DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins vorbereitet durch den Ausschuss Recht der Inneren Sicherheit und unter Mitwirkung des Ausschusses Strafrecht

zum Referentenentwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit sowie eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus

Stellungnahme Nr.: 27/2026 Berlin, im April 2026

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Mitglieder des Ausschusses Strafrecht

- Rechtsanwalt Stefan Conen, Berlin
- Rechtsanwältin Dr. Friederike Goltsche, Münster
- Rechtsanwältin Dr. Gina Greeve, Frankfurt am Main
- Rechtsanwalt Kai Kempgens, Berlin
- Rechtsanwalt Prof. Dr. Stefan Kirsch, Frankfurt am Main
- Rechtsanwältin Dr. Jenny Lederer, Essen
- Rechtsanwalt Prof. Dr. Bernd Müssig, Bonn
- Rechtsanwalt Prof. Dr. Ali B. Norouzi, Berlin (Vorsitzender)
- Rechtsanwältin Dr. Anna Oehmichen, Berlin
- Rechtsanwältin Gül Pinar, Hamburg (stellv. Vorsitzende)
- Rechtsanwalt Prof. Dr. Tilman Reichling, Frankfurt am Main
- Rechtsanwalt Martin Rubbert, Berlin

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Tanja Brexl, Geschäftsführerin, Berlin
- Michael Bimmler, Referent

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

A. Einführung

Das BMI legt zwei Referentenentwürfe vor, nämlich den „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ („Entwurf 1“) und den „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“ („Entwurf 2“). In dem letztgenannten Entwurf sind Änderungen bei Befugnissen aus dem BKAG vorgesehen, die der Abwehr des internationalen Terrorismus dienen sollen und der Zustimmung des Bundesrates bedürfen. Der erste Entwurf enthält Änderungen des BKAG, des BPolG und des AsylG, die nicht zustimmungspflichtig sein sollen.

Das BMI weist in seinem Anschreiben an die Verbände darauf hin, dass es beabsichtigt, „die Befugnisse zur Sicherungsanordnung für das Bundeskriminalamt, die bisher in Artikel 10 des Entwurfs zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren des BMJV enthalten sind, mit dem hier gegenständlichen Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus zu verbinden.“ Insofern wird auf die diesbezügliche Stellungnahme des DAV verwiesen, die unter https://anwaltverein.de/newsroom/sn-8-26-einfuehrung-der-ip-adressspeicherung abrufbar ist.

In beiden Entwürfen geht es primär um die Schaffung von Ermächtigungsgrundlagen für den automatisierten biometrischen Abgleich mit Bildmaterial aus dem Internet und die automatisierte Analyse vorhandener Daten. Damit soll die sog. „Künstliche Intelligenz“ in der Polizeiarbeit Einzug halten (vgl. S. 17 Entwurf 1).

Ein parallel vom BMJV vorgelegter Referentenentwurf für ein „Gesetz zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“ enthält entsprechende Ermächtigungsgrundlagen für den automatisierten biometrischen Abgleich mit Bildmaterial aus dem Internet und die automatisierte Analyse vorhandener Daten auf dem Gebiet der Strafverfolgung, vgl. hierzu die Stellungnahme 26/2026 des DAV[1].

Die Pläne der Bundesregierung sind extrem weitgehend. Das BKA und die weiteren Polizei- und Strafverfolgungsbehörden sollen ermächtigt werden, systematisch öffentliche biometrische Datenbanken zu durchsuchen. Anwendungsfälle sind keineswegs nur die Personenfahndung und -identifizierung bei schwersten Straftaten. Mit den vorgelegten Entwürfen würde die biometrische Rasterfahndung im Internet zum Standardermittlungsinstrument.

Mit der automatisierten Datenanalyse sollen die Polizeibehörden ermächtigt werden, polizeiliche Datenbestände verfahrens- und bundesländerübergreifend mit KI-Tools auszuwerten. Die technischen Voraussetzungen hierfür schafft derzeit eine Bund-Länder-Arbeitsgruppe im Rahmen des Projekts „Polizei 20/20“. In die Analyse sollen auch Daten von beschlagnahmten Mobiltelefonen, Computern etc. und Daten aus Telekommunikationsüberwachungsmaßnahmen einbezogen werden. So entsteht praktisch ein gigantischer Datenbestand, der höchst sensible Informationen von Beschuldigten und Dritten (bspw. Kernbereichsinformationen, Gesundheitsdaten) sowie Daten, die unter verschiedene Berufsgeheimnisse fallen, enthält. Diesen Datenbestand sollen die Behörden mit Tools privater Hersteller wie Palantir auswerten können. Dabei sind auch hier die Anwendungsfälle nicht auf schwerste Straftaten begrenzt. Mehr noch: Das BKA dürfte auch jenseits konkreter Strafverfahren durch eine biometrische

[1] https://anwaltverein.de/newsroom/sn-26-26

Internetauswertung und eine automatisierte Datenanalyse verdachtsgenerierend tätig werden und unterläge dabei nicht der Kontrolle durch Staatsanwaltschaft und Gerichte.

Der Deutsche Anwaltverein warnt daher vor einem gesetzgeberischen Schnellschuss. Würden diese Entwürfe Gesetz, wären damit unübersehbare Folgen für die Architektur des Strafverfahrens verbunden. Der herkömmlich mit Akten- und weiteren Verfahrensrechten und der Kontrolle durch Staatsanwaltschaft und Gericht hergestellte Ausgleich zwischen polizeilichen Ermittlungseingriffen und den Grundrechten Betroffener geriete gänzlich aus den Fugen. Unabhängig davon, dass die Regelungen einer Kontrolle durch das Bundesverfassungsgericht voraussichtlich nicht standhalten würden, sind sie auch den Herausforderungen nicht angemessen, denen alle gesellschaftlichen Institutionen ausgesetzt sind, wenn es um die Etablierung eines grundrechtsschonenden und vernünftigen Umgangs mit der sog. Künstlichen Intelligenz geht.

B. Überblick über die geplanten Änderungen

Die vom BMI vorgelegten Entwürfe enthalten auch Regelungen über die Nutzung polizeilicher Daten zum Zwecke des Trainings von IT-Produkten einschließlich sog. selbstlernender Systeme („Künstliche Intelligenz“):

§ 22 Abs. 3 E-BKAG Weiterverarbeitung von Daten zu weiteren Zwecken
§ 46 Abs. 3 E-BPolG Weiterverarbeitung von Daten zu weiteren Zwecken

Wegen der abermals extrem kurzen Stellungnahmefrist kann darauf in der vorliegenden Stellungnahme nicht vertiefter eingegangen werden. Zwei kritikwürdige Aspekte sollen jedoch bereits exemplarisch am Beispiel der für das BKAG vorgeschlagenen Änderungen hervorgehoben werden:

Bezugspunkt der Weiterverarbeitungsbefugnis sind die „vorhandenen Daten“. § 22 Abs. 3 BKAG-E sieht – anders als bspw. §§ 9a, 9b BKAG-E – nicht vor, dass das Bundeskriminalamt auf diese Daten zur Erfüllung seiner Aufgaben zugreifen darf. Damit sprechen Systematik und Wortlaut dafür, dass auch rechtswidrig erhobene Daten (bspw. unter Verstoß gegen §§ 160a, 100d StPO) bzw. sachlich unrichtig (weiter-)verarbeitete Daten (bspw. unter Verstoß gegen § 47 Nr. 4 BDSG verarbeitete überholte/widerlegte Tatsachen) als Trainingsgrundlage herangezogen werden dürfen. Zum einen werden hiermit rechtswidrige Zustände perpetuiert. Zum anderen ist das Anlernen mit sachlich unrichtigen Informationen kein geeignetes Mittel.

Erschwerend tritt hinzu, dass die Weiterverarbeitungsbefugnis zu Trainingszwecken vom Grundsatz der hypothetisch rechtmäßigen Neuerhebung entkoppelt werden soll. § 12 Abs. 2 Satz 2 BKAG würde den neu zu schaffenden § 22 Abs. 3 BKAG-E „unberührt“ lassen. Damit wird der Zweckbindungsgrundsatz – sowohl nach nationalem als auch nach unionsrechtlichem Verständnis – aufgelöst.

Der Verzicht auf diese grundrechtssichernden Einschränkungen führt jeweils für sich genommen – in jedem Fall aber in ihrer Kumulation – dazu, dass § 22 Abs. 3 BKAG-E weder den nationalen verfassungsrechtlichen noch den primär- und sekundärrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten durch staatliche Stellen genügt.

I. Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit („Entwurf 1“)

1. Änderungen des BKAG

Es sollen Rechtsgrundlagen für den biometrischen Abgleich und die automatisierte Datenanalyse eingefügt werden:

§ 9a Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

§ 9b Automatisierte Datenanalyse

§ 63b Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet
§ 63c Automatisierte Datenanalyse.

2. Änderungen des BPolG

Es sollen Rechtsgrundlagen für den biometrischen Abgleich und die automatisierte Datenanalyse eingefügt werden:

§ 58a Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet
§ 58b Automatisierte Datenanalyse.

3. Änderungen des AsylG

Es soll eine Rechtsgrundlage für den biometrischen Abgleich eingefügt werden:

§ 15b Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

II. Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus („Entwurf 2“)

Es sollen im BKAG Rechtsgrundlagen für den biometrischen Abgleich und die automatisierte Datenanalyse eingefügt werden:

§ 39a Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet
§ 39b Automatisierte Datenanalyse

Wegen des systematischen Zusammenhangs werden in der sich anschließenden Stellungnahme die vorgeschlagenen Vorschriften des BKAG im Zusammenhang kommentiert, auch wenn sie Gegenstand zweier Entwürfe sind (s. oben).

Die Stellungnahme ist teilweise wort-/inhaltsgleich mit der Stellungnahme Nr. 26/2026 des DAV zu dem Entwurf für ein „Gesetz zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“, mit dem Ermächtigungsgrundlagen für den automatisierten biometrischen Abgleich mit Bildmaterial aus dem Internet und die automatisierte Analyse vorhandener Daten auf dem Gebiet der Strafverfolgung[2] vorgeschlagen werden. Die grundlegende Problemstellung der Entwürfe von BMI und BMJV ist identisch.

C. Stellungnahme

I. Automatisierter biometrischer Abgleich mit Bilddaten aus dem Internet

Die Debatte um die Nutzung automatisierter Biometrie-Tools wurde im Rahmen der Festnahme der langjährig gesuchten mutmaßlichen Ex-RAF-Täterin Daniela Klette befeuert. Zuvor hatte ein Investigativjournalist die Beschuldigte anhand von Fahndungsfotos über die von einem Privatkonzern betriebene Gesichtsdatenbank PimEyes ausfindig gemacht. Seitdem mehren sich die Stimmen, auch Ermittlungsbehörden die Nutzung von KI-gestützten Gesichtsdatenbanken ähnlich PimEyes oder Clearview AI zu ermöglichen.

Ein vorheriger Entwurf aus dem Jahre 2024[3] unterwarf entsprechende Maßnahmen damals noch engeren Grenzen. So waren solche Maßnahmen nur zur Identitätsfeststellung und Ermittlung des Aufenthaltsorts bei Katalogtaten des § 100a Abs. 2 StPO, die im Einzelfall schwer wogen, unter Richtervorbehalt vorgesehen. Die nunmehr für den Bereich der Gefahrenabwehr und der Strafverfolgung vorliegenden Entwürfe gehen weit darüber hinaus.

[2] https://anwaltverein.de/newsroom/sn-26-26
[3] https://dserver.bundestag.de/btd/20/128/2012806.pdf

Der Einsatz von Gesichtserkennung zur Strafverfolgung oder zur Gefahrenabwehr greift stets in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) sowie in Art. 8 GRCh ein – auch bei Personen, bei denen kein Treffer erzielt wird.[4] Die Eingriffsintensität ist als hoch einzustufen, da die Maßnahmen eine große Streubreite aufweisen, regelmäßig verdeckt durchgeführt werden und anlasslos in biometrische Daten mit starkem Personenbezug eingreifen. Zwar wird die Intensität dadurch abgemildert, dass die Referenzdaten aus öffentlich zugänglichen Quellen stammen. Der Einsatz von KI verstärkt indes die Eingriffsintensität erheblich, da er den Abgleich mit Milliarden von Bildern erst ermöglicht und damit Streubreite sowie Personenbezug potenziert. Hinzutritt, dass der Abgleich typischerweise ohne das Wissen der Betroffenen vorgenommen wird. Vor diesem Hintergrund erfordern entsprechende Maßnahmen eine spezifische Rechtsgrundlage und sind geeignet, teilweise ganz erhebliche Grundrechtseingriffe darzustellen.

Es stellt sich für den Deutschen Anwaltverein außerdem die Frage, wie ein automatisierter biometrische Abgleich mit öffentlich zugänglichen Daten angesichts des europäischen Rechtsrahmens insbesondere auf der Grundlage der unmittelbar geltenden Datenschutzgrundverordnung sowie der KI-Verordnung rechtskonform in der Praxis durchgeführt werden soll.

Nach Verständnis des Deutschen Anwaltvereins sieht der Entwurf keine Ermächtigung zum Aufbau einer biometrischen Referenzdatenbank auf Vorrat vor. Der eigene Aufbau einer solchen biometrischen „Bürgerdatenbank“ wäre wohl kaum mit deutschem Verfassungsrecht vereinbar. Denn durch den Aufbau einer Biometrik-Datenbank wären überwiegend Grundrechte von Millionen unbeteiligten Personen betroffen, die keinen Anlass für polizeiliche Überwachung gegeben haben. Zudem untersagt Art. 5 Abs. 1 e KI-VO als verbotene Praktik:

[4] BVerfG NJW 2019, 827 (829 Rn. 45); BVerfG NVwZ 2019, 398 (400 Rn. 54).

„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“.

Damit ist nach Ansicht des Deutschen Anwaltvereins explizit klargestellt, dass der Aufbau einer biometrischen Referenzdatenbank staatlicherseits unionsrechtswidrig ist.

Daneben wäre nach Ansicht des Deutschen Anwaltvereins auch ein Zugriff auf Angebote privater Unternehmen wie PimEyes oder Clearview AI unionsrechtswidrig. Die Praktiken insbesondere von Clearview wurden bereits von mehreren Datenschutzbehörden innerhalb der Europäischen Union mit Bußgeldern belegt. Das Unternehmen PimEyes hat seinen Unternehmenssitz vor Jahren aus der Europäischen Union heraus nach wohl derzeit Dubai verlegt. Ein Rückgriff auf private Unternehmen und deren Geschäftspraktiken erscheint aus Sicht der Deutschen Anwaltsvereins ausgeschlossen. Zudem erscheint es nicht vorstellbar, dass in Zeiten eines Strebens nach mehr digitaler Souveränität innerhalb der Europäischen Union eine solche Abhängigkeit bei Ermittlungsmaßnahmen gewünscht ist.

Auch zur grundsätzlichen Sicherstellung der Anwendbarkeit des EU-Datenschutzregimes bedarf es zudem der Vorgabe der Auftragsdatenverarbeitung in der EU bzw. im Schengen Raum.

Der Deutsche Anwaltverein versteht die Begrenzung des Recherchekreis auf „öffentlich zugängliche biometrische Daten“ dahingehend, dass jedenfalls keine Social-Media-Daten nutzbar gemacht werden sollen, die einem beschränkten Nutzerkreis zugänglich gemacht werden sollten[5], was zu begrüßen ist.

[5] So auch die Entwurfsbegründungen S. 20 Entwurf 1.

Der in §§ 9a Abs. 1, 39a Abs. 1, 63b Abs. 1 BKAG-E und § 58a Abs. 1 BPolG-E vorgesehene Einsatzzweck „zur Erforschung des Sachverhalts“ begründet indes für die Maßnahme eine massive Zweckköffnung, was letztlich den Einsatz automatisierter biometrischer Abgleiche zu jedwedem Ermittlungszweck erlaubt und nicht nur auf Personenfahndungen und Personenidentifizierungen beschränkt. Legitimiert wären sämtliche Recherchemaßnahmen, die in ihrer Gesamtheit die Erstellung eines umfassenden Bewegungs- und Persönlichkeitsprofils der Betroffenen bis hin in ihre höchstpersönlichen Beziehungen und Lebensbereiche zulassen. Die Streubreite ist extrem. Der Aspekt, dass Betroffene in vielen Fällen gar keinen Einfluss auf die Fertigung und Veröffentlichung von Bilddarstellungen haben, verdeutlicht die Tiefe des damit verbundenen Grundrechtseingriffs. Hier darf nicht außer Acht gelassen werden, dass viele Menschen ihren persönlichen Lebensbereich umfassend in sozialen Medien abbilden. Die automatisierte Auswertung dieser Inhalte mittels automatisierter biometrischer Analysen ermöglicht eine vollständige (retrograde) Offenlegung höchstpersönlicher privater Beziehungen, Kontakte, Orte, Handlungen, Gewohnheiten und Persönlichkeitsausprägungen. Während Betroffene durch Anonymisierung ihrer Namensidentität auf einen gewissen Schutz ihrer Persönlichkeit hinwirken können, ist dies bei Bildmaterial naturgemäß unmöglich. Aus Sicht des Deutschen Anwaltvereins lässt sich ein solch umfassender automatisierter Analysezugriff darauf vom Ansatz her bereits nicht mit geltendem Verfassungsrecht vereinbaren. Die Möglichkeiten zum automatisierten biometrischen Abgleich sollten dringend auf Zwecke der Personenfahndung und -identifizierung beschränkt werden.

Zu den vorgeschlagenen Vorschriften im Einzelnen:

1. Automatisierter biometrischer Abgleich mit Bilddaten aus dem Internet durch das Bundeskriminalamt (§§ 9a, 39a, 63b BKAG-E)

a) § 9a BKAG-E[6]

Mit § 9a BKAG-E soll das BKA die Erlaubnis erhalten, sämtliche Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, biometrisch mittels automatisierter Systeme mit öffentlich zugänglichen Daten abzugleichen.

aa) Datenbestand, der mit öffentlich zugänglichen Daten abgeglichen werden darf

Das BKA ist Zentralstelle für den polizeilichen Informationsverbund (§§ 2, 29 ff. BKAG) und darf in dieser Funktion auf den gesamten polizeilichen Informationsverbund und die dort gespeicherten Daten zugreifen. Mit § 9a BKAG-E stehen folglich zunächst alle von deutschen Polizeibehörden im Verbundsystem gespeicherten Daten für einen biometrischen Abgleich zur Verfügung. Im Rahmen des Projekt P20 arbeitet eine Bund-Länder-Arbeitsgruppe derzeit an der Zusammenführung der Datenbestände der Landes- und Bundespolizeibehörden. Mittelfristig sollen alle Daten in einem einheitlichen sog. Datenhaus beim BKA gespeichert werden.

Es geht also um einen enormen Datenbestand, der Daten von Beschuldigten ebenso enthält, wie von Dritten, etwa Angehörigen, Zeugen, Geschädigten, Kommunikationspartnern etc.

[6] Art. 1 des Entwurfs eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit.

Absolut ausgenommen sein sollen nur Daten aus Wohnraumüberwachungen und Online-Durchsuchungen/Quellen-TKÜ, vgl. § 9a Abs. 3 S. 2 BKAG-E i. V. m. § 12 Abs. 3 BKAG.

Der verfassungsrechtlich zwingende Zweckbindungsgrundsatz soll durch die Bezugnahme auf § 12 Abs. 2 BKAG (vgl. § 9a Abs. 3 S. 1 BKAG-E) gewahrt werden; demnach dürfen Daten nur verwendet werden, wenn der Abgleich mindestens der Verhütung/Aufdeckung/Verfolgung vergleichbar schwerwiegender Straftaten oder dem Schutz vergleichbar bedeutsamer Rechtsgüter dient, wie die ursprüngliche Erhebung und wenn sich im Einzelfall konkrete Ermittlungsansätze erkennen lassen („hypothetische Datenneuerhebung“).

Es ist unklar, wie der Zweckbindungsgrundsatz bei einem automatisierten Abgleich praktisch umgesetzt werden soll. Dies ist von entscheidender Bedeutung für die verfassungskonforme Ausgestaltung und sollte daher dringend gesetzlich geregelt und nicht der Ausgestaltung durch Verwaltungsvorschriften überlassen werden.

Zudem ist der Begriff der „vergleichbar schwerwiegenden Straftaten“ bzw. der „vergleichbar bedeutsamen Rechtsgüter“ zu vage. So bleibt z. B. offen, ob es abstrakt auf den möglicherweise erfüllten Tatbestand ankommt oder auf das Gewicht der konkret im Raum stehenden Tat im Einzelfall.

In der vorgesehenen Fassung wird daher der Zweckbindungsgrundsatz nicht effektiv umgesetzt. Sie genügt in dieser Hinsicht weder den vom Bundesverfassungsgericht aufgestellten Anforderungen, noch ist die Regelung praktisch geeignet, die für einen Abgleich zur Verfügung stehenden Daten rechtsstaatlich zu beschränken.

bb) Öffentliche Daten, mit denen abgeglichen werden darf („Referenzdaten“)

Der Entwurf sieht hier nur eine einzige Einschränkung vor. So soll der Abgleich mit öffentlich zugänglichen *Echtzeitdaten*, also z. B. live gestreamten Bildern einer privaten Videoüberwachungsanlage, nicht zulässig sein[7].

Sämtliche anderen weltweit öffentlich zugänglichen Bilddaten dürfen nach dem Entwurf herangezogen werden. Dabei spielt es keine Rolle, ob diese rechtmäßig erhoben wurden.

cc) Voraussetzungen für die Durchführung eines Abgleichs

Ein Abgleich der Daten darf durchgeführt werden, wenn (§ 9a Abs. 1 Nr. 1 BKAG-E)

> *bestimmte Tatsachen den Verdacht begründen, dass eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat begangen worden ist*

oder

> *bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat begehen wird,*

und (§ 9a Abs. 1 Nr. 2 BKAG-E)

[7] vgl. auch S. 21 des Referentenentwurfs.

dies zur Ergänzung vorhandener Sachverhalte, zum Zweck der Identifizierung, Aufenthaltsermittlung, Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen mit anderen Straftaten oder Gefahren im Rahmen der Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Absatz 2 Nummer 1 erforderlich ist,

und (§ 9a Abs. 1 Nr. 3 BKAG-E)

die Verfolgung oder Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Die Auswahl der Anlassdelikte, bei denen ein automatisierter biometrischer Abgleich möglich sein soll, lässt sich nicht mit verfassungsrechtlichen Vorgaben vereinbaren. Es findet sich nicht einmal eine absolute Beschränkung auf den Katalog des § 100a Abs. 2 StPO, sondern dieser wird nur exemplarisch herangezogen. Es finden sich auch dort Straftatbestände, die nicht dem Schutz herausragender Schutzgüter dienen, etwa bestimmte Verstöße gegen das Konsumcannabisgesetz (Nr. 7a), Formen der Veruntreuung von Arbeitsentgelten (Nr. 1 lit. q) oder Sozialhilfebetrug (Nr. 1 lit. n) und bestimmte Vorfeldstraftaten. Das BVerfG betont, dass bei tief in die Privatsphäre eingreifenden Überwachungsmaßnahmen eine besonders strenge Eingriffsschwelle und der Schutz überragend wichtiger Rechtsgüter unumgänglich sind[8].

Aus Sicht des Deutschen Anwaltvereins müsste der Anwendungsbereich zumindest auf den Katalog des § 100b Abs. 2 StPO beschränkt werden. Darüber hinaus bedürfte es einer zusätzlichen Beschränkung auf Taten, die im Einzelfall schwer wiegen.

[8] 1 BvL 3/22, Rz. 96

In der Entwurfsbegründung (S. 21 Entwurf 1) wird klargestellt, dass Voraussetzung für ein Tätigwerden des BKA ist, dass bereits Ermittlungsunterlagen vorliegen. Die erstmalige Gewinnung von Verdachts- oder Gefahrenmomenten sei nicht von der Befugnis erfasst. Diese Einschränkung wird im Entwurf aber unzureichend umgesetzt. Dort ist nur die Rede von „vorhandenen Sachverhalten“, was sprachlich nicht identisch ist mit bereits eingeleiteten Ermittlungsverfahren oder gefahrenabwehrrechtlichen Vorgängen. Außerdem lässt § 9a Abs. 1 Nr. 2 BKAG-E zu, dass Zusammenhänge mit „anderen Straftaten oder Gefahren“ ermittelt werden.

Es besteht daher aufgrund des Wortlauts des § 9a Abs. 1 Nr. 2 BKAG-E die Gefahr, dass das BKA umfangreich in allen Bereichen der Strafverfolgung verdachtsgenerierend tätig werden dürfte, was das Aufgabenprofil des BKA grundlegend ändern und die Kompetenzordnung zwischen Strafverfolgungsbehörden, Landespolizeien und BKA chaotisieren würde.

Außerdem geht der Entwurf beim Zweck des biometrischen Abgleichs weit über den Ursprung der Debatte hinaus. Diese wurde ausgelöst, nachdem Journalisten das ehemalige RAF-Mitglied Daniela Klette, nach der jahrelang von der Polizei erfolglos gefahndet wurde, mit Hilfe kommerzieller Biometrie-Software auf Lichtbildern im Internet entdeckt hatten. Daraufhin wurde gefordert, dass auch die Polizei dieses Instrument zu *Zwecken der Personenfahndung* einsetzen können muss. Der vorliegende Entwurf sieht indes vor, dass jede „Erforschung des Sachverhalts“ den biometrischen Abgleich rechtfertigen kann. Dies ist angesichts der Eingriffsintensität dieses Instruments (s. oben) bedenklich.

Der Einsatz biometrischer Abgleichsysteme sollte dringend auf Zwecke der Personenfahndung und -identifizierung beschränkt werden.

§ 9a Abs. 1 Nr. 2 BKAG-E sollte daher wie folgt formuliert werden:

> *Ein Abgleich der Daten darf durchgeführt werden, wenn dies im Rahmen bereits bestehender Ermittlungsverfahren oder gefahrenabwehrrechtlicher Vorgänge zum Zwecke der Identifizierung oder Aufenthaltsermittlung im Rahmen der Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Absatz 2 Nummer 1 erforderlich ist und von der aktenführenden Behörde in Auftrag gegeben wurde,…*

§ 9a Abs. 1 Nr. 3 BKAG-E sieht vor, dass die Maßnahme nur zulässig ist, wenn die Verfolgung oder Verhütung der Straftat „auf andere Weise aussichtslos oder wesentlich erschwert wäre". Dies wird der unionsrechtlichen Anforderung der „unbedingten" Erforderlichkeit im Sinne einer verschärften conditio-sine-qua-non aus Art. 10 der Richtlinie 2016/680/EU und § 48 Abs. 1 BDSG nicht gerecht[9]. Dort wird verlangt, dass sicher ausgeschlossen sein muss, dass der Erkenntnisgewinn auf andere Weise erlangt werden kann.

Zur Gewährleistung dieser unionsrechtlichen Anforderung ist die Maßnahme daher unter die Bedingung der unbedingten Erforderlichkeit zu stellen.

Wegen der erheblichen Eingriffstiefe sollte die Maßnahme zudem generell unter Richtervorbehalt gestellt werden. Eine solche verfahrensrechtliche Absicherung erscheint vor dem Hintergrund der verfassungsrechtlichen Rechtsprechung[10] unabdingbar. Nur so lässt sich insbesondere die Einhaltung des materiellen Verhältnismäßigkeitsprinzips angemessen absichern. Erforderlich wären zudem formelle Anforderungen an die Begründung der beantragten Maßnahme.

[9] vgl. Rückert, StV 2025, 350 - 356
[10] 1 BvR 370/07, Rn. 242, 259.

§ 9a Abs. 8 BKAG-E (Richtervorbehalt) sollte auf Anordnungen nach Abs. 1 erweitert werden.

Zur Sicherstellung der Anwendbarkeit des EU-Datenschutzregimes bedarf es zudem der Vorgabe der Auftragsdatenverarbeitung in der EU bzw. im Schengen-Raum.

§ 9a Abs. 6 BKAG-E sollte ersatzlos gestrichen werden.

Aus Sicht des Deutschen Anwaltvereins ist das Bemühen zu begrüßen, durch die in § 9a Abs. 4 S. 3 BKAG-E i.V.m. § 82 Abs. 1 BKAG normierte Dokumentationspflicht eine ansatzweise Transparenz der Nutzung zu schaffen. Dies greift aber bei Weitem zu kurz. Angesichts der gerade bei Gesichtsidentifikationen zu erwartenden Priming-Effekte bei der nachfolgenden menschlichen Bewertung – beispielsweise in einer späteren strafprozessualen Hauptverhandlung – ist eine präzise Dokumentation der konkreten Suchanfragen einschließlich des verwendeten Referenzmaterials und der jeweiligen Suchergebnisse (einschließlich Negativergebnisse) für die Bewertung der Beweiskraft unabdingbar.

Das BKA sollte zur Schaffung einer Datenlage verpflichtet werden, die eine vollständige Reproduktion des gesamten Suchvorgangs (einschließlich unergiebiger Anfragen) ermöglicht.

b) § 39a BKAG-E[11]

Mit § 39a BKAG-E soll das BKA ermächtigt werden, zur Abwehr terroristischer Gefahren automatisiert biometrische Abgleiche vorzunehmen.

[11] Art. 1 d. Entwurfs eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus.

Auch hier geht der Einsatzzweck weit über die Personenfahndung und -identifizierung hinaus. Es wird daher auf die Ausführungen oben unter C. I. 1. a) cc) verwiesen.

Die Zwecke „Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen von Straftaten oder Gefahren“ in Abs. 1 S. 1 sollten ersatzlos gestrichen werden.

Soweit die Maßnahme eingesetzt werden soll, wenn die Abwehr der Gefahr sonst „wesentlich erschwert“ wäre, widerspricht dies Art. 10 der Richtlinie 2016/680/EU und § 48 Abs. 1 BDSG (s. oben a.a.O.).

Die Abs. 3 ff. des § 39a BKAG-E entsprechen denjenigen des § 9a BKAG-E. Es kann daher ebenfalls auf die Ausführungen unter C. I. 1. a) cc) verwiesen werden.

c) § 63b BKAG-E[12]

Mit § 63b BKAG-E soll das BKA ermächtigt werden, zur Abwehr von Gefahren für Personen und Räumlichkeiten gem. § 6 BKAG automatisierte biometrische Abgleiche vorzunehmen.

Auch hier geht der Einsatzzweck weit über die Personenfahndung und -identifizierung hinaus. Ist wird daher auf die Ausführungen oben unter C. I. 1. a) cc) verwiesen.

Die Zwecke „Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen von Straftaten oder Gefahren“ in Abs. 1 S. 1 sollten ersatzlos gestrichen werden.

[12] Art. 1 des Entwurfs eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit.

2. Automatisierter biometrischer Abgleich mit Bilddaten aus dem Internet durch die Bundespolizei (§ 58a BPolG-E)

§ 58a BPolG-E ist in weiten Teilen analog zu den §§ 9a, 39a, 63b BKAG-E ausgestaltet. Auch hier soll der biometrische Abgleich auch „zur Erforschung des Sachverhalts“ und zur „Ermittlung von Zusammenhängen von Straftaten und Gefahren“ zulässig sein. Der Entwurf geht allerdings noch weiter, da bereits eine Gefahr für die körperliche Unversehrtheit einer Person („Leib“) als Anlass ausreichen soll. Dies würde bedeuten, dass das extrem eingriffsintensive Instrument des biometrischen Abgleichs zur Prävention einfacher Körperverletzungsdelikte eingesetzt werden dürfte.

Die Zwecke „Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen von Straftaten oder Gefahren“ in Abs. 1 S. 1 sollten auch hier ersatzlos gestrichen werden.

Außerdem sollte auch der nur für Zwecke der Personenfahndung und -identifizierung zulässige biometrische Abgleich auf die Abwehr von Gefahren für besonders gewichtige Rechtsgüter beschränkt werden.

3. Automatisierter biometrischer Abgleich mit Bilddaten aus dem Internet durch das Bundesamt für Migration und Flüchtlinge (§ 15b AsylG-E)

Mit dem Entwurf soll der Abgleich von Lichtbildern der Antragsteller im Asylverfahren mit biometrischen Internetdaten zur Standardmaßnahme werden. Dies ist angesichts der Eingriffsintensität und Streubreite der Maßnahme und mit Blick auf Art. 10 der Richtlinie 2016/680/EU und § 48 Abs. 1 BDSG abzulehnen.

Die Formulierung in Abs. 1 „und der Abgleich für die Feststellung der Identität oder Staatsangehörigkeit des Ausländers erforderlich ist“ sollte geändert

werden in „wenn die Identität oder Staatsangehörigkeit des Ausländers ohne den Abgleich nicht festgestellt werden kann“.

II. Automatisierte Datenanalyse

Mit §§ 9b, 39b, 63c BKAG-E und § 58b BPolG-E sollen Ermächtigungsnormen für die Durchführung automatisierter Datenanalysen durch das BKA und die BPol geschaffen werden.

Automatisierte Datenanalyse meint die Zusammenführung und den automatisierten Abgleich vorhandener Datenbestände mit KI-Software. Angesichts der Tatsache, dass im Rahmen des Bund-Länder-Projekts P20 derzeit an der Zentralisierung sämtlicher deutscher Polizeidaten in einem sog. Datenhaus beim BKA gearbeitet wird, hätte eine Befugnis des BKA, sämtliche dort vorgehaltenen Daten automatisiert analysieren zu dürfen, ungeahnte Ausmaße. Die Auswertung beträfe nicht nur die Vorgangsdaten aller Polizeibehörden auf Bundes-, Landes- und kommunaler Ebene, sondern auch sämtliche in laufenden Strafverfahren beschlagnahmten Daten, also die Inhalte einer unüberblickbaren Zahl von Mobiltelefonen, Computern etc., sowie Daten aus Telefonüberwachungsmaßnahmen etc. (so auch ausdrücklich die Entwurfsbegründung, vgl. S. 25 Entwurf 1). Diese Daten betreffen Beschuldigte, für die bekanntlich die Unschuldsvermutung streitet, ebenso aber auch Dritte, etwa Zeugen, Mitbewohner, Angehörige, Geschädigte etc. In den Daten finden sich massenhaft auch solche aus besonders geschützten Vertrauensbeziehungen z. B. unter Eheleuten, mit Verteidigern oder Journalisten, sensible Gesundheitsdaten etc.

Der Entwurf sieht demnach eine Rasterfahndung neuen Typs vor, die angesichts der Datafizierung der heutigen Gesellschaft und des damit verbundenen Datenanfalls bei den Polizeibehörden eine extreme Streubreite hätte.

Die Befugnis des BKA als Zentralstelle soll, so erscheint es jedenfalls anhand des Entwurfs, außerhalb konkreter Strafverfahren oder Gefahrenabwehrvorgänge existieren. Das BKA dürfte im Rahmen seiner Zentralstellenfunktion konkreten Verfahren vorgelagert Daten automatisiert analysieren. Dies hätte u. a. zur Folge, dass herkömmliche Akteneinsichts- und Rechtsschutzmöglichkeiten leerlaufen würden. Das BKA würde im Bereich der Strafverfolgung tätig, ohne dabei Ermittlungsperson der zuständigen Staatsanwaltschaft zu sein. Es wäre dadurch einer effektiven Kontrolle durch die Instrumente der StPO entzogen.

Die Entwurfsbegründung nimmt auf die Grundsatzentscheidung des BVerfG, Az. 1 BvR 1547/19 Bezug (S. 24). Dort ging es aber nicht um den Einsatz von Analyseplattformen zur *Strafverfolgung*. Der vorliegende Entwurf will das BKA im Rahmen von dessen Zentralstellenfunktion aber ermächtigen, Datenanalysen zum Zwecke der Strafverfolgung vorzunehmen.

Soweit der Gesetzesentwurf nicht nur eine Vernetzung bereits vorhandener polizeilicher Vorgangsdaten und Falldaten ermöglicht, sondern einen Zugriff auf in anderen Strafverfahren gewonnenen Beweisdaten legitimieren soll, geht die Eingriffstiefe außerdem deutlich über die in der Grundsatzentscheidung diskutierten Eingriffskonstellation hinaus.

Das BKA würde in die Lage versetzt, eine automatisierte Durchsicht und Analyse fast sämtlicher in Drittverfahren gewonnenen und vorhandenen digitalen Beweisdaten vornehmen zu können. Es könnte daher umfangreiche automatisierte Tiefenrecherchen im Vorrat jeglicher aus laufenden Ermittlungsverfahren vorliegenden digitalen Überwachungs- und Beweisdaten anstellen.

Das Bundesverfassungsgericht hat in der Grundsatzentscheidung 2 BvR 1027/02 nachdrücklich darauf hingewiesen, dass angesichts des mit der Durchsicht elektronischer Beweismittel verbundenen Eingriffs in das Grundrecht auf informationelle Selbstbestimmung eine strenge Beachtung der

Verhältnismäßigkeitsgrundsatzes und des Übermaßverbots zu gewährleisten ist. Dies beinhaltet insbesondere auch, dass vor Beginn einer Durchsicht ein Auffindeverdacht, der die Annahme voraussetzt, dass sich in den konkret sichergestellten Daten überhaupt verfahrensrelevante Informationen befinden, bestehen muss.[13] Auch in der Entscheidung BVerfG 2 BvR 497/03 wurde betont, dass bereits bei der Durchsicht zu berücksichtigen ist, dass die Gewinnung überschießender und vertraulicher, für das Verfahren aber bedeutungsloser Informationen im Rahmen des Vertretbaren vermieden werden müsse. Eine Durchsicht elektronischer Beweismittel ohne jeden konkreten Auffindeverdacht verbietet sich nach diesen Grundsätzen von vornherein.

Eine die automatisierte verfahrensübergreifende Analyse von digitalen Beweisdaten erlaubende Ermächtigung müsste (wenn überhaupt) sicherstellen, dass für jede Datenquelle bereits vor dem Analysevorgang geprüft und festgehalten wird, wieso hinsichtlich des konkret durchsuchten Beweismittels ein Auffindeverdacht bestehen soll und wieso eine Verwertung überhaupt in Betracht kommt. Die Datenquellen sind in dieser Form gesetzlich zu begrenzen. Eine Begründungspflicht ist ausdrücklich zu normieren.
Dies gilt insbesondere auch deshalb, weil durch eine Analysemaßnahme tief in die Rechte unbeteiligter Dritter eingegriffen wird.

Völlig offen bleibt zudem, wie Betroffene im gebotenen Umfang an der Maßnahme beteiligt werden sollen und wie eine Benachrichtigung von einem Datenzugriff erfolgen soll.

Zudem würden Schutzrechte von Berufsgeheimnisträgern ebenso wenig gewährleistet wie der verfassungsrechtliche gebotene Kernbereichsschutz.

Die Analyse der Inhalte von Asservaten und Erkenntnissen aus verdeckten Überwachungsmaßnahmen begegnet daher in besonders hohem Maße

[13] vgl. BVerfG 2 BvR 1027/02 (= NJW 2005, 1917); Szesny, WiJ 2012, 228 ff.

verfassungsrechtlichen Bedenken, zumal die vorgesehenen Analysebefugnisse nicht von Kontrollrechten Betroffener flankiert werden.

Vor diesem Hintergrund hält der DAV die vorgelegten Entwürfe für Rechtsgrundlagen für eine automatisierte Datenanalyse durch Bundeskriminalamt und Bundespolizei insgesamt für verfehlt. Insbesondere eine automatisierte Analyse sämtlicher bei deutschen Polizeibehörden verfügbarer Daten für Zwecke der Strafverfolgung außerhalb eines konkreten Strafverfahrens durch das BKA wäre wegen der Streubreite dieser Maßnahme verfassungsrechtlich nicht zu rechtfertigen. Gleiches gilt für die verfahrensübergreifende Auswertung von asservierten Daten und Daten aus verdeckten Überwachungsmaßnahmen, insb. TKÜ-Daten.

Verteiler

- Bundesministerium der Justiz und für Verbraucherschutz
- Bundesministerium des Innern
- Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages
- Finanzausschuss und Ausschuss für Digitales und Staatsmodernisierung des Deutschen Bundestages
- Innenausschuss des Deutschen Bundestages
- Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
- Fraktionen des Deutschen Bundestages
- Justizministerien der Länder
- Innenministerien der Länder
- Rechts- und Innenausschüsse der Landtage

- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Bundesgerichtshof
- Der Generalbundesanwalt beim Bundesgerichtshof
- Europäische Kommission, Vertretung in Deutschland
- Rechtsausschuss des Bundesrates

- Bundesrechtsanwaltskammer
- Bundesverband der Freien Berufe
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- Deutscher Richterbund
- Gewerkschaft der Polizei
- Deutsche Polizeigewerkschaft
- Bund Deutscher Kriminalbeamter
- Deutscher Juristentag
- Republikanischer Anwältinnen- und Anwälteverein e. V.
- Deutscher Juristentag
- Gesellschaft für Freiheitsrechte (GFF)
- Innocence Project Deutschland – Fehlurteil und Wiederaufnahme e.V.
- Kriminalpolitischer Kreis
- Arbeitskreis Alternativ-Entwurf
- ver.di, Bereich Recht und Rechtspolitik
- Deutsche Vereinigung für Jugendgerichte und Jugendgerichtshilfen
- Strafverteidiger-Forum (StraFo)
- Neue Zeitschrift für Strafrecht (NStZ)
- Strafverteidiger (StV)
- Neue Richter*innenvereinigung e.V.
- Bundesverband Ehrenamtlicher Richterinnen und Richter e.V.
  = Deutsche Vereinigung der Schöffinnen und Schöffen =
- Deutscher Strafverteidiger e.V.
- Regionale Strafverteidigervereinigungen
- Organisationsbüro der Strafverteidigervereinigungen und -initiativen

- Deutscher Juristinnenbund e.V. (djb)
- Wirtschaftsstrafrechtliche Vereinigung e.V. (WisteV)
- Arbeitskreise Recht der im Bundestag vertretenen Parteien
- Vors. des Strafrechtsausschusses des KAV und des BAV
- Strafrechtsausschuss des Deutschen Anwaltvereins
- Geschäftsführender Ausschuss der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins
- Strafrechtsausschuss und Strafprozessrechtsausschuss der Bundesrechtsanwaltskammer

- Mitglieder des Vorstandes des Deutschen Anwaltvereins
- Vorsitzenden der Landesverbände des Deutschen Anwaltvereins
- Vorsitzenden der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Mitglieder des Ausschusses Recht der Inneren Sicherheit des Deutschen Anwaltvereins
- Vors. des FORUM Junge Anwaltschaft des DAV

Presse

- KriPoZ Kriminalpolitische Zeitschrift
- NJW
- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Verlag GmbH
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel
- Juris Newsletter
- JurPC
- Netzpolitik.org
- Heise
- LTO
- Neue Zürcher Zeitung
- Frankfurter Rundschau
- Zeit
- beck-online
- Neue Zeitschrift für Verwaltungsrecht
- Die Öffentliche Verwaltung
- Deubner Verlag, LexisNexis, Verlag Dr. Otto Schmidt, Wolters-Kluwe Online, ZAP Verlag
- Zeitschrift für Rechtspolitik (ZRP)
- Kriminalpolitische Zeitschrift (KriPoZ)
- HRR-Strafrecht
- Zeitschrift für Internationale Strafrechtswissenschaft (ZfIStw)
- Neue Kriminalpolitik (NK)
- Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra)
- Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)
- Strafverteidiger-Forum (StraFo)

- Neue Zeitschrift für Strafrecht (NStZ)
- Strafverteidiger (StV)