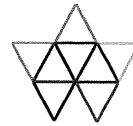
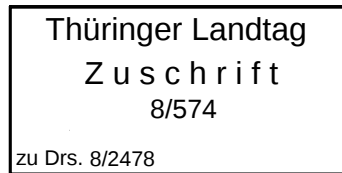


Den Mitgliedern des AfIKL

THÜR. LANDTAG POST
26.05.2026 16:32
1605812026



ALGORITHM
WATCH



/ Stellungnahme

zu dem Zweiten Gesetz zur Änderung des Polizeiaufgabengesetzes (Drucksache 8/2478)

Fassung vom 26.05.2026

verfasst von: Pia Sombetzki, Kilian Vieth-Ditlmann

Einleitung

Diese Stellungnahme beschränkt sich aus Zeitgründen auf die Befugnis für einen *nachträglichen biometrischen Abgleich mit öffentlich frei zugänglichen personenbezogenen Daten aus dem Internet* sowie auf die Befugnis für die *automatische Auswertung von Bild- und Tonaufnahmen im Kontext der Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an besonderen Orten*.

Im Einzelnen betrifft dies die folgende vorgeschlagene Regelungen im Gesetzentwurf „zu dem Zweiten Gesetz zur Änderung des Polizeiaufgabengesetzes (Drucksache 8/2478)“,

- § 33 Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an besonderen Orten
- § 43a Nachträglicher biometrischer Abgleich mit öffentlich frei zugänglichen personenbezogenen Daten aus dem Internet

Der Einsatz KI-gestützter Videoüberwachung in Form einer automatisierten Auswertung von Verhaltensmustern droht die Anonymität im öffentlichen Raum und an Orten, die Menschen nicht meiden können, nahezu vollständig aufzuheben. Dies kann sich negativ auf die Wahrnehmung fundamentaler demokratischer Grundrechte und die Selbstbestimmung auswirken.

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 im Entwurf genannten Zwecke nicht gerechtfertigt.

Die durch den Gesetzesentwurf eingeführten Befugnisse sollten zurückgezogen werden.

Grundsätzliche Unvereinbarkeit mit verfassungsrechtlichen und datenschutzrechtlichen Vorgaben

Die vorgeschlagene biometrische Überwachungsbefugnis ist mit verfassungsrechtlichen und datenschutzrechtlichen Mindeststandards nicht vereinbar. Die Überwachungsmaßnahme berührt zwangsläufig die Grundrechte aller Menschen und ist weder erforderlich noch verhältnismäßig. 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.¹ 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.² 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.³

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

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

² BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, https://www.bverfg.de/e/rs20181218_1bvr014215.html

³ BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, Rn. 87, https://www.bverfg.de/e/rs20230216_1bvr154719.html

grundrechtskonforme Anwendung realistisch 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.⁴ 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.⁵

Unvereinbarkeit mit EU-Recht: Verstoß gegen geltendes Verbot nach KI-VO

Der Gesetzentwurf legt 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 für den Ausgangssachverhalt aufweisen). Allerdings bleibt unklar, wie die angeführte automatisierte Anwendung zur Datenverarbeitung technisch funktionieren soll. Die Gesetzesbegründung spricht abstrakt von einer „technisch gestützte[n] Überprüfung der Übereinstimmung von biometrischen Signaturen mit dem Ergebnis einer Übereinstimmungsbewertung“. Zu §43a Absatz 1 wird erläutert, dass mittels einer „technischen Anwendung [...] Lichtbilder und Videos in einer Form

⁴ 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.

⁵ 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

zusammengeführt und analysiert werden [können], die einen Abgleich ermöglicht.“ Dies bestätigt einerseits das zur Umsetzung der Befugnis eine Datenbank aufgebaut werden muss, verschleiert aber gleichzeitig, dass sich hinter dem Begriff „technische Anwendung“ im Kern ein automatisiertes Verfahren verbirgt, bei welchem zwangsläufig KI-Systeme zum Einsatz kommen.

Das durch AlgorithmWatch beauftragte technische Gutachten⁶ und eine Analyse der Wissenschaftlichen Dienste des Bundestags⁷ haben kürzlich festgestellt, dass ein biometrischer Abgleich zwischen Bildern gesuchter Personen und im Internet verfügbaren Fotos ohne Verwendung einer Datenbank nicht sinnvoll umsetzbar ist. Der Gesetzentwurf ignoriert mit dem Verweis auf eine „technische Anwendung“, 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. So wie auch die Begründung des Gesetzes suggeriert: 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 (oft auch AI Act) verbietet allerdings 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.⁸

Es gilt festzustellen: **Verfassungsrechtliche, datenschutzrechtliche und nicht zuletzt klare EU-rechtliche Grenzen sprechen eindeutig gegen die Einführung der Befugnis, nachträgliche biometrische Abgleiche mit öffentlich frei zugänglichen Daten durchführen zu können.** 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.“ Mit einer

⁶ Vgl. Gutachten „Braucht die Polizei eine Datenbank zum biometrischen Abgleich?“, www.algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/ (zuletzt abgerufen am 26.05.2026)

⁷ 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 26.05.2026)

⁸ Das Gleiche gilt für ähnlich gelagerte Befugnisse, die momentan auf Bundesebene diskutiert werden, siehe diverse Stellungnahmen zum biometrischen Abgleich dort: <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/OESI3/ermittlungsbefugnisse-polizeiarbeit/algorithmwatch.pdf> und <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/OESI3/ermittlungsbefugnisse-intterrorismus/gem-stellg-amnesty-ua.pdf>

Einführung würde man eine ganze Reihe an grund- und menschenrechtlichen Risiken eingehen und durch die enorme Streubreite eine Massenbetroffenheit von Bürger*innen in Kauf nehmen, willkürlich und unbemerkt in das Visier von Ermittlungsbehörden zu geraten.

Unverhältnismäßigkeit von KI-gestützter Videoüberwachung

Auch die Einführung der Befugnis zur „automatische Auswertung“ von Bild- und Tonaufnahmen gemäß § 33 (zur Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an besonderen Orten) ist als unverhältnismäßig abzulehnen.

Ist auf öffentlichen Plätzen, in Bahnhöfen, Stadien oder Einkaufszentren eine technische Infrastruktur vorhanden, um Personen jederzeit automatisiert zu überwachen, berührt das im Kern die demokratische Öffentlichkeit. Die Beschränkung des Einsatzes mit Verweis auf § 14 Absatz 1 auf besondere Orte genügt grundsätzlich nicht, da sogenannte Gefahrengelände öffentlich nicht nachvollziehbar und zeitlich variabel, teils durch einzelne Beamte bestimmt werden. § 33 Absatz 4 führt außerdem eine „automatisierte Nachverfolgung“ von Personen ein, die es ermöglicht Zusammenhänge zwischen Personen, Orten und Objekten herzustellen, die auch direkte Rückschlüsse auf Personen möglich machen.

Durch den Einsatz automatisierter Erkennungssysteme droht die Anonymität im öffentlichen Raum und an Orten, die Menschen nicht meiden können, etwa, weil sie dort Grundbedürfnissen nachgehen, vollständig aufgehoben zu werden. Das kann sich fatal auf die Wahrnehmung fundamentaler demokratischer Grundrechte und die Selbstbestimmung auswirken. Menschen, die das Gefühl haben müssen, dass ihre Handlungen an einem öffentlichen Platz überwacht und sie jederzeit ganz persönlich identifiziert werden können, werden möglicherweise davon abgehalten, sich zu versammeln und ihre Meinung zu äußern: Es könnte sie beispielsweise konkret davon abhalten, an einer Demonstration teilzunehmen, eine religiöse Stätte aufzusuchen oder ein Lokal zu besuchen, das besonders bei Menschen einer bestimmten sexuellen Orientierung beliebt ist. Dass Menschen ihre Grundrechte wahrnehmen und sich im öffentlichen Raum frei und unerkannt bewegen können, ist jedoch eine Grundvoraussetzung für demokratische Gesellschaften.⁹

Grundsätzlich ist die automatisierte Verhaltensanalyse ein Verfahren, das als mangelhaft evaluiert gilt. In Mannheim, wo es 2018 in Deutschland zuerst eingeführt wurde, ist die Testphase bisher weiterhin nicht abgeschlossen und unabhängige Evaluationen fehlen für die bisher in Deutschland bekannten Einsätze. Probleme, die aus öffentlicher Berichterstattung und in Teilen veröffentlichten Evaluationsdokumenten (des Modellprojekts Hansaplatz) hervorgehen, sind u.a. (1) die **hohe Fehleranfälligkeit**, beispielsweise werden ungefährliche Handlungen als vermeintlich gefährlich markiert;

⁹ Siehe u.a. https://algorithmwatch.org/de/wp-content/uploads/2023/08/9_v2.pdf

(2) der **hohe administrative Aufwand für Beamt*innen**, die eine Vielzahl an Fehlalarmen prüfen müssen; (3) der sich grundsätzlich abzeichnende **nicht nachweisbare Nutzen, kriminelle Handlungen vermeiden zu können**, bei gleichzeitig hohen Betriebskosten materieller als auch immaterieller Art, wie den zuvor beschriebenen unverhältnismäßig tiefen Eingriffen in die Grundrechte.¹⁰

Die Befugnis zur automatischen Auswertung setzt daher Fehlanreize, die Videoüberwachung im öffentlichen Raum noch weiter auszubauen und sollte daher zurückgezogen 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

¹⁰ Siehe der teils veröffentlichte Evaluationsprojektbericht zu KI-gestützter Videoüberwachung am Hansaplatz in Hamburg (2024): <https://fragdenstaat.de/anfrage/intensivierung-der-videoueberwachung-am-hansaplatz/926714/anhang/evaluationsbericht.pdf> (zuletzt abgerufen am 26.05.2026); siehe Berichterstattung zur KI-gestützten Videoüberwachung in Mannheim durch AlgorithmWatch (2023) <https://algorithmwatch.org/en/mannheim-system-reports-hugs-police/> (zuletzt abgerufen am 26.05.2026) und [Netzpolitik.org](https://netzpolitik.org/2025/verhaltensscanner-im-mannheim-hier-wird-die-ueberwachung-getestet-die-so-viele-staedte-wollen/) (2025) <https://netzpolitik.org/2025/verhaltensscanner-im-mannheim-hier-wird-die-ueberwachung-getestet-die-so-viele-staedte-wollen/> (zuletzt abgerufen am 26.05.2026)

Landtag Kordilewski, Astrid

Von: Pia Sombetzki <sombetzki@algorithmwatch.org>
Gesendet: Dienstag, 26. Mai 2026 16:32
An: Landtag Poststelle
Betreff: Stellungnahme zu Drucksache 8/2478 (PAG-Reform)
Anlagen: 2026_05_26_Stellungnahme PAG Thüringen .pdf

Sehr geehrte Damen und Herren,

im Anhang übersende ich Ihnen im Auftrag von AlgorithmWatch gGmbH eine schriftliche Stellungnahme zum Zweiten Gesetz zur Änderung des Polizeiaufgabengesetz (Drs. 8/2478).

i.A.

Pia Sombetzki

--

Pia Sombetzki
Senior Policy Manager

<https://algorithmwatch.org>
sombetzki@algorithmwatch.org
Tel.: +49 30 99 40 49 006

Werden Sie Teil von AlgorithmWatch, werden Sie Fördermitglied!
Be part of AlgorithmWatch, become a supporting member!

AW AlgorithmWatch gGmbH
Boyenstraße 41
10115 Berlin

Berlin Charlottenburg HRB 186522 B
Geschäftsführung/Executive Director: Matthias Spielkamp

[Datenschutzerklärung](#) / [Data Protection Policy](#)