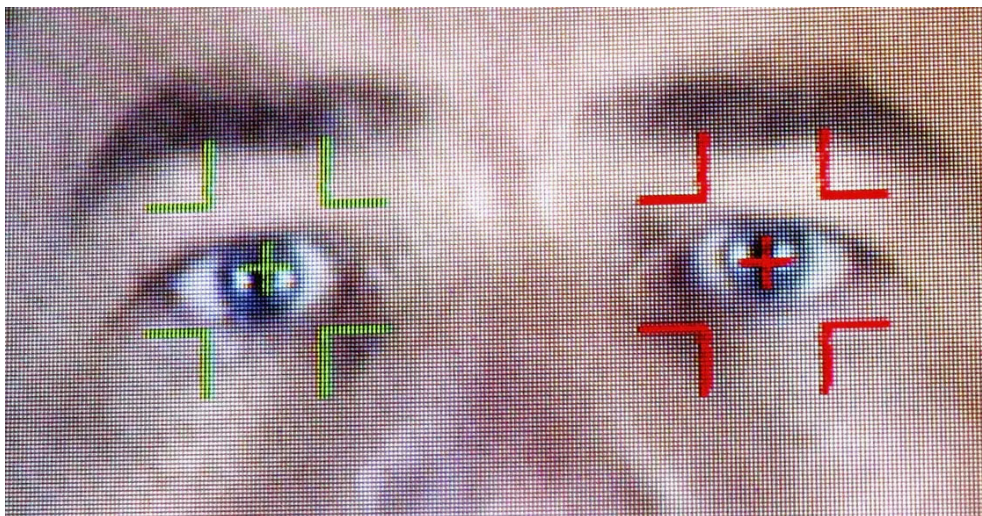


Sand in digitale Augen – der Widerstand gegen die Gesichtserkennung wächst

Die Gesichtserkennung hat in jüngster Vergangenheit rasche Fortschritte gemacht. Doch mit der Leistungsfähigkeit dieser Software wächst – zumindest im Westen – der Widerstand gegen ihre Nutzung.

Stefan Betschon

11.02.2020, 09.39 Uhr



Die Augen sind nur eines von vielen Merkmalen, die bei der Gesichtserkennung analysiert werden.

Ian Waldie / Getty

Der kommerzielle Durchbruch der Gesichtserkennung findet vorerst nicht statt. Zumindest in Europa und in den USA dürfte diese Technik für die Identifizierung von Menschen in naher Zukunft nicht die bedeutende Rolle übernehmen, die man ihr noch vor kurzem zugesprochen hatte. Die Gesichtserkennung ist ausser Rang und Traktanden gefallen. Und das ist gefährlich: Denn jetzt könnte sie ausser Kontrolle geraten.

«Das Gesicht des Terrors»

Die grossen amerikanischen Softwarefirmen zögern bei der Vermarktung dieser Technik, und potenzielle Grosskunden in den USA und in Europa sind auf Distanz gegangen. Doch offenbar sind kleinere Akteure, die sich an ethische Vorgaben nicht gebunden fühlen, bereit, die Lücke auszufüllen. Die junge amerikanische Firma Clearview AI beispielsweise hat eine riesige Fotodatenbank aufgebaut und offeriert auf dieser Basis Gesichtserkennung als Dienstleistung. Die in dieser Datenbank gespeicherten Porträtaufnahmen wurden ohne Wissen der Betroffenen aus dem Internet heruntergeladen.

Die grosse Zeit der Gesichtserkennung begann nach der Jahrtausendwende, als das Zusammenstürzen der Zwillingstürme in New York vielen Amerikanern schlagartig klarmachte, dass ihr Leben auch innerhalb der Landesgrenzen durch terroristische Anschläge bedroht ist. Wenige Tage nach den Terroranschlägen publizierte die amerikanische Visionics Corp. 2001 eine Marketingbroschüre mit dem Titel «Schutz der Zivilisation vor den Gesichtern des Terrors: wie Gesichtserkennung die Sicherheitskontrollen an Flughäfen verbessern kann». Die Redewendung vom «Gesicht des Terrors» verbreitete sich rasch, sie wurde etwa im November 2001 von Politikern aufgegriffen, die in einem Unterausschuss des amerikanischen Senats technische Möglichkeiten der Terrorabwehr diskutierten. Bereits 2002 konnte der Chef von Visionics anlässlich einer Branchentagung einen Aufschwung in Aussicht stellen: Es habe ein «Paradigmenwechsel» stattgefunden.

Heute versucht sich Clearview AI als Vorkämpferin gegen den Terror darzustellen. Im November verschickte die Firma laut Recherchen der amerikanischen Online-Zeitung «Buzzfeed» an potenzielle Kunden in den USA eine E-Mail mit der Behauptung, dass es dank der firmeneigenen Software in New York gelungen sei, einen Terrorverdächtigen sofort zu identifizieren. Der Mann hatte in U-Bahnhöfen Bombenattrappen deponiert. Er konnte verhaftet werden. Doch wie Vertreter der New Yorker Polizei gegenüber «Buzzfeed» erklärten, kam dabei die Software von Clearview AI nicht zum Einsatz.

Die Programmierer von Clearview AI sind nicht die Ersten, die auf die Idee gekommen sind, im Internet auffindbare Porträtaufnahmen ohne Wissen der Betroffenen für Gesichtserkennung zu nutzen. 2011 hatten Informatiker der Carnegie Mellon University gezeigt, dass es mithilfe einer damals handelsüblichen Gesichtserkennungssoftware einfach möglich ist, Fotos von unbekanntem Menschen einem Facebook-Profil zuzuordnen und somit zu identifizieren. Diese brisante Forschungsarbeit hat damals wenig Widerhall gefunden. Doch jetzt hat sich die Stimmung geändert, wiederum hat es einen «Paradigmenwechsel» gegeben.

Verlässliche Leistungsdaten

Wer bei der Google-Suchmaschine den Begriff «Gesichtserkennung» eingibt und die Suchresultate auf Bilder beschränkt, bekommt schöne junge Gesichter zu sehen, auf denen geometrische Figuren eingezeichnet sind. Diese Bilder können zwar nicht zeigen, wie diese Technik funktioniert, aber sie können erklären, warum viele diese Technik fürchten: Das geometrische Konstrukt zerstört wie eine Tätowierung die Schönheit des menschlichen Gesichts. Diese «Mathematisierung» des Gesichts wird als Skandal empfunden.

Manche kritisieren die Leistungsdefizite der Gesichtserkennungssoftware, sie trauen ihr nicht zu, dass sie sich bei der Verbrechensbekämpfung nützlich macht. Andere Kritiker tendieren im Gegenteil dazu, die Fähigkeiten dieser Software zu überschätzen: Sie glauben sich der Möglichkeit beraubt, sich anonym in der Öffentlichkeit zu bewegen.

Wenn über die Leistungsfähigkeit von Gesichtserkennung geredet wird, gilt es die beiden Anwendungsbereiche Verifikation und Identifikation zu unterscheiden. Bei der automatischen Passkontrolle und auch beim Entsperren eines neuen iPhones geht es um eine Verifikation: Dabei werden zwei unter ähnlichen Bedingungen aufgenommenen Porträtbilder miteinander verglichen. Bei der Identifikation muss ein Bild mit Tausenden von Bildern verglichen werden, bis es mit einem namentlich bekannten Menschen in Verbindung gebracht werden kann. Weil die Verifikation sich im Alltag bewähren konnte, wird oft angenommen, dass auch die Identifikation funktionsfähig sei. Diese Annahme ist falsch.

Es ist sehr schwierig, die Leistungsfähigkeit von Gesichtserkennungssoftware zu überprüfen. Es gibt zwar viele synthetische Testverfahren. Doch sie erlauben keine verlässlichen Voraussagen über die Praxis-tauglichkeit einer Software. Feldversuche könnten eine auch für Laien nachvollziehbare Bewertung von Systemen für die automatische Gesichtserkennung ermöglichen. Solche Versuche hat es in den vergangenen 20 Jahren viele gegeben, doch die Testergebnisse werden meist kontrovers diskutiert.

In Deutschland hat die Bundespolizei ab August 2017 während eines Jahres am Berliner Bahnhof Südkreuz die automatisierte Gesichtserkennung einem Test unterzogen. Im Abschlussbericht 2018 wurde behauptet, der Test sei «erfolgreich» gewesen, die Systeme hätten sich «bewährt». Kritiker hingegen bezeichneten die Ergebnisse als «geschönt». Wohl aufgrund der positiven Beurteilung durch die Bundespolizei sah das deutsche Innenministerium im Herbst 2019 in einem Entwurf für ein neues Bundespolizeigesetz die Nutzung der Gesichtserkennung an «sicherheitsrelevanten Orten» vor. Doch wenige Wochen später kamen die Beamten zu einer anderen Einschätzung: In einem neuen Entwurf für das Bundespolizeigesetz, der Mitte Januar publiziert wurde, wird diese Technik nicht mehr erwähnt.

Chinesische Offensive

Die Stimmung gegenüber der Gesichtserkennung ist im vergangenen Jahr gekippt. In den USA haben mehrere städtische Parlamente – beispielsweise in San Francisco – ihren Behörden den Einsatz von Gesichtserkennung verboten. Auch auf Bundesebene und in einzelnen Gliedstaaten der USA gibt es

Bemühungen, den Einsatz dieser Software einzuschränken. Die Reihen des Widerstands hätten sich 2019 geschlossen, schreibt triumphierend die amerikanische Electronic Frontier Foundation in einem Ende Dezember publizierten Bericht. Laut dieser gemeinnützigen, nichtstaatlichen Organisation, die sich für die informationelle Selbstbestimmung engagiert, gab es nicht nur in den USA, sondern auch in mehreren südamerikanischen Staaten sowie in Grossbritannien und Frankreich Widerstandsaktionen gegen Gesichtserkennung.

Doch es war wohl weniger die Gegenwehr westlicher Aktivisten als vielmehr der Enthusiasmus chinesischer Polizeibehörden, der in den USA und in Europa der Gesichtserkennung geschadet hat. Ein Grossteil der Medienberichte, die im vergangenen Jahr in der Deutschschweiz über Gesichtserkennung publiziert wurden, befasst sich mit den Verhältnissen in China. Die Entschlossenheit, mit der die Machthaber in diesem Land den Einsatz der Gesichtserkennung in allen Lebensbereichen ihrer Bürger vorantreiben, dürfte hiesige Medienkonsumenten erschrecken haben.

Die Gesichtserkennung soll in China auch zur Unterdrückung ethnischer Minderheiten eingesetzt worden sein. Wegen solcher Verstösse gegen die Menschenrechte hat die amerikanische Regierung chinesische Hersteller von Gesichtserkennungstechnologie – darunter Hikvision, Megvii, SenseTime oder Yitu Technology – auf eine schwarze Liste gesetzt. Doch auch ohne Kunden in den USA können diese Firmen wachsen, denn sie haben den Export ihrer Technologie in Drittweltländer forciert. Laut einer Studie des amerikanischen Think-Tanks Carnegie Endowment for International Peace setzten mehrere Dutzend Staaten auf Überwachungstechnologie aus China, darunter Brasilien, Kenya, Laos, Simbabwe, Uganda oder Usbekistan.

Grosse Zurückhaltung

Auf die Verbote im Westen reagieren die chinesischen Firmen mit der Forderung nach einer staatlichen Regulierung. Im Zusammenhang mit dem Verbot der Gesichtserkennung in San Francisco sagte der Geschäftsführer von SenseTime im vergangenen Jahr: «Die Regierungen sollten Vorschriften erlassen, anstatt den Einsatz einzuschränken.» Er ahmt so Manager bei Google und von Microsoft nach, die westliche Regierungen auch schon aufgefordert haben, klare Regeln für den Einsatz der Gesichtserkennung festzulegen.

Doch zumindest bei Microsoft ist die Forderung nach staatlichen Vorgaben mit dem Willen zur Selbstregulierung gekoppelt. Brad Smith, Chefjurist bei Microsoft, hat in einem langen offenen Brief die Hersteller in die Pflicht genommen: Bisher hätten sich die Softwarefirmen – das ist ein Seitenhieb gegen

Facebook – an dem Motto «Bewege dich schnell, zerstöre Dinge» orientiert. «Doch wenn wir bei Gesichtserkennung zu schnell vorwärtsmachen, könnte es sein, dass grundlegende Rechte der Menschen kaputtgehen.» Bleibt zu hoffen, dass diese Zurückhaltung, die Microsoft und Google vorleben, in der Branche Nachahmer findet.

Mehr zum Thema



ERKLÄRT

Eine amerikanische Softwarefirma, die im Internet publizierte Fotos analysiert und identifiziert, bedroht die Privatsphäre vieler Menschen. Die wichtigsten Antworten zur automatischen Gesichtserkennung

Die kleine amerikanische Softwarefirma Clearview AI hat im Internet Porträtaufnahmen gesammelt und eine riesige Fotodatenbank für die polizeiliche Fahndung aufgebaut. In den USA gilt das als Tabubruch. Journalisten und Datenschützer sind empört. Ist das das Ende der Privatsphäre?

Stefan Betschon 29.01.2020



Brüssel erwägt temporäres Verbot von Gesichtserkennung im öffentlichen Raum

Die amerikanische, auf Gesichtserkennung spezialisierte Firma Clearview hat eine Datenbank mit drei Milliarden Fotos aufgebaut; die Polizei in den USA nutzt die Dienste des Startups bereits fleissig.

Christoph G. Schmutz, Brüssel, Stefan Betschon 22.01.2020



KOLUMNE

Gesichtserkennung: Der Spiegel im Wasserglas

Es ist zu erwarten, dass sich die Gesichtserkennung weiterhin rasch entwickelt. Bald werden wir alle Burkas tragen müssen. Oder doch nicht?

Stefan Betschon 18.09.2017



Copyright © Neue Zürcher Zeitung AG. Alle Rechte vorbehalten. Eine Weiterverarbeitung, Wiederveröffentlichung oder dauerhafte Speicherung zu gewerblichen oder anderen Zwecken ohne vorherige ausdrückliche Erlaubnis von Neue Zürcher Zeitung ist nicht gestattet.