Das Ende der Anonymität

Ein Experiment mit der Software PimEyes zeigt, wie erschreckend gut Gesichtserkennung bereits funktioniert. Die Suchmaschine für Gesichter verändert unser Leben. VON RUTH FULTERER, FORREST ROGERS (TEXT) UND JONAS OESCH (GRAFIK)

Stellen Sie sich vor, Sie hätten die Superkraft, fremde Menschen zu identifizieren und pikante Details über ihr Leben zu erfahren. Alles, was Sie dazu brauchen, sind ein Foto und ein Handy. Was würden Sie tun? Vielleicht im Strassenverkehr ein Bild machen von dem Typen, der Ihnen die Vorfahrt genommen hat. Vielleicht in einer Bar heimlich ein Foto schiessen, um herauszufinden, wer der gutaussehende Mensch ist, der sich in einer Ecke einen Feierabenddrink gönnt? Vielleicht beim Online-Dating einen Screenshot machen vom Profilbild einer Person, mit der Sie schreiben – um zu sehen, ob sie auch die Wahrheit über sich erzählt?

Was futuristisch und ziemlich gruselig klingt, ist bereits Realität. Ein Unternehmen namens PimEyes hat eine Suchmaschine für Gesichter entwickelt. Um darauf zuzugreifen, braucht es nur einen Internetzugang und ein Abonnement für rund 33 Franken im Monat.

Wie einfach das alles ist, erfahren wir bei einem Selbstversuch. Zuerst laden wir eigene Fotos hoch. Nach ein paar Sekunden tauchen alte Zeitungsartikel und ehemalige Arbeitgeber auf, Bildergalerien von Partys aus jenen Zeiten, in denen noch professionelle Fotografen auf Events Gruppenfotos machten, weil das Selfie noch nicht erfunden worden war.

Von einem Arbeitskollegen erscheinen Bilder, auf denen man ihn kaum wiedererkennt. Statt geschorener Glatze trägt er dunkle Locken, offenbar posiert er als Model. Und eine Passantin, die wir auf dem Sechseläutenplatz treffen und deren Foto wir mit ihrem Einverständnis hochladen, staunt, als wir mit der Software herausfinden, dass sie einen Turnverein nahe Zürich leitet.

Die eigenen Internetsünden herausfinden, schön und gut. Aber kann man mit der Software auch politisch relevante Informationen aufspüren? Wir versuchen, Teilnehmerinnen und Teilnehmer von Demonstrationen zu identifizieren. Im Pressearchiv finden wir ein Bild vom Klimastreik aus dem Jahr 2019: Relativ viele Menschen schauen darauf in die Kamera. Und obwohl das Bild eine Menschenmenge zeigt, ist es nah genug aufgenommen, um Gesichter deutlich zu erkennen. Von jeder fünften Person haben wir mit Hilfe von PimEyes Bilder im Internet gefunden. Jede achte Person konnten wir mit Namen identifizieren. Drei davon haben uns erlaubt, die gefundenen Fotos und ihre Namen zu veröffentlichen. Nicht alle vorgeschlagenen Fotos zeigen auch wirklich die gesuchte Person. Wenn die Menschen auf Schweizer Websites gefunden werden und aussehen wie die auf dem Demo-Bild, gehen wir von einem Treffer aus.

Als Spassprojekt gestartet

Gesichtserkennung ist nicht neu. In den vergangenen Monaten nutzten die ukrainischen Behörden die Technologie, um gefallene russische Soldaten zu identifizieren und deren Familien zu informieren. Sie verwendeten dabei die Gesichter-Datenbank von Clearview AI, die auch von amerikanischen Polizeibehörden eingesetzt wird. Die Software ist allerdings Strafverfolgungsbehörden vorbehalten. Ganz im Gegensatz zu PimEyes, das jeder benutzen kann.

PimEyes ist erst wenige Jahre alt. Zwei polnische Informatik-Studienabgänger programmierten es als Freizeitprojekt, dann zog die Firma auf die Seychellen. Heute hat PimEyes einen georgischen Besitzer. Online gegangen ist die Website 2018 mit Bildern von Donald Trump, Angela Merkel und Jennifer Aniston. Die Prominenten dienten als Beispiel dafür, wie gut die Gesichtersuche im Internet funktioniert. Das machte PimEyes bekannt, und mit der Bekanntheit kam die Kritik: Die Technologie helfe Stalkern und missachte die Privatsphäre der Menschen, deren Gesichter dort auftauchen.

Daraufhin hat sich die Strategie von PimEyes verändert. Heute stellt sich das Unternehmen als Vorkämpfer für die Privatsphäre dar. Auf der Website ist keine Rede mehr vom Suchen fremder Menschen. Stattdessen steht da: «Schütze dein Bildrecht mit PimEyes.» Das hat auch damit zu tun, dass Giorgi Gobronidze die Firma übernommen hat. Der Georgier ist eigentlich Professor für internationale Sicherheit in Tbilissi. In einem Videogespräch erzählt er, er interessiere sich seit den russischen Attacken auf sein Heimatland 2008 für Cybersicherheit. So habe er PimEyes kennengelernt. Nun wolle er mit der Firma Menschen ermöglichen, Kontrolle über eigene Bilder im Internet zu erlangen.

PimEyes bietet seinen Kunden an, Datenschutzbeschwerden an Websites zu schicken, auf denen unerwünschte Bilder von ihnen zu sehen sind. Für 25 Fotos kann man einen Alarm aktivieren, wenn irgendwo im Internet wieder ein ähnliches Bild auftaucht. Für diese Dienste verlangt das Unternehmen 88 Franken, monatlich. Für jene, die auch ganz sicher kein unerwünschtes Foto im Internet übersehen wollen, bietet PimEyes einen – laut eigener Aussage – besonders präzisen Algorithmus. Er heisst «DeepSearch» und gehört zum Advanced-Abo der Firma, welches 328 Franken im Monat kostet.

Pornobilder ausgegraben

Mit diesem Angebot zielt PimEyes auf Menschen wie Cher Scarlett. Sie ist eine erfolgreiche Ingenieurin, in den USA bekannt für ihren Einsatz für Arbeitnehmerrechte in der Tech-Branche. Als sie PimEyes mit einem eigenen Foto ausprobierte, wurde sie von ihrer Vergangenheit eingeholt. Die Software fand pornografische Aufnahmen von ihr. Die Bilder waren markiert mit den Schlagworten «Missbrauch», «Folter», «Teen», «Würgen».

Als Scarlett 19 Jahre alt war, habe sie ein Mann im Internet angeschrieben, ihr Vertrauen gewonnen und sie zu einem Pornodreh überredet, erzählt sie auf der Plattform Medium. Sie bereute ihre Zustimmung schon vor dem Dreh und wehrte sich, aber man zwang sie zum Weitermachen. Lange hatte Scarlett geglaubt, dass die Täter das Material nie veröffentlicht hatten. Bis zur PimEyes-Suche. Die Software hatte die Videos aus den Schmuddelecken des Internets hervorgeholt und mit ihrem Gesicht verknüpft, für jeden auffindbar.

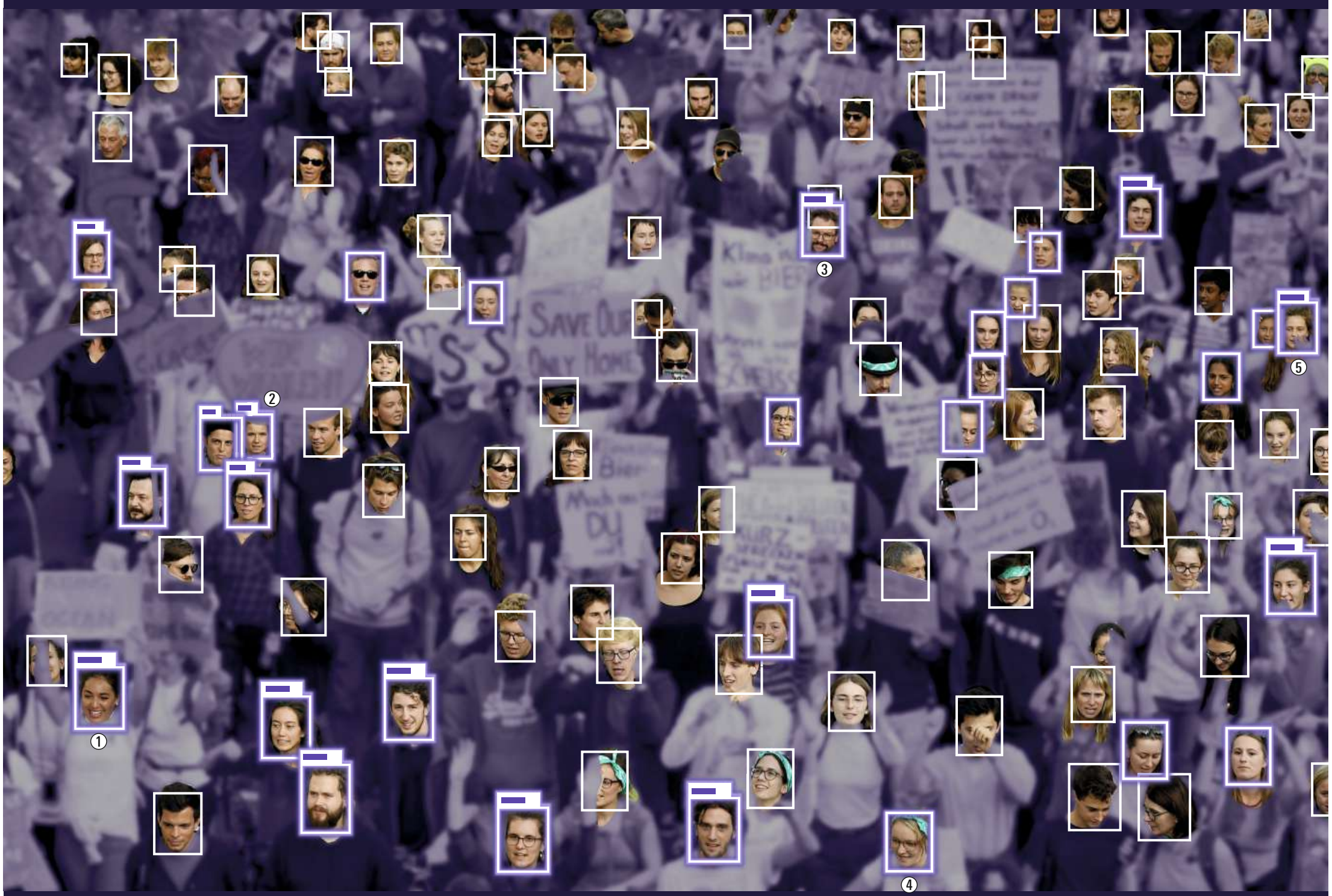
Heute schreibt Scarlett auf Anfrage, dass sie sich das teure Abo nicht dauerhaft leisten könne, um die alten pornografischen Bilder unauffindbar zu machen. Ihrer Meinung nach betreibt das Unternehmen Erpressung: «Wenn es die PimEyes-Suche nicht gäbe, brauchte ich keinen Schutz davor», schreibt sie.

Der PimEyes-Chef widerspricht. Auf Anfrage erklärt er, Scarlett habe ihr Geld inzwischen zurückbekommen. «Keiner muss zahlen, um ein eigenes Foto entfernen zu lassen.» Tatsächlich gibt es eine kostenlose Opt-out-Möglichkeit auf der Website. Das bedeutet: Man kann eigene Bilder aus den Suchergebnissen ausschliessen. Lange war

Ukrainische Behörden nutzten die Technologie, um gefallene russische Soldaten zu identifizieren und deren Familien zu informieren.

Mit der Gesichtserkennungssoftware PimEyes lassen sich viele Teilnehmerinnen und Teilnehmer der Klimademonstration 2019 identifizieren

132 Gesichter sind auf dem Bild erkennbar. Zu 29 Personen hat PimEyes weitere Bilder im Internet gefunden. 16 Personen konnte die NZZ mit Namen identifizieren.



❶ Pamela Giacometti

events.info srk-zuerich.ch pamela giacometti.com

❷ Melanie Wegmann

fachverein.com eatplanted.com

❸ John Flury

solinetz-zh.ch fotointern.ch

PimEyes findet auch Gesichter, bei denen wir zweimal hinsehen müssen.

cevi.ws lgr.ch

«Erstens: Wow. Ich kenne die Fortschritte in der Technologie, aber es ist beeindruckend und ein bisschen beängstigend, wie viele Informationen man so finden kann. Ich finde es bedenklich, wenn private Bilder auftauchen, wie das von mir im Lokal ‹El Toro›. So ein Bild mit Freunden ist zwar ‹unschuldig›, aber ein potenzieller Arbeitgeber könnte es falsch interpretieren. Ohne Kontext kann ein solches Foto ja viele Geschichten erzählen.»

«Als ich kontaktiert wurde, war ich sehr überrascht und ein wenig schockiert. Der Klimastreik ist ja schon länger her, und ich wurde aufgenommen, ohne es wahrzunehmen. Und erkannt, ohne je von dieser Gesichtserkennungssoftware gehört zu haben. Man ist sich heute bewusst, dass mithilfe des Internets sehr viele Informationen über sich selbst zu finden sind. Aber ich finde es krass, dass nun jeder Unbekannte ein Foto von mir in PimEyes einlesen kann und Details wie Name, Arbeitsort und so weiter erfährt. Prinzipiell würde ich beim Thema Gesichtserkennung zwischen privatem und öffentlichem Nutzen unterscheiden. Für polizeiliche Fahndungen, Vermisstenanzeigen und so weiter finde ich es sinnvoll, Gesichtserkennung zu verwenden. Stalking und Fetische werden durch so ein Tool jedoch erleichtert. Ich sehe keinen Mehrwert in der Verwendung durch Privatpersonen.»

«Dass die Gesichtserkennungstechnik schon so weit fortgeschritten ist, überrascht mich zwar nicht. Trotzdem rüttelt mich diese Gegenüberstellung von privater Teilnahme an einer Demonstration und beruflicher Präsenz im Internet schon etwas auf. Diese Verbindung konnten bisher nur Leute machen, die mich gut kennen. Was das für die freie Meinungsäusserung bedeutet, lässt mich Böses erahnen, nicht nur für die Zukunft. Nehmen wir etwa eine Person, welche vor elf Jahren bei den Massenprotesten im Zuge des Arabischen Frühlings fotografiert wurde. Damals war die Technik zwar noch nicht so weit, heute aber eben schon, und sie lässt sich natürlich auch rückwirkend auf Bildmaterial von damals anwenden. Im heutigen politischen Klima in Ägypten halte ich es für absolut möglich, dass Verhaftungen stattfinden auf Basis solcher Aufnahmen.»

Erstaunlich an der Software PimEyes ist, wie wenig Informationen sie braucht, um Personen wiederzuerkennen. Einige der Demonstranten hätten wir in den Suchergebnissen selbst kaum wiedererkannt. Zum Teil tragen sie Sonnenbrille oder Maske – oder sie sind um einiges jünger.

Das Experiment macht glaubhaft, was Studien in den vergangenen Jahren immer wieder nahelegen: Maschinen können Gesichter besser wiedererkennen als Menschen.

sie hinter mehreren Klicks versteckt, jetzt ist sie prominent sichtbar. Doch laut Scarlett funktioniert diese Funktion nicht richtig, PimEyes zeige immer noch Bilder ihres Missbrauchs an.

Es gibt Anzeichen dafür, dass PimEyes nicht nur auf Kunden abzielt, die ihre Privatsphäre schützen wollen. In der teuren «Advanced»-Option kann man den vorher beschriebenen Alarm für 500 Fotos aktivieren. Es klingt unplausibel, dass jemand so viele Bilder vom eigenen Gesicht hochlädt, um sich zu schützen.

Vielmehr eignet sich dieser Alarm als Stalking-Instrument. Stellen wir uns vor, eine Frau verlässt ihren Partner. Dieser stalkt und terrorisiert sie, so dass sie sich gezwungen sieht, umzuziehen und ihren Namen zu ändern. Nun könnte der Ex-Partner einen Alarm für ihre Bilder aktivieren. Das würde bedeuten, dass er automatisch informiert wird, wenn PimEyes ihr Gesicht irgendwo im Netz entdeckt. Wenn sie auf dem Schnappschuss eines Partyfotografen auftaucht oder auf der Homepage des neuen Arbeitgebers, wüsste er sofort, wo sie jetzt lebt.

Recherchen des Portals Netzpolitik und der NGO AlgorithmWatch zeigen, dass an PimEyes und FaceClone – einer App, die ähnlich funktioniert wie PimEyes, aber dazu noch russische soziale Netzwerke durchsucht – vor allem Männer interessiert sind. Sie stöbern damit in der Vergangenheit ihrer Partnerinnen, suchen Dates oder fremde Frauen aus dem Internet. Oder sie finden die Identität von Pornodarstellerinnen heraus, um sie zu erpressen.

Der PimEyes-Chef Giorgi Gobronidze hält dagegen. Im Videointerview lässt er einen kaum zu Wort kommen mit seinem Schwall an Rechtfertigungen. Die Mehrheit der zahlenden Nutzer sei weiblich. Sowieso sei Gesichtserkennung bereits Realität und PimEyes zumindest ein ethischer Anbieter. So habe man seit dem Ukraine-Krieg russische Anwender blockiert. Zudem würden alle Suchen überwacht und Nutzer beispielsweise gesperrt, wenn sie Kinder suchten. Man verzichte auch darauf, Bilder von Social-Media-Websites zu verlinken. «Es gibt gratis illegale Seiten, die zum Stalken besser geeignet sind», sagt der Unternehmenschef.

Auf der Website der Firma steht: «PimEyes stellt nur ein Werkzeug bereit, und der Nutzer ist verpflichtet, es mit Verantwortung zu nutzen. Jeder kann einen Hammer kaufen und damit entweder gestalten oder töten.»

Männer stöbern in der Vergangenheit ihrer Partnerinnen, suchen Dates oder fremde Frauen aus dem Internet.

Fehlende Einwilligung

PimEyes bewegt sich mit seinem Service in einem rechtlichen Graubereich. In der Schweiz werden biometrische Daten, anhand deren man eine Person identifizieren kann, mit der derzeitigen Überarbeitung des Datenschutzgesetzes als «besonders schützenswert» eingestuft. In einem Jahr wird es in Kraft treten. Das Identifizieren von Personen bleibt erlaubt, wenn ein «überwiegendes Interesse» geltend gemacht werden kann.

Im europäischen Datenschutzrecht ist es hingegen grundsätzlich verboten, identifizierende biometrische Daten wie Fingerabdruck, Stimme, DNA oder eben ein Gesicht ohne Einverständnis zu verarbeiten. PimEyes aber stellt es so dar, als wäre alles in Ordnung, solange jeder sich selbst sucht – und dabei die erforderliche Zustimmung erteilen kann.

Unerwähnt bleibt dabei das Datensammeln, welches nötig ist, um diesen Service überhaupt anzubieten: Man kann sich die PimEyes-Suche wie einen Google-Suchalgorithmus vorstellen, nur mit Gesichtern statt mit Wörtern. Damit die Suche funktioniert, muss das Unternehmen vorher das Netz nach Inhalten durchkämmen und diese sortieren. Die Google-Suche verarbeitet Wörter, PimEyes Gesichter, beide bauen eine Datenbank. Nur so kann eine Internetsuche funktionieren. Damit unterscheidet sich Gesichtsidentifikation auch grundsätzlich von der Authentifizierung per Gesichtsscan, wie etwa am Flughafen oder um Geräte zu entsperren. Dafür ist keine grosse Datenbank nötig.

Um die PimEyes-Datenbank zu erstellen, wäre nach europäischem Recht wohl eine Einwilligung der Personen auf den Fotos nötig. Eine solche wurde aber nie eingeholt. Deshalb hat etwa der Datenschutzbeauftragte von Baden-Württemberg ein Verfahren gegen das Unternehmen eröffnet.

Betrug am Skilift aufdecken

PimEyes ist nicht die einzige Firma, die Gesichter identifizieren kann. Die grossen Tech-Unternehmen haben ähnliche Algorithmen entwickelt. Doch sie sind damit zurückhaltender.

Im Google-Betriebssystem Android können Nutzer zwar in den eigenen Fotoalben nach ähnlichen Gesichtern suchen – die Internetsuche mit Google-Bildern schliesst biometrische Merkmale aber absichtlich aus. Auch auf den Verkauf von Gesichtserkennung an Firmenkunden verzichtet Google vorerst und fordert von den Regierungen klare rechtliche Leitplanken.

Amazon wiederum verkauft seinen Gesichtserkennungsalgorithmus bereits an Firmenkunden, etwa an Hersteller von smarten Überwachungskameras. Diese können Alarm schlagen, wenn eine unbekannte Person vor dem Haus auftaucht. Oder wenn ein bekannter Ladendieb in einen Supermarkt zurückkehrt.

In der Schweiz wird die Technik bereits an ersten Orten eingesetzt: In St. Moritz überprüfen Skiliftbetreiber mit Gesichtserkennung, ob sich verschiedene Fahrer einen Tagespass teilen. Der Zürich-Marathon stellte dieses Jahr ein Tool zur Verfügung, mit dem man per Gesicht Fotos von Teilnehmenden suchen konnte.

In Schottland und Brasilien experimentieren Schulen mit «smarten» Kameras, die Schüler identifizieren. Sie sollen die Kinder vom Schwänzen abhalten, deren Sicherheit erhöhen oder auch einfach das Bezahlen des Mittagessens praktischer machen.

So findet die Software das richtige Gesicht

ful. · Wie genau PimEyes funktioniert, hält das Unternehmen geheim. Aber alle einschlägigen Softwares arbeiten nach ähnlichen Prinzipien, wie Sébastien Marcel sagt. Er forscht am Idiap-Institut in Martigny zu biometrischen Methoden.

Die Programme basieren auf dem sogenannten Deep Learning. Das ist eine Methode der künstlichen Intelligenz, bei der ein komplexer Algorithmus mit sehr vielen Daten trainiert wird. Marcel sagt: «Für das Training sind eine bis sechs Millionen Bilder nötig. Darin sollten Tausende verschiedene Personen vorkommen, mit jeweils ein paar hundert Bildern.» Oft bestehen diese Trainingsdatensätze aus Aufnahmen von Schauspielern. Wichtig ist, dass das Gesicht jeder Person in allen möglichen Varianten zu sehen ist: lachend, mit Brille, nach unten schauend, rufend, schlafend, im Profil. Anhand dieses Datensatzes werden zwei wichtige Dinge trainiert: Erstens, dasselbe Gesicht wiederzuerkennen, egal wie jemand blickt. Zweitens, nach welchen Kriterien man Personen am besten unterscheidet.

Das Ergebnis des Trainings mit den Promi-Bildern ist ein Umrechnungsalgorithmus, der aus jedem Foto eines Gesichts einen Zahlencode macht. Wenn man zwei Fotos derselben Person analysiert, ändern sich nur ein paar Stellen im Zahlencode. Wenn es sich um zwei Bilder ganz verschieden aussehender Personen handelt, ist auch der Zahlencode komplett anders. Indem man die Zahlencodes vergleicht, hat man also einen Wert für die Ähnlichkeit zweier Bilder. Man kann auch sagen: ein Mass für die Wahrscheinlichkeit, dass es sich um dieselbe Person handelt. Diesen Umrechnungsalgorithmus wendet PimEyes auf alle Fotos an, welche die Software im Internet finden kann. Für jedes Gesicht, das im Internet zu sehen ist, speichert die Website also einen Zahlencode – und dazu den Link auf die Webseite, auf der das Bild zu sehen ist.

Um ein Gesicht zu suchen, muss man es hochladen. Mit einem Algorithmus wird auch aus diesem Bild ein Code erzeugt. Dann sucht die Website in ihrer Bibliothek aus Gesichtercodes nach Treffern und zeigt die zugehörigen Bilder und Webseiten an.

Wäre es nicht praktisch, wenn die Technologie zu jedem Gesicht gleich die Kontakte auf Social Media einblenden würde?

Diese Systeme unterscheiden sich von PimEyes insofern, als dass sie keine Datenbank mit Milliarden von ohne Einverständnis gesammelten Gesichterdaten mitliefern. Liftbetreiber, Schulen oder Marathonveranstalter legen die Datenbank während der Verwendung der smarten Kameras selbst an. Nicht alle Menschen im Internet sind darin, sondern nur die direkt betroffenen.

Wenn alles korrekt läuft, müssten die abgespeicherten Personen vorab aufgeklärt werden und sich damit einverstanden erklären. Umstritten ist, wie dies praktisch umgesetzt werden kann. Das beschäftigt auch Erik Schönenberger. Der Informatiker setzt sich mit dem Konsumentenschutzverein Digitale Gesellschaft für ein Verbot von Gesichtserkennung im öffentlichen und strenge Regulierung im privaten Bereich ein. «Würden beispielsweise die Migros oder die SBB Gesichtserkennung einführen, dann hätten die Nutzerinnen und Nutzer keine echten Alternativen. Dann sind sie gezwungen zuzustimmen.»

Die Digitale Gesellschaft hat gemeinsam mit dem Verein AlgorithmWatch und Amnesty International Unterschriften gesammelt, um in Zürich und Lausanne die Gesichtserkennung zu stoppen. Man wolle eine Debatte anstossen, sagt Schönenberger, und das sei auf Gemeindeebene am einfachsten.

Schönenberger ist in einem Wettlauf gegen die Zeit. «Das Bewusstsein entsteht langsam, doch die Technologie ist ja bereits da.» Er fürchtet, dass die Debatte von der Realität überholt wird, wie damals in den 1990er Jahren, als es um die Präsenz von Kameras im öffentlichen Raum ging. Überwachungskameras breiteten sich aus, heute sind sie Alltag.

Akzeptanz wird getestet

Wenn Ähnliches auch in Sachen Gesichtserkennung passiert, stehen die Anbieter bereit. Facebook, heute Meta, hat die Funktion zum automatischen Erkennen von Nutzern zwar abgestellt und eine Datenbank mit einer Milliarde Gesichtern gelöscht. Das gilt jedoch nicht für den Algorithmus, der Gesichter wiedererkennt. Das Unternehmen hält sich die Möglichkeit offen, dieses System wieder einzuführen, wenn die Zeichen der Zeit günstiger stehen.

Vor einem Jahr hat Meta gemeinsam mit dem Hersteller Ray-Ban eine smarte Brille lanciert, der man nicht ansieht, dass sie fotografieren und filmen kann. Technisch gesehen wäre mehr möglich, etwa im Gesichtsfeld erste Informationen zur Umgebung einzublenden. Aber damit wartet der Konzern lieber ab. Das Unternehmen teilte relativ offen mit, dass es erst ausprobieren möchte, ob die Menschen es akzeptieren, ständig und überall gefilmt zu werden.

Meta ist damit nicht allein. In allen Big-Tech-Firmen forschen ganze Abteilungen am Metaversum – der Vision, dass digitales und analoges Leben verschmelzen werden. Dann könnte einem eine smarte Brille etwa den richtigen Weg zum bestbewerteten Asia-Restaurant direkt im eigenen Gesichtsfeld einblenden. Wenn man im Tram den schicken Lederschuh eines Pendlers betrachtet, würde einem der Link zum Online-Shop angezeigt. Und wäre es nicht praktisch, würde die Technologie zu jedem Gesicht gleich die Social-Media-Kontakte einblenden? Vor zehn Jahren wäre wohl eine Mehrheit gegen so eine Entwicklung gewesen. Wer damals die probeweise lancierte Google-Glass-Brille trug und die Umgebung damit filmte, wirkte nicht cool, sondern gruselig. Träger wurden bisweilen sogar verprügelt.

Seitdem hat sich die Gesellschaft verändert. Soziale Netzwerke haben uns daran gewöhnt, dass unsere Erlebnisse online eine Spur hinterlassen. Es ist ganz alltäglich, dass Menschen mit dem Smartphone fotografieren und filmen und diese Bilder im Netz teilen – ohne darauf zu achten, wer auf dem Foto sonst noch zu sehen ist. Mit der neuen Superkraft hat all das aber andere Konsequenzen als früher. Egal, wo Sie unterwegs sind und was Sie tun: Wenn ein Foto davon im Internet landet, dann wird man Sie für immer damit in Verbindung bringen können. Ihr Gesicht wird Sie verraten.