



2016/22 Lifestyle

<https://jungle.world/artikel/2016/22/das-ende-der-anonymitaet>

Gesichtserkennungssoftware

Das Ende der Anonymität

Von **Enno Park**

Was bisher Sicherheits- und Geheimdiensten vorbehalten war, kann heute jeder. Ein beliebiges Foto von einer Menschenmenge schießen und mit der App »FindFace« herausfinden, um wen es sich im einzelnen handelt. Wirksame Gegenmaßnahmen gibt es kaum.

Ein Vorgeschmack auf die Konsequenzen der App »FindFace« ist die Hetzjagd, die User des russischen Bilderforums »2channel« auf Prostituierte und Pornodarstellerinnen kürzlich veranstalteten. Sie besorgten sich Fotos der Sexarbeiterinnen auf einschlägigen Websites und identifizierten sie mittels »FindFace«. Anschließend sandten sie Links zu deren Pornofilmen und Sexannoncen an deren Lebenspartner, Familienmitglieder und Freunde auf VKontakte, dem russischen Pendant zu Facebook. »Wenn sie nicht rumhuren, sondern sich mit normalen Typen wie uns abgeben würden, gäbe es diese Aktion nicht«, schreibt einer der User auf »2channel« als Rechtfertigung für seine Veröffentlichung. Seither nimmt die Diskussion um »FindFace« in Russland kein Ende, zumal immer neue Experimente zeigen, wie mächtig die Software ist. So wurde der russische Software-Entwickler Andrei Mima 2010 gebeten, ein Foto von zwei Frauen zu machen und ihnen diese anschließend zuzuschicken – allerdings vergaßen sie, ihre Kontaktdaten zu hinterlassen. Sechs Jahre später lud er die Bilder in »FindFace« hoch, konnte die beiden Frauen identifizieren und ihnen die Bilder schließlich doch noch schicken, wie er freudig im Netz bekannt gab. Noch weiter ging der Versuch des Fotografen Egor Tsvetkov aus Sankt Petersburg. Er machte zahlreiche Fotos von Menschen in der Moskauer U-Bahn, die bewusst verwackelt oder aus verschiedensten Winkeln aufgenommen waren. Rund 70 Prozent der fotografierten Personen konnte er anschließend identifizieren. Er wollte mit seinem Projekt zeigen, dass es mit Software wie »FindFace« keine Anonymität mehr im öffentlichen Raum gibt.

Wer die technologische Entwicklung der vergangenen Jahre verfolgt hat, dürfte von den Ereignissen nicht überrascht sein. Bereits seit den sechziger Jahren gab es Versuche, Computern das Erkennen menschlicher Gesichter beizubringen. Das funktionierte allenfalls unter Laborbedingungen mit genormten Fotos von Gesichtern, bis dem Neuroinformatiker Christoph von der Malsburg an der Universität Bochum der große Durchbruch gelang. Seine Software »ZN Face« konnte erstmals Gesichter wiedererkennen, die aus

verschiedenen Richtungen und bei unterschiedlicher Helligkeit aufgenommen waren. Mittlerweile ist diese Technik allgegenwärtig. Computer vergleichen am Frankfurter Flughafen die Gesichter der Reisenden mit ihren Passfotos – wenn auch bisher nur die von EU-Bürgern und auf freiwilliger Basis. Die Systeme sind so ausgefeilt, dass sie auch erkennen, wenn jemand versucht, ein lebensgroßes Foto einer anderen Person vor die Kamera zu halten. Der chinesische Internetriese Alibaba arbeitet daran, Zahlungen per Smartphone und Gesichtserkennung möglich zu machen. Passwörter und Zahlencodes würden damit der Vergangenheit angehören. Spielkasinos wollen bekannte Spielsüchtige bereits am Eingang erkennen und abweisen. Mit der Gesichtserkennungssoftware »Churchix« können Pfarrer feststellen, wer an ihren Gottesdiensten teilnimmt, wovon dem Hersteller zufolge weltweit 30 Kirchengemeinden Gebrauch machen. Immerhin müssen sich die Pfarrer die Vergleichsfotos ihrer Schäfchen vorab noch selbst besorgen. Und der Futterspender »Bistro« kann gar die Gesichter von Katzen auseinanderhalten und entsprechend Futter zuteilen. Die Überwachungskamera »Netatmo Welcome« hat nicht nur ständig die Eingangstür im Blick, sondern erkennt die Gesichter der zum Haushalt gehörigen Personen und schlägt Alarm, sollten Fremde in der Wohnung auftauchen. Das Gerät kann unter anderem bei Amazon für weniger als 200 Euro bestellt werden. Und wer selber so etwas bauen möchte: »Open Face« ist eine freie Gesichtserkennungssoftware, die jeder aus dem Netz herunterladen und nach eigenen Wünschen anpassen kann. Eigentlich ist also »FindFace« nichts Besonderes, auch wenn die Software aus Russland den Ruf hat, zu den besten und schnellsten der Branche zu gehören. Neu an »FindFace« ist, dass eine solche Software erstmals Zugriff auf ein großes soziales Netzwerk hat – nämlich das russische VKontakte. Wer dort kein Profil unterhält, hat bis auf weiteres wenig zu befürchten. Die großen Internet-Firmen wie Facebook oder Google geben ihre Datenschätze für eine solche Software bislang nicht her – schon um Skandale zu vermeiden. Allerdings verfügt Facebook selbst über eine Gesichtserkennungssoftware und verwendet sie in »Facebook Moments«. Wenn verschiedene Leute Fotos auf einer Feier machen, erkennt Facebook das und stellt für alle Beteiligten ein entsprechendes Fotoalbum zusammen. Nicht jedoch in Deutschland, wo die Funktion gegen Datenschutzgesetze verstößt.

Allerdings helfen Datenschutzgesetze nur auf den ersten Blick gegen den Kontrollverlust. Es ist eher eine Frage der Zeit, bis es Hackern gelingt, große Mengen von Fotos samt zugehörigen Namen und weiteren Angaben zu erbeuten und mit Software wie »FindFace« durchsuchbar zu machen. Ist das in der EU illegal, steht der Server eben in Russland. Wird er im europäischen Internet geblockt, ist sie per VPN-Tunnel erreichbar – eine Technik, die kein Spezialwissen mehr ist, seitdem Zuschauer von Streamingdiensten solche VPN-Tunnel massenhaft nutzen, um Filme und Serien ansehen zu können, die nur in anderen Ländern angeboten werden.

Gesichtserkennung à la »FindFace« kann hierzulande zwar verboten werden, das dürfe aber nicht von ihrer Nutzung abhalten. Um Verbote werden sich auch Staaten und Sicherheitsbehörden nicht kümmern, die Gesichtserkennung für moderne Formen der Rasterfahndung einsetzen. Aber ausgerechnet Geheimdienste werden nervös angesichts der aktuellen Entwicklung: Wenn jede Person von solchen Systemen enttarnt werden kann, bedeutet das auch, dass es für Agenten nicht mehr ausreicht, mit falschem Pass und angeklebtem Bart durch die Gegend zu laufen. Ausgerechnet die seit 2010 für Pässe und Personalausweise vorgeschriebenen biometrischen Passfotos machen dem BND

Probleme – aber auch das Internet. So legt der BND für seine Scheinidentitäten auch Profile auf sozialen Netzwerken wie Facebook an. Und die könnten leicht auffliegen, würde jemand die Fotos anhand einer entsprechenden Gesichtserkennungssoftware vergleichen. Deshalb will der BND nun 100 000 Euro für ein Forschungsprojekt ausgeben, das klären soll, inwiefern sich die Fotos der eigenen Agenten so verfremden lassen, dass sie Software überlisten können, den zugehörigen Menschen aber weiterhin ähnlich sehen. Solche Möglichkeiten bleiben der Normalbevölkerung verschlossen, zumal es wenig hilft, auf Facebook ein verfremdetes Foto zu verwenden, wenn die Gesichtserkennung auf der Überwachungskamera an der nächsten Ecke läuft. Deshalb schlägt der Designer Adam Harvey in seinem Projekt »CV Dazzle« seltsame asymmetrische Frisuren und kontrastreich geschminkte Gesichter vor, die Gesichtserkennungsalgorithmen verwirren sollen. Solange die aber nicht in Mode sind, dürften Menschen, die so gestylt herumlaufen, eher Aufsehen erregen als ihre Anonymität zu schützen. Da es keine wirksamen Möglichkeiten gibt, die eigene Anonymität zu schützen, bliebe noch die Flucht nach vorn: Post-Privacy oder der radikale Verzicht auf Anonymität. Der Gedanke dahinter: Wenn wir all unsere Schwächen kennen und offenlegen, müssen wir uns nicht für sie schämen und sind nicht mehr erpressbar. Das ist natürlich reine Utopie, solange es Länder gibt, in denen Minderheiten verfolgt werden, oder Gesellschaften, die offen feindlich gegenüber Homosexuellen eingestellt sind. Auch in Ländern, wo Frauen im Netz regelmäßig Opfer von verbalen Übergriffen und Stalking werden, ist Post-Privacy eher etwas für Privilegierte.