PRIVACY NEWS

STIFTUNG DATENSCHUTZ

Aus Sicht der Stiftung Datenschutz

Privatsphäre für das Antlitz

Frederick Richter, LL. M.

Als ich vor genau zwei Jahren für diese Zeitschrift eine erste Kolumne zum Thema Gesichtserkennung beisteuern durfte,[1] ahnte ich, dass eine weitere folgen könnte. Das Bekanntwerden der aktuellen Praktiken des Unternehmens *Clearview AI* aus den USA gibt nun guten Anlass dazu. Ebendort und auch in Kanada sollen etliche Ermittlungsbehörden in großem Stil Bilddaten nutzen, die das private Unternehmen aus öffentlich zugänglichen Datensammlungen entnahm.[2]

Wohin wird die Entwicklung wohl gehen? Und: Schützt uns nicht der Datenschutz vor ubiquitärer Gesichtsdatenverarbeitung? Über ersteres lässt sich derzeit nur spekulieren – entweder in dystopischer Richtung, mit China als Wegweiser, auf dem Weg zur Totalüberwachung des öffentlichen Raums. Oder etwas zuversichtlicher, mit San Francisco als Vorbild, wo Gesichtserkennungsmaßnahmen durch öffentliche Einrichtungen im vergangenen Frühjahr von der Kommunalverwaltung verboten wurden.[3]

Hilft denn nicht die DSGVO?

Letzteres ist eine spannende Frage. Die automatische Verarbeitung abgelichteter Gesichtsfelder als biometrische Daten erfolgt im Falle von *Clearview* den bisherigen Medienberichten zu Folge vor allem unter Nutzung öffentlich abgreifbarer Daten, mittels Durchkämmens des frei zugänglichen Internets, vor allem der üblichen sozialen Netzwerke. Indem Personen Bilder von sich selbst, die als Referenzmaterial für Gesichtserkennungsprogramme dienen können, ohne technische Zugangsschranken für Suchmaschinen ins Netz stellen, machen sie die im Bild enthaltenen personenbezogenen Daten öffentlich zugänglich. Das ist insofern entscheidend für den Datenschutz, als dass nach Art. 9 Abs. 1 DSGVO die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person zwar grundsätzlich untersagt ist. Nach Abs. 2 lit. e) dieser Norm aber ist die Verarbeitung dann erlaubt, wenn die betroffene Person die Biometriedaten „offensichtlich öffentlich gemacht hat". Denn dann wird eine besondere Schutzbedürftigkeit nicht mehr angenommen.[4] Ob dabei immer ein ausreichendes Bewusstsein vorliegt, dass mit dem Hochladen eines Fotos des eigenen Gesichts zugleich sensible biometrische Daten zugänglich gemacht werden, darf gleichwohl bezweifelt werden.

Frederick Richter ist ständiger Autor bei „Privacy in Germany". Seit Anfang 2013 leitet er die in Leipzig ansässige Bundesstiftung für Privatheit und Datenschutz. *(Foto: Lorenz Becker)*

Bevor man sich der Frage der Rechtmäßigkeit der Clearview-Praxis weiter nähert, steht die Frage im Raum, ob die DSGVO hier überhaupt zur Anwendung kommen und somit Betroffenen aus Europa helfen kann. Denn das Unternehmen *Clearview* scheint seine Dienstleistung gar nicht in der Europäischen Union anzubieten.

Helfen denn nicht Aufsicht und Politik?

Gewisse Unruhe und der Wille, etwas entgegenzusetzen, sind jedenfalls spürbar. So hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte – die schweizerische Datenschutzaufsicht auf Bundesebene – angekündigt, bei *Clearview* in New

1 Aus Sicht der Stiftung Datenschutz: Gesichtserkennung auf dem Vormarsch; Heft 2/2018.
2 Eine Software schockiert *Amerika*; Süddeutsche Zeitung vom 20. 1. 2020; abrufbar unter: www.sueddeutsche.de/digital/gesichtserkennung-clearview-app-polizei-gesicht-1.4764389.
3 San Francisco is first US city to ban facial recognition; Pressebericht vom 15. 5. 2019, abrufbar unter: www.bbc.com/news/technology-48276660.
4 *Schulz*, in: Gola, DSGVO, Art. 9, Rn. 23.

York ein Auskunfts- und Löschbegehren stellen zu wollen. Der Beauftragte wolle „stellvertretend für die betroffenen Personen in der Schweiz“ das Auskunfts- und Löschgesuch in Bezug auf Daten zu seiner eigenen Person stellen.[5]

Die Politik ist noch nicht entschieden, wie sie sich der Herausforderung stellen will. So hatte die EU-Kommission kurz vor dem Bekanntwerden der *Clearview*-Praxis zunächst eine Art Moratorium zur Gesichtserkennung angekündigt. Ein mehrjähriges Verbot solle Zeit verschaffen. Die Anwendung der brisanten Technologie sollte in der EU erst dann erlaubt werden, wenn sie deutlich ausgereifter ist und wenn ein adäquater Regulierungsrahmen geschaffen ist. Kurz vor Redaktionsschluss des vorliegenden Heftes dann stand das angekündigte Verbot wieder in Frage. Auch die Bundesregierung scheint hin- und hergerissen. Zunächst sah der innenministeriale Entwurf zu einem neuen Bundespolizeigesetz eine eigene Rechtsgrundlage vor, wonach Daten aus Überwachungskameras automatisch mit biometrischen Daten hätten abgeglichen werden können. Wohl nicht zuletzt unter dem Eindruck des *Clearview*-Falles wurde der Passus wieder getilgt. Mit dem Gesetzesentwurf hatte erreicht werden sollen, dass an 135 deutschen Bahnhöfen und 14 Verkehrsflughäfen entsprechend ausgerüstete Kamerasysteme eingesetzt werden können. Nun wolle der Bundesinnenminister erst im parlamentarischen Verfahren darüber diskutieren. Die Opposition im Bundestag fordert mittlerweile ein Verbot des Gesichtserkennungseinsatzes.

Längst nicht jeder Schuss ein Treffer …

Wie wenig ausgereift die derzeit verfügbare Technik noch ist, zeigt die geringe Trefferquote. In dem öffentlichen Versuch am Berliner Bahnhof Südkreuz hatte selbst das beste der drei dort getesteten Systeme nur eine Trefferquote von 65,8 Prozent erreicht.[6] Zuzugestehen ist dabei, dass es technisch deutlich schwieriger ist, mit an öffentlichen Plätzen eingesetzten Systemen Gesichter aus Menschenmengen zu erfassen und mit einem Datensatz abzugleichen als – wie im Falle von *Clearview* – ein konkret vorliegendes Gesicht in einer Datenbank zu finden.

Ein fast schon erheiterndes Resultat lieferte die noch nicht perfekte Technik zur Personensuche Ende 2018 ausgerechnet in China, dem „Mutterland der Gesichtserkennung“. Dort gehört es zum guten Ton der Alltagskontrolle und Volkserziehung, dass Bürgerinnen und Bürger, die Verwaltungsunrecht begehen, indem sie Straßenübergänge bei roter Ampel überqueren, für dieses unerwünschte Verhalten öffentlich gebrandmarkt werden. Auf Monitoren an der Straße wird nach Erkennen des Individuums ein Foto mit dem Namen gezeigt – auf dass sich die Person derartige Unbotmäßigkeiten das nächste Mal doch besser zweimal überlegen möge und bei „rot“ gefälligst stehenbleibe. Opfer dieses “naming and shaming” wurde infolge des Einsatzes der Erkennungstechnik eine der erfolgreichsten Geschäftsfrauen des Landes – obwohl sie an der fraglichen Straßenkreuzung gar nicht anwesend war. Der Scanner hatte ihr Gesicht korrekt erkannt und zugeordnet; er hatte es allerdings lediglich auf einer Werbeanzeige für das von der Frau geführte Unternehmen auf einem an der roten Ampel vorbeifahrenden Bus „gesehen“.[7]

Was die Datensammelpraxis von *Clearview* anbelangt, so plant *Twitter* nun gegen das Abgreifen von Fotos aus seinem Angebot vorzugehen. Doch die Chancen dessen sind unklar. Im vergangenen Jahr war bereits das Netzwerk *LinkedIn* damit gescheitert, dem Datenanalyseanbieter *hiQ* zu verbieten, die öffentlich zugänglichen Mitgliederdaten abzuschürfen.[8]

Zu erwarten ist jedenfalls, dass das Thema Gesichtserkennung die Leserinnen und Leser der PinG auch weiter beschäftigen wird. Im Alltag ist die Technik längst angekommen. Viele Menschen nutzen die Technologie freiwillig – um bequem ihr Smartphone zu entsperren.

5 Statement des EDÖB zur Applikation Clearview vom 21. Januar 2020, abrufbar unter: www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#1146521667.

6 Bericht des CCC zur Videoüberwachung: „Der Südkreuz-Versuch war kein Erfolg“; abrufbar unter: www.ccc.de/de/updates/2018/debakel-am-suedkreuz.

7 Facial recognition camera catches top businesswoman „jaywalking“ because her face was on a bus; Meldung abrufbar unter: www.abacusnews.com/digital-life/facial-recognition-camera-catches-top-businesswoman-jaywalking-because-her-face-was-bus/article/2174508.

8 Entscheidung des United States Court of Appeals for the Ninth District No. 17-16783; D.C. No. 3:17-cv-03301-EMC; abrufbar unter: www.eff.org/document/hiq-v-linkedin-ninth-circuit-decision.