Beitrag: **Überwachung per Gesichtserkennung: Ende der Privatsphäre?**

Bericht: Jochen Taßler, Niklas Schenk
Datum: 30.01.2020

Georg Restle: „Und jetzt zu einem der größten Datenskandale unserer Zeit. Stellen Sie sich mal vor, dass Ihre privatesten Facebook-Fotos, intime Details, sich plötzlich auf den Computern US-amerikanischer Polizeibehörden wiederfinden. Falls Sie das für ein völlig ausgeschlossenes Horrorszenario halten, liegen Sie allerdings falsch. Denn genau das ist passiert. Das US-Unternehmen Clearview hat Milliarden an Fotos aus dem Internet in einer Datenbank gesammelt und diese an Polizeibehörden verkauft; darunter auch Fotos aus Europa und Deutschland. Ein Skandal, der bei uns völlig undenkbar wäre? Jochen Taßler und Niklas Schenk zeigen Ihnen jetzt, was mit Gesichtserkennungsprogrammen bei uns schon alles möglich ist.“

Nachrichten im US-Fernsehen (Übersetzung Monitor): „Clearview AI kann persönliche Informationen nur anhand eines Fotos herausfinden.”

Es ist vielleicht der größte Daten-Raub unserer Zeit.

Yvonne Hofstetter, Autorin und IT-Unternehmerin: „Niemand hatte bis jetzt die Dreistigkeit, Daten auf diese Art und Weise abzugreifen.“

Das US-Startup „Clearview AI” hat offenbar drei Milliarden Bilder von Gesichtern aus dem Netz gezogen und in einer Datenbank gespeichert.

Nachrichten im US-Fernsehen (Übersetzung Monitor): „Sie können jemanden clearviewen und so alle Bilder von ihm im Netz finden.”

Praktisch jeder könnte so mit einem Klick identifizierbar sein.

Thomas Zerdick, Referatsleiter IT Policy, Europäischer Datenschutzbeauftragter: „Da werden einfach Informationen eingesaugt und benutzt."

Die New York Times schreibt schon vom „Ende der Privatsphäre". Und das steckt dahinter: Mit Hilfe von Gesichtserkennungs-Software kann Clearview offenbar Bilder von Gesichtern mit rund drei Milliarden Aufnahmen in einer gigantischen Datenbank abgleichen. Darin sind öffentlich zugängliche Fotos gespeichert – inklusive Link, woher sie stammen. Die Vergleichsbilder in der Datenbank hat Clearview etwa aus sozialen Medien wie Facebook abgegriffen. Was öffentlich zugänglich war, wurde automatisiert abgesaugt – ohne Zustimmung der Nutzer, ohne Kontrolle. Mit der Software könnten Stalker zum Beispiel mit einem Klick privateste Daten über ihre Opfer herausfinden. Arbeitgeber könnten Mitarbeiter und Bewerber komplett durchleuchten, Behörden könnten Bürger ausforschen. Clearview verkauft sein Programm bislang offenbar vor allem an staatliche Stellen. Hunderte US-Polizeibehörden sollen die Software schon getestet oder gekauft haben. Diese Frau etwa soll mit Hilfe von Clearview eines Diebstahls überführt worden sein. Die Software glich ihr Fahndungsbild mit der Datenbank ab. So kamen die Ermittler auf ihr Facebook-Profil. Und konnten sie an ihrem Tattoo endgültig zuordnen. Bei Ermittlungen kann so eine Software hilfreich sein. Aber was, wenn Fehler passieren? Wo liegen die Grenzen?

Yvonne Hofstetter, Autorin und IT-Unternehmerin: „Das ist eine neue Dimension, mit der wir konfrontiert sind und wir haben im Moment auch dafür, wie für viele andere Dinge in der Digitalisierung, noch keine Lösung."

In Deutschland wird Clearview bislang offenbar nicht eingesetzt. Aber die Frage, wie wir mit so einer Technologie umgehen wollen, betrifft uns genauso. Auch hierzulande werden Technologien zur Gesichtserkennung an vielen Stellen bereits eingesetzt oder getestet. Berlin – Bahnhof Südkreuz. Bis vor kurzem haben Bahn und Bundespolizei hier Gesichtserkennung in Echtzeit erprobt. Freiwillige wurden gefilmt und per Software mit Test-Datenbanken abgeglichen. Künftig könnten so Straftäter auf der Flucht gefasst werden. Aber dann würden eben auch Unbeteiligte aufgezeichnet. Datenschützern geht das zu weit, auch, weil die Fehlerquote bislang hoch ist. Bundesinnenminister Seehofer wollte die Echtzeiterkennung trotzdem auf vielen Bahnhöfen und Flughäfen einführen. Nach den Enthüllungen zu Clearview legte er das Projekt auf Eis – vorerst. Andere Gesichtserkennungssysteme sind längst im Einsatz. Passkontroll-Systeme etwa an Flughäfen. Die Dresdener Firma Cognitec stellt solche und andere Systeme her. Die Branche erlebe gerade einen Aufschwung, sagen sie hier.

Elke Oberg, Cognitec Systems GmbH: „Die letzten fünf Jahre werden in unserer Industrie als Gesichtserkennungsrevolution bezeichnet, weil von 2013 bis 2019 die Genauigkeit unglaublich zugenommen hat."

Cognitec hat auch Programme im Angebot, die mit Hilfe automatischer Gesichtserkennung Fotos mit Datenbanken abgleichen können. Beim BKA und auch in einigen LKAs ist diese Technologie bereits im Einsatz. Etwa um herauszufinden, ob Verdächtige bereits in Polizeidatenbanken registriert sind. Das mache die Arbeit effizienter und diene der Sicherheit, sagen Befürworter. Datenschützer warnen.

Thomas Zerdick, Referatsleiter IT Policy, Europäischer Datenschutzbeauftragter: „Das allgemeine Problem ist, dass in dem Moment, wo man anfängt, solche Daten zu erheben, dass dann der Datenhunger immer größer wird."

Wie groß der Hunger werden kann, zeigt ein Blick nach Hamburg. 2017 kam es beim G20-Gipfel zu heftigen Krawallen. Bis heute laufen Verfahren gegen Randalierer. Um Straftaten nachweisen zu können, haben die Behörden gigantische Mengen an Videomaterial gesammelt. Es wurde sogar ein Portal eingerichtet, wo jeder Privataufnahmen hochladen kann. Das Material wird nun mit Gesichtserkennungssoftware nach Verdächtigen durchforstet. Aber auf den Bildern sind auch viele Unbeteiligte, die rein zufällig in der Nähe waren – oder auf den vielen friedlichen Demos. Die Gesichter tausender unbescholtener Demonstranten seien biometrisch erfasst und gespeichert worden, kritisiert der Hamburger Datenschutzbeauftragte Johannes Caspar.

Johannes Caspar, Datenschutzbeauftragter Hamburg: „Erstens weiß kein Mensch, ob er überhaupt in diesem Material drin ist. Und zweitens ist vollkommen unklar, in welcher Weise dieses Material dann im Endeffekt verwendet wird."

Lukas Theune ist Anwalt. Er vertritt auch G20-Beschuldigte. Am Beispiel eines aktuellen Mandanten zeigt er uns, auf wie viel Material die Ermittler zugreifen können. Allein in diesem Fall wurde über eine Stunde Bildmaterial zusammengestellt. Ein praktisch lückenloses Bewegungsprofil. Und so ein Mitschnitt könnte nun wohl von vielen erstellt werden, die zufällig vor Ort waren oder friedlich demonstrieren wollten.

Lukas Theune, Rechtsanwalt: „Das ist der Weg in einen polizeilichen Überwachungsstaat. Ja, das muss man einfach so sehen. Das führt auch letztlich dazu, dass sich die Einzelne oder der Einzelne ganz genau überlegen muss, gehe ich denn überhaupt noch auf eine Versammlung? Das

mache ich doch im Zweifel lieber nicht, wenn danach noch jahrelang computergestützt auswertbar ist, auf welcher Demo ich denn war."

Und es geht längst nicht mehr nur um reine Gesichtserkennung. Einige Bundesländer arbeiten bereits mit Software, die Informationen automatisch verknüpfen kann. Hessen zum Beispiel. Das Programm „HessenDATA" kann mit Hilfe von Algorithmen Verbindungen zwischen verschiedenen polizeilichen Datenbanken herstellen und auch Informationen aus dem Internet einbinden. Mitgeschnittene Telefongespräche, abgefangene Mails, Kontakte, Aufenthaltsorte. All das kann dann zu Profilen zusammengeführt werden. So sollen die Netzwerke von Verdächtigen schneller erfasst werden. Aber was, wenn die Polizei sich irrt? Wenn die Technologie missbraucht wird? Wenn Unschuldige oder sogar politische Gegner so gerastert werden?

Johannes Caspar, Datenschutzbeauftragter Hamburg: „Der Rechtsstaat kann es nicht, darf es auch nicht verhindern, dass Kriminalität verfolgt wird. Er muss aber auch gleichzeitig verhindern, dass diese Verfolgung von Kriminalität ausufert und in eine … in einen Bereich der Unkontrollierbarkeit absinkt. Und wenn es dann … wenn das nicht gelingt, dann verlieren wir sozusagen die Bindung, die wir im Rechtsstaat eben gegenüber einem Willkürstaat haben, wo die Polizei machen kann, was sie will."

Es sind Gesetze, die genau davor schützen, die Grenzen setzen müssen. Aber die Hürden für polizeiliche Maßnahmen sind in den letzten Jahren immer weiter gesenkt worden. In mehreren Ländern darf die Polizei nicht mehr nur bei realen Gefahrensituationen eingreifen – sondern bereits, wenn eine Gefahr nur droht. Aber ab wann „droht" Gefahr? Wird es nicht irgendwann willkürlich? Überlassen wir es Algorithmen, anhand von Annahmen und Erfahrungswerten zu berechnen, wer einmal gefährlich werden könnte? Und wer will das noch rechtsstaatlich kontrollieren?

Yvonne Hofstetter, Autorin und IT-Unternehmerin: „Zwischen den Möglichkeiten, die die Technologie zur Verfügung stellt in Bezug auf Kontrolle, in Bezug auf Überwachung, in Bezug auf Freiheitseinschränkungen schützt uns nur die ganz dünne, hauchdünne Schicht des Rechts in einem Rechtsstaat. Und wenn ich aber sage, ich gebe das auf, dann sind wir auf dem besten Wege abzurutschen in eine Herrschaftsform, wo eben dieses, diese dünne Schicht des Rechts aufgelöst wird und wir eben unsere Freiheit tatsächlich auch ad acta legen können."

Clearview war ein Tabubruch. Aber die Möglichkeiten zur Überwachung gehen längst weiter. Die Debatte darüber, wo wir die Grenzen setzen müssen, hat erst begonnen.