

/ Stellungnahme

zum Entwurf für ein Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit (Drucksache 20/4284)

Fassung vom 11.09.2026

verfasst von: Pia Sombetzki

Einleitung

Diese Stellungnahme beschränkt sich aus Zeitgründen auf die folgenden durch den Entwurf für ein Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit (Drucksache 20/4284) einzuführenden Befugnisse:

- § 184 Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten
- § 184b Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen
- § 184c Durchführung der Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen
- § 195b Nachträgliche Fernidentifizierung
- § 195c Durchführung der nachträglichen Fernidentifizierung

Der Einsatz KI-gestützter Videoüberwachung in Form einer automatisierten Auswertung von Verhaltensmustern und zum Zweck der Identifizierung 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.

Die nachträgliche Fernidentifizierung per Abgleich biometrischer Daten mit biometrischen Daten aus dem Internet schafft 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 biometrischer Überwachungsbefugnisse mit verfassungsrechtlichen und datenschutzrechtlichen Vorgaben

Die vorgeschlagenen biometrischen Überwachungsbefugnisse sind mit verfassungsrechtlichen und datenschutzrechtlichen Mindeststandards nicht vereinbar. Sie berühren zwangsläufig die Grundrechte aller Menschen und sind 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.). Der Gesetzesentwurf senkt die Voraussetzungen für den Einsatz von Videoüberwachung durch Polizei oder weitere Ordnungsbehörden im öffentlichen Raum durch die vorgeschlagenen Änderungen an § 184 noch zusätzlich ab. Die Menge an Personen, die unbegründet von Überwachungsmaßnahmen betroffen sind, erhöht sich dadurch.

Biometrische Daten sind besonders sensible Daten, auch weil sie lebenslangen Bestand haben. Gleichzeitig hat das Bundesverfassungsgericht 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 der Rechtsprechung des Bundesverfassungsgerichts immer einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.² Auch ein jüngeres Verfassungsgerichtsurteil über die

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

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 sind zu breit und nicht gewichtig genug, als dass eine grundrechtskonforme Anwendung realistisch erscheint. Das Erfassen von Daten, die den Kernbereich privater Lebensgestaltung berühren, wird durch den Verweis auf Maßnahmen nach § 186a Absatz 1 und 5 zwar als Problem anerkannt, ist aber praktisch nicht zu verhindern. Durch die enorme Streubreite des vorgeschlagenen biometrischen Abgleichs, insbesondere mit Daten aus dem Internet, ist immer 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 Speziell 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, unter anderem Podcasts, in Zukunft durch KI-Systeme von Polizei- und Strafverfolgungsbehörden ausgewertet werden.⁵

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

Der Gesetzentwurf legt die technische Ausgestaltung des massenhaften biometrischen Abgleichs gänzlich unzureichend und realitätsfern dar. Es sollen die

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

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 2. März 2010, 1 BvR 256/08, Rn. 212, https://www.bverfg.de/e/rs20100302_1bvr025608.html

im Rahmen des biometrischen Abgleichs erhobenen und verarbeiteten Daten nach dessen Durchführung und Prüfung „unverzüglich“ gelöscht werden (insofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen). Ferner sollen laut § 195c Absatz 1 „organisatorische und technische Vorkehrungen“ die Einhaltung der Vorgaben des Absatzes sicherstellen. Laut § 195c Absatz 3 sollen diese Einzelheiten in einer Verwaltungsvorschrift, lediglich im „Benehmen“, nicht im Einvernehmen (was einer Zustimmung gleichkäme), mit der Landesbeauftragten für Datenschutz erstellt werden.

Allerdings bleibt unklar, wie die nachträgliche Fernidentifizierung per biometrischem Abgleich rechtskonform praktisch umgesetzt werden soll. In der Begründung wird zwar die Einschätzung vertreten, dass „eine Verarbeitung von öffentlich zugänglichen Daten [...] dagegen von dem Verbot des Artikels 5 Absatz 1 Buchstabe e nicht erfasst [ist], sofern Gesichtsbilder nur anlassbezogen gewonnen werden und nur für diesen Anlass verarbeitet werden, nicht aber auch für zukünftige Verarbeitungsvorgänge in einer Datenbank vorrätig gehalten werden.“

Ein durch AlgorithmWatch beauftragtes technisches Gutachten⁶ und eine Analyse der Wissenschaftlichen Dienste des Bundestags⁷ haben allerdings 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 vermeintlich anlassbezogene Erhebung und Aufbereitung biometrischer Daten und allgemeiner Löschvorgaben, 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 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 der 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

⁶ Vgl. Gutachten „Braucht die Polizei eine Datenbank zum biometrischen Abgleich?“, www.algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/ (zuletzt abgerufen am 11.09.2026)

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 11.09.2026)

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

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 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 und Gefahren von KI-gestützter Videoüberwachung

Auch die Einführung der Befugnis zur automatisierten Auswertung von Daten, Bild- und Tonaufnahmen zur Erkennung und Auswertung von Bewegungsmustern nach § 184 Absatz 5 sowie die Befugnis zur biometrischen Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen nach § 184a und § 184b sind als unverhältnismäßig abzulehnen.

Wenn auf öffentlichen Plätzen, in Bahnhöfen, Stadien oder Einkaufszentren eine technische Infrastruktur vorhanden ist, die eine automatisierte Überwachung von Personen ermöglicht, betrifft das die demokratische Öffentlichkeit in ihrem Kern. Der Einsatz wird nur minimal begrenzt und ist, wenn er offen erfolgt, sogar auf allen allgemein zugänglichen Flächen erlaubt. Bei öffentlichen Veranstaltungen und Ansammlungen reicht es bereits aus, dass Tatsachen annehmen lassen, dass Ordnungswidrigkeiten von erheblicher Bedeutung begangen werden könnten. Der Zusatz, dass Bewegungsmuster erkannt und ausgewertet werden sollen, würde außerdem eine „automatisierte Nachverfolgung“ von Personen ermöglichen, die Zusammenhänge zwischen Personen, Orten und Objekten, ermöglicht, was einer Profilbildung gleichkommt. § 184 Absatz 5 bestimmt zwar, dass zur automatisierten Nachverfolgung „nicht körperliche Merkmale zu verwenden“ sind, auch weil „eine automatisierte Identifizierung der gekennzeichneten Person anhand biometrischer Merkmale nicht zulässig“ wäre. Dabei sind Umgehungen, die auf eine Person Rückschlüsse ziehen lassen, aber leicht denkbar – fokussiert man beispielsweise auf ein bestimmtes Kleidungsstück oder einen mitgeführten Gegenstand einer Person und verfolgt sie damit von Ort zu Ort. Gleichzeitig verweist § 184 Absatz 6 auf die konkrete Möglichkeit einer Zweckänderung für die Verwendung der Aufnahme/Aufzeichnung. Diese könnte also nachträglich zur Identifizierung genutzt werden, solange die Zweckänderung dokumentiert wird. Die Hürde, solch eine Zweckänderung vorzunehmen, ist dadurch auf das Mindestmaß herabgesetzt, und das, obwohl die

geltenden rechtlichen Anforderungen an eine biometrische Identifizierung um ein Wesentliches höher sind. Bezieht man außerdem den Umstand ein, dass in den meisten Fällen das gleiche Kamerasystem zur Mustererkennung wie zur Identifizierung eingesetzt wird, drohen die jeweiligen Befugnisse kaum trennscharf voneinander angewandt zu werden.

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 etwa 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

Biometrische Überwachung betrifft auch das Recht auf Gleichbehandlung. Grundsätzlich gilt zwar: Je besser die biometrische Fernidentifizierung funktioniert, desto gefährlicher wird sie. **Dennoch besteht auch eine Gefahr der Diskriminierung in der bestehenden hohen Fehleranfälligkeit der Erkennungssysteme, insbesondere bei Personengruppen mit bestimmten Eigenschaften, die in Datensätzen unterrepräsentiert sind.** Hinzu kommt die Gefahr der gezielten Diskriminierung, die genau den Zweck verfolgt, bestimmte Personen oder Gruppen anhand biometrischer Merkmale herauszufiltern. Für bereits benachteiligte oder von Diskriminierung betroffene Personen und Gruppen sowie für politische Aktivist*innen zeigen sich die Auswirkungen von biometrischer Massenüberwachung oft in verstärkter Form. Eine solche Überwachungsinfrastruktur aufzubauen, birgt Gefahren, die bereits heute abgesehen werden können und vermieden werden sollten.¹⁰

Auch die automatisierte Verhaltens- oder Situationsanalyse gilt als riskantes und zudem mangelhaft evaluiertes Verfahren. Davon, dass „Schwächen der manuellen Auswertung“ tatsächlich ausgeglichen werden, wie es das Gesetz suggeriert, kann nicht direkt ausgegangen werden. In Mannheim, wo die automatisierte Verhaltensanalyse 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

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

¹⁰ Vgl. aktuellen Bericht aus Georgien, wo Gesichtserkennungssoftware als Rückgrat für die Unterdrückung von Protesten eingesetzt wird, „Gefilmt, bestraft, zum Schweigen gebracht: Wie russische Überwachungssoftware die Rechte der georgischen Zivilgesellschaft unterdrückt.“ <https://algorithmwatch.org/de/gefilmt-bestraft-zum-schweigen-gebracht-russische-ueberwachungsssoftware-georgien/> (zuletzt abgerufen am 11.09.2026)

veröffentlichten Evaluationsdokumenten (des Modellprojekts Hansaplatz) hervorgehen, sind u. a. (1) die **hohe Fehleranfälligkeit**, beispielsweise werden ungefährliche Handlungen als vermeintlich gefährlich markiert; (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.¹¹

Die Befugnis zur automatisierten 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

¹¹ 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 11.09.2026); siehe Berichterstattung zur KI-gestützten Videoüberwachung in Mannheim durch AlgorithmWatch (2023) <https://algorithmwatch.org/en/mannheim-system-reports-hugs-police/> (zuletzt abgerufen am 11.09.2026) 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 11.09.2026)