Donnerstag, 22. September 2022, 16:00 Uhr
~11 Minuten Lesezeit

Der Schlüssel zum Panoptikum

Digitale Gesichtserkennung könnte schon bald dazu führen, dass jeder unserer Schritte von der Macht beobachtet und bewertet werden kann.

von Willy Meyer
Foto: Maxx-Studio/Shutterstock.com

Nichts ist individueller als das menschliche Gesicht. Nichts lässt sich eindeutiger zuordnen und zugleich

schwerer fälschen. Eher noch kann ein erfahrener Hacker ein Passwort knacken als mit dem „falschen" Gesicht einen Bereich betreten, den er nach Ansicht von Machthabern nicht betreten sollte. Dies gilt im realen wie im virtuellen Raum. Kein Wunder, dass modernste Gesichtserkennungssoftware zum Lieblingsspielzeug der Überwachungsfetischisten geworden ist. China marschiert wie so oft stramm voran und verbindet die Gesichtserkennung mit einem rigiden Social-Credit-System. Vieles spricht dafür, dass auch unsere Zukunft so ähnlich aussehen wird, wie es in den am weitesten „fortgeschrittenen" chinesischen Städten schon jetzt Realität ist.

Damit wir uns künftig bequem und sicher in den entstehenden Smart Cities und dem Internet der Dinge bewegen können, bedarf es einer unfehlbaren Authentifizierung. Nichts scheint da geeigneter als unser Gesicht. In seinem Zoomvortrag „Facial Recognition: Digital ID or Digital Dictatorship?" (1) wirft der Technologieexperte Aman Jabbi einen ebenso kenntnisreichen wie warnenden Blick auf unsere zukünftigen Lebensverhältnisse.

Digitale Gesichtserkennung kommt bereits in vielen Bereichen unseres Alltags zum Einsatz; häufig bietet sie beispielsweise das Smartphone als Entriegelungsfunktion an. Die Moskauer U-Bahn erleichtert ihren Kunden dadurch Zugang und Bezahlung (2), in China öffnet sie den Konsumenten Verkaufsautomaten (3). Die Vorteile liegen auf der Hand: Ein jeder Gesichtsausdruck ist einmalig; diesen zur individuellen Authentifizierung zu nutzen, ist bequem, sicher und zuverlässig, unsere Gesellschaften können sich so vor Missbrauch durch üble Gesellen schützen, Dieben etwa,

Terroristen oder Kindesverführern.

In Shenzen/China gehört die digitale Gesichtskontrolle bereits zum Alltag. Shenzen ist eine sogenannte Smart City, überall verfolgen Kameras die Bürger, sie speichern Autonummern und das Fahrverhalten, Bewegungen in Geschäften und das Einkaufsverhalten und vieles mehr. Bildschirme empfehlen vorbildliches Verhalten, weisen auf Neuerungen hin und geben unverblümt zu, dass alle Bürger ständig beobachtet werden.

Die riesige Menge der gesammelten Daten geht ein in das Sozialkreditsystem, welches für jeden Menschen einen persönlichen Punktestand aufweist und damit einem jeden die soziale Kompatibilität seines Verhaltens spiegelt. 250 Millionen Chinesen sind schon darin erfasst, die große Mehrheit nimmt es hin, und unter jungen Leuten ist es sogar hip, seinen Score auf dem Smartphone zu vergleichen. Es ist ja auch nicht schlimm, man muss sich doch nur an die Regeln halten und tun, was gewünscht ist, wobei es allerdings Algorithmen sind, die die Daten sammeln, auswerten und die Punktestände errechnen.

Das Ergebnis ist ein weitgehend angepasstes gesellschaftliches Verhalten, man beugt sich den Vorgaben, schließlich möchte man vielleicht bald einmal verreisen, eine größere Wohnung anmieten, ein Kind bekommen.

Die freiheitlichen Demokratien des Westens zeigen angewidert mit dem Finger auf derlei Totalitarismus. In der *Zeit* und der *Süddeutschen* echauffiert sich die kritische Journaille (4); den Lesern gebietet der gesunde Menschenverstand, einen solchen Big-Brother-Staat möglichst weit von sich zu weisen. Doch sind gerade die Demokratien des sogenannten Wertewestens auf dem besten Wege, China nicht nur nachzueifern, sondern es überwachungsmäßig gar zu überholen. In London zum Beispiel verfolgen pro 1.000 Einwohner 73 Überwachungskameras jeden

ihrer Schritte — weltweit ist das Platz 3 unter den Großstädten. 2022 sind auf der Erde etwa 20 Milliarden datenlesende Kameras im Einsatz: Sie stecken in Smartphones, Autos, digitalen Hausgeräten, Tablets.

Zusammen bilden sie smarte, mit künstlicher Intelligenz (KI) begabte Wächter, die uns rund um die Uhr ausspionieren und ihre gesammelten Daten in einer Cloud zusammenführen. Abseits einsamer Natur sind wir nirgends mehr ganz allein. Das Internet of Eyes (and Ears) sieht uns auf Kreuzungen, in selbstfahrenden Autos ebenso wie in neueren herkömmlichen Fahrzeugen; Infrarotsensoren scannen den Autoinnenraum, Kennzeichenlesegeräte öffnen Garagen, unser Gesicht entriegelt das Handy und den Rechner, Satelliten verfolgen uns im Freien — und alles nur, damit wir sicher und bequem durchs Leben wandeln. Mit „eyes@home“ bieten auch schon die großen Konzerne des „Stakeholder Capitalism“ (Teilhaberkapitalismus) wie Google, Amazon, Apple, Samsung, Facebook und Microsoft eilfertig ihre Dienste an.

Willkommen im Panoptikum

Wir nähern uns hier dem vom französischen Philosophen Michel Foucault beschriebenen Gesellschaftssystem des Panoptikums an (5). Im beginnenden 20. Jahrhundert wurden Gefängnisse wie Amphitheater angelegt: rundherum viele Etagen hoch die mit Gitterstäben verriegelten Zellen, in der Mitte ein zentraler Wachturm für die Wärter.

Heute werden die menschlichen Wärter ersetzt durch smarte Straßenlaternen, von denen es bis 2030 global mindestens 600 Millionen geben soll. Diese senden pulsierendes LED-Licht und versprechen damit einen Nutzen für die Umwelt und gegen die

Erwärmung des Klimas. Sie können aber auch als „LED Incapacitators“ (deutsch etwa LED-Unfähigmacher) eingesetzt werden, indem sie die Pulsierung ihres Lichts so schnell verändern, dass uns Menschen beim Hinschauen spontan sehr übel wird.

Darüber hinaus verfügen diese smarten Straßenlaternen über Lautsprecher, um Vorübergehende zu instruieren, über „Digital Signage“ (digitale Anzeigentafeln), welche ebenfalls zu Anweisungen taugen, über Sensoren, die die Luftqualität beziehungsweise die Luftverschmutzung messen, über eine Aufladestation für Drohnen in luftpolizeilichem Auftrag und natürlich über einen Sensor zur digitalen Gesichtserkennung.

All diese Laternen stehen drahtlos in Verbindung mit einer Cloud und miteinander. Ihre Scanreichweite beträgt bis zu sechs Meilen, das sind knapp zehn Kilometer. Spätestens mit ihnen verwandelt sich die Sammlung digitaler Daten in eine digitale Überwachung und unsere Welt in eine Art digitales Open-Air-Gefängnis.

Ein neuer Gesellschaftsvertrag

Immer ganz dicht am Puls der Zeit unterbreitete das Weltwirtschaftsforum (WEF) schon 2018 einen neuen digitalen Gesellschaftsvertrag (6), dessen Kern die digitale Identität bildet. Schlüssel zu jeglicher gesellschaftlichen Teilhabe wird der Punktestand des Sozialkreditsystem, und dieser fußt auf drei Säulen: dem „Carbon Credit“ (CO_2-Verbrauchskapital), dem „Reputation Capital“ (Sozialpunktekapital) und dem Impfstatus.

Dieser Vertrag wird freilich nicht öffentlich diskutiert oder gar dem Wahlvolk zur Abstimmung unterbreitet, nein, er soll auf dem Weg der „Global Governance“ (globales Steuerungssystem) durch supranationale Organisationen wie den Vereinten Nationen (UNO)

oder der Europäischen Union (EU) oktroyiert werden. In Verbindung mit dem gleichzeitig einzuführenden digitalen Zentralbankgeld (CBDCs, Central Bank Digital Currencies) und dem dadurch individuell zugewiesenen universellen Grundeinkommen sind die Bürger nun vollends in der Hand der Kontrollalgorithmen.

Möchte man also reisen, einkaufen, die Krankenversicherung in Anspruch nehmen oder einen Freund anrufen, so muss man sich zuerst durch die digitale Gesichtserkennung ausweisen; ein Algorithmus gleicht den aktuellen Sozialkreditpunktestand mit dem Vorhaben des Bürgers ab und schaltet entsprechende digitale Geldeinheiten frei — oder auch nicht. Denn durch die lückenlose Überwachung in den Smart Cities (siehe dazu auch „The 100 Climate-Neutral and Smart Cities by 2030“ der Europäischen Union (7)) wird der individuelle Punktestand stetig neu angepasst, je nachdem, mit wem man sich trifft, was man liest, schaut, hört oder konsumiert. Und unversehens befinden wir uns in der vom WEF angepriesenen Neuen Weltordnung nach dem Great Reset.

Zero Trust

Damit jeglicher Missbrauch ausgeschlossen wird — und gleichzeitig jeglicher Freiraum zugesperrt —, implementieren die großen Softwareanbieter geschlossen das Verfahren „Zero Trust in Cyber Security“ (Null Vertrauen in Cybersicherheit). Damit entfallen alle individuellen Sicherheitsmaßnahmen wie Passwörter oder Pins und auch die https-Verschlüsselung. Der Benutzer kann seinen Zugang einzig mit seinem Gesicht freischalten; im Gegenzug werden eingebaute Kameras und einprogrammierte Algorithmen jeden Tastendruck und Gesichtsausdruck erfassen, speichern und bewerten.

Wir verlassen damit die uns bekannte Welt, in der erlaubt ist, was

nicht verboten ist, und treten ein in die Welt des „Default Denial“ (Standard-Verweigerung), wo Zugang so lange nicht möglich ist, bis wir uns durch unseren Sozialkreditpunktestand als zuverlässig und würdig ausweisen können. Eine Welt, die es in Shenzen und vielen weiteren Städten Chinas bereits gibt.

> ***Der digitale Gesichtsausdruck wird also zum Schlüssel für den Zugang zu allem, was lebensnotwendig ist oder einfach nur Spaß macht.***

Damit auch dieser in sicheren Händen liegt, offerieren Internetfirmen längst IDaaS — Identity as a Service (Identität als Dienstleistung) —, ein Geschäftsmodell mit unermesslichen Wachstumsmargen.

Eine weitere Dienstleistung, für die sich hingegen eher die Hüter der Macht interessieren dürften, ist Geofencing, geografisches Um- oder Einzäunen. Geofencing umreißt den Bewegungsradius des Einzelnen entsprechend seinem Sozialkreditpunktestand, und dies sowohl in der realen wie auch der virtuellen Welt. Der zugeordnete Algorithmus entscheidet, ob man dieses Spiel spielen, jenes Video ansehen oder jenen Avatar benutzen darf. Im Rahmen der im Entstehen begriffenen „15-minute cities“ und „20-minute neighborhoods“ (8) setzt es unserer individuellen Bewegungsfreiheit vorgegebene Grenzen und ahndet Verstöße, beispielsweise durch die entsprechende elektromagnetische Pulsierung eines LED-Incapacitators.

Wer sich nun an verschiedentliche Maßnahmen zur Eindämmung der sogenannten Coronapandemie erinnert fühlt, hat schon einen verlässlichen Vorgeschmack auf unser Leben in den Smart Cities. Es wird die totale Kontrolle unseres Wohlverhaltens sein, zu unser aller Bestem, versteht sich.

Früh übt sich

Die vollständige Überwachung via digitalem Gesichtsausdruck durchdringt jeden Winkel unseres Alltags, um überall Sicherheit zu gewährleisten. Sie übersieht dabei auch die Kleinsten nicht und heftet sich von der Wiege bis zum Berufsbeginn an die Fersen der Kinder.

Schon heute „monitoren“ fürsorgliche Eltern den Umgang ihrer Kinder durch Spielzeug mit integriertem „Talk Pedometer“ (deutsch etwa Kindergesprächsanzeige) (9). Dessen KI belauscht die Kinder beim Spielen und alarmiert gegebenenfalls die Sozialdienste, sollte das Kindeswohl gefährdet sein. Sie scannt jedoch genauso leicht die Unterhaltungen der Eltern mit ihren Kindern auf die gewünschten Erziehungsideale ab. Dass sich Verfehlungen dabei ungünstig auf den zukünftigen Sozialkreditpunktestand der Eltern auswirken werden, liegt auf der Hand.

„We Play Smart“ ist ein Brettspiel, in welchem eine KI Aufgaben und Schwierigkeitsgrade gemäß den Nutzern modelliert (10). Damit gehört es in den Bereich der „Human Capital Value Extraction“ (Abschöpfung des Humankapitalwertes), eines Geschäftsfeldes, das die Entwicklungsmöglichkeiten und späteren Bedürfnisse der jungen Menschen errechnen und abschöpfen möchte.

Im schulischen Bereich geschieht dies über die „Social and Emotional Learning (SEL) Scores“, die Ergebnisse im sozialen und emotionalen Lernen der Schüler. Ziel von SEL ist mitnichten ein Erkenntnis- oder Wissenszuwachs, sondern es sollen bestimmte Einstellungen und Neigungen in den Schülern hervorgerufen und verfestigt werden.

Firmen mit dem Geschäftsfeld der „Human Capital Value Extraction“ nutzen dabei die Testergebnisse der Schüler und treffen

in Verbindung mit ihren „Pathways“ Aussagen über den akademischen Erfolg der Schüler (11); so gibt es dann „Prodigy Asset Groups“ (Wunderkind-Wert-Gruppen), denen eine universitäre Laufbahn mit den entsprechenden Kosten und Gewinnen prophezeit werden. Als lukrativer gelten Schulversager, da im Verlauf ihres Lebens vermutlich eine Vielzahl gesellschaftlicher Interventionen anfallen, auf welche solche Firmen wetten wie Hedgefonds auf fallende Kurse an der Börse.

Wem gehört das Internet?

Ursprünglich angepriesen als Hort der absoluten Freiheit, des unzensierten Austauschs von Meinungen und Informationen, der Möglichkeit zu individueller Entfaltung ist das Internet immer weiter unter die Fittiche großer, global agierender Konzerne geraten, die sich unbequeme Mitspieler einfach einverleiben. Geht das nicht durch freundliche Übernahmen, werden die Regierungen an sich souveräner Staaten oder Staatenbünde durch subtiles Agieren im Hintergrund dazu gebracht, die Aufgabe des kontrollierenden, gar zensierenden Büttels zu übernehmen, wofür der Cyber Resilience Act (Gesetz über Cyberresilienz) der EU ein anschauliches Beispiel liefert (12).

Empfehlungen und Vorgaben von UNO und WEF bringen nun die digitale Identität als globalen Zugangsstandard ins Spiel, wodurch das Internet schnell zum essenziellen Werkzeug der angestrebten „Multi-Stakeholder International Governance“ (13) mutiert, zu dem nur der Zutritt erhält, der sich den Anweisungen der Zero-Trust-Agenda unterwirft, sich brav durch Gesichtskennung authentizifiert und entsprechend seinem vorbildlichen Verhalten ausreichend Punkte auf dem Sozialversicherungskonto sammeln konnte.

Düstere Perspektiven

Von der dräuenden Totalüberwachung aufgeschreckte Bürger mögen nun versuchen, auf lokaler Ebene die Politik so zu beeinflussen, dass keine Überwachungskameras oder 5G-Masten auf öffentlichem Raum installiert werden. Es mögen sogar Mehrheiten entstehen, die dies beschließen und angehen; allein, private Unternehmen werden sich auf privatem Land kaum an solche Einschränkungen beim Datensammeln gebunden fühlen, wurde doch das Sammeln der Kundendaten zu einem wesentlichen Geschäftsbereich fast aller größerer Unternehmen.

Es reicht, sich im örtlichen Supermarkt einmal umzuschauen, wie viele künstliche Augen stets und überall dem Kunden folgen. Auf den dazugehörigen großen Parkplätzen ragen panoptikumartig mit Kameras bestückte Laternenmasten in den Himmel. Und damit sich bloß kein Protest gegen die millionenfach aufgestellten 5G-Masten rege, werden diese in Schornsteinattrappen versteckt oder als Bäume verkleidet.

Private, der Datensammelei verpflichtete Firmen wie Clearview AI von Peter Thiel (14) bieten interessierten Behörden gar Dienste wie das „Predictive Policing“ an, die das Verhalten der Beobachteten auf kriminelle Neigung hin analysieren, ganz wie in Steven Spielbergs Film „Minority Report“ von 2002.

Eine weitere Firma im Bereich der öffentlich-privaten Partnerschaften ist ID.me, welche damit wirbt, für Inklusivität, Diversität und Gleichstellung zu stehen, und die es ihren Kunden ermöglicht, durch die Zusammenführung ihrer Sozialversicherungsnummer und der Gesichtserkennung problemlosen Zugang zu den Diensten etwa ihrer Krankenversicherung und Banken zu erhalten (15).

Und als wäre diese dystopische Welt der sich abzeichnenden Totalüberwachung allen Lebensraums und aller Menschen nicht erschreckend genug, setzt der notorische Vordenker des WEF, Yuval Harari, noch eins drauf und enthüllt das Ziel der supranationalen Eliten in einer Rechenformel: B (biologisches Wissen) mal C (Computerkraft) mal D (Daten) ergibt AHH („Ability to Hack Humans“ — die Fähigkeit, Menschen zu hacken) (16).

Das Tor zum Transhumanismus steht schon sehr weit offen. Die allermeisten Menschen aber, weil sie es gern bequem, sicher und zuverlässig haben und ohnehin in Zeiten von gesellschaftlicher Spaltung, grassierendem Kaufkraftverlust und angedrohter Ressourcenknappheit mit ihren Gedanken ganz woanders sind, scheinen das nicht zu bemerken und folgen der verlockenden Melodie der Internetverheißungen bereitwillig.

Der Legende nach führte derartiges Verhalten in Hameln einst in eine Katastrophe.

Quellen und Anmerkungen:

(1) **https://brandnewtube.com/watch/dr-carrie-madej-aman-jabbi-facial-recognition-amp-digital-prisons_uk2izj91njt43b1.html?lang=turkish** (https://brandnewtube.com/watch/dr-carrie-madej-aman-jabbi-facial-recognition-amp-digital-prisons_uk2izj91njt43b1.html?lang=turkish)
(2) **https://www.themoscowtimes.com/2021/10/15/moscow-metro-introduces-worlds-first-pay-by-face-system-a75300** (https://www.themoscowtimes.com/2021/10/15/moscow-metro-introduces-worlds-first-pay-by-face-system-a75300)

(3) **https://www.theguardian.com/world/2019/sep/04/smile-to-pay-chinese-shoppers-turn-to-facial-payment-technology** (https://www.theguardian.com/world/2019/sep/04/smile-to-pay-chinese-shoppers-turn-to-facial-payment-technology)
(4) **https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2F2019%2F03%2Fchina-regime-ueberwachungsstaat-buerger-kontrolle-polizei%2Fkomplettansicht** (https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2F2019%2F03%2Fchina-regime-ueberwachungsstaat-buerger-kontrolle-polizei%2Fkomplettansicht) und **https://www.sueddeutsche.de/digital/china-kredit-sesame-sozialkredit-ueberwachung-1.4442172** (https://www.sueddeutsche.de/digital/china-kredit-sesame-sozialkredit-ueberwachung-1.4442172)
(5) Michel Foucault, Surveiller et Punir, III., Kapitel 3: Le panoptisme. Gallimard 1975.
(6) **https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf** (https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf)
(7) **https://eurocities.eu/latest/the-100-climate-neutral-and-smart-cities-by-2030/** (https://eurocities.eu/latest/the-100-climate-neutral-and-smart-cities-by-2030/)
(8) **https://www.cnu.org/publicsquare/2021/02/08/defining-15-minute-city** (https://www.cnu.org/publicsquare/2021/02/08/defining-15-minute-city)
(9) **https://www.lena.org/** (https://www.lena.org/)
(10) **https://www.hatchearlylearning.com/technology/weplaysmart** (https://www.hatchearlylearning.com/technology/weplaysmart)
(11) **https://www.pathways.in/static/pathways_prodigies_students**

(https://www.pathways.in/static/pathways_prodigies_students)
(12) **https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Gesetz-uber-Cyberresilienz-neue-Cybersicherheitsvorschriften-fur-digitale-Produkte-und-Nebendienstleistungen_de**
(https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Gesetz-uber-Cyberresilienz-neue-Cybersicherheitsvorschriften-fur-digitale-Produkte-und-Nebendienstleistungen_de)
(13) Deutsche Bedeutung etwa „Internationale Zusammenarbeit staatlicher, halbstaatlicher und privater Interessensverbände auf Grundlage eines selbst gegebenen, global verbindlichen Regelwerks"; siehe auch:
https://de.wikipedia.org/wiki/Multistakeholder-Governance
(https://de.wikipedia.org/wiki/Multistakeholder-Governance)
(14) **https://www.clearview.ai/** (https://www.clearview.ai/)
(15) **https://www.id.me/** (https://www.id.me/)
(16) **https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/**
(https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/)

Dieser Artikel erschien bereits auf www.rubikon.news.

Willy Meyer, Jahrgang 1963, ist alleinerziehender Vater von drei Kindern und Lehrer. Er lebt in Hamburg und engagiert sich seit zwei Jahren lokal für Aufklärung und gesellschaftliche Veränderung.