Junge Welt / 09.06.2026 / Schwerpunkt / Seite 9

»Damit endet die Privatsphäre im öffentlichen Raum«

Das »Sicherheitspaket 2.0« der Bundesregierung bricht mit allen rechtsstaatlichen Prinzipien, sagt Maya Mosch

Von Marc Bebenroth

Deutsche Innenminister sind auf jeden Anschlag vorbereitet. Ihre Schubladen sind gefüllt mit Entwürfen für neue Befugnisse für Polizei und Geheimdienste. Worin besteht aktuell die besondere Dringlichkeit, mit der das Netzwerk »Sicherheit ohne Überwachung« für den 13. Juni zur Protestdemonstration in Berlin aufruft?

Das sogenannte Sicherheitspaket 2.0 in Form von drei Gesetzentwürfen der Bundesregierung soll vermutlich noch vor der parlamentarischen Sommerpause durch den Bundestag gejagt werden. Deswegen sind wir mit Druck hinterher, für kommenden Sonnabend diese Demo zu organisieren und das Netzwerk auszubauen.

Bundesinnenminister Alexander Dobrindt von der CSU hatte am 29. April sein Vorhaben vom Kabinett beschließen lassen, wonach das Bundeskriminalamt und die Bundespolizei die Erlaubnis erhalten sollen, sämtliche im Internet verfügbaren biometrischen Daten zu durchleuchten und einzusammeln. Was macht diesen Plan so gefährlich?

Das ist nur eine von zwei Säulen des Gesetzespakets. Die geplanten Befugnisse werden das Machtverhältnis zwischen Staat und Bevölkerung grundsätzlich verändern. Der biometrische Abgleich bedeutet im Endeffekt das Ende der Privatsphäre im öffentlichen Raum, weil jedes Foto, jedes Video, jede Tonaufzeichnung genutzt werden kann, um Menschen zu identifizieren, zu lokalisieren und alles Mögliche an »Sachverhalten aufzuklären«, wie es im Gesetzentwurf heißt. Die zweite Säule an Befugnissen ist die automatisierte Datenanalyse, die der Polizei erlaubt werden soll. Diese bricht ebenfalls mit allen bestehenden rechtsstaatlichen Prinzipien und Geboten. Allein schon mit dem Gebot der Zweckbindung, wonach einmal gesammelte Daten nicht einfach für ganz andere Zwecke genutzt werden dürfen.

Wie muss man sich das Einsammeln dieser Unmenge an biometrischen Daten technisch vorstellen?

Gesichtserkennung wird am meisten diskutiert, weil das derzeit am häufigsten bereits von Strafverfolgungsbehörden genutzt wird und

technologisch am weitesten entwickelt ist. Theoretisch wäre auch eine biometrische Erkennung anhand der Stimme, des individuellen Gangs oder des Fingerabdrucks möglich. Sogar die Form der Ohrmuschel kann ein Merkmal sein.

Ein altes Fahndungsfoto kann der Ausgangspunkt sein. Damit wird eine Software gefüttert, die prüft, ob ein Gesicht zu erkennen ist, und justiert das Bild so, dass es die Person nach vorne guckend zeigt und so mit anderen Bildern verglichen werden kann. Schließlich wird ein darauf trainiertes neuronales Netz eingesetzt. Das erfasst die wichtigsten individuellen Merkmale des Gesichts selbständig und fasst sie als Vektor zusammen, also als Zahlenbeschreibung mit Hunderten von Werten. Diese lange Zeichenkette wiederum wird mit den Ergebnissen zu anderen Bildern verglichen. Dafür braucht man eine Referenzdatenbank.

Handelt es sich dabei um ein gänzlich neues Verfahren?

Nein, die Polizei macht schon seit längerer Zeit biometrische Abgleiche mit einer Referenzdatenbank. Allerdings ist das bislang nur mit Daten aus Inpol erlaubt, dem zentralen Informationssystem der Polizei. Dort sind circa sieben Millionen Fotos abgespeichert – von Straftätern, aber auch von allen anderen Menschen, die erkennungsdienstlich behandelt wurden oder die einen Asylantrag gestellt haben. Jetzt wollen sie diesen Abgleich mit sämtlichen Daten aus dem Internet machen. Dazu muss man diese mindestens vorübergehend herunterladen. Und irgendwer muss diese Millionen oder Milliarden Dateien vorrätig haben. Die Gesetzentwürfe sehen vor, dass das entweder die deutschen Behörden oder auch Dritte, sogar außerhalb der EU, unter Umständen sein können. Implizit sind damit Firmen gemeint wie Clearview AI oder Pim Eyes. Die haben bereits solche riesigen Datenbanken voller Daten, die sie seit Jahren aus dem Internet gesaugt haben. Dabei verbieten es Plattformen mitunter, ohne Einwilligung der Nutzer deren Bilder zu nehmen und für kommerzielle Zwecke zu nutzen. So wurden bereits Bußgelder ausgesprochen, weil die Datenschutzgrundverordnung die Rechte der Betroffenen am eigenen Bild vor solcher Nutzung schützt. Die Regierung will nun mit diesen Firmen zusammenarbeiten.

Deren Dienste sollen auch dafür genutzt worden sein, das frühere RAF-Mitglied Daniela Klette zu identifizieren.

Ein Journalist hat Pim Eyes benutzt und einen Abgleich mit Fotos von Klette, die seit Jahren auf der Flucht vor der Justiz lebte, in einem Kreuzberger Capoeira-Verein gemacht. Von seinem Fund hat er in einem Podcast erzählt. Wenig später wurde Klette festgenommen. Schnell wurden die Stimmen aus der Regierung laut, die nach der Legalisierung solcher Methoden für die Polizei riefen. Aber wie so oft lagen diese ganzen Vorschläge bereits in der Schublade. Nun geht es der Regierung darum, sämtliche Menschen identifizieren und Netzwerke auf die Weise womöglich besser aufklären zu können als mit herkömmlichen Methoden.

Womit wir bei der zweiten Säule, der automatisierten Auswertung großer Datenbestände sind. Oft wird dabei auf das global agierende IT-Rüstungsunternehmen Palantir verwiesen. Dessen Software wird

von einigen Landespolizeien bereits getestet. Wie funktioniert die Datenanalyse mit solchen Anwendungen?

Dabei werden alle bislang getrennt geführten Datenbestände der Polizei zusammengeführt und verfügbar gemacht. Ändert sich etwas in einer Datenbank, wird das direkt übernommen für die Analyse. Vom maschinellen Lernen, dem Verfahren hinter KI-Systemen, versprechen sie sich, Verbindungen aufgezeigt zu bekommen, die der Polizei vorher so nicht ersichtlich waren. Grundlage soll alles sein, was jemals polizeilich erfasst wurde, egal ob man eine Zeugenaussage gemacht, eine Anzeige erstellt hat oder Datenträger beschlagnahmt wurden. Alles wird zusammengeführt.

So werden Verbindungen zu ganz vielen anderen Menschen hergestellt. Damit verschiebt sich der Fokus von Tat und Täter auf Netzwerke von hauptsächlich unschuldigen Personen. Und anders als bei Methoden wie Funküberwachung oder Abhören von Telefonaten ist kein Richtervorbehalt vorgesehen. Am Ende kann somit jeder Polizist auf alle diese Daten gebündelt zugreifen.

Wie kann man sich da noch gegen eine mögliche Falschbezichtigung wehren, wenn doch niemand weiß, wie diese KI-Systeme zu ihren Ergebnissen gekommen sind?

In diesen Gesetzentwürfen wird immer wieder gesagt, es dürfe keine Rechtsfolge unmittelbar basierend auf dem KI-Ergebnis geben. Praktisch ist das aber sehr schwer zu überprüfen, weil niemand sagen kann, warum die KI zu einem bestimmten Ergebnis gekommen ist. Das bleibt eine Blackbox. Keine Firma gibt ihren Quellcode raus, auch Palantir und Co. nicht.

Der biometrische Abgleich soll ja auch fürs Bundesamt für Flucht und Migration komplett legalisiert werden. Stellt jemand dann ohne Ausweisdokumente einen Asylantrag, wird per Software analysiert, ob die geschilderte Fluchtgeschichte stimmen kann. Spuckt die Maschine irgend etwas zu einem Menschen aus einem ganz anderen Land aus, der dem Antragsteller irgendwie ähnelt, werden die Behördenmitarbeiter vermutlich früher oder später einfach der Maschine glauben.

Für linke Organisationen stellt sich angesichts dieses Machtzuwachses die Frage: Was tun? Was bleibt an Optionen übrig, außer sich aus dem gesamten Internet zu löschen?

Datensparsamkeit hilft. Aber im Zweifelsfall bin ich trotzdem mindestens einmal im Hintergrund vorbeigelaufen, als Touristen ein Foto gemacht haben. Kurz gesagt: Es ist unmöglich, alle Datenspuren zu vernichten. Viel wichtiger ist, dass wir die Themen Überwachung und KI im Zuge der Militarisierung im Innern aus der rein netzpolitischen Blase rausholen und breit zugänglich machen. Alle linken Gruppen müssen sich diesen Themen widmen. Deshalb sind wir auch ein relativ breit aufgestelltes Netzwerk von Akteuren aus dem linken Spektrum sowie dem zivilgesellschaftlich-bürgerlichen Milieu. Darüber hinaus sind wir gerade dabei, mit der Szene der Fußballfans zusammenzuarbeiten, die selbst schon lange besonderen Repressions- und Überwachungsmaßnahmen ausgesetzt ist.

→ Demo: Sa., 13.6., ab 14 Uhr, Marchlewskistr./Warschauer Str., Berlin

Maya Mosch spricht für das Netzwerk »Sicherheit ohne Überwachung«, das über das geplante »Sicherheitspaket 2.0« der Bundesregierung aufklärt sowie Protest dagegen mobilisiert

https://www.jungewelt.de/artikel/523947.anlasslose-massenüberwachung-damit-endet-die-privatsphäre-im-öffentlichen-raum.html