ALGORITHM WATCH

/ Stellungnahme

zum „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit" (BMI) und zum „Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen" (BMJV)

02.04.2026

Verfasst von: Pia Sombetzki & Kilian Vieth-Ditlmann

Unsere Empfehlung in Kürze

Die vorgeschlagenen Befugnisse sind europarechtswidrig, verletzen verfassungsrechtliche Mindestanforderungen und widersprechen datenschutzrechtlichen Grundsätzen.

Diese verfassungs- und menschenrechtliche Unverhältnismäßigkeit lässt ausschließlich die Empfehlung zu, die Gesetzentwürfe zurückzuziehen und ein grundsätzliches gesetzliches Verbot des Einsatzes biometrischer Massenerkennungssysteme für öffentliche und private Stellen einzuführen.

Einleitung

Diese Stellungnahme beschränkt sich aus Zeitgründen auf die Befugnisse für einen *automatisierten biometrischen Abgleich mit öffentlich verfügbaren Daten aus dem Internet*.[1] Im Einzelnen betrifft dies folgende vorgeschlagene Regelungen in den Gesetzentwürfen „zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“[2] und „zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“[3]:

- § 9a im Bundeskriminalamtgesetz: nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet
    - zum Zweck der Identifizierung, Aufenthaltsermittlung, Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen von Straftaten oder Gefahren
- § 63b Bundeskriminalamtgesetz, sowie § 58a 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 Erforschung des Sachverhalts, zur Identitätsfeststellung oder zur Ermittlung des Aufenthaltsorts des Beschuldigten oder eines Zeugen
- § 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

Der biometrische Abgleich ermöglicht die Identifizierung von Personen im öffentlichen Raum und im Internet auf Basis biometrischer Merkmale und schafft somit die technischen Voraussetzungen für eine flächendeckende Verfolgung aller Menschen im (digitalen) öffentlichen Raum.

Die Einführung dieser Systeme stellt einen fundamentalen Eingriff in Grundrechte dar und gefährdet rechtsstaatliche Grundsätze wie Transparenz, Diskriminierungsfreiheit und effektiven Rechtsschutz. Diese Gefahren werden durch die in den Entwürfen benannten Zwecke nicht gerechtfertigt. Sie wiederholen damit die Fehler und Mängel

---

[1] Für eine Bewertung der weiteren Befugnisse zu *Automatisierten Datenanalyse* und zur *Weiterverarbeitung von Daten zum Trainieren von IT-Produkten* sei auf die gemeinsame Stellungnahme im Rahmen der Verbändebeteiligung verwiesen: https://www.rav.de/presse/pressemitteilung/lex-palantir-gefaehrdet-grundrechte-1245

[2] Referentenentwurf des Bundesministeriums des Innern (Bearbeitungsstand 09.03.2026): https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/OESI3/refE-ermittlungsbefugnisse-polizeiarbeit.pdf?__blob=publicationFile&v=1

[3] Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (veröffentlicht am 12.03.2026): https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_Digitale_Ermittlungsma%C3%9Fnahmen.pdf?__blob=publicationFile&v=2

des sogenannten Sicherheitspakets der Ampelkoalition, die schon 2024 ähnliche Überwachungsbefugnisse einführen wollte.

Die Gesetzesentwürfe sollten zurückgezogen werden. Stattdessen sollte ein grundsätzliches gesetzliches Verbot des Einsatzes biometrischer Massenerkennungssysteme für öffentliche und private Stellen eingeführt werden.

Grundsätzliche Unvereinbarkeit mit verfassungsrechtlichen und datenschutzrechtlichen Vorgaben

Die vorgeschlagenen biometrischen Überwachungsbefugnisse sind mit verfassungsrechtlichen und datenschutzrechtlichen 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, beispielsweise zum Abgleich mit Datenbankbeständen, verletzt insbesondere aber nicht ausschließlich die Grundrechte auf informationelle Selbstbestimmung und freie Meinungsäußerung. Das Eingriffsgewicht ist besonders hoch, weil die Maßnahme heimlich erfolgt und eine extrem hohe Streubreite hat: Betroffen sind alle Menschen, von denen Gesichtsbilder oder Audiodateien im Internet zugänglich sind. Hinzu kommt, dass erhebliche Diskriminierungsrisiken bestehen und besonders sensible Daten erfasst werden können (z.B. Aufnahmen von Demonstrationen, Parteiveranstaltungen, Pride-Events, Gewerkschaftskundgebungen, Gottesdiensten usw.).

Das Bundesverfassungsgericht hat bereits für die großflächige automatisierte Verarbeitung von Kfz-Kennzeichen durch Polizei und Strafverfolgungsbehörden hohe verfassungsrechtliche Anforderungen aufgestellt.[4] Dort ging es nicht um besonders sensible biometrische Daten wie Gesichter, sondern lediglich 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.[5] Auch ein jüngeres Verfassungsgerichtsurteil über die automatisierte Datenanalyse für die vorbeugende Bekämpfung von Straftaten stellt mit Verweis auf das Grundrecht auf informationelle Selbstbestimmung klar, dass der automatische Abgleich biometrischer Daten besondere Voraussetzungen nachweisen muss.[6]

Die Anforderungen für die vorgeschlagene massenhafte Verarbeitung biometrischer Daten sind zu unspezifisch und die Einsatzzwecke und Tatbestandsmerkmale zu breit und nicht gewichtig genug, als dass eine grundrechtskonforme Anwendung realistisch

[4] BVerfG, Urteil des Ersten Senats vom 11. März 2008, 1 BvR 2074/05, https://www.bverfg.de/e/rs20080311_1bvr207405.html
[5] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, https://www.bverfg.de/e/rs20181218_1bvr014215.html
[6] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, Rn. 87, https://www.bverfg.de/e/rs20230216_1bvr154719.html

erscheint. Der Straftatenkatalog des § 100a Abs. 2 StPO wird regelmäßig erweitert und angepasst, weshalb er nicht zur klaren Begrenzung der Maßnahmen auf schwerwiegende Straftaten geeignet ist. Das Erfassen von Daten, die den Kernbereich privater Lebensgestaltung berühren, wird durch den Entwurf nicht grundsätzlich ausgeschlossen und ist praktisch nicht zu verhindern. Durch die enorme Streubreite des vorgeschlagenen biometrischen Abgleichs ist davon auszugehen, dass auch Erkenntnisse aus dem Kernbereich privater Lebensführung erhoben werden (z.B. Fotos von privaten Familienfeiern wie Hochzeiten oder Kindergeburtstagen). Dass diese höchst privaten Daten nicht verwertet werden dürfen und unverzüglich zu löschen sind, stellt keinen hinreichenden Schutz dar. Allein die Möglichkeit der entsprechenden Datenerfassung erhöht den Überwachungsdruck und schränkt somit die grundrechtlich garantierte Privatsphäre ein.

Die öffentliche Verfügbarkeit der Daten, die für einen Abgleich herangezogen werden, ändert nichts daran, dass Schutzbereiche der Grundrechte berührt sind.[7] Insbesondere dann nicht, wenn besonders schützenswerte, lebenslang unveränderbare biometrische Daten wie Stimm- oder Gesichtsmuster abgeleitet werden. Die Rechtsprechung des Bundesverfassungsgerichts spannt einen Schutzschirm, der darauf abzielt, Einschüchterungseffekte zu verhindern, die entstehen können, wenn Einzelne nicht mit ausreichender Sicherheit die Verbreitung ihrer Daten überblicken können. Die massenhafte biometrische Identifizierung hat eine zutiefst einschüchternde Wirkung, da Menschen nicht wissen, ob, wann und wie Foto- und Videoaufnahmen oder anderes Datenmaterial, beispielsweise Podcasts, in Zukunft durch KI-Systeme von Polizei-, Strafverfolgungs- und Migrationsbehörden ausgewertet werden.[8]

Ineffiziente technische Ausgestaltung des biometrischen Bildabgleichs und mögliche Umgehung geltender Verbote

Die Gesetzentwürfe legen die technische Ausgestaltung des massenhaften biometrischen Abgleichs völlig unzureichend dar. Es sollen zwar die im Rahmen des biometrischen Abgleichs erhobenen und verarbeiteten Daten nach dessen Durchführung „unverzüglich" gelöscht werden (insofern sie keinen konkreten Ermittlungsansatz aufweisen). Allerdings bleibt unklar, wie die angeführte automatisierte Anwendung zur Datenverarbeitung technisch funktionieren soll.

[7] 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.

[8] 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

Ein durch AlgorithmWatch beauftragtes Gutachten[9] und eine Analyse der Wissenschaftlichen Dienste des Bundestags[10] haben kürzlich festgestellt, dass ein biometrischer Abgleich zwischen Bildern gesuchter Personen und im Internet verfügbaren Fotos ohne Verwendung einer Datenbank nicht sinnvoll umsetzbar ist. Die Gesetzentwürfe ignorieren mit ihrem Verweis auf eine „automatisierte Anwendung zur Datenverarbeitung", dass Bilder (und andere Datenbestände) gesammelt und vorverarbeitet werden müssen, um für einen Abgleich nach ihnen suchen zu können. Für diese Vorverarbeitung müssen zwangsläufig KI-Systeme zum Einsatz kommen, die biometrische Muster aus diesen Datenbeständen extrahieren. Die Vorverarbeitung ist so komplex, dass sie nicht erst dann durchgeführt werden kann, wenn eine Suchanfrage gestellt wird. Erst das Sammeln und Vorverarbeiten der Daten ermöglicht eine effiziente Suche. Für den Zugriff auf die vorverarbeiteten Bilder ist es notwendig, sie in einer Datenbank zu speichern. Es ist dementsprechend technisch nicht realisierbar, öffentlich verfügbare Bilder aus dem Internet für einen biometrischen Abgleich zu verwenden, ohne ein KI-System einzusetzen und ohne eine Datenbank zu erstellen.

Artikel 5, Absatz 1 Buchstabe e KI-VO verbietet 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". Um europarechtskonform zu sein, müsste der Aufbau einer Datenbank mittels KI-Systemen gesetzlich klar ausgeschlossen sein. Dies ist nicht der Fall.

Stattdessen enthalten die Gesetzentwürfe eine Art **Auslagerungsbefugnis**, für den Fall, dass Polizei- und Strafverfolgungsbehörden den Abgleich technisch nicht selbst durchführen können. **Sie erlaubt ausdrücklich eine Übermittlung von Daten zum Zweck eines biometrischen Abgleichs an öffentliche Stellen und private Anbieter sowohl im Inland als auch im Ausland, innerhalb wie außerhalb der Europäischen Union.**

Hinsichtlich der Umsetzung dieses Befugnisses wird lediglich auf grundsätzliche Bestimmungen für die Übermittlung personenbezogener Daten verwiesen, etwa nach dem Gesetz über die internationale Rechtshilfe in Strafsachen, insbesondere Paragraf 77d und Paragraf 81 des Bundesdatenschutzgesetzes, der die sonstige Datenübermittlung an Empfänger in Drittstaaten regelt.

Eine Erlaubnis für solch eine Auslagerung des biometrischen Abgleichs ins (Nicht-EU-)Ausland führt sämtliche durch die Gesetzestexte eingeführten Beschränkungen ad absurdum. Damit wird der in den Gesetzentwürfen beschriebene Vorgang des Löschens aller verarbeiteten Daten nach jeder einzelnen Suchanfrage zur theoretischen Fassade. Mutmaßlich, weil die praktisch ineffiziente und wirkungslose Durchführung als Problem bekannt ist. Aus diesem Grund, so die Vermutung, wird auf die Übermittlung von Daten an Dritte verwiesen, welche den Abgleich im Auftrag deutscher Behörden durchführen würden. Relevante Anbieter von

[9] Vgl. Gutachten „Braucht die Polizei eine Datenbank zum biometrischen Abgleich?", www.algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/ (zuletzt abgerufen am 30.03.2026)

[10] Vgl. Analyse „Biometrischer Abgleich mit Bildern aus dem Internet. Technische Umsetzung und Vereinbarkeit mit der KI-Verordnung", https://www.bundestag.de/resource/blob/1149732/EU-6-074-25-WD-5-105-25.pdf (zuletzt abgerufen am 30.03.2026)

Gesichtersuchmaschinen sind unter anderem im Nicht-EU-Ausland ansässig, etwa in den USA, in Dubai oder in Israel. Wichtig zu betonen ist in diesem Kontext, dass der Staat dem Rechtsstaatsprinzip nach selbst keine rechtswidrigen Angebote Dritter nutzen darf. Ein Delegieren der Umsetzung ins Ausland stellt entsprechend keine europa- und grundrechtskonforme Lösung dar.

Genau diese Konstellation wäre im Falle eines biometrischen Abgleichs mit öffentlich verfügbaren Daten aus dem Internet allerdings gegeben. So haben etliche Datenschutzbehörden die Datenverarbeitung durch Anbieter wie dem Unternehmen ClearView AI, das just solche biometrischen Abgleiche für Strafverfolgungsbehörden anbietet, aufgrund zahlreicher Verstöße gegen die Datenschutzgrundverordnung (DSGVO) beanstandet und in den Vorjahren immer wieder mit hohen Bußgeldern belegt:

- Die niederländische Datenschutzbehörde AP erließ ein Bußgeld in Höhe von 30,5 Mio. Euro gegen ClearView AI.[11]
- Die französische Datenschutzbehörde CNIL verhängte eine Geldbuße in Höhe von 20 Mio. Euro gegen ClearView AI.[12]
- Die griechische Datenschutzaufsicht verhängte ein Bußgeld in Höhe von 20 Mio. Euro gegen ClearView AI.[13]
- Die britische Aufsichtsbehörde ICO verhängte eine Geldstrafe in Höhe von 7,5 Mio. GBP gegen ClearView AI.[14]
- Die italienische Datenschutzbehörde GPDP erließ ein Bußgeld in Höhe von 20 Mio. Euro gegen ClearView AI.[15]

Die europäischen Datenschutzbehörden, der Europäische Datenschutzbeauftragte, der Europäische Datenschutzausschuss[16] und die ehemalige UN-Hochkommissarin für Menschenrechte[17] sehen in dem massenhaften biometrischen Abgleich allesamt gravierende Verstöße gegen elementare Datenschutzregeln und grundrechtliche Garantien. Hinzu kommt, dass das oben beschriebene Verbot nach Artikel 5, Absatz 1 Buchst. e KI-VO auch und insbesondere bei Angeboten von privaten Anbietern wie ClearView AI, PimEyes und weiteren gilt.

---

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

[12] Siehe European Data Protection Board: https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en

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

[14] Siehe Information Commissioner's Office (ICO):https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/10/uk-upper-tribunal-hands-down-judgment-on-clearview-ai-inc/

[15] Siehe Garante per la protezione dei dati personali (GPDP): https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751323

[16] Siehe EDPB / EDPS: https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

[17] Siehe OHCHR: https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469

Es gilt festzustellen: **Verfassungsrechtliche, datenschutzrechtliche und schließlich EU-rechtliche Grenzen dürfen nicht durch ein in den Gesetzentwürfen angelegtes Auslagern einer solchen Praxis umgangen werden.** Erwägungsgrund 43 KI-Verordnung verweist explizit auf das mit einem biometrischen Abgleich „einhergehende **Gefühl der Massenüberwachung** [, welches] verstärkt und zu **schweren Verstößen gegen die Grundrechte**, einschließlich des Rechts auf Privatsphäre, führen kann."

Anstatt den Sachverhalt so diffus zu beschreiben, dass augenscheinlich zu **verschleiern versucht wird, wann und durch welche Institutionen oder Unternehmen sensible biometrische Daten verarbeitet werden, müssen diese schweren Grundrechtsverstöße klar gesetzlich ausgeschlossen werden.** Schließlich ist trotz der beschriebenen grundsätzlichen Bestimmungen praktisch nicht sicherzustellen, dass Dritte ihre Löschpflichten erfüllen. Derart schwerwiegende Grundrechtseingriffe dürfen nicht an private Unternehmen oder öffentliche Stellen in Drittstaaten ausgelagert werden. Dies gilt auch für das Training von IT-Produkten mit personenbezogenen Daten durch private Unternehmen, das durch die Regelungen ermöglicht wird.

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/

Kontakt zu den Autor*innen:

Pia Sombetzki, sombetzki@algorithmwatch.org

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