Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)494

/ Stellungnahme

zu den Gesetzentwürfen zur „Verbesserung der Terrorismusbekämpfung“ (BT-Drucksache 20/12806) und „Verbesserung der inneren Sicherheit und des Asylsystems“ (BT-Drucksache 20/12805)

20. September 2024

Eingereicht durch *AlgorithmWatch* für das *Bündnis Gesichtserkennung Stoppen!*

Unsere Empfehlung in Kürze

Die vorgeschlagenen biometrischen Überwachungsbefugnisse sind europarechtswidrig, verletzen verfassungsrechtliche Mindestanforderungen und widersprechen datenschutzrechtlichen Grundregeln. Das betrifft die Entwürfe für §§ 10b, 39a und 63b BKA-Gesetz, § 34b BPolG, § 98d StPO und § 15b AsylG. Die Regelungen müssen deshalb gestrichen werden.

Kontext

Diese Stellungnahme beschränkt sich allein aus Zeitgründen auf die biometrischen Überwachungsbefugnisse, wie sie am 12.09.2024 in erster Lesung vom Bundestag beraten wurden.[1] Im Einzelnen sind das folgende vorgeschlagene Regelungen in den Gesetzentwürfen „zur Verbesserung der Terrorismusbekämpfung“[2] und „zur Verbesserung der inneren Sicherheit und des Asylsystems“[3]:

- § 10b im Bundeskriminalamtgesetz: nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet zur
    - Identifizierung oder Ermittlung des Aufenthaltsorts einer Zielperson
    - Verfolgung und Verhütung von Straftaten
- § 39a und § 63b Bundeskriminalamtgesetz, sowie § 34b im Bundespolizeigesetz: nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet zur Gefahrenabwehr
- § 98d Strafprozessordnung: nachträglicher Abgleich biometrischer Daten mit im Internet öffentlich zugänglichen Daten mittels einer automatisierten Anwendung zur Datenverarbeitung, zur Identitätsfeststellung oder zur Ermittlung des Aufenthaltsorts einer beschuldigten oder sonstigen Person, nach der für Zwecke eines Strafverfahrens gefahndet wird
- § 15b Asylgesetz: nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet durch das Bundesamt für Migration und Flüchtlinge (BAMF)
    - wenn ein Ausländer [sic!] keinen gültigen Pass oder Passersatz besitzt und der Abgleich für die Feststellung der Identität oder Staatsangehörigkeit eines Ausländers [sic!] erforderlich ist

Trotz schwerwiegender offener Fragen zur Wirksamkeit und Rechtmäßigkeit dieser vorgeschlagenen Maßnahmen sollen die Gesetzesentwürfe im Eilverfahren verabschiedet werden. Es zeichnet jedoch sowohl die parlamentarische Demokratie als auch den Rechtsstaat aus, nicht überhastet und hart, sondern besonnen und verhältnismäßig zu agieren.

Im Koalitionsvertrag verpflichten sich die Regierungsparteien gleich an zwei Stellen, biometrische Überwachung in Deutschland zu verhindern. So heißt es, dass „[b]iometrische Erkennung im öffentlichen Raum“ europarechtlich auszuschließen sei, auch der „Einsatz von biometrischer Erfassung zu Überwachungszwecken“ wird explizit abgelehnt. Ebenso hat die Koalition festgehalten, dass „das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet“ zu gewährleisten ist.[4] Im Folgenden legen wir dar, warum die vorgeschlagenen Befugnisse nicht nur einen Bruch des

[1] BT-Drs. 20/12806 und 20/12805, vgl. https://www.bundestag.de/dokumente/textarchiv/2024/kw37-de-innere-sicherheit-1016976
[2] BT-Drucksache 20/12806 https://dserver.bundestag.de/btd/20/128/2012806.pdf
[3] BT-Drucksache 20/12805 https://dserver.bundestag.de/btd/20/128/2012805.pdf
[4] Koalitionsvertrag 2021- 2025 zwischen SPD, BÜNDNIS 90 / DIE GRÜNEN und FDP, S. 15 und 86f, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf

geltenden Koalitionsvertrags bedeuten, sondern auch mit unionsrechtlichen und verfassungsrechtlichen Vorgaben unvereinbar sind.

1) Unvereinbarkeit mit EU-Recht

Die vorgeschlagenen biometrischen Überwachungsbefugnisse sind europarechtswidrig. Sie widersprechen der jüngst in Kraft getretenen EU KI-Verordnung (KI-VO), die EU-weit harmonisierte Regelungen zum Einsatz von KI-Systemen beinhaltet.

Angesichts des enormen Schädigungspotenzials für Grundrechte und Demokratie verbietet die KI-Verordnung „das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern“ (Art. 5 Absatz 1 Buchstabe e KI-VO). Dieses Verbot wird bereits am 2. Februar 2025 gültig und umfasst sowohl private KI-Anbieter als auch öffentliche Stellen wie Polizei-, Strafverfolgungs- und Migrationsbehörden, die ein solches KI-System anschaffen, betreiben oder nutzen.

Die in den Gesetzentwürfen vorgesehene Befugnis zum nachträglichen biometrischen Überwachen sämtlicher öffentlich zugänglicher Daten aus dem Internet kann ohne den Einsatz dieser EU-weit verbotenen KI-Systeme nicht umgesetzt werden. Dabei spielt es keine Rolle, ob die Behörden die biometrischen Erkennungssysteme selbst entwickeln oder von Dritten beschaffen; beides ist explizit untersagt. Der Staat darf keine rechtswidrigen Angebote Dritter nutzen. Eine Umsetzung dieser Befugnis ohne den Einsatz eines solchen KI-Systems kommt weder theoretisch noch praktisch in Betracht, da immer KI-Systeme benötigt werden, um die biometrischen Muster von Gesichtern aus Bilddaten zu extrahieren.[5]

Die KI-VO sieht für dieses eindeutige Verbot keine Ausnahmen vor. Lediglich solche KI-Systeme, die „ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit in Verkehr gebracht, in Betrieb genommen oder, mit oder ohne Änderungen, verwendet werden“ (Art. 2 Abs. 3 Satz 2 KI-VO) sind generell von der KI-VO ausgenommen. Die in den Entwürfen vorgesehenen Einsatzzwecke zur Gefahrenabwehr, zur Strafverfolgung und zur Identitätsfeststellung im Zuge von Asylverfahren sind eindeutig von der Verordnung erfasst. Alle KI-Systeme, die „etwa für zivile oder humanitäre Zwecke oder für Zwecke der Strafverfolgung oder öffentlichen Sicherheit“ verwendet werden, fallen in den Anwendungsbereich dieser Verordnung (Erwägungsgrund 24, KI-VO).

[5] Die Gesetzesbegründung führt aus, dass die biometrische Überwachungsbefugnis für das BAMF die Vorgabe aus Artikel 14 KI-VO einhalten soll. Dort geht es darum, dass Hochrisiko-KI-Systeme von natürlichen Personen wirksam beaufsichtigt werden müssen, etwa um Risiken für Grundrechte zu minimieren. Hier geht man also davon aus, dass KI-Systeme zum Einsatz kommen (BT-Drucksache 20/12805, S. 23).

Die Echtzeit-Fernidentifikation ist gemäß Art. 5 Abs. 1 Buchstabe h der KI-Verordnung nur in engen Grenzen erlaubt, was die Entwürfe nur unzureichend berücksichtigen: Ein Echtzeit-Abgleich ist nicht für Stimmen ausgeschlossen, nur für Bild- und Videoaufnahmen. Damit könnte etwa in einem Live-Stream trotzdem nach den biometrischen Stimmmustern einer Person gesucht werden. Hinzu kommt, dass nicht definiert wird, wann eine Echtzeit-Aufnahme endet. Auf YouTube und anderen Video-Plattformen ist es zum Beispiel gang und gäbe, dass Veranstaltungen in Echtzeit übertragen werden und bereits kurz danach und zeitlich unbegrenzt als Videodateien öffentlich verfügbar bleiben. Einen Schutz dagegen, diese Live-Streams mit kurzem Zeitversatz zu erfassen und auszuwerten, gibt es weder rechtlich noch technisch. Die KI-VO verweist in EG 95 darauf, dass „Bedingungen für die nachträgliche biometrische Fernidentifizierung keinesfalls eine Grundlage dafür bieten [sollten], die Bedingungen des Verbots und der strengen Ausnahmen für biometrische Echtzeit-Fernidentifizierung zu umgehen", lässt aber gleichzeitig offen, ab wann eine Echtzeit-Auswertung aufhört und eine nachträgliche Auswertung anfängt. An der gleichen Stelle wird vorausgesetzt, dass die nachträgliche Fernidentifikation stets „auf einem geschlossenen Datensatz rechtmäßig erworbener Videoaufnahmen basieren" muss. Die Absicht, sämtliche öffentlich zugängliche Daten aus dem Internet heranzuziehen, widerspricht der KI-VO auch in dieser Sache.

Auch die EU-weiten Datenschutz-Vorgaben sind nicht mit dem biometrischen Massenabgleich vereinbar. Artikel 10 der Richtlinie über Datenschutz in der Strafverfolgung (EU Richtlinie 2016/680) fordert, dass die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person nur dann erlaubt werden darf, wenn sie unbedingt erforderlich ist. Diese Erforderlichkeit ist in keiner Weise dargelegt worden. Außerdem muss sichergestellt sein, dass die Rechte und Freiheiten der betroffenen Person geschützt werden und die Maßnahme der Wahrung lebenswichtiger Interessen dient, was ebenfalls in den vorliegenden Entwürfen nicht gegeben ist.

2) Verletzung verfassungsrechtlicher Mindestanforderungen

Die vorgeschlagenen biometrischen Überwachungsbefugnisse sind mit verfassungsrechtlichen Mindeststandards nicht vereinbar. Die Überwachungsmaßnahme berührt zwangsläufig die Grundrechte aller Menschen und ist weder erforderlich noch verhältnismäßig. Die KI-basierte Erfassung und Auswertung von Gesichtern und Stimmen verletzt die Grundrechte auf informationelle Selbstbestimmung, auf freie Meinungsäußerung und weitere. Das Eingriffsgewicht ist besonders hoch, weil die Maßnahme heimlich erfolgt und eine extrem hohe Streubreite hat, denn betroffen sind alle Menschen, von denen Gesichtsbilder oder Audiodateien im Internet zugänglich sind. Dazu kommt, dass erhebliche Diskriminierungsrisiken bestehen und besonders sensible Daten aufgedeckt werden können (z.B. bei

Aufnahmen von Demonstrationen, Parteiveranstaltungen, Pride-Events, Gewerkschaftskundgebungen, Gottesdiensten etc.).

Das Bundesverfassungsgericht hat bereits für die großflächige, automatisierte Verarbeitung von Kfz-Kennzeichen durch Polizei und Strafverfolgungsbehörden hohe verfassungsrechtliche Anforderungen aufgestellt.[6] Und dort ging es nicht um besonders sensible biometrische Daten wie Gesichter, sondern nur um Kfz-Kennzeichen. Die automatisierte Erhebung und Auswertung von öffentlich zugänglichen personenbezogenen Daten stellt nach Rechtsprechung des Bundesverfassungsgerichts immer einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.[7] Auch ein jüngeres Verfassungsurteil über die automatisierte Datenanalyse für die vorbeugende Bekämpfung von Straftaten stellt mit Verweis auf das Grundrecht auf informationelle Selbstbestimmung klar, dass automatische Abgleiche biometrischer Daten besonders voraussetzungsvoll sind.[8]

Die Anforderungen für die vorgeschlagene massenhafte Verarbeitung biometrischer Daten sind zu unspezifisch und die Einsatzzwecke und Tatbestandsmerkmale sind zu breit und nicht gewichtig genug. Insbesondere der Straftatenkatalog des § 100a Abs. 2 StPO wird ständig erweitert und angepasst, wodurch er nicht zur klaren Begrenzung von Maßnahmen auf schwerwiegende Straftaten geeignet ist. Und weder die Referenz-Datenbanken gesuchter Personen, noch die zu durchsuchenden Bild- oder Videodaten sind hinreichend konkretisiert, etwa hinsichtlich zeitlicher und räumlicher Beschränkung. Das Erfassen von Daten, die den Kernbereich privater Lebensgestaltung berühren, wird durch den Entwurf nicht grundsätzlich ausgeschlossen und ist praktisch auch nicht zu gewährleisten. Durch die enorme Streubreite des vorgeschlagenen biometrischen Abgleichs ist davon auszugehen, dass regelmäßig Erkenntnisse aus dem Kernbereich privater Lebensführung als „Beifang“ erhoben werden. Dass diese höchst privaten Daten nicht verwertet werden dürfen und unverzüglich zu löschen sind, stellt keinen hinreichenden Schutz dar. Schon die Möglichkeit der Datenerfassung erhöht den Überwachungsdruck und schränkt die grundrechtlich garantierte Privatsphäre ein.

Die öffentliche Verfügbarkeit der Daten, die für einen Abgleich herangezogen werden, ändert nichts daran, dass die Schutzbereiche der Grundrechte berührt sind.[9] Schon gar nicht, wenn besonders schützenswerte, lebenslang unveränderbare biometrische Datensätze wie Stimm- oder Gesichtsmuster daraus abgeleitet werden. Die Rechtsprechung des Bundesverfassungsgerichts spannt einen Schutzschirm, um Einschüchterungseffekte zu verhindern, die entstehen können, wenn Einzelne nicht mit

---

[6] BVerfG, Urteil des Ersten Senats vom 11. März 2008, 1 BvR 2074/05, https://www.bverfg.de/e/rs20080311_1bvr207405.html

[7] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, https://www.bverfg.de/e/rs20181218_1bvr014215.html

[8] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, Rn. 87, https://www.bverfg.de/e/rs20230216_1bvr154719.html

[9] Vgl. z.B. Hornung: Künstliche Intelligenz zur Auswertung von Social Media Massendaten. Möglichkeiten und rechtliche Grenzen des Einsatzes KI-basierter Analysetools durch Sicherheitsbehörden, Archiv des öffentlichen Rechts, 147. Band (2022), Heft 1;
Sosna: „Fundgrube Internet“ – vom tatsächlich möglichen und rechtlich zulässigen Sammeln der Nachrichtendienste im Netz, GSZ 2024, 53.

ausreichender Sicherheit die Verbreitung ihrer Daten überschauen können. Die massenhafte biometrische Identifizierung hat eine enorme einschüchternde Wirkung, da Menschen nicht wissen (und nicht wissen können), ob und wann Foto- und Videoaufnahmen oder anderes Datenmaterial wie Podcasts in Zukunft mit KI-Systemen von Polizei-, Strafverfolgungs- und Migrationsbehörden ausgewertet werden.[10] Die KI-basierte Analyse von biometrischen Daten ist ein elaboriertes technisches Verarbeitungsverfahren und keine technische Arbeitshilfe für manuelle Verfahren.[11]

3) Konflikt mit Datenschutzvorgaben

Der Vorschlag verletzt grundlegende datenschutzrechtliche Vorgaben. Eine informierte Einwilligung oder ein berechtigtes Interesse kann im Kontext des vorgeschlagenen biometrischen Massenabgleichs im gesamten öffentlich zugänglichen Internet nicht gegeben sein. Weder das eine noch das andere kann strukturell aufgrund der Vielzahl an potenziell betroffenen Personen angenommen werden. Keine Stelle kann aus dem Hochladen eines Inhalts ins Internet ein Einverständnis in die Datenerhebung herleiten.

Die Gesetzentwürfe legen die technische Ausgestaltung des massenhaften biometrischen Abgleichs nur unzureichend dar. Dennoch ist davon auszugehen, dass die technische Vorgehensweise der des Unternehmens ClearView AI Inc. zumindest ähnelt. Etliche Datenschutzbehörden haben die Datenverarbeitung durch ClearView AI aufgrund zahlreicher Verstöße gegen die DSGVO beanstandet und mit hohen Bußgeldern belegt:

- Die niederländische Datenschutzbehörde AP erließ ein Bußgeld in Höhe von 30,5 Mio. Euro gegen ClearView AI.[12]
- Die französische Datenschutzbehörde CNIL verhängte eine Geldbuße in Höhe von 20 Mio. Euro gegen ClearView AI.[13]
- Die griechische Datenschutzaufsicht verhängte ein Bußgeld in Höhe von 20 Mio. Euro gegen ClearView AI.[14]

---

[10] Siehe zum schwerwiegenden Grundrechtseingriffsgewicht von anlasslosen Datenspeicherungen und den damit verbundenen Missbrauchsmöglichkeiten auch das Urteil zur Vorratsdatenspeicherung: BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08, Rn. 212, https://www.bverfg.de/e/rs20100302_1bvr025608.html

[11] Vgl. die datenschutzrechtliche Einordnung und Beanstandung der Gesichtserkennungssoftware „Videmo 360“ in Hamburg: Tätigkeitsbericht Datenschutz 2018 des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, S.86f: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Taetigkeitsberichte_Datenschutz/Taetigkeitsberichte_PDF/27._Taetigkeitsbericht_Datenschutz_2018.pdf

[12] Siehe Autoriteit Persoonsgegevens (AP): https://autoriteitpersoonsgegevens.nl/actueel/ap-legt-clearview-boete-op-voor-illegale-dataverzameling-voor-gezichtsherkenning

[13] Siehe Commission Nationale de l'Informatique et des Libertés (CNIL): https://www.cnil.fr/fr/reconnaissance-faciale-sanction-de-20-millions-deuros-lencontre-de-clearview-ai

[14] Siehe Griechische Datenschutzaufsichtsbehörde (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα): https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-stin-etaireia-clearview-ai-inc

- Die britische Aufsichtsbehörde ICO verhängte eine Geldstrafe in Höhe von 7,5 Mio. GBP gegen ClearView AI.[15]
- Die italienische Datenschutzbehörde GPDP erließ ein Bußgeld in Höhe von 20 Mio. Euro gegen ClearView AI.[16]

Die europäischen Datenschutzbehörden, der Europäische Datenschutzbeauftragte, der Europäische Datenschutzausschuss[17] und die ehemalige UN-Hochkommissarin für Menschenrechte[18] sehen allesamt gravierende Verstöße gegen elementare Datenschutzregeln und grundrechtliche Garantien, wenn ein massenhafter biometrischer Abgleich zum Einsatz kommt.

AlgorithmWatch ist eine Menschenrechtsorganisation mit Sitz in Berlin und Zürich, die sich mit den gesellschaftlichen Auswirkungen von algorithmischen Entscheidungssystemen (ADM) und Künstlicher Intelligenz (KI) befasst. Wir setzen uns dafür ein, dass solche Technologien Menschenrechte, Demokratie und Nachhaltigkeit stärken, statt sie zu schwächen. Dazu tragen wir mit politischen Kampagnen, Lobbyarbeit, journalistischen Recherchen, Forschung und Technikentwicklung bei.

Webseite von AlgorithmWatch: https://algorithmwatch.org/

Webseite des Bündnisses Gesichtserkennung Stoppen!
https://gesichtserkennung-stoppen.de/

Kontakt zum Autor:

Kilian Vieth-Ditlmann, vieth-ditlmann@algorithmwatch.org

[15] Siehe Information Commissioner's Office (ICO):
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/
[16] Siehe Garante per la protezione dei dati personali (GPDP):
https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751323
[17] Siehe EDPB / EDPS:
https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf
[18] Siehe OHCHR:
https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469