Was kann ich tun?

- Informiere andere
- Schreibe Abgeordneten / Ausschussmitgliedern, was du denkst
  - Ausschussmitglieder Inneres und Sport der Regierungsfraktionen:
    - Michael Lühmann (GRÜNE)
    - Nadja Weippert (GRÜNE)
    - Doris Schröder-Köpf (SPD), Vorsitzende
    - Deniz Kurku (SPD)
    - Alexander Saade (SPD)
    - Julius Schneider (SPD)
    - Ulrich Watermann (SPD)
    - Sebastian Zinke (SPD)
  - Namen deiner lokalen Abgeordneten: https://www.abgeordnetenwatch.de/niedersachsen/abgeordnete

Weitere Informationen / Links

Eine ausführliche Zusammenstellung von Quellen gibt es auf:
https://kleindatenverein.org/tags/npog/

Außerdem gibt es ähnliche Vorhaben im Bundesinnenministerium, siehe:
https://sicherheit-ohne-ueberwachung.org/

← NPOG

Bund →

Der Kleindatenverein ist eine Gruppe von Datenschutz- und Grundrechtsaktivisti aus Braunschweig und Berlin. Wir halten informationelle Selbstbestimmung für eine Grundvoraussetzung einer freien, demokratischen Gesellschaft und sorgen uns um zunehmend autoritäre Tendenzen.

Kontakt

post@kleindatenverein.org

www.kleindatenverein.org

Offener Matrix-Kanal:
#kleindatenverein:stratum0.org

Fediverse (Mastodon):
https://fedifreu.de/@kleindatenverein

Überwachungsdystopie der Landesregierung verhindern!

Übersicht über den Entwurf zur Änderung des NPOG (Niedersächsisches Polizei- und Ordnungsgesetz)

kleindatenverein.org

Worum geht es?

Ein Gesetzesvorschlag der Landesregierung (rot/grün) sieht eine deutliche Erweiterung der Überwachungs- und Fahndungsbefugnisse der Polizei vor. Der ausgiebige Einsatz verschiedener Formen von „KI“ soll Überwachung im digitalen, öffentlichen und privaten Raum stark ausweiten und ermöglicht dystopische Zustände, die wir sonst nur aus autoritären Staaten kennen. Dazu gehören u.a.:

- Automatisierte Verhaltenserkennung auf öffentlichen Aufnahmen (§ 32)
- Biometrische Echtzeit-Fernidentifizierung (§ 32b)
- Nachträgliche Biometrische Identifizierung mittels öffentlich verfügbarer Daten aus dem Netz (§ 32c)
- Automatisierte Datenanalyse (§ 45)

Gerade in Zeiten aufstrebender autoritärpopulistischer Parteien halten wir das für extrem kurzsichtig und gefährlich.

Und die Opposition?

CDU und der anderen Oppositionspartei geht der Vorschlag nicht weit und die Einführung nicht schnell genug. Außerdem befürworten beide explizit die Software von Palantir.

Besonders gefährliche Vorschläge

Automatisierte Verhaltenserkennung auf öffentlichen Aufnahmen (§ 32)
Aufnahmen an öffentlichen Orten und Veranstaltungen sollen automatisiert auf „gefährliches Verhalten“ untersucht werden. Undurchsichtige (und fehleranfällige) Software entscheidet hierbei, welche Menschen sich ordnungsgemäß verhalten und bei welchen Alarm notwendig ist. Solche Systeme haben das Potential, „angemessenes Verhalten“ (im Sinn der aktuellen Machtinhaber:innen bzw. deren Software) zu erzeugen und ein Klima der Angst zu schaffen, das einer offenen, demokratischen Gesellschaft entgegensteht. Durch die geringen Personalkosten sinken zudem die Hürden für zeitliche und räumliche Ausweitungen des Einsatzes.

Biometrische Echtzeit-Fernidentifizierung (§ 32b)
Durch Mittel wie Gesichtserkennung soll auf Aufnahmen nach Personen gesucht werden können. Dadurch droht eine Erstellung von Bewegungsprofilen, und ein anonymes Bewegen im öffentlichen Raum wird unmöglich, wodurch wir alle einem permanenten Überwachungsdruck ausgesetzt werden. Einsatzbereiche dieser Methode sollen bewusst ungekennzeichnet sein, um ein Fernbleiben von gesuchten Personen zu verhindern.

Nachträgliche Biometrische Identifizierung mittels öffentlich verfügbarer Daten aus dem Netz (§ 32c)
Hierbei geht es um die Auswertung, z. B. von Social-Media-Bildern, zur Personenfahndung, bekannt aus dem Fall der RAF-Terroristin Daniela Klette. Jede Handykamera wird so zum potentiellen Fahndungswerkzeug.

Automatisierte Datenanalyse (§ 45)
Datenbanken sollen zusammengeführt und automatisiert durchsucht werden können – auch durch „selbstlernende Systeme“. Die Daten umfassen auch Menschen, die nie straffällig geworden sind (z. B. Zeug:innen oder Anzeigestellende). Zudem ist unklar, wie ein solches System die Zweckbindung wahren soll. Die Fehleranfälligkeit der vorgesehenen Algorithmen und das Risiko von Diskriminierung sollen per Gesetz „verboten“ werden. Die Regierungsparteien sprechen sich zwar gegen das hochproblematische Unternehmen Palantir aus, laut Landesdatenschutzbeauftragtem wäre die aktuelle Fassung aber ausreichend für einen Einsatz von dessen Software (den die Opposition explizit fordert). Zudem ist das Grundkonzept dieser Software – auch aus europäischer Hand – nicht mit einer freien Demokratie vereinbar.

Weitere Inhalte
Zudem vorgesehen sind u.a. erweiterte Befugnisse zum Einsatz (§ 32d) und der Abwehr (§ 32e) von Drohnen, auch zum Filmen bei Veranstaltungen, und zum Einsatz von Bodycams (§ 32a; auch in privaten Räumen und mit 30s „pre-recording“, die bei Auslösen einer Aufnahme mitgespeichert werden).