Matthias Monroy

Wozu nutzt Interpol Gesichtserkennung?

Die internationale Polizeiorganisation entwickelt ein System, mit dem unbekannte Personen mithilfe von Lichtbildern identifiziert werden sollen. In einer Datei speichert Interpol Fotos und Videos, die von Internetanbietern und anderen Firmen stammen. Für die Gesichtserkennung hat Interpol auch Dienste von Clearview ausprobiert.

Die US-amerikanische Firma *Clearview AI* hat rund drei Milliarden Bilder von Menschen aus dem Internet eingesammelt und daraus eine Datenbank zur Gesichtserkennung erzeugt. Das hatte die New York Times vor sechs Wochen berichtet[1]. Die Bilder stammen größtenteils aus Profilfotos Sozialer Medien, vermutlich werden auch die dazugehörigen Nutzerdaten bei Clearview gespeichert. Clearview bietet Firmen und Behörden an, mit einer Abfrage der Datenbank Personen zu identifizieren. Die Gesichtsbilder können Berichten zufolge auch mit einer Foto-App abgefragt werden, die Anwendung ist der New York Times zufolge[2] unter „Reichen" verbreitet.

Das US-Magazin Buzzfeed ist an eine Kundenliste von Clearview gelangt[3]. Darauf stehen über 2.200 Firmen, Regierungen und Polizeibehörden, darunter auch Interpol. Die weltweit tätige Polizeiorganisation hat demnach mehr als 320 Suchanfragen durchgeführt.

„Monitoring-Plattformen, Industrie und kommerzielle OSINT"

Das Interpol-Generalsekretariat in Lyon hat den JournalistInnen bestätigt, dass „eine kleine Anzahl von Beamten" die Anwendung genutzt hat. Es gebe jedoch keine Geschäftsbeziehung mit Clearview, vielmehr habe es sich um einen kostenlosen 30-Tage-Probeaccount gehandelt.

Das ist plausibel, denn die Organisation entwickelt derzeit ein eigenes System zur Gesichtserkennung. Im April vergangenen Jahres startete Interpol das zweijährige Projekt DTECH, das Fotos und Videos aus Sozialen Medien verarbeitet. Interpol erhält die Dateien auf offiziellem Weg, schreibt das deutsche Bundesinnenministerium[4]. Demnach basiert DTECH auf Gesichtsbildern, die über „nationale Behörden, regionale Monitoring-Plattformen, Industrie und kommerzielle OSINT" bereitgestellt werden. Sie werden anschließend bei Interpol gespeichert.

Wie Clearview wird auch DTECH zur Identifizierung von Personen genutzt. Laut der Bundesregierung sollen damit unbekannten Personen „nominelle Daten" (also Personendaten, Ausweisnummern, etc.) zugeordnet werden. Allerdings ist nicht bekannt, mit welchen Referenzdateien bei Interpol die über DTECH erlangten Gesichter abgeglichen werden. Möglich wäre dies im Projekt *Facial, Imaging, Recognition, Searching and Tracking*[5] (FIRST), mit dem unbekannte Terrorismusverdächtige identifiziert werden sollen.

Neue Datei mit Fahndungsfotos

Einen ersten Anlauf startete FIRST in Gefängnissen im Niger. Interpol hat von dortigen Anti-Terrorismus-Behörden Gesichtsbilder erhalten und diese zunächst in eigenen Dateien gesucht. Anschließend wurden die Fotos unbekannter Personen als sogenannte *Blue Notices* zur Identifizierung und Aufenthaltsermittlung an die 192 Interpol-Mitgliedstaaten verteilt. Sofern die dortigen Behörden über ein Gesichtserkennungssystem verfügen, können die Fotos dort mit eigenen Beständen verglichen werden. Beim Bundeskriminalamt (BKA) ist dies die INPOL-Datei, dort sind derzeit rund 5 Millionen Gesichtsbilder durchsuchbar gespeichert.

Auch Interpol baut derzeit eine als *Criminal Information System* (ICIS) bezeichnete Datenbank mit Gesichtern auf. Dabei handelt es sich um Bilder, die im Rahmen von Fahndungsersuchen aus den Mitgliedstaaten ohnehin bei der Polizeiorganisation verfügbar sind. Sie werden auf ihre Eignung zur Gesichtserkennung überprüft und anschließend in einer eigenen „Gesichtserkennungsdatenbank" gespeichert. Im vergangenen Jahr waren dort rund 54.000 Personendatensätze mit durchsuchbarem Lichtbild[6] gespeichert.

Die neue Datei kann nach Angaben von Interpol[7] von den Behörden aller Interpol-Mitgliedstaaten abgefragt werden. Die dabei genutzte Software zur Gesichtserkennung *MorphoFace Investigate* stammt von der Firma Safran Identity and Security. Auch das BKA will die „Gesichtserkennungsdatenbank" nutzen, seit 2016[8] scheiterte dies aber aus Gründen des Datenschutzes. Fraglich ist das Verfahren[9], nachdem andere Polizeibehörden über „Treffer", also gefundene Gesichter, informiert wer-

Matthias Monroy

Matthias Monroy[7] Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift *Bürgerrechte & Polizei/CILIP*[8]. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Alle Texte unter *digit.so36.net*, auf englisch *digit.site36.net*, auf Twitter *@matthimon*. Viel zu selten auf der Straße (dafür im Internet) gegen Faschismus, Rassismus, Sexismus, Antisemitismus. Kein Anhänger von Verschwörungstheorien jeglicher Couleur. Benutzt das Binnen-I trotz Gepolter nervtötender Maskulisten.

den. Zuerst muss im BKA überprüft werden, ob es sich nicht um einen *false positive* handelt – also ein Gesicht irrtümlich „erkannt“ wurde.

Clearview will Bilder von Polizeien

Interpol betreibt mit den *Red Notices* außerdem eine Datenbank mit gesuchten und zur Verhaftung ausgeschriebenen StraftäterInnen. Jeder Mitgliedstaat kann diese Fahndungen an beliebige andere Interpol-Mitglieder verteilen. Denkbar ist, dass Interpol das Internet nach Informationen zu dort gespeicherten Personen durchsucht. Falls die Betroffenen beispielsweise über Accounts in Sozialen Medien verfügen, könnten diese Informationen bei der Aufenthaltsermittlung helfen. Eine derartige Nutzung bietet auch Clearview seinen NutzerInnen an.

Laut OneZero[10] bittet Clearview auch Polizeibehörden um Gesichtsbilder, das US-Magazin hat einen entsprechenden Mailwechsel über eine Informationsfreiheitsanfrage erhalten. Schon jetzt nutzen Clearview und seine Konkurrenten demnach Fahndungsfotos von abgegrasten Internetseiten, auf denen Bilder aus der erkennungsdienstlichen Behandlung durch US-Polizeien abrufbar sind. Eine ähnliche Datei[11] findet sich auch auf der Interpol-Webseite. Clearview könnte sich auf diese Weise als Hilfspolizistin andienen, indem etwa alle drei Milliarden Gesichtsbilder mit polizeilichen Fahndungen abgeglichen und etwaige Treffer an die Polizei verkauft würden.

Aus Datenschutzgründen dürften die Polizeien aber den eigenen Abgleich bevorzugen. Laut dem Hamburger Datenschutzbeauftragten Johannes Caspar wäre beispielsweise die Nutzung von Diensten wie Clearview nicht grundsätzlich problematisch. Rechtswidrig wäre aber, wenn die polizeilich abgefragten Gesichtsbilder bei einem privaten Anbieter liegen.

Arbeitsgruppe zur Gesichtserkennung

Für die verschiedenen Verfahren zur Gesichtserkennung hat Interpol eine *Facial Recognition Working Group* eingerichtet, an der auch das BKA teilnimmt. Zu den Sitzungen werden Polizeien aus Australien, Frankreich, Israel, Großbritannien und den USA eingeladen. Die Behörden stellen dabei neue Techniken und Anwendungsgebiete für Gesichtserkennung vor.

Die Themen der Gruppe hat das Bundesinnenministerium in der Antwort auf eine schriftliche Frage[12] benannt. Demnach erörtern die TeilnehmerInnen Möglichkeiten zur „Umsetzung der Gesichtserkennung auf nationaler Ebene“, die „Internationale Zusammenarbeit im Bereich der Gesichtserkennung und des Datenaustausches“ sowie „Entwicklungsschritte im Bereich der Gesichtserkennung“. Dort erlangte Informationen können „auch in die Weiterentwicklung nationaler Systeme einfließen“. Gut vorstellbar, dass auf einer dieser Sitzungen auch die Nutzung von Clearview behandelt wurde.

Quelle: https://netzpolitik.org/2020/wozu-nutzt-interpol-gesichtserkennung/

Anmerkungen

1 *https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html*
2 *https://www.nytimes.com/2020/03/05/technology/clearview-investors.html*
3 *https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement*
4 *https://dip21.bundestag.de/dip21/btd/19/086/1908683.pdf*
5 *https://www.interpol.int/Crimes/Terrorism/Identifying-terrorist-suspects*
6 *http://dipbt.bundestag.de/dip21/btd/19/059/1905954.pdf*
7 *https://www.interpol.int/How-we-work/Forensics/Facial-Recognition*
8 *http://dipbt.bundestag.de/doc/btd/18/106/1810604.pdf*
9 *http://dipbt.bundestag.de/doc/btd/19/019/1901908.pdf*
10 *https://onezero.medium.com/clearview-ai-we-are-working-to-acquire-all-u-s-mugshots-from-past-15-years-645d92319f33*
11 *https://www.interpol.int/How-we-work/Notices/View-Red-Notices*
12 *http://dipbt.bundestag.de/doc/btd/19/019/1901908.pdf*

Marie Bröckling

Neue Überwachungs-Werkzeuge für die saarländische Polizei

Mit Änderungen am Polizeigesetz will die schwarz-rote Landesregierung den Weg frei machen für neue Tools zur digitalen Beobachtung. Geplant sind unter anderem die anlasslose Videoüberwachung und die elektronische Fußfessel. Nicht nur der Paragraf zur geplanten Spähsoftware ist noch reichlich holprig.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Ein neues Polizeigesetz für das S… nächsten Monaten im Landtag S… den. Der Polizei stünde dann ne… Verfügung, beispielsweise die elektronische Fußfessel, Bodycams und Spähsoftware.

Heute gaben eingeladene ExpertInnen ihre Verbesserungsvorschläge zu den geplanten Änderungen ab. Auch ich bin als Sachverständige im Innenausschuss und habe vorab eine schriftliche Stellungnahme eingereicht[2]. Hier die wichtigsten Punkte zusammengefasst.

…liche Verpflichtung, …gnisse auszubauen

In dem Gesetzentwurf aus dem CDU-geführten saarländischen Innenministerium heißt es, dass sich gesetzgeberischer Handlungsbedarf unter anderem aus dem Urteil des Bundesverfassungsgerichts zum BKA-Gesetz[3] ergebe. Diese Argumentation ist nicht neu: Immer wieder haben PolitikerInnen den Ausbau der polizeilichen Befugnisse in den letzten drei Jahren mit rechtlicher Notwendigkeit begründet[4].