STAATSANZEIGER
Wochenzeitung für Wirtschaft, Politik und Verwaltung in Baden-Württemberg

Essay

# Keine einfachen Antworten bei der biometrischen Gesichtserkennung

**Sicherheitskräfte fordern mehr biometrische Möglichkeiten. Doch Datenschützer warnen vor den Folgen. Ein Essay von Stefanie Schlüter.**

Biometrische Gesichtserkennung: Chancen und Risiken für Sicherheit und Privatsphäre in der digitalen Welt.

(Foto: © dpa/Westend61/Emma Innocenti)

Stefanie Schlüter

20.02.2025, 11:12 Uhr

Vor einem Jahr wurde die frühere RAF-Terroristin Daniela Klette in Berlin festgenommen, nach 30 Jahren im Untergrund. Zuvor hatte ein kanadischer Journalist sie mittels der Software PimEyes, einem Tool für biometrische Gesichtserkennung im Internet aufgespürt. Er hat dafür angeblich nur 30 Minuten benötigt. Ob dies tatsächlich der Auslöser für Klettes Festnahme war, ist unklar, wenn auch wahrscheinlich. Die Polizei sprach damals nur von einem Hinweis aus der Bevölkerung. In jedem Fall hat die Festnahme der Forderung nach biometrischer Gesichtserkennung zur Fahndung Auftrieb gegeben.

Doch hier stehen sich zwei zentrale Rechtsgüter gegenüber: die öffentliche Sicherheit und die Privatsphäre. Von Seiten vieler Innenpolitiker und der Polizei wird argumentiert, dass sich durch die biometrische Gesichtserkennung neue Chancen bei der Kriminalitätsbekämpfung eröffnen.

Beim Bundeskriminalamt gibt es bereits seit 2008 eine Software, die durch maschinelles Lernen immer besser geworden ist und biometrische Daten inzwischen sehr gut vergleichen kann. Mit ihr können beispielsweise Fahndungsfotos oder auch Handyvideos von Zeugen mit Fotos in der polizeilichen Datenbank abgeglichen werden. Ein große Unterschied zu Programmen wie PimEyes oder Videoüberwachung mit integrierter biometrischer Gesichtserkennung: Hier werden von den Ermittlern Bilder von Tatverdächtigen mit einer Datenbank verglichen – nachdem eine Tat begangen wurde. Und die Daten sind nicht Live noch stehen alle Daten aus dem Internet zum Abgleich zur Verfügung.

Den Sicherheitskräften reichen die Tools des BKA nicht, wie bei einer Diskussionsveranstaltung der Evangelischen Akademie Bad Boll deutlich wurde. Dort machte der stellvertretende Bundesvorsitzende der Gewerkschaft der Polizei, Alexander Poitz klar, dass Kriminelle längst ihre Tätigkeiten in den virtuellen Raum verlagert hätten. Diese orientieren sich auch nicht an Fragen des Datenschutzes oder fragen danach, welche Systeme sie nutzen dürfen und welche nicht. „Übertriebener Datenschutz ist indirekter Täterschutz“, so Poitz.

Es ist verständlich, dass die Polizei Gefährder, die Anschläge planen nicht erst fassen will, wenn bereits auf einem Weihnachtsmarkt, in einem Zug oder bei einer Feier Menschen getötet wurden. Zu solchen Taten sollte es nicht kommen. Auch CDU-Chef Friedrich Merz fordert mehr Befugnisse für Sicherheitsbehörden, etwa durch Videokameras mit biometrischen Möglichkeiten im öffentlichen Raum, an Bahnhöfen, auf Flughäfen.

Die Argumente der Polizei sind verständlich, gibt es doch auch Schutzmechanismen, wie etwa den Richtervorbehalt. Und: Das Sicherheitsbedürfnis der Bürger ist groß. Doch was passiert, wenn die Polizei tatsächlich so weitreichende Befugnisse bekommt. Bringt dies tatsächlich ein mehr an Sicherheit? Oder bedroht dies die Freiheit? Für Kilian Vieth-Ditlmann von Algorithm Watch ist die Antwort klar: Wenn Behörden Menschen überall finden und erkennen können, greift das tief in die demokratischen Freiheitsrechte ein. Wie er sprechen sich Datenschutz- und Menschenrechtsorganisationen gegen eine entsprechende Überwachung mit biometrischer Gesichtserkennung aus. Denn bei allen Chancen für die Polizei gibt es auch eine Reihe von Risiken. Etwa wenn Menschen durch solche Softwareabgleiche falsch verdächtigt werden. Ein bekanntes Beispiel ist die Verhaftung und das elfstündige Verhör einer Frau in den USA, die im achten Monat schwanger war. Gerade Frauen, Kinder und Menschen mit dunkler Hautfarbe werden laut Studien von den Systemen immer wieder fälschlich als Tatverdächtige identifiziert.

Zugleich bedeutet eine solche Überwachung auch das Ende der Anonymität. Und auch das kann Folgen über die Kriminalitätsbekämpfung hinaus haben. Menschen könnten Demonstrationen und Beratungsstellen zu heiklen Themen wie zu Schwangerschaftsabbruch meiden und vielleicht auch bei einem Streik nicht mehr in der ersten Reihe stehen wollen. Da stellt sich die Frage, was das mit unserer Gesellschaft und unserer Demokratie auf Dauer macht. Es könnte etwa ein entsprechender Konformitätsdruck entstehen.

Will man biometrische Daten für die Kriminalitätsbekämpfung in größerem Umfang nutzen, muss das Für und Wider in jedem Fall in einem gesellschaftlichen Prozess diskutiert werden. Es gibt hier keine einfachen und schnellen Antworten.