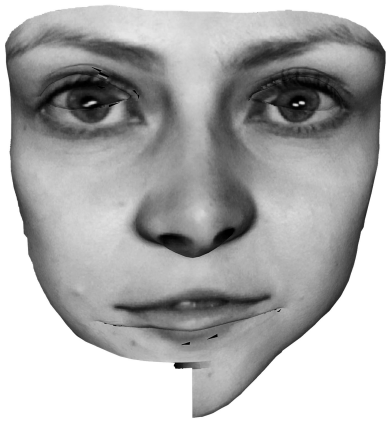


Passwort: Dein Gesicht

Bald werden wir unsere Gesichter im Netz identifizierbar machen. Weil wir es selbst so wollen. Dank fragwürdiger Kommentarschreiber und manipulativer Marketingstrategien.

Von Adrienne Fichter (Text) und Adam Broomberg & Oliver Chanarin (Bilder), 05.07.2018

Seit circa einem Jahr schreiben westliche Medien über das geplante Social-Scoring-System. Alltagsnah und konkret berichten Journalisten, was die Überwachungsoffensive für die Bürgerinnen Chinas bedeutet.

Doch trotzdem konnte sich bis vor kurzem niemand recht vorstellen, wie ein Staat unsere täglichen Gehschritte bewerten kann. Erst die jüngste Nachricht von insgesamt 600 Millionen installierten Kameras in China machte diese Dystopie fassbar.

Denn nun ist klar: Ab dem Moment, in dem man in China zur Tür hinaus auf die Strasse tritt, ist man eine eindeutig identifizierbare Nummer. Wir sind ID 3968467 oder ID 12957346.

Sobald wir eine Bananenschale auf den Boden werfen oder bei Rot über die Strasse gehen, verlieren wir Punkte auf unserem persönlichen Guthabenkonto.

Was in China ab 2020 der Bürgerdisziplinierung dient, wird in den USA bereits angewendet. Auch in gewissen amerikanischen Städten ist man bereits eine Nummer. In Chicago arbeitet die Polizei im Testbetrieb mit dem Gesichtserkennungssystem von Amazon mit dem Namen «Rekognition».

Die gute Nachricht dabei: Geht es bei der Gesichtserkennung um Hardware – also etwa eine Überwachungskamera –, funktioniert der mediale Diskurs. Medien machen Beobachtungen der Polizei publik. Datenschützer appellieren auf ein Recht auf Anonymität. Behörden argumentieren mit öffentlicher Sicherheit und dergleichen.

Unter einer Kamera kann sich jede Leserin etwas vorstellen. Das Internet als Metapher für Überwachung taugt hingegen wenig. Gesichtserkennung

in Form einer Software ist kaum sichtbar. Die Opposition dagegen gering. Die mediale Debatte bleibt aus.

Dafür gibt es auch einen anderen Grund: Software-Hersteller haben sich unsere «Gesichtsfreigabe» in den letzten Jahren laufend erschlichen.

Fake News, gefälschte Identitäten, Roboterprofile – diese Vorfälle haben Plattformen wie Twitter und Facebook in Verruf gebracht. Doch ironischerweise trugen diese Schlagzeilen gleichzeitig zur Popularität der automatisierten Gesichtserkennung bei. Denn nur mit unserer persönlichen Visage sind wir gefeit vor Diebstahl und Rufschädigung im Internet. So lautet das Versprechen von Amazon, Google, Apple oder Facebook.

Die Technik existiert seit 2011

Drehen wir die Zeit um sieben Jahre zurück. 2011 haben die Big Player ihre ersten marktfähigen Prototypen vorgestellt. Facebook in Form der «Tag suggestions»-Funktion, Google mit der «Find my face»-Anwendung.

Damals existierte noch keine Datenschutz-Grundverordnung. Die europäische DSGVO befand sich gerade mal im Ideenstadium (die EU-Kommission verabschiedete einen Plan zur Vereinheitlichung nationaler Datenschutzgesetze). Und weil es noch kein Gesetz gab, das Datenschutz zum Standard verpflichtet, herrschte Laisser-faire.

Dies bedeutete auch: Alle Innovationen waren sofort nach ihrer Geburt aktiv. «Eingeschaltet» war die Norm. Opt-out, das Aussteigen, das die Eigeninitiative jedes Internet-Nutzers erfordert, die Ausnahme. So aktivierten Facebook und Google gleich bei allen Nutzerinnen die automatische Gesichtserkennung.

2011 war also die erste Generation von Gesichtserkennungstechnologie bereits reif für den Markt. Nur war die Gesellschaft noch nicht bereit für die Technologie. Denn Europa pfiff Facebook zurück, dank der Hilfe des irischen Datenschützers. Das Markierungswerkzeug wurde sofort entfernt. Europäische Gesichter blieben damit weiterhin offiziell verschleiert.

Google war in seiner Kommunikation geschickter vorgegangen. Der Suchmaschinen-Konzern präsentierte das Werkzeug bei Google Plus, dem hauseigenen sozialen Netzwerk. Gesichtserkennung soll sich auf das persönliche Umfeld beschränken: Nur wer sich in denselben «Kreisen» bewegte – die Kreise sind das Google-Äquivalent zu Facebook-Freundschaften –, könne sein Gesicht markieren.

Datenbrille 2014 war ein Flop

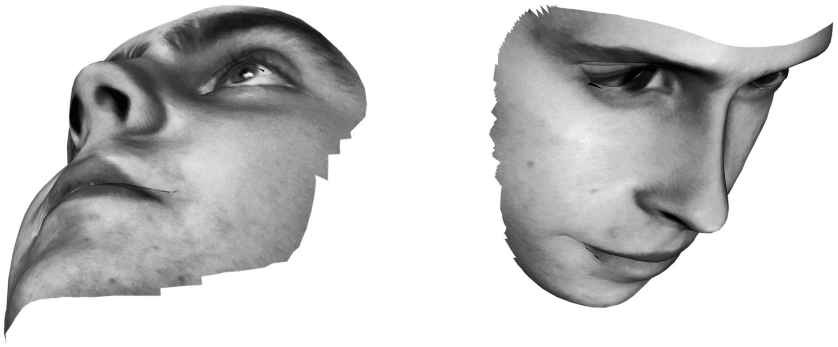
Behutsam wollte Google die Welt an das Thema Gesichtserkennung heranführen.

Der Suchmaschinen-Konzern argumentierte damals mit dem schönen Begriff «Reputationsmanagement». Wer wisse, wo er mit seinem Gesicht im Netz auftauche, habe die Kontrolle über sein digitales Selbst.

Doch auch Google bekam später den Volkszorn zu spüren – nämlich bei der Lancierung der Brille «Google Glass» im Jahr 2014. Niemand wollte auf der offenen Strasse von einem Fremden mit einem futuristischen Brillengestell geröntgt werden.

Google beteuerte zwar stets, keine Gesichtserkennungs-Apps für sein Betriebssystem zuzulassen. Doch wozu sonst spaziert man mit einer Datenbrille durch die Gegend?

Google Glass war ein Flop, der Konzern drosselte die Produktion. Die gesellschaftliche Akzeptanz fehlte 2014 also immer noch. Doch das hielt die Tech-Giganten nicht davon ab, im Hintergrund weiterzutüfteln.



Die Revolution: Das Faceprinting

2014 war auch das Jahr, in dem die Forschungsabteilungen das «Faceprinting» perfektionierten. Der Gesichtsabdruck ist neben der Aufnahme und der Authentifizierung zum wichtigsten Schritt für eine korrekte Gesichtsermittlung geworden. Facebook arbeitet dafür mit einem 3-D-Modell.

Dazu ein kleiner technischer Exkurs: Dank der sogenannten Deep-Face-Technologie wird der vorhandene Bildausschnitt (auch wenn jemand von der Seite fotografiert wurde) mithilfe von mehreren Datenpunkten in einem 3-D-Modell nachgebaut. Die Software fertigt also eine Art Gipsgesicht aus einer Fotografie an. Die Augen dienen dabei als Ankerinformation, weil sie die präzisesten Datenpunkte darstellen. In der Simulation wird das konstruierte 3-D-Gesicht so gedreht, dass es direkt in die Kamera blickt. Wie eine Frontalaufnahme.

Das 3-D-Gesicht wird wiederum mithilfe eines Algorithmus in die zweite Dimension (denn alle unsere Bilder auf Social Media sind 2-D-Aufnahmen) rückübersetzt. Anschliessend folgt der Abgleich mit der Bilderdatenbank von Facebook. Eindeutige Treffer werden gespeichert.

Die Revolution dabei: Konnten Personen zuvor nur mit einer Frontalaufnahme – dem bekannten «Verhaftungs-Mugshot» – richtig identifiziert werden, so war nun die Erkennungsrate auch bei schlechtem Licht oder suboptimalen Seitenaufnahmen hoch.

Kurz: Die Gesichtserkennungstechnologie war also bereits 2014 ausgereift.

Doch das Input-Problem, nämlich die Einwilligung des Nutzers, sein Gesicht herzugeben, war damit noch nicht gelöst. Denn die besten Systeme nützen nichts, wenn sie nicht mit Inhalt gefüttert werden und dazulernen können. Je mehr Bilder in eine Datenbank eingespeist werden, desto genauer wird die Bilderkennungssoftware.

Die Proteste gegen Google und Facebook (und auch gegen die russische App «FindFace», die angeblich jede Person auf der Strasse identifiziert) in Euro-

pa und in den USA haben aber gezeigt: Ein grosser Teil der Bevölkerung war immer noch nicht bereit, ihr Gesicht für die Pläne der Technologie-Konzerne herzugeben.

Die Nutzer mussten gefügig gemacht werden. Die Technologie-Konzerne erhielten dafür externe Unterstützung. Und zwar von unerwarteter Seite: aus Ländern wie Mazedonien, Russland und Bangladesh. Dank Heerscharen von Klick-Arbeitern, Betrügern und Kommentar-Schreiberinnen.

Zahl der Scheinprofile explodiert

Angefangen hat es ungefähr vor fünf Jahren. Erste Medienberichte über sogenannte Klick-Farmen in Asien wurden publik. Zum Beispiel shareyt.com: Die Firma aus Bangladesh generierte auf Anfrage 60'000 Scheinprofile, und diese Fake-Fans müssen dafür dreistellige Beträge bezahlen. 25'000 Klick-Arbeiter sorgten dafür, dass beispielsweise Gurken-Hersteller über Nacht eine Internet-Sensation wurden. Auch wenn es nur eine Schein-Popularität war. Sämtliche Kunden von shareyt.com, zu ihnen zählte auch Coca-Cola, wollen davon nichts gewusst haben.

Der falsche Follower-Handel wurde zum lukrativen Geschäft. Unternehmensmarken, deren Fanzahl auf Facebook im peinlichen dreistelligen Bereich verharrte, erkauften sich bequem eine fiktive Anhängerschaft.

Der rasante Siegeszug von Social Media verhalf Betrügern zu leichter Beute. Noch nie war man so einfach an Bilder und Fotos von Fremden geraten. Das britische National Fraud Intelligence Bureau meldete 2015 gut 33 Prozent mehr Fälle von Identitätsdiebstahl im Netz als im Jahr zuvor. Immer wieder geriet dabei auch die Dating-App Tinder in die Schlagzeilen.

Besonders junge Frauen wurden Opfer von «Scammers» – Betrügern, die mit geklauten Profilbildern Single-Profile kreierten. Kombiniert mit raffinierten Bot-Programmen, die mit unwissenden Männern Unterhaltungen pflegten und diese auf betrügerische Websites lotsten, wandelten sich Flirtversuche in finanzielle Desaster.

Mit den US-Wahlen wurden die Fake-Identitäten zum Politikum. Der Bericht des US-Justizministeriums gegen 13 Russen enthüllte, dass die Internet Research Agency aus St. Petersburg Hunderte Social-Media-Profile von echten amerikanischen Bürgern kreiert hatte.

Damit konnten Zahlungen verschleiert und mit diffamierenden Postings Unruhe gestiftet werden. Auch die beste künstliche Intelligenz kann eine derartige ausländische Einflussnahme nicht verhindern. Denn alle Schritte spielen sich – legal – in den USA ab.

Das Ausmass von Fake-Profilen und geklauten Identitäten wurde für die Plattformen und Online-Dienste immer mehr zum Imageproblem. Wer schon einmal ungewollte Doppelgänger von sich im Internet vorgefunden hat, kennt das Gefühl von Ohnmacht. Die Beweislast lag stets beim Opfer. Ignorante Kundenteams weit weg im Silicon Valley reagierten nicht oder nur mit tagelanger Verzögerung auf die Hinweise.

Timing Matters

Nun, im Jahr 2018, ist die Funktion «automatisierte Gesichtserkennung» wieder zurück und gesellschaftlich akzeptiert. Die Plattformbetreiber legi-

timieren ihr beliebtes Feature mit einem beherzten «Kampf gegen Identitätsdiebstahl».

Wer sich mit seinem Gesicht ausweist, kann verhindern, dass ein krimineller Doppelgänger mit seinen Bildern im Netz Unheil anrichtet. Mittlerweile kennt jeder jemanden, dessen Profil gehackt oder kopiert worden ist. Das langjährige «Reputationsmanagement»-Versprechen von Google trifft nun den Zeitgeist. Timing matters.

Die Konzernchefs Sundar Pichai (Google), Mark Zuckerberg (Facebook) und Jeff Bezos (Amazon) müssten sich also theoretisch bei den Russen, Mazedonierinnen oder Bangladeshern für die Hacking-Attacken bedanken. Je mehr wir Betrügern aufsitzen, desto empfänglicher werden wir für die Sicherheitsverheissungen der Technologie-Branche.

Auch die europäische Datenschutzgrundverordnung DSGVO kommt dabei ganz gelegen. Sie löst das langjährige Kernproblem: unsere Autorisierung als Datenfutter.

«Giving consent» heisst das Schlüsselwort der Stunde. Auf Deutsch: explizite Zustimmung oder eine informierte Einwilligung. Das entsprechende Fensterchen war dezent im obligaten Häkchenformular vom 25. Mai 2018 platziert. Facebook warnte eindringlich: «Verhindern Sie Identitätsdiebstahl, aktivieren Sie die Gesichtserkennung.»

Hauptargument: Schutz der Privatsphäre

Mit einer «sicheren Authentifizierung» wirbt auch eine Hardware-Firma, die darauf stolz ist, nicht mit persönlichen Daten ihr Geld zu verdienen: Apple. «Dein Gesicht ist jetzt dein Passwort.» Das neueste iPhone kann mit einem Faceprint entsperrt werden. (Apple betont, dass die Daten verschlüsselt auf dem Gerät verbleiben.)

Und Amazon bietet an, Bezahlungen mit einem Selfie durchführen zu lassen. Weil es als «sicherste» Art der Transaktion gilt.

Kritiker wie der Privacy-Forscher Wolfie Christl ärgern sich über diese manipulativen Marketingstrategien. Man nennt dieses Vorgehen auch «Nudging» (sanftes Anstupsen). Seit ihren Anfängen vor sieben Jahren gilt Gesichtserkennung als eine der grösste Bedrohungen der Privatsphäre. Ist es daher nicht dreist, dass Technologie-Konzerne gerade mit ebenjenem Schutz werben?

Dabei kann Gesichtserkennung umgekehrt zu Identitätsmissbrauch führen. Auch darauf weisen Wissenschaftler seit 2011 hin. Forscher der Carnegie Mellon University haben damals in einem Experiment mittels der Gesichtserkennung unwissende Studentinnen auf einem Campus identifiziert und in Kürze deren Sozialversicherungsnummern ermittelt.

Auch Apples Entsperrungsfunktion haben verschiedene Sicherheitsforscher bereits überlisten können. Es brauchte dafür einfach einen 3-D-Drucker. Oder ganz analog: jemand, der ein Gipsgesicht detailgetreu anfertigen konnte.

Fazit: Geraten Gesichtserkennungssysteme in falsche Hände oder werden sie ausgetrickst, so sind Konten im Nu geplündert.

Was haben die Grossen damit vor?

Seit 2014 sind die Techniken vorhanden, 97 Prozent der Gesichter wurden in Testversuchen korrekt erkannt. Doch die Resultate blieben in den Forschungslaboren. Denn der Aufschrei der Netzgemeinschaft gegen die Gesichtserkennung liess die Chefetagen von Google, Amazon und Facebook vorerst verstummen.

Heute, im Jahr 2018, scheint der richtige Moment gekommen zu sein. «Angst funktioniert als Technologie-Treiber grundsätzlich recht gut», sagt der Internet-Soziologe Stephan Humer, der regelmässig die gesellschaftliche Akzeptanz von digitalen Innovationen erhebt.

Die vergangenen Cyber-Verbrechen passen hervorragend in die Missbrauchsrhetorik der Plattformbetreiber. Mit der Gesichtserkennung könnte Facebook das Problem der ausländischen Interventionen bei nationalen Wahlen lösen, indem Werbekunden sich zum Beispiel per Gesicht als US-Bürger ausweisen.

Das Wettrüsten geht weiter, die Systeme werden billiger, die Nachfrage wächst. Der Markt für Facial-Recognition-Systeme umfasst heute drei Milliarden Dollar, er soll bis 2021 auf sechs Milliarden Dollar wachsen. Amazon und Microsoft bieten offene Schnittstellen ihrer Systeme an, sodass auch ein Laie sein persönliches Gesichtserkennungsprogramm nachbauen kann.

Nicht bei jedem Grosskonzern ist klar, was er damit plant: Bei Amazon sind Ziele und Einsatzfelder (Verkauf von «Rekognition» für Militär und Unternehmen, wobei sich auch hier intern Widerstand formiert) mehr oder weniger bekannt und stehen unter Beobachtung. Über die Pläne von Facebook – «der weltweit grössten Datenbank von Gesichtsabdrücken» – weiss man wenig. Mehrere Sprecher haben verlauten lassen, dass die Gesichtserkennungsdaten nicht für Werbekunden oder externe Entwickler zur Verfügung stehen.

Das Motiv von Google ist ebenfalls unklar. Aktuell protestieren Mitarbeiter gegen eine Zusammenarbeit mit dem US-Verteidigungsministerium. Streitpunkt war der Einsatz von Google-Überwachungsdrohnen in bewaffneten Konflikten. Die Pentagon-Projekte sind nun auf Eis gelegt.

Damit wissen wir zumindest eines: Googles Gesichtsdaten könnten für alles Mögliche eingesetzt werden, jedoch (vorerst) nicht für die Identifizierung der nächsten Drohnenopfer.

Was steckt hinter den Bildern in diesem Artikel?

Die Fotografen Oliver Chanarin (England) und Adam Broomberg (Südafrika) waren bei einem Besuch in Moskau gleichzeitig fasziniert und beunruhigt, als sie Bilder von Überwachungskameras sahen, die etwa an Zollübergängen, Bahnhöfen oder bei Sportveranstaltungen benutzt werden: Die Kameras erfassen ein Gesicht in Sekundenbruchteilen aus verschiedenen Perspektiven und bauen dann ein 3-D-Modell des Gesichts zusammen, das in einem Datenarchiv aufbewahrt wird.

Fasziniert waren Broomberg und Chanarin, weil es eigenartige, fremd wirkende Porträts waren: Da die betreffenden Personen nichts von der Kamera wussten, fand keinerlei Interaktion mit ihr statt, die Porträts gleichen deshalb Totenmasken. Beunruhigt waren sie, weil die Porträts dazu dienten, mit Fragmenten von Gesichtern abgeglichen zu werden, die zum Beispiel an einer Demonstration aufgezeichnet wurden; die Porträts können dann vor Gericht als Beweismittel eingesetzt werden.

Broomberg und Chanarin organisierten sich eine dieser Kameras und nahmen die Porträts von 120 Menschen auf, eine davon war die politische Aktivistin Jekaterina Samuzewitsch. Sie wurde als Mitglied der russischen Protestgruppe Pussy Riot zu zwei Jahren Gefängnis auf Bewährung verurteilt.

Im Dialog mit der Redaktion

Haben Sie Fragen? Anregungen? Kritik? Lob? Die Autorinnen und Autoren nehmen Ihre Rückmeldungen gerne entgegen. Hier geht es zum Dialog mit der Redaktion.