „Ja“, sagen dann die meisten Leute und sind gern bereit, ihre Daten preiszugeben.

Sprecher:
Nur in Deutschland seien die Menschen etwas kritischer, sagt Ragazzi. Da hätten viele noch Nazizeit und Stasi im Hinterkopf. Wirklich skeptisch aber zeige sich nur eine kleine Minderheit.

O-Ton 18 Francesco Ragazzi (englisch), darüber Übersetzung:
Besorgt um ihre Daten sind Leute, die Probleme mit den Behörden haben: politische Aktivisten, Angehörige sexueller Minderheiten, kritische Journalisten. Bei diesen Leuten handelt es sich allerdings um eine sehr kleine Gruppe; um jene kleine Gruppe von Menschen, die in der Tat befürchten müssen, mithilfe der neuen Technologien überwacht zu werden.

Sprecher:
Und dies nicht ohne Grund: Denn rein technisch ist es heute möglich, die Aufnahmen zehntausender Überwachungskameras abzugleichen mit mehreren hundert Millionen Führerschein- und Passbildern fast aller EU-Bürger – und mit Bildern aus sozialen Medien.

O-Ton 19 Francesco Ragazzi, darüber Übersetzung:
Potenziell lässt sich die bestens erprobte Technik problemlos verbinden mit den gewaltigen Mengen gespeicherter Daten über uns. Rein technisch ist es deshalb durchaus möglich, sehr schnell eine Massenüberwachung einzuführen, wie sie in China bereits existiert. Die Daten über die einzelnen Menschen sind vorhanden, die Algorithmen und die Erkennungstechnologie.

Sprecher:
Und nicht nur das: Im Zweifelsfall hätten Überwacher Zugriff auch auf die GPS-Daten unserer Autos, Daten aus unseren Smartphone-Apps und irgendwann vielleicht auf die unfassbar reichhaltigen Informationen aus unserer DNA. Chinas Regierung sammelt bereits die DNA sämtlicher männlicher Chinesen.

Um einen solchen Alptraum bei uns zu verhindern, fordern in Europa über 200 Organisationen der Zivilgesellschaft ein kategorisches Verbot von Gesichtserkennung im öffentlichen Raum.

Und die EU-Institutionen arbeiten zurzeit an einem Gesetz über künstliche Intelligenz, dem ersten weltweit. Für die Gesichtserkennung blieben die Regeln der Datenschutz-Grundverordnung unverändert gültig, betont Johannes Bahrke, digitalpolitischer Sprecher der EU-Kommission.

O-Ton 20 Johannes Bahrke:
Es ist zunächst einmal verboten, mit klaren Ausnahmen: Suche nach einem vermissten Kind, die terroristische Bedrohung, die unmittelbar ist und konkret, oder Täter oder Verdächtiger schwerer Straftaten. Und auch dann nur durch richterliche

Anordnung. Und dann gibt es auch Beschränkung in Bezug auf die Dauer, auf den Ort, dass man das so eingegrenzt wie möglich nur machen kann.

Sprecher:
„Schöne Worte“, meint der grüne EU-Parlamentarier Patrick Breyer. Aber leider liste der Gesetzentwurf der Kommission eine lange Latte von Straftaten auf, die mit biometrischer Massenüberwachung verfolgt werden dürfen: Gewaltverbrechen, Terror, Kindesmissbrauch, Geldwäsche und so weiter. Die Folge:

O-Ton 21 Patrick Breyer:
Es sind ständig hunderte und tausende Personen zur Fahndung ausgeschrieben. Das heißt: Es gäbe dauerhaft viele gerichtliche Anordnungen, die so etwas erlauben würden. Und damit, im Endeffekt, dass an jeder Straßenecke gescannt wird, ob man vielleicht in irgendeiner Datenbank ausgeschrieben ist zur Fahndung. Und das ist keine freie und offene Gesellschaft mehr.

Atmo 12:
Krawalle 07.07.2017 in Hamburg

Sprecher:
Krawalle wie in Hamburg 2017, Terror, heikle Interessen Mächtiger, Krieg. Kritiker der Gesichtserkennung wie Patrick Breyer befürchten, dass unter massivem Druck auch demokratisch gewählte Regierungen der Versuchung erliegen könnten, alle verfügbaren Machtmittel einzusetzen; auf den Rechtsstaat könne man sich dann nicht immer verlassen. Strikte Gesetze zur automatischen Gesichtserkennung und engmaschige Kontrollmechanismen seien deshalb eine Voraussetzung für unser aller Freiheit.

Abspann:

SWR2 Wissen (mit Musikbett)

Sprecher:
Gesichtserkennung und Tracking. Von Cäcilia und Thomas Kruchem. Redaktion Dirk Asendorpf.

Abbinder

*****

(1) Pete Fussey & Daragh Murray: Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology. Juli 2019: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

(2) Coop is using facial recognition tech to scan and track shoppers. Wired.co.uk 10.12.20:

https://www.wired.co.uk/article/coop-facial-recognition#:~:text=Southern%20Co%2Dop%20is%20using,see%20if%20there's%20a%20match

(3) The Secretive Company That Might End Privacy as We Know IT, NYT 18.1.20: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

(4) Gesichtserkennung prägt die moderne Kriegsführung. NZZ 17.4.22: https://www.nzz.ch/technologie/gesichtserkennung-praegt-die-moderne-kriegsfuehrung-ld.1679422

(5) Mark Andrejevic & Neil Selwyn: Facial Recognition technology in schools: critical questions and concerns. Learning, Media and Technology Vol. 45 2020 Issue 2: https://www.tandfonline.com/doi/full/10.1080/17439884.2020.1686014

(6) Biometric & Behavioural Mass Surveillance in EU Member States – Report for the Greens/EFA in the European Parliament. Oktober 2021: https://www.greens-efa.eu/biometricsurveillance/

Weiterführender Link:
London is buying heaps of facial recognition tech. Wired.co.uk 27.9.21: https://www.wired.co.uk/article/met-police-facial-recognition-new#:~:text=The%20UK's%20biggest%20police%20force,bid%20to%20track%20down%20suspects