GESELLSCHAFT FÜR FREIHEITSRECHTE

2. April 2026

Stellungnahme der Gesellschaft für Freiheitsrechte e.V.

im Rahmen der Verbändebeteiligung

zu den Referentenentwürfen des Bundesministeriums des Inneren „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ und „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“

A. Vorbemerkung

Die Referentenentwürfe sind **zum Großteil verfassungswidrig**. Vor diesem Hintergrund sollte davon abgesehen werden, die darin vorgeschlagenen Befugnisse und Änderungen einzuführen. Mindestens müssen die Entwürfe aber an vielen Stellen geändert werden.

Besonders besorgniserregend ist, dass die Referentenentwürfe staatliche **digitale Souveränität vollkommen ausblenden**. Biometrische Abgleiche im Internet sollen auch von privaten Anbieter*innen im Ausland durchgeführt werden dürfen. Damit soll den Sicherheitsbehörden wohl ermöglicht werden, Anbieter*innen wie PimEyes zu nutzen, deren Produkte mit unionsrechtlichen Vorgaben sowie den Grundrechten unvereinbar sind. Es steht zu befürchten, dass die Sicherheitsbehörden regelmäßig den Weg über private Anbieter*innen im Ausland nutzen werden, um Abgleiche durchführen zu lassen. Darüber hinaus ist auch im Rahmen der Datenanalysebefugnis der Einsatz von Softwaretools privater Anbieter*innen wie z.B. Gotham des US-Unternehmens Palantir auf Grundlage des Entwurfs möglich. Der vorliegende Entwurf sieht keinerlei Vorgaben vor, die sensibelste Polizeidaten vor Fehlern, Datenlecks, unberechtigtem Zugriff, missbräuchlicher Nutzung oder Manipulation schützen. Auch zum KI-Training dürfen polizeiliche Daten an private Unternehmen übermittelt werden.

Die Entwürfe sehen eine **massive Ausweitung heimlicher Überwachungsbefugnisse** für das Bundeskriminalamt und die Bundespolizei vor. Bei den neuen Überwachungsbefugnissen – automatisierte verfahrensübergreifende Datenanalysen sowie automatisierte biometrische Abgleiche mit öffentlich verfügbaren Daten aus dem Internet – handelt es sich um Instrumente, die zu **schwerwiegenden Grundrechtseingriffen** führen. Es handelt sich gerade nicht um gezielte Maßnahmen gegen einzelne Personen, sondern Instrumente zur potenziellen

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

Massenüberwachung. Gleichzeitig liegen keinerlei Nachweise vor, dass diese Befugnisse tatsächlich zu einer effektiven Polizeiarbeit beitragen. Vielmehr sind KI-Tools fehleranfällig und diskriminierend.

In § 15b AsylG, der das BAMF bereits jetzt zur Durchführung biometrischer Abgleiche im Internet ermächtigt, werden gezielt Schutzvorkehrungen gestrichen, wie beispielsweise der Kernbereichsschutz. Das führt zu einer deutlichen **Verschärfung für Asylsuchende**. Auch hier soll ein Rückgriff auf private Anbieter*innen künftig möglich sein. Die Befugnis ist auch in der aktuell geltenden Fassung nicht verhältnismäßig und sollte gestrichen werden.

Datenschutzrechtlich **höchst problematisch** sind außerdem die Befugnisse, die das Bundeskriminalamt und die Bundespolizei ermächtigen, künftig unter viel zu geringen Voraussetzungen mit großen Mengen polizeilicher Daten IT-Systeme zu entwickeln und zu trainieren. Dafür wird ihnen erlaubt, zum Teil auch hoch sensible personenbezogenen Daten zu verwenden.

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

B. Bewertung im Einzelnen

Die einzelnen Befugnisse werfen eine Vielzahl gravierender verfassungs- und unionsrechtlicher Probleme auf.

1. Automatisierter biometrischer Abgleich mit öffentlich verfügbaren Daten aus dem Internet (§§ 9a, 39a, 63b BKAG-E, § 58a BPolG-E und § 15b AsylG-E)

Der Entwurf sieht mehrere neue Befugnisse für das Bundeskriminalamt und die Bundespolizei vor, um automatisierte biometrische Abgleiche mit öffentlich verfügbaren Daten aus dem Internet vorzunehmen. Das BAMF hat diese Befugnis (§ 15b AsylG) bereits. Im Referentenentwurf ist diesbezüglich vorgesehen, zahlreiche Schutzvorkehrungen für Betroffene abzubauen.

a) Befugnisse für Bundeskriminalamt und Bundespolizei

aa) Verfassungsrechtliche Bewertung

Die Befugnisse genügen nicht den verfassungsrechtlichen Anforderungen an besonders eingriffsintensive Überwachungsmaßnahmen.

Die Befugnisse ermöglichen schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Die Streubreite der Maßnahme ist enorm. Auch wenn die Befugnis den Aufbau einer umfassenden biometrischen Referenzdatenbank durch entsprechende Löschpflichten (§§ 9a Abs. 4 Satz 1, 39a Abs. 4 Satz 1, 63b Abs. 4 Satz 1 BKAG-E, § 58a Abs. 4 Satz 1 BPolG-E) ausschließt (der im Übrigen verfassungs- und unionsrechtlich unzulässig wäre) ermächtigt sie zu Eingriffen in die Grundrechte potenziell aller Menschen. Auch wenn diese selbst nicht Zielpersonen einer Maßnahme sind und keinen Anlass für Ermittlungsmaßnahmen gegeben haben, werden doch auch deren Grundrechte beeinträchtigt, da bei Abgleichen auch Nicht-Treffer Grundrechtseingriffe darstellen.[1] Einzelne Personen können nur begrenzt beeinflussen, ob zum Beispiel Bild- und Videomaterial oder Tonaufnahmen von ihnen gegen ihren Willen im Internet veröffentlicht werden. Erfasst sind auch solche Daten, die nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung genutzt werden können[2], wie es typischerweise bei verschiedenen Sozialen Medien der Fall ist. Das Bundesverfassungsgericht hat mehrfach herausgestellt, dass biometrische Daten besonders

[1] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, Rn. 51
[2] Entwurfsbegründung, S. 12.

schutzwürdig sind.[3] Außerdem können Rückschlüsse auf besonders sensible Daten wie politische Einstellungen und sexuelle Orientierung gezogen werden (z.B. bei Aufnahmen von Demos, Parteiveranstaltungen, Gottesdiensten etc.). Anonymität im Internet, das einen erheblichen Teil des öffentlichen Raumes darstellt, wird damit faktisch unmöglich gemacht. Das ist mit enormen Abschreckungseffekten verbunden und hat erhebliche Auswirkungen auf die Ausübung von Grundrechten. Insbesondere die Ausübung der Meinungsfreiheit (Art. 5 Abs. 1 GG) über öffentliche Profile in Sozialen Medien wird damit besonders beeinträchtigt. Es ist auch nicht ausgeschlossen, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung durch die Maßnahme erlangt werden. In diesem Zusammenhang ist beispielsweise an Dating Plattformen, sexualisierte Deep Fakes sowie an die Vielzahl sensibler Aufnahmen zu denken, die oftmals auch ohne Einverständnis der abgebildeten Personen erstellt und im Internet veröffentlicht werden. Die Systeme zum biometrischen Abgleich sind darüber hinaus höchst fehleranfällig und potentiell diskriminierend.[4] Wie das Bundesverfassungsgericht bereits ausgeführt hat, können mit einer weitergehenden Automatisierung von Polizeiarbeit spezifische Diskriminierungsrisiken einhergehen, die verfassungsrechtlich umso weniger hinzunehmen sind, je mehr sich die Wirkungen der automatisierten Datenanalyse oder -auswertung einer nach Art. 3 Abs. 3 GG unzulässigen Benachteiligung annähern könnten.[5] Eingriffsintensivierend wirkt zudem, dass die Abgleiche heimlich stattfinden und Rechtsschutzmöglichkeiten damit erheblich beschränkt sind.

Vor allem auch der weit gefasste Adressat*innenkreis verschärft das Eingriffsgewicht. Die Befugnisse lassen nicht nur den Abgleich der Anlassperson, also tatverdächtiger Personen oder Störer*innen zu, sondern beispielsweise auch von Zeug*innen, Hinweisgeber*innen (§ 9a Abs. 2 Nr. 2 BKAG-E) und nicht verantwortlichen Personen (§§ 9a Abs. 2 Nr. 2, 39a Abs. 2 Nr. 2, 63b Abs. 2 Nr. 2 BKAG-E, § 58a Abs. 2 Nr. 2 BPolG-E). Auch Berufsgeheimnisträger*innen sind teilweise nicht geschützt (§ 62 BKAG gilt nicht für §§ 9a und 63b BKAG-E). Immerhin ist ein Abgleich mit öffentlich zugänglichen Echtzeitdaten (§§ 9a Abs. 1, Satz 2, 39a Abs. 1 Satz 2, 63 b Abs. 1, Satz 2 BKAG-E, § 58 Abs. 1 Satz 2 BPolG-E) sowie mit Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder verdeckten Eingriff in informationstechnische Systeme erlangt wurden, unzulässig (§§ 9a Abs. 3 Satz 2, 39a Abs. 3. Satz 2, 63b Abs. 3 Satz 2 BKAG-E, § 58a Abs. 3 Satz 2 BPolG-E). Damit verbleiben aber Daten aus anderen schwerwiegenden Überwachungsmaßnahmen, wie beispielsweise

[3] BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 53: „höchstpersönliche Merkmale wie das Gesicht"; vgl. auch BVerfG, Urteil des Ersten Senats vom16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 87.

[4] Vgl. insb. zur Auswirkung von Fehleranfälligkeit und Diskriminierungsgefahr auf die Eingriffsintensität, BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 90.

[5] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 77.

Telekommunikationsüberwachung, im Anwendungsbereich der Befugnisse, sodass sich das Eingriffsgewicht durch den Ausschluss nicht maßgeblich reduziert.

Bei Überwachungsmaßnahmen mit hoher Eingriffsintensität im Bereich der Gefahrenabwehr erfordert der Grundsatz der Verhältnismäßigkeit grundsätzlich eine mindestens konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut.[6] Im Bereich der Strafverfolgung bedarf es als Eingriffsschwelle einer gesicherten Tatsachenbasis sowohl für die Annahme eines Tatverdachts als auch für die Erstreckung der Maßnahme auf Dritte.[7] Bei Befugnissen mit hoher Eingriffsintensität ist im repressiven Bereich außerdem eine Begrenzung auf besonders schwere Straftaten[8] geboten, wenn sich aus einer Gesamtschau der Eingriffsvoraussetzungen keine Absenkung des erforderlichen Gewichts ergibt.[9] Da es sich um heimliche Überwachungsmaßnahmen handelt, kommt dem Grundsatz der Bestimmtheit und Normenklarheit eine besondere Bedeutung zu.

Ausgehend von diesem Befund sind die Befugnisse zu bewerten:

§ 9a Abs. 1 Satz 1 Nr. 1 Var. 1 BKAG-E: Da sich auch aus der Gesamtschau der Eingriffsvoraussetzungen, namentlich des qualifizierten Anfangsverdachts sowie des Subsidiaritätsvorbehalts (§ 9a Abs. 1 Satz 1 Nr. 3 BKAG-E) keine Absenkung des erforderlichen Gewichts ergibt, wie das Bundesverfassungsgericht erst vor Kurzem festgestellt hat,[10] verbleibt es bei der verfassungsrechtlich erforderlichen Begrenzung auf besonders gewichtige Straftaten. § 9a Abs. 1 Satz 1 Nr. 1 Var. 1 BKAG-E lässt aber „eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat" ausreichen. Diese Voraussetzung erfüllt in mehrerlei Hinsicht nicht die verfassungsrechtlichen Anforderungen. Erstens genügen „erhebliche Straftaten" nicht dem verfassungsrechtlich notwendigen Gewicht einer besonders schweren Straftat. Zweitens werden die erfassten Straftaten nicht hinreichend konkretisiert. Der Gesetzgeber muss dafür entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen.[11] Eine Generalklausel oder lediglich die abstrakte Verweisung auf Straftaten von besonderer Schwere reichen nicht aus.[12] Diese Anforderung ist nicht erfüllt, wenn der Gesetzgeber, wie vorliegend abstrakt an „Straftaten von auch im Einzelfall erheblicher

[6] Vgl. Trojaner I Rn. 126 m.w.N.
[7] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 178.
[8] Ausführlich zu den Voraussetzungen besonders schwerer Straftaten BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 209 ff.
[9] Vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 178, 205.
[10] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 205.
[11] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 208.
[12] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 208, 214.

Bedeutung“ anknüpft und lediglich teilweise („insbesondere“) auf einen Katalog verweist. Das verstößt auch gegen die Grundsätze der Bestimmtheit und Normenklarheit. Drittens hat das Bundesverfassungsgericht bereits festgestellt, dass ein erheblicher Teil der in § 100a Abs 2 StPO genannten Straftaten nicht die Voraussetzungen von besonders schweren Straftaten erfüllt.[13]

§ 9a Abs. 1 Satz 1 Nr. 1 Var. 2 BKAG-E: Auch die präventive Variante verstößt aus denselben Gründen gegen Verfassungsrecht, indem sie „eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat“ ausreichen lässt.

§ 63b Abs. 1 Satz 1 Nr. 1 BKAG-E: Die Befugnis erfasst jede Gefahr für eine zu schützende Person und enthält damit bisher keine Beschränkung auf Gefahren für besonders bedeutende Rechtsgüter.

§ 63b Abs. 1 Satz 1 Nr. 2 BKAG-E: Bei den „bedeutenden Sachwerten einer zu schützenden Person“ handelt es sich nicht um besonders bedeutende Rechtsgüter. Zwar kann darunter grundsätzlich auch der Schutz von Sachen von bedeutendem Wert fallen, deren Erhaltung im öffentlichen Interesse geboten ist. Das Bundesverfassungsgericht legt dafür aber ein enges Verständnis zu Grunde, wonach etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen gemeint sind.[14]

§ 63b Abs. 1 Satz. 1 Nr. 3 BKAG-E: Es wird unzulässigerweise[15] auch für nicht terroristische Straftaten auf das individuelle Verhalten von Personen für die Eingriffsschwelle der konkretisierten Gefahr abgestellt.

§ 58a Abs. 1 Satz 1 Nr. 2 und Nr. 3 BPolG-E: In Nr. 3 wird in unzulässigerweise[16] auch für nicht terroristische Straftaten auf das individuelle Verhalten von Personen für die Eingriffsschwelle der konkretisierten Gefahr abgestellt. Nr. 2 und Nr. 3 nehmen Bezug auf Straftaten im Zusammenhang mit lebensgefährdenden Schleusungen. Es bleibt unklar, welche Delikte darunter zu fassen sind. Die Regelung genügt daher nicht den Anforderungen an Bestimmtheit und Normenklarheit. Gleiches gilt für die Bezugnahme auf Straftaten, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs. Hier wäre eine abschließende Aufzählung der Tatbestände erforderlich. Stattdessen folgen einige Beispiele, die insbesondere darunterfallen sollen. Der Gesetzgeber kann durchaus auch im Rahmen der Gefahrenabwehr an

[13] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 213 ff.
[14] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 2466/19, Rn. 135 m.w.N.
[15] BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 112 f., 164 f., 213.
[16] BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 112 f., 164 f., 213.

Straftatbestände anknüpfen. Allerdings muss dann eine klare und abschließende Auswahl an Straftatbeständen erfolgen.

Die Befugnisse sehen außerdem nur wenige flankierende Schutzvorkehrungen vor. Die Protokollierungspflichten (§§ 9a Abs. 4 Satz 3 und Satz 4, 39a Abs. 4 Satz 3 und 4, 63b Abs. 4 Satz 3 und 4, BKAG-E) sind grundsätzlich zu begrüßen, um überhaupt Anknüpfungspunkte für eine datenschutzrechtliche Kontrolle zu haben, gewährleistet allein aber keinesfalls eine effektive Kontrolle. Auch die explizite Verpflichtung technisch-organisatorische Maßnahmen zu treffen, um die Daten gegen unbefugte Kenntnisnahme zu schützen (§§ 9a Abs. 4, Satz 2, 39a Abs. 4 Satz 2, 63b Abs. 4. Satz 2 BKAG-E, § 58a Abs. 4 Satz 2, BPolG-E), erscheint sinnvoll, wird allerdings durch die umfangreichen Übermittlungsbefugnisse an staatliche und private Stellen im In- und Ausland konterkariert (siehe dazu unten). Die vorgesehenen Gerichtsvorbehalte (§§ 9a Abs. 8, 39a Abs. 8, 63b Abs. 8 BKAG-E, § 58a Abs. 8 BPolG-E) betreffen lediglich Fälle, in denen die Sicherheitsbehörden den Abgleich durch Stellen in Drittstaaten durchführen lässt. Auch in allen anderen Fällen wäre eine unabhängige gerichtliche Kontrolle geboten. Die Verweise auf die Zweckbindungsvorschriften (§§ 9a Abs. 3 Satz 1, 39a Abs. 3 Satz 1, 63b Abs. 3 Satz 1 BKAG-E, § 58a Abs. 3 Satz 1 BPolG-E) sind verfassungsrechtlich angezeigt.[17] Ein Kernbereichsschutz ist, trotz der Möglichkeit, dass kernbereichsrelevante Daten erhoben werden, nicht vorgesehen. Auch Benachrichtigungspflichten sind nicht vorgesehen. Diese wären aber notwendig, um Rechtsschutz zu erlangen.

bb) Verbleibende praktische Anwendungsfälle ohne Datenbankaufbau

Art. 5 Abs. 1 lit. e KI-VO verbietet insbesondere die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet erstellen oder erweitern. Auch verfassungsrechtlich wäre der Aufbau einer Referenzdatenbank auf Vorrat unzulässig. Vor diesem Hintergrund schließt der Entwurf richtigerweise den Aufbau einer biometrischen Referenzdatenbank auf Vorrat aus, indem er Löschverpflichtungen enthält.

Wie ein Gutachten aus dem letzten Jahr eindrücklich zeigt, ist es aus technischen Gründen aber praktisch unmöglich, für jede einzelne Abgleichmaßnahme den gesamten Datenbestand im Internet erneut zu durchsuchen.[18] Dies würde schlichtweg sehr lange dauern. Deshalb arbeiten

[17] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 65.
[18] Lewandowski, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, September 2025, abrufbar unter https://algorithmwatch.org/de/wp-content/uploads/2025/10/2025-AW-Gutachten-V9.pdf (abgerufen am 2.4.2026).

auch Suchmaschinen mit Datenbanken. Lediglich Daten aus beispielsweise öffentlichen Facebook-Gruppen oder öffentlichen Channels könnten damit abgeglichen werden. Damit ist der praktische Anwendungsbereich der Befugnisse sehr klein und der Effektivitätsgewinn dürfte sich in Grenzen halten.

Da unter öffentlich zugängliche Daten auch solche Daten fallen, deren Nutzung eine Registrierung erfordert oder für die bezahlt werden muss, ist der Rückgriff auf kommerzielle Angebote grundsätzlich von der Befugnis erfasst. Somit wäre den Behörden auch die Nutzung der biometrischen Datenbanken von Privatanbieter*innen wie PimEyes oder Clearview AI erlaubt. Anbieter*innen wie PimEyes verstoßen sowohl gegen das Scraping-Verbot der KI-Verordnung als auch gegen Datenschutzrecht. Beispielweise hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg ein Bußgeldverfahren eröffnet.[19] Einen Rückgriff auf rechtswidrige Angebote Privater ist für den Staat, der gemäß Art. 20 Abs. 3 GG an Gesetz und Recht gebunden ist, aber ausgeschlossen.

cc) Rückgriff auf private Anbieter und andere Staaten zur Durchführung des Abgleichs

Der Entwurf sieht umfassende Möglichkeiten vor, den Abgleich durch andere öffentliche Stellen sowie durch private Anbieter im In- und Ausland – auch außerhalb der EU – durchführen zu lassen (§§ 9a Abs. 5-8, 39a Abs. 5-8, 63b Abs. 5-8 BKAG-E, § 58a Abs. 5-8 BPolG-E). Angesichts der technischen Unmöglichkeit, das gesamte Internet ohne den Aufbau einer Datenbank ad hoc zu durchsuchen, steht es zu befürchten, dass die Inanspruchnahme privater Anbieter in Drittstaaten außerhalb der EU zum Regelfall wird. Zwar sehen die Normen ein gestuftes Vorgehen vor, sodass zunächst auf öffentliche oder nicht öffentliche Stellen im Inland oder einem anderen EU-Mitgliedsstaat zuzugreifen ist. Dabei wird die Zweckbindung, die grundsätzlich bei Datenübermittlungen vorgeschrieben ist, aufgehoben (§§ 9a Abs. 5, 39a Abs. 5, 63b Abs. 5 BKAG-E, § 58a Abs. 5 BPolG-E). Da die Anforderungen der DSGVO und der KI-VO in allen EU-Mitgliedsstaaten gelten, wird es auch hier zu denselben technischen Defiziten kommen, zumal ein Rückgriff auf illegale Angebote ausgeschlossen ist (siehe oben).

Ist der Abgleich durch diese Stellen unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich, kann auf Stellen in Drittstaaten zurückgegriffen werden. Einschränkend wird weiterhin gefordert, dass dies zum „Zweck des Schutzes der nationalen Sicherheit" erforderlich sei und die Voraussetzungen des § 27 Abs. 8 BKAG und des § 81 BDSG erfüllt sind. Zunächst ist festzuhalten, dass der „Schutz der nationalen Sicherheit" nicht den verfassungsrechtlichen Grundsätzen an

[19] PimEyes: LfDI eröffnet Bußgeldverfahren, 21. Dezember 2022, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/ (abgerufen am 2.4.2026).

Bestimmtheit und Normenklarheit genügt. Der Begriff knüpft an die Kompetenzverteilung zwischen Union und Mitgliedsstaaten in Art. 4 Abs. 2 Satz 2 und Satz 3 EUV an. Im Kontext der vorgeschlagenen Befugnisse bleibt aber unklar, was genau davon erfasst sein soll, da das deutsche Sicherheitsrecht nicht mit diesem Begriff operiert. Sollen darunter „Tätigkeiten des Bundeskriminalamts im Bereich der Abwehr, Verhütung und Verfolgung von Terrorismus, Spionage, Sabotage und Straftaten einer § 5 Absatz 1 Satz 2 vergleichbaren Dimension" fallen, muss das hinreichend deutlich im Normtext erkenntlich sein. Dadurch, dass insbesondere von § 81 Abs. 4 BDSG, der vorsieht, dass der Empfänger verpflichtet werden muss, die Daten nur zu dem Zweck zu verarbeiten, zu dem sie übermittelt wurden, abgewichen werden darf, steigt die Gefahr, dass polizeiliche Daten in den Systemen privater Anbieter unkontrolliert weiterverarbeitet werden.

Mit §§ 9a Abs. 6, 39a Abs. 6, 63b Abs. 6 BKAG-E und § 58a Abs. 6 BPolG-E werden spezialgesetzliche Regelungen eingeführt, um eine Umgehung der für den Staat geltenden rechtlichen Anforderungen zu ermöglichen. Selbst wenn kommerzielle Datenbanken im Ausland legal erstellt würden, da sie nicht den Vorgaben der KI-VO und DSGVO unterliegen, dürfte der Staat die für ihn geltenden rechtlichen Grenzen nicht umgehen, indem er auf diese Anbieter zurückgreift. In diesem Sinne hat das Bundesverfassungsgericht (für die Zusammenarbeit mit ausländischen Nachrichtendiensten) betont, dass dem solchen Praktiken inhärenten Potential einer Umgehung innerstaatlicher Bindungen und den spezifischen Grundrechtsgefährdungen, die durch die Zusammenarbeit eintreten können, Rechnung zu tragen ist.[20] Die Grenzen der inländischen Datenerhebung und -verarbeitung des Grundgesetzes dürfen durch einen Austausch von Daten nicht in ihrer Substanz unterlaufen werden.[21] Auch der EGMR fordert, dass Rechtsgrundlagen soweit wie möglich Umgehungen verhindern müssen.[22] Eine Umgehung über die Einführung von speziellen Rechtshilfevorschriften scheidet deshalb aus.

dd) Änderungsbedarf

Vor diesem Hintergrund sollten mindestens **folgende Anpassungen** erfolgen:

- Die **Eingriffsschwellen und die zu schützenden Rechtsgüter** müssen entsprechend des oben genannten Befundes an die verfassungsrechtlichen Vorgaben angepasst werden.

[20] BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17, Rn. 250 mit Verweis auf EGMR.
[21] Vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09 und 1 BvR 1140/09, Rn. 327 zur Übermittlung an eine ausländische staatliche Stelle.
[22] Vgl. EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., Rn. 424.

- **Personen, die keine tatverdächtigen Personen oder Störer*innen sind** sollten als Zielpersonen gestrichen werden, außerdem muss auch für §§ ein Schutz von Berufsgeheimnisträger*innen für §§ 9a und 63b BKAG-E vorgesehen werden.
- Es sollten **Daten, die aus weiteren schwerwiegenden Grundrechtseingriffen** erlangt wurden, ausgeschlossen werden.
- Es sollte ein **Kernbereichsschutz** verankert werden.
- Die **Einbindung der Bundesdatenschutzbeauftragten** muss angesichts der datenschutzrechtlichen Risiken ausgeweitet werden: Es müssen verpflichtende regelmäßige Kontrollen vorgeschrieben werden, sowie entsprechende Anordnungsbefugnisse. Außerdem sollte eine Ermächtigungsgrundlage für den Erlass einer Rechtsverordnung eingeführt werden, die das Nähere zum technischen Verfahren sowie Schutzvorkehrungen enthalten muss und das Einvernehmen mit der BfDI voraussetzt.
- Weiterhin sollte für alle Tatbestandsvarianten ein **Gerichtsvorbehalt** eingeführt werden. Es sollten außerdem Mindestvorgaben für den Antrag und die gerichtliche Entscheidung gesetzlich geregelt werden.
- Es sollten **Benachrichtigungspflichten** eingeführt werden.
- Ein Abgleich durch private Anbieter*innen in Drittstaaten sollte gesetzlich ausgeschlossen werden. Die in den Entwürfen vorgesehenen Übermittlungsbefugnisse sollten gestrichen werden. Stattdessen sollte im Normtext verankert werden, dass **Auftragsverarbeiter*innen ihren Sitz ausschließlich innerhalb der Europäischen Union**, einschließlich der Schengen-assoziierten Staaten, haben dürfen und personenbezogene Daten nur an solche Personen übermittelt werden, die Amtsträger*innen oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind.

b) Verschärfungen in § 15b AsylG

Bei den für § 15b AsylG vorgesehenen Änderungen handelt es sich keinesfalls lediglich um rein redaktionelle Anpassungen. Vielmehr werden **gezielt Schutzvorkehrungen abgebaut**. Dies zeigt sich besonders daran, dass es sich nicht lediglich um Wiederholungen der unmittelbar geltenden KI-VO handelt, die im Übrigen keinesfalls schädlich sind, sondern darüber hinaus auch andere Schutzvorkehrungen, wie etwa der Kernbereichsschutz oder die Vorab-Informationspflicht nunmehr gestrichen werden. Auch ein Rückgriff auf private Anbieter soll ermöglicht werden (§ 15b Abs. 4 AsylG-E).

Der biometrische Abgleich durch das BAMF für Zwecke der Identitätsfeststellung verletzt aber von vornherein die Anforderungen an die Verhältnismäßigkeit und sollte deshalb gestrichen und nicht noch verschärft werden. Der zu Grunde liegende weite Identitätsbegriff, wie ihn die

Gesetzesbegründung enthält, impliziert eine vollständige Ausleuchtung Asylsuchender, die für das Asylverfahren keinesfalls erforderlich ist.

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

2. Automatisierte verfahrensübergreifende Datenanalyse (§§ 9b, 39b, 63c BKAG-E und § 58b BPolG-E)

Die Gesetzesentwürfe sehen Befugnisse zur automatisierten Datenanalyse für das BKA (§§ 9b, 63c BKAG-E und § 39b BKAG-E) und die Bundespolizei (§ 58b BPolG-E) vor.

a) Datenanalysen als Gefahr für die Grund- und Menschenrechte

Mit automatisierten Datenanalysen können große Mengen auch bislang ungefilterter oder getrennt gespeicherter Daten in kürzester Zeit mit weiteren Daten verbunden und verarbeitet werden, um so „neues Wissen zu generieren".[23] Ziel ist gerade, dass durch automatisierte technische Prozesse Erkenntnisse gewonnen werden, die den Ermittlungspersonen noch nicht bekannt waren. Bei hochkomplexen Analysealgorithmen sind deren Ergebnisse für die Anwender*innen dabei nicht nachvollziehbar („Blackbox"). Für automatisierte Datenanalysen werden unüberschaubare, teils ungefilterte Mengen sensibler Daten zusammengeführt und mit komplexen Algorithmen analysiert, wobei auch weitgehende Sachverhaltsbewertungen und Profilerstellungen (Profiling) und damit automatisierte Ermittlungen in Form von predictive policing möglich sind. Dabei besteht die Gefahr, dass aufgrund von Fehlern im Analyseprogramm, insbesondere aufgrund diskriminierender Algorithmen, Menschen fälschlicherweise ins Visier der Sicherheits- und Strafverfolgungsbehörden geraten, obwohl sie dafür keinen Anlass geboten haben. Allein die heimliche automatisierte Verarbeitung von gespeicherten Daten greift bereits tief in die Grundrechte der Bürger*innen ein. Noch intensiver sind die Auswirkungen auf die Grundrechte aber, wenn aufgrund der Analysen sicherheitsbehördliche Eingriffe wie Überwachungsmaßnahmen, Durchsuchungen oder Festnahmen folgen. Schon das Wissen darum, dass eigene bei der Polizei gespeicherte Daten in solche Analysetools geraten (könnten), entfaltet zudem schwere Einschüchterungseffekte und kann ein Gefühl der dauerhaften Überwachung erzeugen. Gleichzeitig liegen keine Statistiken zur Wirksamkeit von und belastbare Zahlen zu Ermittlungserfolgen durch polizeiliche Datenanalysen vor, obwohl in Bundesländern wie Hessen und Nordrhein-Westfalen Analysetools schon seit Jahren zum Einsatz kommen.

Datenanalysekompetenzen dürfen zudem nicht isoliert betrachtet werden. Vielmehr ist zu berücksichtigen, dass durch immer stärkere Überwachungs- und Ermittlungsbefugnisse auch immer mehr und immer sensiblere Daten in den Polizeidatenbanken gespeichert werden. Dies gilt besonders für biometrische Überwachungsbefugnisse, wie sie in diesen Entwürfen ebenfalls vorgesehen sind. Automatisierte Datenanalysen sind mächtige Überwachungsmaßnahmen. Wenn solche Maßnahmen ermöglicht werden sollen, ist eine strenge Beschränkung zum Schutz

[23] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 67.

der Grundrechte unerlässlich. Der Einsatz von Datenanalysetools in anderen Staaten (aktuell der Einsatz von Palantir Gotham und anderer Software durch die US-Behörden wie ICE[24]) und auch in militärischen Konflikten[25] zeigen, wie weitgehende Überwachung und auch Steuerung staatlichen Handelns diese Tools ermöglichen. Angesichts der mit sog. Datamining verbundenen Risiken und Gefahren für Grund- und Menschenrechte müssen die Befugnisse der vorliegenden Entwürfe eingeschränkt werden.

Die Datenanalyse sollte dabei insbesondere ausdrücklich auf **einfach-automatisierte Abgleiche und reine Suchvorgänge** begrenzt werden. Algorithmische Sachverhaltsbewertungen, Profiling und KI-basierte Analysen müssen ausgeschlossen werden. Die Menge der einbezogenen Daten ist stark zu begrenzen. Die Eingriffsschwellen für automatisierte Datenanalysen müssen erhöht und Schutzmaßnahmen gegen Fehler, Diskriminierung und Intransparenz aufgenommen werden.

b) Nichteinhaltung der verfassungsrechtlichen Anforderungen

Die verfassungsrechtlichen Anforderungen an derartige Ermächtigungsgrundlagen ergeben sich aus dem Datenanalyseurteil des Bundesverfassungsgerichts,[26] in dem das Gericht über Rechtsgrundlagen zur polizeilichen Datenanalyse zum Zwecke der Gefahrenabwehr entschied. Die in den Entwürfen vorgesehenen Rechtsgrundlagen bleiben hinter den verfassungsrechtlich erforderlichen Voraussetzungen zurück.

aa) Hohes Eingriffsgewicht

Die Befugnisnormen ermöglichen schwerwiegende Eingriffe in Art. 10 GG, das Recht auf informationelle Selbstbestimmung und das IT-System-Grundrecht (jeweils Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Die ermöglichten Datenanalysen sind nicht ausreichend gesetzlich beschränkt, um das Eingriffsgewicht zu verringern.

[24] Dazu insbesondere „Mit Palantir und Paragon auf Migrantenjagd“, netzpolitik.org (Monroy) vom 17. Januar 2026, https://netzpolitik.org/2026/us-einwanderungsbehoerde-mit-palantir-und-paragon-auf-migrantenjagd/.
[25] Dazu insbesondere „"Targeting": Palantir unterstützt die Ukraine bei der Kriegsführung“, heise.de (Mewes) vom 2. Februar 2023, https://www.heise.de/news/Targeting-Palantir-unterstuetzt-die-Ukraine-bei-der-Kriegsfuehrung-7481072.html sowie ein Werbeclip des Unternehmens Palantir zu seiner Software Gotham, https://www.youtube.com/watch?v=rxKghrZU5w8.
[26] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20.

Die Befugnisse enthalten zum Teil keinerlei, jedenfalls nur unzureichende Einschränkungen in Bezug auf Art und Umfang der Daten sowie hinsichtlich der Methode der Datenverarbeitung.[27] BKA und Bundespolizei dürfen in die Datenanalysen Daten, auf die sie zur Erfüllung ihrer Aufgaben zugreifen dürfen, und damit unbeschränkt sämtliche verfügbaren Datentöpfe einbeziehen. In diesen befinden sich auch von anderen Behörden (wie Geheimdiensten) oder Staaten erhobene Daten sowie in großer Menge Daten unbeteiligter bzw. unverdächtiger Personen.[28] Die Entwürfe ermöglichen auch die Analyse besonders sensibler Datenarten wie biometrischer Daten, genauso wie Fotos und Videos, Tonaufnahmen oder Telekommunikations- oder Standortdaten.

Auch die ermöglichten Analysemethoden sind sehr weit. Insbesondere sind keinerlei methodische Einschränkungen zum Einsatz selbstlernender Systeme oder anderer Formen künstlicher Intelligenz enthalten, was das Eingriffsgewicht der Maßnahmen deutlich verschärft.[29] Die Entwürfe ermöglichen damit auch umfassende Sachverhaltsanalysen, die Erstellung von Personenprofilen und predictive policing.[30] Solche Analysemethoden sind im Vorfeld konkretisierter Gefahren verfassungsrechtlich unzulässig.[31]

bb) Unzureichende Eingriffsschwellen

Nach den Maßstäben des Bundesverfassungsgerichts aus dem Datenanalyse-Urteil handelt es sich folglich um schwerwiegende Grundrechtseingriffe. Befugnisse zur Durchführung von Datenanalysen, die sich als besonders schwerwiegende Grundrechtseingriffe darstellen, sind nur unter den engen Voraussetzungen zu rechtfertigen, die das Bundesverfassungsgericht allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen entwickelt hat.[32] Die dadurch erforderlichen Eingriffsschwellen einer konkretisierten Gefahr für besonders gewichtige Rechtsgüter sind in den Entwürfen des BKAG-E und BPolG nicht in allen Fällen gewahrt. Insoweit verletzen die geplanten Befugnisse Art. 10 GG sowie das allgemeine Persönlichkeitsrecht und das IT-System-Grundrecht (jeweils Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

[27] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 78 ff., 90 ff.
[28] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 77.
[29] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 100, 101.
[30] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 98.
[31] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 121.
[32] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 104 ff.

(1) Zu den Datenanalysebefugnissen für das Bundeskriminalamt im Einzelnen

Bei den vorgesehenen Eingriffsgrundlagen handelt es sich – wie erläutert – um schwerwiegende Grundrechtseingriffe. Insbesondere ist mit den Vorgaben zur Maßnahmerichtung in § 9b Abs. 2, § 63c Abs. 2 BKAG-E gerade nicht sichergestellt, dass nicht auch die in den Datenpools befindlichen Daten Unbeteiligter in die Analyse und so durch Fehler ins Visier des BKA geraten. Die genannten Daten umfassen gerade auch potenzielle Zeug*innen, Opfer von Straftaten, Kontaktpersonen oder Hinweisgeber*innen.

Die **Eingriffsschwellen** der §§ 9b, 63c BKAG-E sind in Teilen **unzureichend**:

- **§ 9b BKAG-E**: Die Regelung des § 9b Abs. 1 Nr. 1 BKAG-E ermächtigt das BKA für Datenanalysen zur Strafverfolgung. Dabei genügt der Verweis auf § 100a Abs. 2 StPO als Straftatenkatalog nicht für eine verfassungsrechtliche Rechtfertigung, da es sich, wie vom Bundesverfassungsgericht in seiner Trojaner-II-Entscheidung festgestellt,[33] nicht bei allen im Katalog genannten Straftaten um besonders schwere Straftaten handelt.
- **§ 63c BKAG-E:**
  - In § 63c Abs. 1 Satz 2 Nr. 1 BKAG-E wird in unzulässigerweise[34] auch für nicht terroristische Straftaten auf das individuelle Verhalten von Personen für die Eingriffsschwelle der konkretisierten Gefahr abgestellt.
  - In beiden Fällen des § 63c Abs. 1 Satz 2 BKAG-E sind die als Anlässe genutzten Straftaten nicht bestimmt und normenklar genug genannt. Erforderlich wäre vielmehr ein Straftatenkatalog. Generalklauseln oder abstrakte Verweisungen auf Straftaten von besonderer Schwere genügen nach Rechtsprechung des Bundesverfassungsgerichtes nicht.[35]

(2) Zur Datenanalysebefugnis für die Bundespolizei im Einzelnen

Für die Bundespolizei sieht § 58b BPolG-E eine Rechtsgrundlage für automatisierte Datenanalysen vor. Auch bei dieser Maßnahme handelt es sich um einen schwerwiegenden Grundrechtseingriff.

---

[33] Vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 213 ff. zu repressiven Maßnahmen.
[34] Vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 112 f., 164 f., 213.
[35] Vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 208 zu repressiven Maßnahmen.

Die zur Rechtfertigung dieses Eingriffs erforderlichen **Eingriffsschwellen sind jedoch nicht gewährleistet.** In § 58b Abs. 1 Nr. 3 BPolG-E wird in unzulässigerweise[36] auch für nicht terroristische Straftaten auf das individuelle Verhalten von Personen für die Eingriffsschwelle der konkretisierten Gefahr abgestellt.

cc) Fehlen von flankierenden Schutzmaßnahmen und zureichender Kontrolle

Darüber hinaus fehlt es in den Entwürfen an Regelungen, die den verfassungskonformen und rechtmäßigen Betrieb der Datenanalyseplattformen tatsächlich im Einsatz sichern. Da die Befugnisse den Einsatz komplexer Systeme und auch statistische Auswertungen erlauben, bedarf es Vorkehrungen gegen eine hiermit spezifisch verbundene Fehler- und Diskriminierungsanfälligkeit und zur Sicherung der Nachvollziehbarkeit.[37]

In Frage kommen u.a. Vorgaben zu Ausgewogenheit und Qualität von Trainingsdaten[38] sowie zu Analysekriterien (insbesondere zu Proxys, also diskriminierenden Stellvertreterkriterien).[39] Ebenso denkbar sind Transparenzmaßnahmen wie Tests[40] und Vorgaben zur Erklärbarkeit von Analyseergebnissen[41] sowie Regeln zur Entscheidungsfindung aufgrund von Analyseergebnissen (Vermeidung von sog. automation biases).[42] Hierzu muss der Gesetzgeber konkrete praktische Maßnahmen vorsehen oder zumindest anleiten. Solche Vorkehrungen sind besonders wichtig, da der Entwurf technologieoffen ausgestaltet ist und auch der Einsatz von Tools und Software privater Unternehmen mit Sitz außerhalb der EU möglich ist.

Ebensolcher Maßnahmen bedarf es zudem, um die Einhaltung des Zweckbindungsgrundsatzes auch praktisch sicherzustellen.[43]

---

[36] Vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 112 f., 164 f., 213.
[37] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 95, 100, 101, 109.
[38] *Hüger*, Künstliche Intelligenz und Diskriminierung, 2023, S. 158 ff. m.w.N.; *Lauscher/Legner*, ZfDR 2022, 367, (371).
[39] Dazu *Rabe* in: Bäuerle/Denker/Geminn et al, KI und Big Data bei der Polizei, 2025, S. 15 (39 f.); *Beck*, Künstliche Intelligenz und Diskriminierung, 2019, S. 17; *Buchholtz/Scheffel-Kain*, NVwZ 2022, 612 ff.; *Tinhofer*, DRdA 1a/2022, Heft 399, 170 (174 ff.).
[40] Dazu insbesondere *Hüger*, Künstliche Intelligenz und Diskriminierung, 2023, S. 153 ff. m.w.N.
[41] Dazu insbesondere *Ibold,* GSZ 2024, 10 (15 f.).
[42] Dazu insbesondere *Rabe* in: Bäuerle/Denker/Geminn et al, KI und Big Data bei der Polizei, 2025, S. 15 (34); zum Begriff näher *Ruschemeier* in: Proceedings of the Weizenbaum Conference 2023: AI, Big Data, Social Media, and People on the Move, 2023, S. 1 (4).
[43] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 118.

Diese Vorgaben zu konkreten Maßnahmen sind in keinem der Entwürfe ausreichend vorhanden. Abstrakte Gebote, nach denen sicherzustellen ist, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden, genügen gerade nicht zur praktischen Durchsetzung. Erforderlich wäre wenigstens ein verbindlicher hinreichend bestimmter Auftrag an die Verwaltung zur Ausarbeitung entsprechender Konzepte und zu deren Veröffentlichung.[44]

Ebenfalls müssen regelmäßige, verdachtsunabhängige Kontrollen der Datenanalysepraxis durch interne und externe Datenschutzbeauftragte vorgesehen werden,[45] die spätestens alle zwei Jahre erfolgen.[46]

Es wird außerdem darauf hingewiesen, dass beim Einsatz selbstlernender und sonstiger KI-Systeme auch die Vorgaben für Anbieter*innen aus der KI-VO eingehalten werden müssen, wenn die Behörde die KI-Systeme mit ihrem Namen versieht oder wesentliche Veränderungen an ihnen vornimmt, Art. 25 Abs. 1 lit. a, b KI-VO („Quasi-Anbieter").[47] Darüber hinaus finden die Vorgaben der KI-VO bislang noch keine unmittelbare Anwendung.[48] Jedenfalls bis zu deren unmittelbarer Geltung muss der Gesetzgeber selbst ausreichende Schutzmaßnahmen vorsehen.

c) Besonderes Risiko bei Software privater Anbieter*innen

Jedenfalls sollte zur Ausübung der Befugnisse nicht auf die Softwareangebote privater Unternehmen zurückgegriffen werden. Anderenfalls können Manipulation, unbefugte Datenzugriffe und Leaks nicht ausgeschlossen werden. Es drohen Abhängigkeiten des Staates von privaten Anbieter*innen, die – in faktischen Monopolstellungen – Preise und Nutzungsbedingungen frei diktieren können. Auch bei einer Nutzung als „Übergangslösung" besteht das Risiko von Lock-In-Effekten, die einen Wechsel zu einer anderen Lösung erschweren. Bei außereuropäischen Anbieter*innen ist zudem die Rechtsdurchsetzung deutscher und europäischer Schutzvorschriften bei Vertragsverletzungen wie Datenleaks und unbefugten Datenzugriffen nicht gewährleistet. Aus diesen Gründen hat sich die Bundesministerin der Justiz und für Verbraucherschutz 2026 gegen eine Lizensierung von Analysesoftwareprodukten des

[44] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 118.
[45] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 109.
[46] Vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 141.
[47] Vgl. *Martini/Botta*, DÖV 2025 1033 (1037 f.).
[48] Die Bestimmungen zum Umgang mit Hochrisiko-KI-Systemen werden frühestens am 2. August 2027 wirksam, Art. 113 Abs. 3 lit. c KI-VO, so nicht durch den aktuell vorliegenden Verordnungsvorschlag „Digital Omnibus on AI" ein noch späterer Zeitpunkt des Inkrafttretens festgesetzt wird.

US-Anbieters Palantir ausgesprochen.[49] Die Bundesregierung gibt an, bislang keine Entscheidung über die Beschaffung bestimmter Softwarelösungen zur Auswertung und Analyse für Bundespolizei und BKA getroffen zu haben.[50]

Die Entwürfe enthalten jedoch keinerlei Vorgaben zur Sicherung der staatlichen digitalen Souveränität. Auch der Einsatz von Softwaretools privater Anbieter wie z.B. Gotham des US-Anbieters Palantir wäre auf Grundlage der Entwürfe möglich.

Aufgrund des Wesentlichkeitsgrundsatzes und der hohen Bedeutung für die Grundrechte der Bürger*innen ist zu fordern, dass der Gesetzgeber Anforderungen an die Anbieter*innen und ihre angebotenen Analyseprogramme im Gesetz zumindest in Grundzügen vorgibt. Festzuschreiben wäre, dass die genutzten Tools transparent sein müssen. Dazu erforderlich ist, dass der Quellcode vor Inbetriebnahme und vor Updates zur umfassenden Prüfung zur Verfügung steht. Nur so kann eine verfassungs- und europarechtskonforme Datenanalysepraxis sichergestellt werden. Zudem muss ausgeschlossen sein, dass Analysetools außereuropäischer Anbieter*innen zum Einsatz kommen, damit nationales und europäisches Recht sicher durchgesetzt werden kann. Als Analysetools kommen in diesem Falle insbesondere öffentliche Softwareprogramme (beispielsweise nach Entwicklung in einem europäischen Verbund) in Betracht.

d) Änderungsbedarf

Vor diesem Hintergrund sollten mindestens folgende Anpassungen erfolgen:

- Die Datenanalyse sollte auf **einfach-automatisierte Abgleiche und reine Suchvorgänge** begrenzt werden. **Algorithmische** Sachverhaltsbewertungen, Profiling und KI-basierte Analysen sollten **ausgeschlossen** werden.
- Die **Eingriffsschwellen und die zu schützenden Rechtsgüter** müssen entsprechend des oben genannten Befundes an die verfassungsrechtlichen Vorgaben angepasst werden. Insbesondere sollte für die Eingriffsschwellen statt an § 100a Abs. 2 StPO an den Katalog des **§ 100b Abs. 2 StPO** angeknüpft werden.

[49] „Einführung der bundesweiten Nutzung von Palantir wird es mit SPD nicht geben“, Welt.de (Breyton, Woldin, Fürsen), 23. Januar 2026, https://www.welt.de/politik/deutschland/article696dec0d173ea7f40d17cd3d/umstrittene-polizei-software-einfuehrung-der-bundesweiten-nutzung-von-palantir-wird-es-mit-spd-nicht-geben.html.

[50] BT-Drs. 21/4923 (Antwort der Bundesregierung. auf die Kleine Anfrage der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD – Drucksache 21/4599 – Zum möglichen Einsatz der Software der Firma Palantir bei der Bundespolizei und beim Bundeskriminalamt), S. 2.

- Es müssen effektive, technisch-organisatorische **Vorkehrungen zur Vermeidung von Fehlern und Diskriminierung, sowie zur Einhaltung der Zweckbindung** sichergestellt werden. Dafür ist ein verbindlicher hinreichend bestimmter Auftrag an die Verwaltung zur Ausarbeitung entsprechender Konzepte und zu deren Veröffentlichung im Gesetz notwendig.
- Die **Einbindung der Bundesdatenschutzbeauftragten** sollte angesichts der datenschutzrechtlichen Risiken ausgeweitet werden: Es müssen verpflichtende regelmäßige Kontrollen vorgeschrieben werden.
- Im Lichte digitaler Souveränität sollten im Gesetz selbst **Vorgaben zur Transparenz der eingesetzten Tools** und **Anforderungen an die Anbieter*innen möglicherweise genutzter Tools** festgeschrieben werden.

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

3. Entwicklung, Überprüfung, Änderung und Training von IT-Produkten einschließlich selbstlernender Systeme (§ 22 Abs. 3 und Abs. 4 BKAG-E, § 46 Abs. 3 und 4 BPolG-E)

Die Gesetzesentwürfe sehen Befugnisse für die Weiterverarbeitung von Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten einschließlich selbstlernender Systeme für das BKA (§ 22 Abs. 3 und 4 BKAG-E) und die Bundespolizei (§ 46 Abs. 3 und 4 BPolG-E) vor. KI-Systeme und KI-Modelle werden nicht ausdrücklich benannt, sind aber über den Begriff der selbstlernenden Systeme erfasst. Ausweislich der Gesetzesbegründung[51] beziehen sich die Befugnisnormen nicht nur auf eigene IT-Anwendungen des BKA, sondern „auch im Einzelfall" auf „die Unterstützung im Rahmen der Aufgabe des Bundeskriminalamts als Zentralstelle".

a) Nichteinhaltung verfassungs- und unionsrechtlicher Anforderungen

Sie genügen nicht den verfassungsrechtlichen Vorgaben für die Zweckänderung bereits erhobener Daten (dazu unter aa). Darüber hinaus haben sie ein über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehendes hohes Eigengewicht (dazu unter bb) und sind auch daran gemessen unverhältnismäßig (dazu unter cc). Es fehlen insbesondere wesentliche flankierende Schutzvorkehrungen und Verfahrensvorschriften (dazu unter dd). Schließlich unterschreiten sie wesentliche Vorgaben des unionsrechtlichen Datenschutzrechts (dazu unter ee).

Vor diesem Hintergrund sollten die Befugnisse nicht in dieser Form eingeführt werden. Um den verfassungs- und unionsrechtlichen Anforderungen zu genügen, bedarf es einer **umfassenden Überarbeitung** der Normen.

aa) Verstoß gegen die Grundsätze der Zweckänderung

Die Befugnisse in § 22 Abs. 3 und 4 BKAG-E sowie § 46 Abs. 3 und 4 BPolG-E erfüllen nicht die verfassungsrechtlichen Anforderungen an eine zweckändernde Weiterverarbeitung bereits erhobener Daten, da sie zu weitreichend und undifferenziert sind.

Die gesetzliche Ermächtigung für eine Datennutzung zu neuen Zwecken begründet einen neuen Eingriff in das Grundrecht, in das durch die Datenerhebung eingegriffen wurde.[52] Nach den Grundsätzen der Zweckänderung orientiert sich das Eingriffsgewicht einer solchen Befugnis an

[51] Entwurfsbegründung, S. 28.
[52] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 61; BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 285.

dem der ursprünglichen Datenerhebung.[53] Gleiches gilt für die Anforderungen an die Verhältnismäßigkeit, deren Beurteilung sich nach dem Kriterium der hypothetischen Datenneuerhebung richtet: Bei Behörden bereits vorhandene personenbezogene Daten dürfen nur zweckändernd weiterverarbeitet werden, wenn sie für den neuen Verarbeitungszweck mit vergleichbar schwerwiegenden Mitteln hätten erhoben werden dürfen.[54]

Diesen Anforderungen tragen die Befugnisse in § 22 Abs. 3 und 4 BKAG-E und § 46 Abs. 3 und 4 BPolG-E nur unzureichend Rechnung. Die Normen ermächtigen BKA und Bundespolizei zur Weiterverarbeitung aller bei ihnen vorhandenen personenbezogenen Daten, ohne zwischen Art, Umfang und Herkunft dieser Daten zu unterscheiden. Weder das Eingriffsgewicht der jeweiligen ursprünglichen Datenerhebung – das je nach Maßnahme stark variieren kann - noch die damit einhergehenden Verhältnismäßigkeitsanforderungen finden Berücksichtigung. So dürfen BKA und Bundespolizei personenbezogene Daten, die aus besonders eingriffsintensiven Maßnahmen stammen, unter denselben Voraussetzungen weiterverarbeiten wie Daten, die durch weniger eingriffsintensive Maßnahmen erlangt wurden.

Allein für das Training von IT-Produkten sehen § 22 Abs. 3 S. 2 BKAG-E und § 46 Abs. 1 S. 2 BKAG-E einen Ausschluss für personenbezogene Daten vor, die durch verdeckte Wohnraumüberwachungsmaßnahmen sowie verdeckte Eingriffe in informationstechnische Systeme erlangt wurden. Nicht erfasst sind hingegen Maßnahmen vergleichbarer Eingriffsintensität wie die Erstellung von heimlichen Bildaufzeichnungen, das geheime Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes, die längerfristige Observation oder der Einsatz verdeckter Ermittler und von Vertrauenspersonen. Auch für die Entwicklung, Überprüfung und Änderung von IT-Produkten ist ein solcher Ausschluss nicht vorgesehen, obwohl das Kriterium der hypothetischen Datenneuerhebung insoweit gleichermaßen uneingeschränkt gilt.

Eine derart pauschale Ermächtigung in § 22 Abs. 3 und 4 BKAG-E und § 46 Abs. 3 und 4 BPolG-E wird den verfassungsrechtlichen Anforderungen nicht gerecht und ist unverhältnismäßig.[55] Der Gesetzgeber ist gehalten, eine ausdifferenzierte Regelung zu schaffen, die dem Eingriffsgewicht der jeweiligen ursprünglichen Datenerhebung auch hinsichtlich der neuen Nutzung ausreichend

[53] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 61.
[54] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 61 f.; BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 287, 330.
[55] So auch Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin zu § 42d ASOG, S. 22, abrufbar unter https://cdn.netzpolitik.org/wp-upload/2025/09/2025-09-29-Stellungnahme-ASOG-Kamp.pdf.

Rechnung trägt und die Zulässigkeit der Weiterverarbeitung an die jeweils damit einhergehenden Verhältnismäßigkeitsmaßstäbe knüpft.

bb) Eigenständiges hohes Eingriffsgewicht

Die Befugnisse in § 22 Abs. 3 und 4 BKAG-E sowie § 46 Abs. 3 und 4 BPolG-E greifen zusätzlich in eigenständiger Weise in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein, da sie spezifische Belastungseffekte mit sich bringen, die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen.[56]

In diesem Zusammenhang weisen die Befugnisse ein hohes Eingriffsgewicht auf. Dem BKA und der Bundespolizei wird der Zugriff auf sämtliche bei ihnen vorhandene personenbezogene Daten eröffnet, ohne dass die Befugnisnormen nach Art, Sensibilität oder Umfang der Daten differenzieren. Die Weiterverarbeitung besonders schutzbedürftiger Datenkategorien wie biometrische Daten oder Gesundheitsdaten ist nicht ausgeschlossen. Auch dürfen personenbezogene Daten von unbeteiligten Personen wie Zeug*innen, Anzeigeerstatter*innen, Opfern oder vermissten Personen in Test- und Trainingsprozesse eingespeist werden. Die hohe Streubreite der Befugnisse bestimmt das Eingriffsgewicht maßgeblich mit.[57]

Der Verwendungszweck ist denkbar weit gefasst. Die Normen ermächtigen BKA und Bundespolizei im Rahmen ihrer Aufgabenerfüllung zu jeglicher Weiterverarbeitung personenbezogener Daten zu Zwecken der Entwicklung, Überprüfung, Änderung und des Trainings von IT-Produkten einschließlich KI-Systemen und KI-Modellen. Eine Einschränkung auf bestimmte Arten oder spätere Einsatzfelder von IT-Produkten ist nicht vorgesehen. Damit fallen unter die Befugnisse gleichermaßen die Entwicklung und das Training interner digitaler Verwaltungssysteme wie auch besonders eingriffsintensiver Systeme wie biometrischer Identifizierungssysteme, ohne dass die Normen insoweit unterschiedliche Anforderungen vorsehen.

Die Heimlichkeit der Maßnahme erhöht die Eingriffsintensität zusätzlich.[58] Da die Weiterverarbeitung typischerweise ohne Wissen der Betroffenen und teils automatisiert erfolgt, erfahren diese regelmäßig weder, dass ihre Daten zu den in den Normen aufgezählten Zwecken

[56] So das Bundesverfassungsgericht in Bezug auf die automatisierte Datenanalyse, BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 67.
[57] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 76 f.
[58] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 76.

weiterverwendet werden, noch welche IT-Produkte damit trainiert werden, die später möglicherweise im Rahmen von polizeilichen Maßnahmen gegen sie eingesetzt werden können.

Besonderes Gewicht kommt der Befugnis zu, soweit sie die Nutzung personenbezogener Daten für das Training von KI-Systemen und KI-Modellen erlaubt. Das Bundesverfassungsgericht hat im Rahmen seiner Entscheidung zur automatisierten Datenanalyse hervorgehoben, dass der Einsatz selbstlernender Systeme das Eingriffsgewicht eigenständig erhöht.[59] Für die Trainingsphase gilt dies in gesteigertem Maße, denn in diesem Stadium werden die Grundlagen gelegt, auf denen das System später eigenständig Muster generiert, Zusammenhänge herstellt und ggf. Aussagen über Personen trifft. Fehler, Verzerrungen und diskriminierende Algorithmen, die in dieser Phase entstehen, wirken in sämtlichen späteren Anwendungsschritten fort und sind nachträglich kaum zu korrigieren. Daher ist auch für das Training von KI-Systemen ein gesteigertes Eingriffsgewicht anzunehmen. Auch hier ist die Nachvollziehbarkeit der entwickelten Systeme und ihre ggf. automatisierten selbstständig verlaufenden Lernprozesse nicht gewährleistet.

Schließlich wirkt eingriffsverstärkend, dass personenbezogene Daten, die zum Training selbstlernender Systeme verwendet werden, faktisch dauerhaft in den trainierten Modellen verbleiben können.[60] Eine nachträgliche Löschung aus einem trainierten KI-Modell ist nach dem Stand der Technik nicht bzw. nur schwer möglich[61] und verfestigt den Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Es besteht darüber hinaus das Risiko, dass Trainingsdaten aus Modellen re-extrahiert oder re-identifiziert werden können.[62]

cc) Unverhältnismäßigkeit

Gemessen an dem hohen Eingriffsgewicht sind § 22 Abs. 3 und 4 BKAG-E sowie § 46 Abs. 3 und 4 BPolG-E unverhältnismäßig. Es fehlt an hinreichend bestimmten Voraussetzungen, die den damit verbundenen Grundrechtseingriff in einem angemessenen Maße begrenzen.

---

[59] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 100.

[60] *EDSA*, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, 2024, S. 15 f., Rn. 31 ff., abrufbar unter https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_de.pdf.

[61] *Cooper, A. Feder, Choquette-Choo, Christopher A. et al.*, Machine Unlearning Doesn't Do What You Think: Lesson for Generative AI Policy and Research, 2025, Stanford Public Law Working Paper, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5288768.

[62] *BfDI*, Bericht über das Konsultationsverfahren zum datenschutzkonformen Umgang mit personenbezogenen Daten in KI-Modellen, 2026, S. 5 m.w.N., abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/4_KI-Modelle-pbD/Bericht-Konsultation-KI.pdf?__blob=publicationFile&v=2.

Die Zulässigkeit der Weiterverarbeitung wird nach § 22 Abs. 3 Satz 1 BKAG-E und § 46 Abs. 3 Satz 1 BPolG-E lediglich davon abhängig gemacht, dass dies zur Erfüllung der jeweiligen behördlichen Aufgabe erforderlich sei. Weder die Kategorie der verarbeiteten Daten noch die Art der zu entwickelnden IT-Produkte oder deren mögliche spätere Einsatzszenarien finden eine differenzierte Berücksichtigung. Damit wird der Verwendungszweck nicht hinreichend normenklar geregelt. Insbesondere in Bezug auf besonders schützenswerte Datenkategorien tragen die Befugnisnormen dem hohen Eingriffsgewicht nicht ausreichend Rechnung.

Die Regelbeispiele für die Erforderlichkeit der Aufgabenerfüllung in § 22 Abs. 3 Satz 1 Nr. 1 und 2 BKAG-E und § 46 Abs. 1 Satz 1 Nr. 1 und 2 BPolG-E ermöglichen weitreichende Befugnisse zur Weiterverarbeitung von personenbezogenen Daten. Sie sehen vor, dass auf personenbezogene Echtdaten zurückgegriffen werden darf, insbesondere wenn unveränderte Daten benötigt werden oder eine Anonymisierung oder Pseudonymisierung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Die Aufzählung ist ausweislich der Entwurfsbegründung[63] nicht abschließend, sodass der Behörde ein erheblicher Spielraum bei der Begründung des Rückgriffs auf Echtdaten verbleibt.

In der Praxis dürfte die Anonymisierungsvorgabe weitgehend leerlaufen. Da für das Training selbstlernender Systeme typischerweise große Datenmengen erforderlich sind, dürfte eine wirksame Anonymisierung regelmäßig bereits wegen des damit verbundenen Aufwands als unverhältnismäßig eingestuft werden. Die Beurteilung verbleibt dabei allein bei der Behörde und ist stark von ihren internen technischen und organisatorischen Kapazitäten abhängig, sodass die Norm zu keiner wirksamen Einschränkung des Rückgriffs auf Echtdaten führt.

Darüber hinaus bleibt das Verhältnis der beiden Regelbeispiele zueinander unklar. Das zweite Regelbeispiel (die Unverhältnismäßigkeit einer Anonymisierung bzw. Pseudonymisierung) setzt bereits voraus, dass Echtdaten benötigt werden, und schließt damit das erste Regelbeispiel ein. Die alternative Auflistung führt dazu, dass der Vorrang der Anonymisierung bzw. Pseudonymisierung unterlaufen wird.[64]

Auch unterschreitet die Erforderlichkeitsklausel die verfassungsrechtlichen Anforderungen insoweit, als sie sich allein auf den Entwicklungs- und Trainingsvorgang bezieht, nicht jedoch auf

[63] Entwurfsbegründung, S. 28, 31.

[64] So die Stellungnahme des Landesbeauftragten für Datenschutz und die Informationsfreiheit Baden-Württemberg vom 22. Mai 2025 zum Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften zu § 57a PolG-E, S. 9, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2025/08/Stellungnahme-06_2025-PolG-E.pdf.

den späteren polizeilichen Einsatz des Systems. Wäre dieser nicht erforderlich, vermag auch das Training des entsprechenden KI-Systems den damit verbundenen Grundrechtseingriff nicht zu rechtfertigen.[65]

Die Zulässigkeit der Verarbeitung personenbezogener Daten allein an wirtschaftliche oder kapazitätsbezogene Erwägungen der Behörde zu knüpfen, genügt nicht, um die Verhältnismäßigkeit der Maßnahme sicherzustellen. Daher müssen die Regelbeispiele in § 22 Abs. 3 Satz 1 Nr. 1 und 2 BKAG-E und § 46 Abs. 1 Satz 1 Nr. 1 und 2 BPolG-E gestrichen und die Verarbeitungsschwelle erheblich angehoben und abhängig von Datenkategorie und -herkunft sowie Art des zu trainierenden IT-Produkts und dessen späteren Einsatzmöglichkeiten in einem angemessenen Verhältnis zur Schwere des Grundrechtseingriffs differenziert ausgestaltet werden. Die Weiterverarbeitung besonders sensibler Datenkategorien wie Fotos, Videos und biometrischer Daten sollten gesetzlich ausgeschlossen oder müssen jedenfalls unter strenge materielle Anforderungen gestellt werden.

Schließlich begegnet die Verwendung des Begriffs „selbstlernender Systeme" in § 22 Abs. 3 Satz 1 BKAG-E und § 46 Abs. 1 Satz 1 BPolG bestimmtheitsrechtlichen Bedenken, da die Entwürfe vom Begriff des KI-Systems nach Art. 3 Nr. 1 KI-VO abweichen. Dies erzeugt Rechtsunsicherheiten hinsichtlich des Anwendungsbereichs der KI-Verordnung und der sich daraus ergebenden Anforderungen, insbesondere mit Blick auf die Verbote des Art. 5 und den Vorgaben an Hochrisiko-KI-Systeme i.S.d. Art. 6 KI-VO. Im Interesse der Normenklarheit und der Kohärenz mit dem Unionsrecht sollte zumindest die Terminologie der KI-Verordnung übernommen werden.

dd) Fehlen von flankierenden Schutzvorkehrungen und Verfahrensvorschriften

Den Eingriffsbefugnissen fehlen wesentliche Schutzvorkehrungen und Verfahrensvorschriften, die geeignet sind, die Verhältnismäßigkeit abzusichern.

§ 22 Abs. 3 Satz 3 BKAG-E sieht lediglich vor, dass durch organisatorische und technische Maßnahmen sicherzustellen ist, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Diese werden im Gesetzestext nicht näher spezifiziert. Konkrete Vorgaben zu Diskriminierungsschutz, Qualitätssicherung, Protokollierungspflichten oder zur Nachvollziehbarkeit von Trainingsprozessen fehlen vollständig. Das Bundesverfassungsgericht

[65] So auch *Kühne/Golla/Schäfer*, KI-Innovation mit Echtdaten, GSZ 2025, 272 (281).

hat in seiner Entscheidung zur automatisierten Datenanalyse ausdrücklich klargestellt, dass abstrakte Gebote dieser Art zur praktischen Durchsetzung der Grundrechte nicht genügen.[66]

Notwendig wären konkrete gesetzlich verankerte Schutz- und Verfahrensvorkehrungen, insbesondere:

- klare Lösch- und Protokollierungspflichten,
- die Pflicht zur Sicherstellung, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden,
- ein ausdrückliches Verbot der De-Anonymisierung und der Wiederherstellung personenbezogener Daten aus trainierten Modellen,
- und ein Verbot der Verwendung personenbezogener Daten zu Trainingszwecken von Systemen, die nicht ihrerseits für eine entsprechende Datenerhebung eingesetzt werden dürften.

All diese Vorgaben müssen zudem durch praktische Maßnahmen flankiert werden, die der Gesetzgeber hinreichend konkret zumindest anleitet.

ee) Unionsrechtliche Verstöße

(1) Unklarer normativer Rahmen

Bereits der anwendbare unionsrechtliche Rechtsrahmen ist in den Gesetzesentwürfen nicht hinreichend geklärt. Die Entwicklung und Testung von IT-Produkten kann je nach Entwicklungsstadium und Verwendungszweck unterschiedlichen datenschutzrechtlichen Regimen unterfallen. Soweit die Verarbeitung personenbezogener Daten im Rahmen von Entwicklungs- und Testprozessen erfolgt, die noch keinen hinreichend konkreten Bezug zu einem konkreten Strafverfolgungs- oder Gefahrenabwehrzweck aufweisen, dürfte der Anwendungsbereich der DSGVO eröffnet sein.[67] Dient die Verarbeitung hingegen der Entwicklung und Testung von Systemen, die unmittelbar zur Gefahrenabwehr oder Strafverfolgung eingesetzt werden sollen, ist die JI-Richtlinie und deren Umsetzung im BDSG maßgeblich.[68] Da beide Regime unterschiedliche Anforderungen stellen, hätte der Gesetzgeber für die jeweiligen

[66] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 109.
[67] Vgl. *Kühne/Golla/Schäfer*, GSZ 2025, 272 (276).
[68] Vgl. *Botta*, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin zu § 42d ASOG-E, S. 5 f., abrufbar unter https://www.parlament-berlin.de/ados/19/InnSichO/vorgang/iso19-0228-v_Stellungnahme-2.pdf.

Einsatzszenarien differenzierte Regelungen treffen und das anwendbare Datenschutzrecht klarstellen müssen.

Unabhängig davon, welches Regime im Einzelfall zur Anwendung kommt, werden jedenfalls in beiden Fällen die Befugnisnormen den jeweiligen datenschutzrechtlichen Anforderungen nicht gerecht.

(2) Verstoß gegen die DSGVO

Soweit die DSGVO Anwendung findet, genügen die Befugnisnormen nicht den Anforderungen des Art. 6 Abs. 3 DSGVO. Die Normen beschränken die Weiterverarbeitung personenbezogener Daten weder mit Blick auf deren Art, Sensibilität und Herkunft noch hinsichtlich der Kategorie des zu entwickelnden oder zu trainierenden IT-Systems in differenzierter und hinreichend zweckgebundener Weise. In ihrer Gesamtheit erfüllen die Befugnisnormen damit nicht das Erfordernis, dass der Eingriff in einem angemessenen Verhältnis zum verfolgten legitimen Zweck stehen muss.

Hinzu treten die strengeren Maßgaben des Art. 9 Abs. 2 lit. g DSGVO für die Verarbeitung besonderer Kategorien personenbezogener Daten. Dieser erhöht die Anforderungen an die Erforderlichkeit und verlangt spezifische Maßnahmen zum Schutz der Grundrechte und Interessen der Betroffenen. Solche flankierenden Schutzmaßnahmen fehlen in den Gesetzesentwürfen vollständig.

Um die Konformität mit der DSGVO zu wahren, sollten mindestens folgende Anpassungen erfolgen:

- hinreichende Eingrenzung der Verarbeitungszwecke,
- Festlegung von Speicherfristen,
- Vorsehen von konkreten Garantien und Maßnahmen gegen unbefugten Zugang und unrechtmäßige Übermittlung,
- Vorgabe umfassender Dokumentationspflichten,
- Bereitstellen von Regelungen, um Transparenz gegenüber Betroffenen zu gewährleisten, und zum Umgang mit Betroffenenrechten.[69]

[69] So auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit in seinem 33. Tätigkeitsbericht Datenschutz 2024, S. 115 f. für § 13 HmbVwDiG, abrufbar unter https://datenschutz-

(3) Verstoß gegen die JI-Richtlinie

Soweit die JI-Richtlinie Anwendung findet, sind die Befugnisnormen mit mehreren Grundprinzipien der Richtlinie unvereinbar.

Art. 4 Abs. 2 JI-Richtlinie lässt eine Weiterverarbeitung für einen anderen als den ursprünglichen Zweck nur zu, wenn eine gesetzliche Grundlage besteht und sie nach Unions- oder nationalem Recht erforderlich und verhältnismäßig ist. Dafür muss die Ermächtigungsgrundlage klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen.[70] Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme, die die Verarbeitung solcher Daten vorsieht, getroffen werden darf, damit gewährleistet ist, dass der Eingriff auf das absolut Notwendige beschränkt wird.[71] Darüber hinaus fordert Art. 10 JI-Richtlinie für besondere Kategorien personenbezogener Daten eine unbedingte Erforderlichkeit und geeignete Garantien. Da die Befugnisnormen weder Art und Umfang der verarbeiteten Daten hinreichend bestimmt begrenzen noch angemessene Eingriffsschwellen abhängig von der Art und Einsatzmöglichkeiten der zu trainierenden IT-Produkte und wirksame Schutzvorkehrungen vorsehen, erfüllen sie diese Anforderungen nicht.[72] Ein bloßer pauschaler Verweis auf technische und organisatorische Maßnahmen in den Entwürfen ist nicht ausreichend, um das unionsrechtlich geforderte Schutzniveau zu gewährleisten.

Schließlich verpflichtet Art. 6 JI-Richtlinie zur Differenzierung zwischen verschiedenen Kategorien betroffener Personen wie etwa Tatverdächtige, Verurteilte, Opfer, Zeug*innen und sonstige Beteiligte. Die pauschale Einbeziehung aller Daten unabhängig von ihrer Herkunft, einschließlich der Daten Unbeteiligter, verletzt diese Anforderung.[73]

---

hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Taetigkeitsberichte_Datenschutz/Taetigkeitsberichte_PDF/33._Taetigkeitsbericht_Datenschutz_2024-web.pdf.

[70] EuGH, Urteil vom 2. März 2021 – C-746/18 (Prokuratuur), Rn. 48 m.w.N.

[71] Ebd.

[72] Ebenso *Botta*, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin zu § 42d ASOG-E, S. 7, abrufbar unter https://www.parlament-berlin.de/ados/19/InnSichO/vorgang/iso19-0228-v_Stellungnahme-2.pdfS. 7.

[73] So auch Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel

Vor diesem Hintergrund müssen die Befugnisnormen derart ausgestaltet werden, dass sie insbesondere der Art und Sensibilität verschiedener Datenkategorien, der Eingriffsintensität der ursprünglichen Datenerhebung und dem konkreten Einsatzzweck des jeweiligen IT-Produkts differenziert Rechnung tragen und konkrete Mindestvorgaben für die Gewährleistung der Datensicherheit aufstellen.

b) Besonderes Risiko bei Übermittlung an private Anbieter*innen

§ 22 Abs. 4 BKAG-E und § 46 Abs. 4 BPolG-E erlauben die Übermittlung der weiterzuverarbeitenden personenbezogenen Daten an inländische öffentliche oder nichtöffentliche Stellen sowie an Stellen in EU-Mitgliedstaaten.

Diese Befugnisse sind viel zu weitgehend und mit grundrechtlich nicht hinnehmbaren Risiken verbunden. Sie ermächtigen das BKA und die Bundespolizei dazu, ohne nennenswerte Einschränkung **beliebig Echtdaten etwa an private IT-Unternehmen** zu übermitteln. Die bloße Eingrenzung auf die Erforderlichkeit öffnet Tür und Tor für übermäßig viele Datenübermittlungen. Es ist schon fraglich, warum für die Zwecke der Entwicklung, Überprüfung, Änderung oder des Trainierens überhaupt Übermittlungen an Dritte notwendig sind. Der Gesetzentwurf setzt sich nicht mit der Option auseinander, dass die Daten beim BKA verbleiben und der IT-Dienstleister von dort aus operiert.

Die als Schutzmaßnahme vorgesehene Geheimhaltungsverpflichtung und die Zweckbindung der übermittelten Daten sind nicht geeignet, die mit der Weitergabe verbundenen Grundrechtsrisiken auf ein verfassungsrechtlich vertretbares Maß zu reduzieren. Nach der Überlassung der Daten an private Dritte kann nicht gewährleistet werden, dass die Verwendung tatsächlich rechtmäßig und entsprechend den vereinbarten Zwecken erfolgt. Insbesondere besteht die Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte[74], was zu erheblichen Risiken für die Datensicherheit führt. So besteht etwa bei Wartungs- und Korrekturvorgängen die konkrete Gefahr, dass Personal privater Unternehmen Zugriff auf hochsensible Informationen von Personen erhält, die in den polizeilichen Datenbanken gespeichert sind. Angesichts dieser erheblichen und nicht beherrschbaren Risiken sollten § 22 Abs. 4 BKAG-E und § 46 Abs. 4 BPolG-E gestrichen und stattdessen ausdrücklich klargestellt werden, dass eine Übermittlung personenbezogener Daten an Dritte ausgeschlossen ist.

29 der Verfassung von Berlin zu § 42d ASOG, S. 21, abrufbar unter https://cdn.netzpolitik.org/wp-upload/2025/11/Stellungnahme-BlnBDI-zu-Teilen-d.-Aenderungsantrags-zum-ASOG_E.pdf.

[74] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 100.

c) Änderungsbedarf

Vor diesem Hintergrund sollten **umfassende Überarbeitungen** erfolgen:

- Die Verarbeitungsschwelle muss **erheblich angehoben** und abhängig von Datenkategorie und -herkunft sowie Art und Einsatzmöglichkeiten des zu entwickelnden oder zu trainierenden IT-Produkts **differenziert und hinreichend bestimmt** ausgestaltet werden.
- Die Anknüpfung der Erforderlichkeit an einen **unverhältnismäßigen Aufwand der Anonymisierung bzw. Pseudonymisierung** sollte gestrichen werden.
- Es sollte ein **Ausschluss** für die Weiterverarbeitung besonders sensibler Datenkategorien sowie für Daten, die durch besonders eingriffsintensive Maßnahmen erhoben wurden, gesetzlich vorgesehen werden.
- Es bedarf umfassender konkreter **Vorkehrungen und Verfahrensvorschriften** zum Schutz personenbezogener Daten, von Betroffenenrechten sowie zur Vermeidung von Fehlern und Diskriminierung (dazu oben unter a) dd) und ee)).
- Eine **Übermittlung personenbezogener Daten an Dritte** sollte ausgeschlossen werden.

Kontakt:

Dr. Simone Ruf
Stellvertretende Leitung Center for User Rights
simone.ruf@freiheitsrechte.org
PGP Key ID 0x9FE452FA136F5C9F