



Ausschussdrucksache 21(4)214 D
vom 17. September 2026

Schriftliche Stellungnahme

von Pia Sombetzki, AW Algorithm Watch gGmbH, Berlin vom
17.09.2026

zu dem

- a) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus
BT-Drucksachen 21/6131, 21/7265
- b) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit
BT-Drucksachen 21/6132, 21/6511
- c) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen
BT-Drucksache 21/6806

/ Stellungnahme

zu den Gesetzentwürfen

„Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ (Drucksache 21/6132)

„Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“ (Drucksache 21/6131)

„Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“ (21/6806)

Fassung vom 17.09.2026

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 zugänglichen Daten aus dem Internet* sowie für die *Weiterverarbeitung von Daten zu weiteren Zwecken*. Im Einzelnen betrifft dies folgende vorgeschlagene Regelungen in den Gesetzentwürfen „zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“¹, „zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“² und „zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“³:

- § 9a, § 39a und § 63b 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
- § 58a Bundespolizeigesetz: nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet zur Gefahrenabwehr zum Zweck der Identifizierung, Aufenthaltsermittlung, Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen von Straftaten oder Gefahren
- § 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
- § 22 im Bundeskriminalamtgesetz und § 46 im Bundespolizeigesetz: Weiterverarbeitung von Daten zu weiteren Zwecken

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

¹ Gesetzentwurf der Bundesregierung (Bearbeitungsstand 26.05.2026):

<https://dserver.bundestag.de/btd/21/061/2106132.pdf>

² Gesetzentwurf der Bundesregierung (Bearbeitungsstand 26.05.2026):

<https://dserver.bundestag.de/btd/21/061/2106131.pdf>

³ Gesetzentwurf der Bundesregierung (Bearbeitungsstand 01.07.2026):

<https://dserver.bundestag.de/btd/21/068/2106806.pdf>

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 der Rechtsprechung des Bundesverfassungsgerichts immer einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.⁵ 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 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 sind zu breit und nicht gewichtig genug, als dass eine grundrechtskonforme Anwendung realistisch erschiene. So soll der biometrische Abgleich im Kontext polizeilicher Ermittlungen und der Strafverfolgung nicht allein zum Zweck der Identifizierung und zur

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

Aufenthaltsermittlung eingesetzt werden, sondern ganz generell zur Erforschung eines Sachverhalts und zur Ermittlung von Zusammenhängen von Straftaten oder Gefahren. Die in diesem Kontext angeführten Bedingungen für den biometrischen Abgleich sind derart weit gefasst, dass sie kaum abgrenzenden Effekt haben. Bereits eine allgemeine Prognose, dass eine Person eine relevante Straftat begehen könnte, soll ausreichen, um Anlass für einen biometrischen Abgleich zu bieten. Es wird auf den Straftatenkatalog des § 100a Abs. 2 StPO als Richtschnur für schwerwiegende Straftaten verwiesen, allerdings nicht abschließend. Vielmehr verweisen § 9a BKA-G-E und § 98d StPO-E auf „Straftaten von erheblicher Bedeutung“, was zu einer ungenauen Abgrenzung des angelegten Straftatenkatalogs führt. Grundsätzlich eignet sich der Straftatenkatalog des § 100a Abs. 2 StPO nicht als Grundlage, um den Einsatz auf schwerwiegende Straftaten zu begrenzen. Ferner wird er regelmäßig erweitert und angepasst, was ihn noch zusätzlich ungeeignet macht, um einen echten begrenzenden Effekt zu haben.

Das Erfassen von Daten, die den Kernbereich privater Lebensgestaltung berühren, wird durch den Entwurf nicht prinzipiell 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.

Asylsuchende sind als dem Staat gegenüberstehende besonders vulnerable Gruppe noch zusätzlich einer ganzen Reihe folgenreicher Risiken ausgesetzt: Liegen keine Identitätsdokumente vor, könnte der biometrische Abgleich für sie zur Standardmaßnahme werden, so wie er durch § 15b AsylG (angepasst) geregelt wird. In der Begründung des Gesetzes wird der biometrische Abgleich gegenüber der Durchsuchung von privaten Datenträgern (wie in § 15a AsylG geregelt) als die mildere Maßnahme beschrieben, was dieses Bedenken unterstreicht. Biometrische Erkennungssysteme basieren auf Datensätzen, in denen nicht-weiße Personengruppen unterrepräsentiert sind. Bei diesen Gruppen ist deshalb das Risiko von Fehlidentifizierungen deutlich höher einzuschätzen – eine Problematik, die insbesondere People of Colour betrifft, die einen signifikanten Anteil der Asylsuchenden ausmachen dürften.

Grundsätzlich ändert auch die öffentliche Verfügbarkeit der Daten, die für einen Abgleich herangezogen werden, nichts daran, dass Schutzbereiche der Grundrechte berührt sind. Vornehmlich 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, etwa Podcasts, in Zukunft durch KI-Systeme von Polizei-, Strafverfolgungs- und Migrationsbehörden ausgewertet werden.

7

Ineffiziente technische Ausgestaltung des biometrischen Bildabgleichs und mögliche Umgehung geltender Verbote

Die Gesetzentwürfe legen die technische Ausgestaltung des massenhaften biometrischen Abgleichs völlig unzureichend und realitätsfern dar. Es sollen die im Rahmen des biometrischen Abgleichs erhobenen und verarbeiteten Daten nach dessen Durchführung „unverzüglich“ gelöscht werden, insofern sie „keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt“ und (neu) „für ein anderes (Straf-) Verfahren“ aufweisen (§ 9a Abs. 4 BKA-G-E, § 63b Abs. 4, § 58a Abs. 4 BPol-G-E, § 39a BKA-G, § 98d Abs. 3 StPO-E). Diese Ausweitung der Ausnahme deutet bereits darauf hin, dass in der Praxis ausreichend Spielraum bestehen bleiben soll, diese Löschpflicht zu umgehen. In der Begründung zu § 9a Abs. 4 BKA-G wird zwar konkretisiert, dass „auch technische Exzerpte der erhobenen Daten“ von der Löschpflicht umfasst sind, sie droht dennoch in ihrer praktischen Umsetzung ins Leere zu laufen. Schließlich widerspricht dies den technischen Grundprinzipien, nach denen ein biometrischer Abgleich funktioniert.

Ein durch AlgorithmWatch beauftragtes **technisches Gutachten**⁸ und eine Analyse der Wissenschaftlichen Dienste des Bundestags⁹ 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 zum Einsatz kommende „automatisierte Anwendung zur Datenverarbeitung“, dass Bilder (und andere Datenbestände) gesammelt und vorverarbeitet werden müssen, um für einen Abgleich nach ihnen suchen zu können. Bei der Vorverarbeitung müssen zwangsläufig KI-Systeme zum Einsatz kommen. Die Vorverarbeitung von Daten, in der biometrische Muster aus diesen Datenbeständen extrahiert werden, 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

⁷ 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

⁸ Vgl. Gutachten „Braucht die Polizei eine Datenbank zum biometrischen Abgleich?“, www.algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/ (zuletzt abgerufen am 16.09.2026)

⁹ 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 16.09.2026)

dementsprechend technisch nicht realisierbar, öffentlich verfügbare Bilder (und andere Datenbestände) 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 der 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 dieser Befugnisse wird lediglich auf grundsätzliche Bestimmungen für die Übermittlung personenbezogener Daten verwiesen, etwa nach dem Gesetz über die internationale Rechtshilfe in Strafsachen, insbesondere Paragraph 77d und Paragraph 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 Löschsens aller verarbeiteten Daten nach jeder einzelnen Suchanfrage nur umso offensichtlicher 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 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 kommerzielle 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.¹⁰
- Die französische Datenschutzbehörde CNIL verhängte eine Geldbuße in Höhe von 20 Mio. Euro gegen ClearView AI.¹¹
- Die griechische Datenschutzaufsicht verhängte ein Bußgeld in Höhe von 20 Mio. Euro gegen ClearView AI.¹²
- Die britische Aufsichtsbehörde ICO verhängte eine Geldstrafe in Höhe von 7,5 Mio. GBP gegen ClearView AI.¹³
- Die italienische Datenschutzbehörde GPDP erließ ein Bußgeld in Höhe von 20 Mio. Euro gegen ClearView AI.¹⁴

Die europäischen Datenschutzbehörden, der Europäische Datenschutzbeauftragte, der Europäische Datenschutzausschuss¹⁵ und die ehemalige UN-Hochkommissarin für Menschenrechte¹⁶ 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, Buchstabe e der KI-VO auch und insbesondere bei Angeboten von privaten Anbietern wie ClearView AI, PimEyes und weiteren gilt.

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 der 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

¹⁰ Siehe Autoriteit Persoonsgegevens (AP):

<https://autoriteitpersoonsgegevens.nl/actueel/ap-legt-clearview-boete-op-voor-illegale-dataverzameling-voor-gezichtsherkenning>

¹¹ Siehe European Data Protection Board:

https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en

¹² Siehe Griechische Datenschutzaufsichtsbehörde (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα):

<https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-stin-etaireia-clearview-ai-inc>

¹³ 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/>

¹⁴ Siehe Garante per la protezione dei dati personali (GPDP):

<https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751323>

¹⁵ Siehe EDPB / EDPS:

https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

¹⁶ Siehe OHCHR:

<https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469>

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.

Keine polizeilichen Datenbestände für das KI-Training freigeben

Der Gesetzentwurf zur „Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ (Drs. 6132) führt Befugnisse sowohl im BKA- als auch im BPol-Gesetz (§ 22 BKA-G, § 46 BPol-G) ein, durch die die Weiterverarbeitung von Daten zur „Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten einschließlich selbstlernender Systeme“ möglich werden soll.

Die beim Bundeskriminalamt und bei der Bundespolizei vorhandenen Datenbestände sollen für diese Zwecke herangezogen werden. Sie umfassen unter anderem Angaben von Zeuginnen und Zeugen, Erhebungen mit weitreichender personeller Streuung wie Funkzellenabfragen, personenbezogene Informationen aus Asservatenbeständen oder Erkenntnisse der Telekommunikationsüberwachung sowie biometrische Daten, also besonders personenbezogene Daten mit hohem Schutzbedürfnis. Die Verwendung des nahezu gesamten Datenbestandes ist unverhältnismäßig.

Eine Verarbeitung personenbezogener Daten soll bereits zulässig sein, wenn der mit einer Anonymisierung oder Pseudonymisierung verbundene Aufwand als unverhältnismäßig hoch eingestuft wird. Die Beurteilung darüber wird dem Ermessen der jeweiligen Behörde überlassen, anstatt sie im Gesetz klar zu regeln. Damit können häufig nicht anonymisierte Daten zur Verwendung kommen, ohne unabhängige Kontrolle, ob das tatsächlich notwendig und verhältnismäßig ist. Grundsätzlich sollten immer nur anonymisierte oder synthetische Daten für externes KI-Training verwendet werden.

Dass bei der Weiterverarbeitung sicherzustellen sei, dass „diskriminierende Algorithmen weder herausgebildet noch verwendet werden“, stellt keine echte Absicherung dar, da diese Bedingung an keine konkreten Prozessvorgaben sowie Referenzstandards geknüpft ist.

Ferner bleibt das Risiko unadressiert, dass sensible **personenbezogene Daten aus KI-Modellen reproduzierbar** sind und unbefugten Dritten zukommen könnten. Wissenschaftliche Analysen zeigen zum Beispiel, dass durch „Memorization-Angriffe“ Trainingsdaten aus KI-Modellen wieder extrahiert werden können. Außerdem ist es u. U. möglich, zu rekonstruieren, ob eine Person oder bestimmte Daten Teil eines Trainingsdatensatzes waren.¹⁷ Nutzer*innen können „Data Leakage“ auch unabsichtlich

¹⁷ Siehe Xiong, Zhao, Pappu, Song (15.12.2025), „The Landscape of Memorization in LLMs: Mechanisms, Measurement, and Mitigation“, <https://arxiv.org/abs/2507.05578> (zuletzt abgerufen am 16.09.2026)

auslösen. Dadurch können Löschvorschriften für Trainingsdaten insgesamt ins Leere laufen.

Bei der Weitergabe an Dritte besteht das grundsätzliche Risiko eines Datenmissbrauchs oder -verlusts. Die Verwendung nicht anonymisierter Daten ist hier besonders schwerwiegend. Insbesondere an Dritte sollten Daten nicht ohne Anonymisierung weitergegeben werden. Es stellt sich zudem die grundsätzliche Frage, ob Daten der Bevölkerung überhaupt der Verbesserung der kommerziellen Produkte Dritter dienen sollten. Sofern es dem Gesetzgeber mit der Erlaubnis zum IT-Training darum geht, von kommerziellen Produkten mittelfristig unabhängiger zu werden, sollte die Verwendung polizeilicher Daten nur für Entwicklung und Training staatlicher Anwendungen erlaubt werden.

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