WA13 KI und Sicherheit

Gremium:	Lag Digitales und Medien
Beschlussdatum:	07.10.2025
Tagesordnungspunkt:	8. Weitere Anträge

Antragstext

1. Wir lehnen den anlasslosen Einsatz von KI Software zur Bewertung von Bewegungs- und Verhaltensmustern im öffentlichen Raum ab. Pauschales Scoring von Verhalten in der Öffentlichkeit darf es nicht geben. Ausnahmen kann es nur beim Anlass durch schwerste Straftaten in einem engen und begrenzten örtlichen und zeitlichem Rahmen geben.

2. Wir lehnen Datenbanken ab, die wahllos Bilder von allen Bürger:innen aus dem Internet sammeln, um eine permanente biometrische Fernidentifizierung im öffentlichen Raum zu ermöglichen.

3. Analyseprogramme im Rahmen von Polizeiarbeit müssen transparent und demokratisch kontrolliert sein.

Begründung

Künstliche Intelligenz hat in den letzten Jahren einen unvergleichlichen Siegeszug angetreten. Ob in der Wissenschaft, der Wirtschaft oder der täglichen Arbeit: die Unterstützung durch KI ist nicht mehr wegzudenken. Sie unterstützt Radiolog:innen, fasst Texte in der täglichen Arbeit zusammen oder hilft beim Verstehen von Zusammenhängen in Datenanalysen. Auch unter Berücksichtigung damit auftretender negativer Auswirkungen kann ihr positiver Nutzen Menschen entlasten und unterstützen.

Mit diesen Entwicklungen einher gehen aber auch neue Möglichkeiten in der Sicherheitspolitik, die jetzt vielerorten genutzt werden wollen: Kameras, die menschliches Verhalten bewerten oder permanent Gesichter gegen Fahndungslisten prüfen. Analyseprogramme, die Daten aus unterschiedlichen Quellen zusammenführen, um Muster und somit Verdächtige erkennen sollen. Die wesentliche Gemeinsamkeit dieser Anwendungen ist die Anlasslosigkeit ihres Einsatzes — schon bevor es zu einer Tat kommt, soll die Kamera das Verhalten auf eine mögliche Gefahr hin bewerten oder die Analysesoftware wie etwa von Palantir aus den bei den Polizeibehörden vorliegenden Daten mögliche Straftaten und Straftäter:innen vorhersagen. In den USA zum Beispiel geht die Trump Regierung noch einen Schritt weiter und will ihre „Datensilos“ öffnen, um möglichst alle staatlicherseits vorhandenen Daten über Bürger:innen auswerten zu können. Sicherheit wird dort gleichgesetzt mit möglichst viel datengetriebener Prophylaxe im Vorfeld.

Hierdurch werden allerdings mehrere Grenzen überschritten. Im Beispiel der öffentlichen Kameraüberwachung wird dann jede:r Bürger:in permanent einer Analyse unterzogen. Statt einer passiven Aufzeichnung für mögliche spätere Ermittlungen findet ein Scoring statt, mit dem das Verhalten von Menschen nach potentieller Gefährlichkeit bewertet wird. Kommt die KI durch ihr Training zum Schluss, dass das Verhalten eine Gefahr darstellt, können Sicherheitskräfte benachrichtigt werden. Dabei ist auch durch das intransparente Training der KI häufig nicht mehr nachvollziehbar, welche Kriterien hier überhaupt zum Einsatz kommen, die eine Gefährlichtkeit bestimmen. Welches Verhalten in der Öffentlichkeit wäre denn eine Gefährdung und warum? Der öffentliche Raum wird somit nicht mehr nur passiv durch Kameras überwacht – das Verhalten von Bürger:innen wird durch die KI dann permanent bewertet, und das potentiell zum Beispiel im gesamten ÖPNV zu jeder Zeit.

Zum anderen werden durch Analyseprogramme bei den Polizeibehörden Daten von Menschen analysiert, die bisher überhaupt keiner Tat verdächtigt werden, nur um mögliche Verdächtige ermitteln zu können. In allen auch oben beschriebenen Fällen ist auch das Training mit enorm vielen Daten von auch völlig unschuldigen Menschen notwendig, um abweichendes Verhalten erkennen zu können. So ist beispielsweise auch geplant, sämtliche frei verfügbaren Bilder aus dem Internet bei den Sicherheitsbehörden zu speichern. Wer sich etwa auf einem Parteitag fotografieren lässt, landet in Datenbanken der Sicherheitsbehörden. Auch die Bilder aus Personalausweisen und Reisepässen sollen in Zukunft zur biometrischen Überwachung im öffentlichen Raum genutzt werden.

Ebenfalls problematisch ist die mangelnde demokratische Kontrolle all dieser Software. So gibt der Hersteller Palantir weiterhin keine transparenten Auskünfte darüber ab, wie die Software im Einzelnen überhaupt funktioniert und für ihren Betrieb müssen auch noch Mitarbeiter des Herstellers vor Ort sein. Dass in einer Demokratie Software in der Öffentlichkeit und mit Daten von Bürger:innen Einschätzungen vornimmt, die durch die Gesellschaft nicht mehr nachvollziehbar sind und deren Regeln verborgen bleiben, stellt eine Gefahr dar. Auch das Training der Künstlichen Intelligenz muss, sofern man diese überhaupt im öffentlichen Raum einsetzen will, von Anfang bis Ende demokratisch kontrollierbar sein. Eine Black Box, die anhand von unklaren Trainingsdaten eine Entscheidung trifft, darf es nicht geben.

Noch sehr viel weiter gehen auch Vorschläge der EU Kommission und Ratspräsidentschaft, die zum Beispiel Inhalte privat versandter Nachrichten von Bürger:innen in Europa permanent durch eine KI auswerten lassen wollen – die sogenannte „Chatkontrolle“. Hier wird endgültig eine Grenze überschritten, die Grundrechte massiv einschränken würde.

Für uns Grüne ist daher klar: Wir lehnen eine anlasslose Überwachung des Verhaltens von Bürger:innen durch Kameras oder Datenanalyse ab. Instrumente dieser Art müssen immer an konkrete Anlässe und allerschwerste Taten geknüpft sein. Nur in einem sehr begrenzten Rahmen, der zudem völlig transparent und demokratisch kontrollierbar ist, können solche Werkzeuge überhaupt diskutiert werden. Es muss auch immer die Frage gestellt werden, ob eine noch intensivere Überwachung der Öffentlichkeit überhaupt notwendig ist.

Links:

1. https://netzpolitik.org/2025/als-erstes-bundesland-hessen-setzt-live-gesichtserkennung-ein/

2. https://www.hamburg.de/politik-und-verwaltung/behoerden/bvm/aktuelles/pressemeldungen/sicherheit-im-oepnv-1004084

3. https://finance.yahoo.com/news/trump-administration-silently-employs-palantir-213150870.html

4. https://taz.de/Gesichtserkennung-im-Internet/!6026767/

5. https://www.heise.de/hintergrund/Polizeiarbeit-Training-von-KI-System-mit-Material-aus-Videoueberwachung-10547282.html

6. https://netzpolitik.org/2025/biometrische-gangerkennung-zeige-mir-wie-du-gehst-und-ich-sage-dir-wer-du-bist/

7. https://www.heise.de/news/Datenschuetzer-fordern-strenge-Regeln-fuer-polizeiliche-Datenanalysen-10661124.html