

Gemeinsame Stellungnahme zu den Gesetzentwürfen zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit u.a.

Gemeinsame Stellungnahme im Rahmen der Verbändebeteiligung zu den Gesetzentwürfen zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit sowie zum Gesetzentwurf zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus zu den Gesetzentwürfen betreffend §§ 98d, 98e StPO sowie §§ 9a, 9b, 22a, 39a, 39b, 63b, 63c BKAG, §§ 46, 58a, 58b BPolG, § 15b AsylG

I. Einleitung und Gegenstand der Stellungnahme

Die unterzeichnenden Verbände nehmen gemeinsam Stellung zu den zwei vorliegenden Gesetzentwürfen, die einen automatisierten biometrischen Abgleich mit öffentlich verfügbaren Internetdaten sowie die automatisierte Datenanalyse - wie etwa durch Systeme wie PimEyes und von Palantir - für Bundes- und Landespolizeibehörden ermöglichen sollen. Das Vorhaben umfasst einen Entwurf des Bundesinnenministeriums zum Gefahrenabwehrrecht sowie einen Entwurf des Bundesjustizministeriums zur Strafverfolgung. Wir lehnen die Regelungen aus grundsätzlichen verfassungs- und menschenrechtlichen Erwägungen ab – und zwar sowohl für den strafprozessualen als auch für den gefahrenabwehrrechtlichen Bereich.

Die Bundesregierung trägt Verantwortung dafür, dass die Grundrechte der Bürgerinnen und Bürger auch im Zeitalter automatisierter Massenüberwachung wirksam geschützt bleiben. Die vorgesehene Einführung dieser Überwachungsinstrumente steht dieser Verantwortung diametral entgegen.

II. Grundsätzliche Ablehnung der Vorhaben

Der automatisierte biometrische Abgleich mit öffentlich zugänglichen Internetdaten – wie er durch Systeme wie PimEyes oder Clearview AI ermöglicht wird – stellt einen qualitativen Sprung in der Überwachungsinfrastruktur dar. Mit enormer Streubreite greift er in das Recht auf informationelle Selbstbestimmung aller Menschen ein, die im Internet Fotos, Videos und andere Inhalte mit biometrischen Merkmalen veröffentlichen, ohne dass diese dafür einen Anlass gegeben hätten. Betroffen sind ferner Personen, die auch ohne ihr Wissen und Wollen etwa im Hintergrund auf einem Foto abgebildet sind. Auch "Nicht-Treffer" stellen einen Grundrechtseingriff dar. [1] Da Meinungs- und Versammlungsfreiheit heute wesentlich auch im digitalen Raum ausgeübt werden – etwa über die Publikation von Aufnahmen von Versammlungen in den sozialen Medien, um auf das eigene Anliegen aufmerksam zu machen – geht mit der Befugnis zudem auch ein möglicher Abschreckungseffekt auf die Ausübung dieser Rechte einher.

Der biometrische Abgleich erlaubt die Identifizierung von Personen im öffentlichen Raum und im Netz auf der Grundlage biometrischer Merkmale und schafft damit die technischen Voraussetzungen für eine flächendeckende Verfolgbarkeit der Bevölkerung. Dies ist mit dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) sowie dem Recht auf Schutz personenbezogener

Daten (Art. 8 GRCh und Art. 8 EMRK) aus unserer Sicht unvereinbar. Eine zusätzliche Gefährdung des Diskriminierungsverbots (Art. 3 Abs. 3 GG) ergibt sich aus der zahlreich empirisch belegten erhöhten Fehleranfälligkeit biometrischer Systeme insbesondere bei People of Colour. Diese könnten häufiger zu Unrecht von polizeilichen Folgemaßnahmen betroffen sein.

Gleiches gilt für die automatisierte Datenanalyse mittels Systemen wie denen von Palantir. Die in den Regelungen vorgesehene Zusammenführung und algorithmische Auswertung massenhafter Datenbestände erlaubt die Erzeugung tiefgreifender Persönlichkeitsprofile. Sie ermöglicht Schlussfolgerungen, die weit über die ursprünglichen Erhebungszwecke der analysierten Daten und auch über das Ziel der eigentlichen Suchanfrage an das Analysesystem hinausgehen. Solche Systeme sind strukturell fehleranfällig, intransparent und diskriminierungsfördernd. Dies gilt in verstärktem Maße für KI-Systeme, die auch nach Einführung weiterhin selbstlernend sind und in den Entwürfen nicht ausgeschlossen werden. Ihre Funktionsweise ist für Betroffene und möglicherweise auch Anwendende nicht nachvollziehbar. Für die Bevölkerung ist auch nicht vorhersehbar, welche grundrechtlich geschützten Verhaltensweisen Datenspuren hinterlassen könnten, die zu einem verdachtserzeugenden "Treffer" führen (etwa eine Anzeige zu erstatten; eine Versammlung zu besuchen, bei der es zu einer Identitätsfeststellung kommt; Kontakt zu bestimmten Personen; Social-Media-Aktivitäten u.v.m.). Dies kann zu einschüchternden Auswirkungen auf die Grundrechtsausübung führen.

Besonders problematisch ist der Umfang der in die automatisierte Datenanalyse einbezogenen Daten. So ist etwa in § 9b BKAG-E ausdrücklich vorgesehen, dass das BKA alle Daten, auf die es im Rahmen seiner Aufgabe als Zentralstelle zugreifen darf, zur automatisierten Datenanalyse einbeziehen kann. Dies setzt ausweislich der Gesetzesbegründung voraus, dass die entsprechenden Datenbestände weitgehend zusammengeführt und in einem einheitlichen Format und vom Einzelfall unabhängig vorliegen und aufbereitet sind. Angesichts der schieren Masse dieser Daten - sämtliche im polizeilichen Informationsverbund vorliegenden Fall- und Vorgangsdaten, Daten aus Asservaten und Telekommunikations- Verkehrs- und Nutzungsdaten sowie im Einzelfall auch automatisiert abzurufende Registerdaten und Daten aus dem Internet - entsteht eine umfassende "Super-Datenbank". Diese würde neben den Daten von Beschuldigten und Verdächtigen auch die Daten von Opfern, Zeugen und sogar gänzlich unbeteiligten Personen enthalten und zum Objekt einer automatisierten Datenanalyse werden.

Die Einführung dieser Systeme bedeutet einen fundamentalen Eingriff in Grundrechte und eine Gefahr für rechtsstaatliche Grundsätze wie Transparenz, Diskriminierungsfreiheit und effektiven Rechtsschutz, der durch die im Entwurf vorgesehenen Zwecke nicht gerechtfertigt wird.

Ferner führen die Regelungen die Möglichkeit ein, sensible personenbezogene Daten der Bevölkerung zum Testen und Trainieren von IT-Produkten, einschließlich Künstlicher Intelligenz, zu verwenden. Die ermöglichte Verwendung des nahezu gesamten Datenbestandes, auch in nicht anonymisierter Form, ist unverhältnismäßig. Dieser umfasst u.a. Daten von Zeug*innen, aus Maßnahmen mit großer Streubreite wie etwa aus Funkzellendatenabfragen, persönliche Informationen aus Asservaten oder Telekommunikationsüberwachung und besonders sensible Daten wie biometrische Informationen.

Die Entwürfe lassen die Nutzung personenbezogener Daten bereits zu, wenn der Aufwand einer Anonymisierung oder Pseudonymisierung als unverhältnismäßig hoch angesehen wird – und zwar selbst dann, wenn für das Training gar keine unveränderten Daten benötigt würden (§ 22 BKAG-E, § 46 BPolG-E). Da einerseits unbestimmt ist, wann ein Aufwand als unverhältnismäßig gilt, und dies andererseits der Selbsteinschätzung der Behörden überlassen ist, besteht das Risiko, dass häufig nicht anonymisierte Daten zur Verwendung kommen werden.

Zudem ist die Sicherheit der genutzten Daten und die Einhaltung ihrer Löschfristen gefährdet. Wie wissenschaftliche Arbeiten belegen [2], konnten Trainingsdaten oftmals wieder aus KI-Anwendungen extrahiert werden. Belegt ist die erfolgreiche Rekonstruktion von Text- und Bilddaten, etwa Namen, Telefonnummern, E-Mail-Adressen und Bildern. Nutzer*innen können sogenanntes "Data Leakage" auch unabsichtlich auslösen. Es besteht daher ein grundsätzliches, in der konkreten Ausprägung vom jeweiligen

KI-System abhängiges Risiko, dass sensible personenbezogene Daten selbst nach Ablauf ihrer Löschvorschriften und durch Unbefugte (darunter auch private Unternehmen, die das Training durchführen dürfen, § 22 Abs. 4 BKAG-E, § 46 Abs. 4 BPolG-E) rekonstruierbar sind.

III. Keine verfassungskonforme Ausgestaltung möglich

Die von BMI und BMJV vorgeschlagene konkrete Ausgestaltung der Eingriffsbefugnisse verschärft die grundrechtliche Problematik weiter. Im Einzelnen:

- **Kein Richtervorbehalt:** Weder §§ 98d, 98e StPO noch die parallelen Regelungen im BKAG, BPolG und AsylG sehen einen Richtervorbehalt vor. Angesichts der Eingriffstiefe der biometrischen Identifizierung und der automatisierten Massenauswertung ist dies mit dem Gebot effektiven Rechtsschutzes (Art. 19 Abs. 4 GG) und dem Schutz der Grundrechte nicht vereinbar. Dies gilt erst recht, wenn die Polizei solche Maßnahmen bei - selbst definierter - "Gefahr im Verzug" selbst anordnet.
- **Ungenügende Transparenz für Betroffene:** Die Entwürfe sehen zwar [teilweise] eine Benachrichtigungspflicht gegenüber den von dem biometrischen Abgleich betroffenen Personen vor. Ohne Kenntnis eines Eingriffs ist es den Betroffenen faktisch unmöglich, ihre Rechte geltend zu machen. Angesichts der enormen Streubreite der vorgesehenen Maßnahmen ist davon auszugehen, dass das Problem der unzureichenden Benachrichtigung Betroffener [3] sich weiter verschärfen wird. In Bezug auf die vorgesehene automatisierte Datenanalyse ist eine Benachrichtigung der betroffenen Personen gar nicht erst vorgesehen. Beides verletzt das Recht auf effektiven Rechtsschutz.
- **Unzureichende Dokumentation:** Zwar sehen die Entwürfe im Grundsatz Protokollierungspflichten nach § 76 BDSG vor. Allerdings wird der Vorgang der automatisierten Datenanalyse respektive des biometrischen Abgleichs dadurch nicht aktenkundig. Es wird offenbleiben, wie genau die eingesetzten Programme arbeiten; das Black-Box-Problem, das mit derartigen Systemen einhergeht, wird nicht gelöst. Ohne belastbare Dokumentation sind parlamentarische, gerichtliche und unabhängige datenschutzrechtliche Kontrolle strukturell ausgehöhlt.
- **Kaum Einschränkung von Art und Umfang der in die automatisierte Analyse einbezogenen Daten:** Wie das BVerfG festgestellt hat, stellt die Verarbeitung bereits erhobener Daten im Rahmen einer automatisierten Datenanalyse einen eigenen Eingriff in die informationelle Selbstbestimmung dar. Dieser wiegt umso schwerer, je weniger die in die Analyse einbezogenen Daten ihrer Art und ihrem Umfang nach eingeschränkt werden. [4] Die Entwürfe erlauben die automatisierte Analyse kaum eingeschränkter, enormer Datenmengen. Dazu gehören Daten aus Eingriffen mit großer Streubreite wie Funkzellenabfragen, besonders sensible Daten wie biometrische Daten, Daten von Personen, die keinen Anlass zu polizeilicher Beobachtung gegeben haben wie Zeug*innen aus Vorgangsdaten, Daten persönlicher Natur aus Telekommunikationsüberwachung oder Asservaten oder gesondert hinzugefügte Daten aus Social Media u.v.m. Positiv zu werten ist, dass nach § 98e Abs. 2 StPO-E einige Datenbestände explizit ausgewählt werden müssen, um in die Analyse einbezogen zu werden, und dies nur zulässig ist, "soweit dies erforderlich ist". Diese Regelung findet sich in den Entwürfen zu BPolG und BKAG jedoch nicht und hat ohnehin keinen tatsächlich einschränkenden Charakter. Im Umkehrschluss zeigt sich zudem, dass die umfangreichen sonstigen Datenbestände offenbar auch dann in die Analyse einbezogen werden, wenn dies nicht erforderlich ist und keine Anhaltspunkte dafür vorliegen, dass die einzubeziehenden Daten in Verbindung zum konkreten Suchanlass stehen könnten. Die Einführung der automatisierten Datenanalyse birgt im polizeilichen Alltag die Gefahr, dass Daten weniger verdachtsgeleitet und deutlich zahlreicher ausgewertet werden, da dies in sehr kurzer Zeit mit geringem Aufwand automatisiert möglich ist.
- **Unzureichende Einschränkung der Analysemethoden:** Neben Art und Umfang der einbezogenen Daten wird das Eingriffsgewicht auch durch die zugelassene Methode der Datenanalyse bestimmt. [5] Zwar gibt es eine abschließende Aufzählung der erlaubten Analyseschritte, doch erlauben diese maschinelle Sachverhaltsbewertungen und gehen weit über einen einfachen Datenabgleich hinaus

(z.B. automatisierte qualitative und quantitative Klassifizierung und Analyse von Beziehungen und Zusammenhängen). Dabei ist auch die Nutzung von nach ihrer Einführung im behördlichen Einsatz weiter selbstlernender KI nicht ausgeschlossen. Der Einsatz solcher KI-Systeme stellt ein inakzeptables Risiko für die Rechte auf Nicht-Diskriminierung und effektiven Rechtsschutz dar. Durch die insoweit fehlende Einschränkung stellen sich die Regelungen auch als evident unverhältnismäßig dar.

- **Schwerwiegende Grundrechtseingriffe durch private Unternehmen:** Erkennbar wurde sich darum bemüht, den Grundrechtseingriff beim biometrischen Abgleich durch die Vorgabe zu verringern, dass hierfür aus dem Internet erhobene Daten anschließend zu löschen sind. Dieses Bemühen konterkariert, dass der Abgleich auch durch andere öffentliche und nichtöffentliche Stellen - also insbesondere auch private Unternehmen - und (außer im Asylverfahren) sogar Stellen in nichteuropäischen Drittstaaten durchgeführt werden darf. Es bleibt offen, ob und wie die Löschpflichten durch Dritte sichergestellt werden sollen oder ob diese durch die Auslagerung der Maßnahme umgangen werden können. Die Übermittlung biometrischer Daten an private Unternehmen birgt zudem ein Risiko für die Datensicherheit. Bereits aus grundsätzlichen Erwägungen sollten derart schwerwiegende Grundrechtseingriffe auch nicht an private Unternehmen ausgelagert werden. Dies gilt auch für das durch die Regelungen ermöglichte Training von IT-Produkten mit personenbezogenen Daten durch private Unternehmen.
- **Unzureichende Sicherstellung menschlicher Entscheidungsfindung und mangelnder Schutz vor nachteiligen Folgen automatisierter Entscheidungen:** Die Regelungen zur automatisierten Datenanalyse sehen jeweils vor, dass "eine ausschließlich auf der Maßnahme (...) beruhende automatisierte Entscheidungsfindung, die unmittelbar eine nachteilige Rechtsfolge für die betroffene Person hat oder diese erheblich beeinträchtigt", unzulässig ist (§§ 9b Abs.5, 39b Abs.5, 63c Abs.5 BKAG-E, § 58b Abs.5 BPol-GE). Eine ausschließlich automatisierte Entscheidungsfindung ist aus rechtsstaatlichen Gesichtspunkten jedoch per se inakzeptabel. Dies gilt auch, wenn diese zusätzlich auf anderen automatisierten Maßnahmen beruhen sollte, nur eine mittelbar nachteilige Rechtsfolge für Betroffene hätte oder diese nur in einer Weise beeinträchtigt, die noch nicht als erheblich gilt.

Wir betonen, dass eine grundrechtskonforme Ausgestaltung dieser Befugnisse auch durch Nachbesserungen im Verfahrensrecht nicht erreichbar wäre. Die genannten Mängel sind keine bloßen Ausgestaltungsfehler, sondern symptomatisch für das strukturelle Defizit des gesamten Regelungsvorhabens. Schon dem Grunde nach fehlt es an einem verfassungsrechtlich tragfähigen Fundament.

IV. Besondere Kritik: § 15b AsylG

§ 15b AsylG gibt Anlass zu besonderer Besorgnis. Asylsuchende befinden sich in einer strukturellen Schutzlosigkeit: Sie sind auf staatliche Verfahren angewiesen, verfügen häufig über eingeschränkte Möglichkeiten zur Rechtswahrnehmung und sind besonders vulnerabel gegenüber staatlichem Missbrauch. Die Erstreckung biometrischer Massenabgleiche auf diesen Personenkreis verschärft ihre vulnerable und exponierte Situation. Sie birgt das ernste Risiko, dass biometrisch erhobene Daten für Zwecke genutzt werden, die dem Schutzzweck des Asylrechts diametral widersprechen.

Gegenüber dem derzeitigen § 15b AsylG entfallen bisher explizit im Wortlaut des Gesetzes aufgenommene Schutzmaßnahmen. Auch insofern sich diese aus anderweitigen gesetzlichen Vorgaben ergeben, verstieße die Streichung der Schutzvorschriften aus der Norm selbst aus unserer Sicht gegen das Gebot der Normenklarheit und ist daher abzulehnen.

Problematisch ist weiterhin der extrem weite Identitätsbegriff, der der Regelung zugrunde liegt. Zur Identität, zu deren Feststellung der biometrische Abgleich genutzt werden darf, gehören ausweislich der Begründung "Merkmale, die einen Menschen von anderen Menschen unterscheidet [sic] und damit zu einer individuellen Persönlichkeit macht". Nicht abschließend werden Merkmale aufgezählt, "die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität

der Person sind", außerdem "Geburtsland, das Land des gewöhnlichen Aufenthalts, der Familienstand, die Volks- und Religionszugehörigkeit sowie die Sprachkenntnisse des Ausländers." Dies erlaubt, sofern keine Identitätsdokumente vorliegen, den biometrischen Abgleich als Standardmaßnahme. Es ermöglicht das "Weitersuchen" und zahlreiche weitere Abgleiche auch dann, wenn zentrale Fragen bereits beantwortet und Angaben der Schutzsuchenden, wie sie sich aus einem Identitätsdokument ergeben hätten, bereits bestätigt sind. Eine derart umfassende Ausforschung von Asylsuchenden ist für die Durchführung eines Asylverfahrens nicht erforderlich und mit dem Recht auf Privatsphäre nach Art. 7 GRCh sowie Art. 8 EMRK nicht vereinbar. Der Entwurf reiht sich damit in eine lange Kette von Maßnahmen zum Abbau der Rechte von Schutzsuchenden ein.

V. Empfehlungen

Wir empfehlen:

- die Rücknahme der Gesetzentwürfe;
- ein grundsätzliches gesetzliches Verbot des Einsatzes biometrischer Massenerkennungssysteme;
- eine transparente parlamentarische und gesamtgesellschaftliche Debatte über den Einsatz algorithmischer Datenanalysesysteme sowie verbindliche Regelungen zu Transparenz, Kontrolle und Haftung;
- die Stärkung des Richtervorbehalts sowie effektiver Benachrichtigungs- und Protokollierungspflichten bei allen Befugnissen zur digitalen Überwachung;
- umfassende Transparenz über den Einsatz Künstlicher Intelligenz durch Sicherheitsbehörden, die über die Anforderungen der EU KI-Verordnung hinausgeht, da diese Transparenzausnahmen für die Bereiche Strafverfolgung und Asyl vorsehen.

Unterzeichnende Organisationen:

- AG Kritis
- Algorithm Watch
- Amnesty International
- Chaos Computer Club
- D64 Zentrum für Digitalen Fortschritt
- Digitale Gesellschaft
- Humanistische Union
- LOAD e.V.
- Komitee für Grundrechte und Demokratie
- Neue Richter*innenvereinigung
- Pro Asyl Bundesarbeitsgemeinschaft BAG
- Republikanischer Anwältinnen- und Anwälteverein
- Seebrücke
- Vereinigung Demokratischer Jurist*innen

Hier können Sie die Stellungnahme als PDF herunterladen:

[1] BVerfG, Urteil vom 18. Dezember 2018, 1 BvR 142/15, Rn. 51.

[2] Vgl. etwa Shokri et. al., Membership Inference Attacks Against Machine Learning Models, 2017 IEEE Symposium on Security and Privacy, 2017, S. 3-18; Ahmed et. al., Extracting Books from Production Language Models, 2026, online abrufbar: <https://arxiv.org/abs/2601.02671>; verschiedene Studien von Nicholas Carlini, online abrufbar: <https://nicholas.carlini.com/papers/>.

[3] Vgl. dazu nur Kahmen, Die Vorschriften zur Benachrichtigungspflicht gemäß § 101 IV-VI StPO und ihre praktische Umsetzung, 2017

[4] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 78 ff.

[5] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 77, 90ff.

<https://www.humanistische-union.de/publikationen/mitteilungen/mitt-258/publikation/gemeinsame-stellungnahme-zu-den-gesetzentwurfen-zur-staerkung-digitaler-ermittlungsbefugnisse-in-der-polizeiarbeit-u-a/>

Abgerufen am: 16.08.2026