



Ausschussdrucksache 21(4)214 G
vom 18. September 2026

Schriftliche Stellungnahme

von Dr. Andreas Schmidtke, Richter am Oberlandesgericht Düsseldorf
vom 18.09.2026

zu dem

- a) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus
BT-Drucksachen 21/6131, 21/7265
- b) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit
BT-Drucksachen 21/6132, 21/6511
- c) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen
BT-Drucksache 21/6806

Düsseldorf, den 18. September 2026

Stellungnahme zu den Gesetzentwürfen zur Stärkung digitaler Ermittlungsbefugnisse (BT-Drs. 21/6806, 21/6131 und 21/6132)

A.	Zusammenfassende Bewertung	1
B.	Änderungen der Strafprozessordnung	4
I.	Einführung des § 98d StPO-E – Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet	4
II.	Einführung des § 98e StPO-E – Automatisierte verfahrensübergreifende Datenanalyse .	17
III.	Anpassung der Benachrichtigungs- und Rechtsschutzregelungen	27
C.	Änderungen des Bundeskriminalamtgesetzes	28
I.	Automatisierter biometrischer Abgleich als Zentralstellenbefugnis (§ 9a BKAG-E)	28
II.	Automatisierte Datenanalyse als Zentralstellenbefugnis (§ 9b BKAG-E)	32
III.	Entwicklung, Überprüfung, Änderung und Training von IT-Produkten, § 22 Abs. 3 und 4 BKAG-E	35
IV.	Biometrischer Abgleich und automatisierte Datenanalyse zur Abwehr von Gefahren des internationalen Terrorismus, § § 39a, 39b BKAG-E	36
V.	Sicherung von Verkehrsdaten, § § 10b, 52 Abs. 3 bis 8 BKAG-E	37
VI.	Biometrischer Abgleich und automatisierte Datenanalyse im Personenschutz, § § 63b, 63c BKAG-E	37
D.	Änderungen des Bundespolizeigesetzes	38
E.	Änderung des Asylgesetzes – Automatisierter biometrischer Abgleich, § 15b AsylG-E	39

A. Zusammenfassende Bewertung

Die Entwürfe eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen¹, eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit² und eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus³ schaffen erstmals ausdrückliche Rechtsgrundlagen für den automatisierten biometrischen Internetabgleich und die automatisierte verfahrensübergreifende Datenanalyse und übertra-

¹ BT-Drs. 21/6806.

² BT-Drs. 21/6132.

³ BT-Drs. 21/6131.

gen entsprechende Befugnisse auf das Bundeskriminalamt und die Bundespolizei. Hinzu treten Regelungen über die Entwicklung und das Training von IT-Produkten sowie über die Sicherung von Verkehrsdaten.

Aus richterlicher Sicht ist die Schaffung ausdrücklicher Rechtsgrundlagen für den automatisierten biometrischen Internetabgleich und die automatisierte verfahrensübergreifende Datenanalyse uneingeschränkt zu begrüßen. Die vorgesehenen Instrumente entsprechen den veränderten tatsächlichen Bedingungen moderner Strafverfolgung und Gefahrenabwehr und können insbesondere in umfangreichen und komplexen Verfahren erheblich dazu beitragen, vorhandene Erkenntnisse effektiver nutzbar zu machen. **Gerade in datenintensiven Ermittlungsverfahren werden automatisierte Verfahren zunehmend zu einem unverzichtbaren Instrument effektiver Strafverfolgung.**

Aus verfassungsrechtlicher Sicht bestehen gegen die Einführung dieser Ermittlungsinstrumente als solche keine grundsätzlichen Bedenken. Ihre konkrete Ausgestaltung muss jedoch dem jeweiligen Eingriffsgewicht durch hinreichend bestimmte materielle und **verfahrensrechtliche Begrenzungen** Rechnung tragen. **Dies ist insbesondere bei der automatisierten verfahrensübergreifenden Datenanalyse in der derzeit vorgesehenen Ausgestaltung noch nicht durchgängig gewährleistet.** Nachbesserungsbedarf besteht dort sowohl hinsichtlich der zweckändernden Einbeziehung bereits erhobener Daten als auch – grundlegend – bei der gesetzlichen Einhegung des für spätere Analysen vorgehaltenen Grunddatenbestands. **Solange Art und Umfang dieses Datenbestands sowie Speicherzweck, Speicherschwelle und Speicherdauer nicht hinreichend bestimmt geregelt sind, kann die automatisierte Datenanalyse ein sehr hohes Eingriffsgewicht erreichen, dem die vorgesehenen Eingriffsschwellen nicht in jeder Hinsicht Rechnung tragen.** Auch beim biometrischen Internetabgleich bestehen in einzelnen Einsatzkonstellationen punktuelle Nachbesserungserfordernisse. **Die aufgezeigten Defizite stellen die verfolgten Regelungsziele und die Einführung der Instrumente als solche nicht in Frage, erfordern aber in zentralen Punkten eine verfassungsrechtliche Nachschärfung der Entwürfe.**

Vor diesem Hintergrund geben die Entwürfe Anlass zu folgenden zusammenfassenden Anmerkungen:

- **Die Einführung des automatisierten biometrischen Internetabgleichs nach § 98d StPO-E ist aus praktischer Sicht ausdrücklich zu begrüßen.** Für die Identitätsfeststellung und Aufenthaltsermittlung eines Beschuldigten ist die vorgesehene Eingriffsschwelle grundsätzlich ausreichend. Bei der Einbeziehung von Zeugen bedarf es allerdings einer zusätzlichen personenbezogenen Tatsachenschwelle; die Sachverhaltserforschung sollte wegen ihres weitergehenden Erkenntnispotentials auf gesetzlich näher bestimmte schwere Straftaten beschränkt werden. Die beispielhafte Bezugnahme auf § 100a Abs. 2 StPO könnte bei der Identitätsfeststellung und Aufenthaltsermittlung entfallen, da der Katalog keine einheitliche Tatgewichtskategorie bezeichnet und teilweise auch Delikte einfachen Gewichts erfasst.
- **Auch die automatisierte Erhebung öffentlich zugänglicher biometrischer Vergleichsdaten zum Zwecke des Abgleichs ist grundsätzlich nicht zu beanstanden.** Sie sollte allerdings als eigenständiger Verarbeitungsschritt ausdrücklich gesetzlich geregelt werden. **Art. 5 Abs. 1**

Buchst. e KI-VO steht einer für konkrete biometrische Abgleiche erforderlichen Vorverarbeitung und datenbankartigen Vorhaltung von Vergleichsdaten **nicht generell entgegen**.

- **Die Schaffung einer ausdrücklichen Rechtsgrundlage für die automatisierte verfahrensübergreifende Datenanalyse nach § 98e StPO-E ist ebenfalls nachdrücklich zu begrüßen.** Nachbesserungsbedarf besteht allerdings bei der zweckändernden Einbeziehung bereits erhobener Daten, **für die ein hinreichend spezifischer Bezug zum konkreten Ermittlungsverfahren gesetzlich gewährleistet werden muss**, und – insbesondere – bei der **gesetzlichen Einhegung** des für spätere Analysen vorgehaltenen Grunddatenbestands.
- **Dieser Grunddatenbestand bedarf eines eigenständigen, gesetzlich hinreichend bestimmten Speicherregimes.** Dieses muss insbesondere **Speicherzweck, Speicherschwelle**, einbeziehbare Daten und Personengruppen sowie **Speicherdauer** festlegen und ist bislang nicht vorgesehen. Werden diese Defizite behoben, erscheint die Anknüpfung an schwere Straftaten nach § 100a Abs. 2 StPO grundsätzlich tragfähig; aus dem Katalog sollten allerdings diejenigen Tatbestände ausgenommen werden, die bereits abstrakt kein hinreichendes Gewicht aufweisen.
- **Zur weitergehenden Nutzung des Potentials automatisierter Datenanalysen erscheint allerdings ein abgestuftes Regelungsmodell vorzugswürdig.** Höhere materielle Eingriffsschwellen könnten mit weitergehenden Datenbeständen oder leistungsfähigeren Analysemethoden verbunden werden und damit das verfassungsrechtliche Wechselverhältnis zwischen Eingriffsgewicht und Eingriffsvoraussetzungen unmittelbar **im Regelungskonzept** abbilden.
- **Gegen den biometrischen Internetabgleich des Bundeskriminalamts nach § 9a BKAG-E bestehen im Ergebnis keine Bedenken.** Die gegenüber § 98d StPO-E weitergehenden personellen und zweckbezogenen Begrenzungen tragen insbesondere dem erhöhten Eingriffsgewicht der Sachverhalts- und Zusammenhangserforschung hinreichend Rechnung. Ergänzungsbedarf besteht hinsichtlich der Benachrichtigung der Zielperson. Auch die subsidiäre Durchführung durch externe Stellen ist bei funktionaler Beschränkung der Verarbeitung auf den konkreten Abgleich sachgerecht.
- **Gegen die konkrete automatisierte Datenanalyse nach § 9b BKAG-E bestehen bei hinreichender Einhegung des zugrunde liegenden Datenbestands keine weiteren verfassungsrechtlichen Bedenken.** Nachbesserungsbedarf besteht hinsichtlich des vorgelagerten Grunddatenbestands, für den es eines eigenständigen gesetzlichen **Speicherregimes** mit hinreichend bestimmten Regelungen zu **Speicherzweck, Speicherschwelle und Speicherdauer** bedarf.
- **Die vorgesehene Rechtsgrundlage für die Entwicklung, Überprüfung, Änderung und das Training von IT-Produkten einschließlich selbstlernender Systeme nach § 22 Abs. 3 und 4 BKAG-E ist zu begrüßen.** Die allgemeine Erforderlichkeitsvoraussetzung, der Ausschluss besonders eingriffsintensiv erhobener Daten vom Training sowie die Zweck- und Geheimhaltungsbindungen bei der Einbeziehung externer Stellen gewährleisten eine hinreichende Begrenzung. Ein vollständiger Verzicht auf das Training mit personenbezogenen Daten erscheint nicht erforderlich.

- **Auch gegen die Befugnisse des Bundeskriminalamts zur Terrorismusabwehr nach §§ 39a und 39b BKAG-E bestehen keine eigenständigen durchgreifenden Bedenken. Entsprechendes gilt für die Befugnisse zum biometrischen Internetabgleich und zur automatisierten Datenanalyse im Personenschutz nach §§ 63b und 63c BKAG-E.** Für eine vom konkreten Analyseanlass unabhängige Zusammenführung und Vorhaltung eines analysefähigen Grunddatenbestands gelten jedoch auch hier die zu § 9b BKAG-E dargestellten Anforderungen.
- **Entsprechendes gilt für die parallel ausgestalteten Befugnisse der Bundespolizei.** Bei der automatisierten Datenanalyse ist wiederum sicherzustellen, dass ein vom konkreten Analyseanlass unabhängiger Grunddatenbestand nur auf hinreichend bestimmter gesetzlicher Grundlage vorgehalten wird.
- **Auch die Einführung der vorläufigen Sicherung von Verkehrsdaten nach §§ 10b, 52 Abs. 3 bis 8 BKAG-E ist aus praktischer Sicht zu begrüßen.** Die Sicherungsanordnung verhindert lediglich den Verlust vorhandener Daten und ersetzt nicht die Voraussetzungen einer späteren Erhebung. Ein genereller Richtervorbehalt für die erstmalige Sicherung ist deshalb nicht erforderlich.
- **Gegen den biometrischen Internetabgleich nach § 15b AsylG-E bestehen keine Bedenken.** Die Maßnahme ist auf die Feststellung von Identität oder Staatsangehörigkeit bei fehlendem gültigen Pass oder Passersatz beschränkt und unterliegt besonderen Zweckbindungs-, Lösungs- sowie organisatorischen und technischen Schutzvorgaben.

B. Änderungen der Strafprozessordnung

I. Einführung des § 98d StPO-E – Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

1. Praktische Bedeutung und Entwicklung gegenüber dem Entwurf 2024

Mit § 98d StPO-E soll erstmals eine ausdrückliche strafprozessuale Ermächtigungsgrundlage für den automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen biometrischen Daten geschaffen werden. Der Abgleich soll zur Erforschung des Sachverhalts sowie zur Identitätsfeststellung oder Ermittlung des Aufenthaltsortes eines Beschuldigten oder Zeugen zulässig sein.⁴ **Für die Schaffung einer solchen Befugnis besteht ein erhebliches praktisches Bedürfnis.** Insbesondere in datenintensiven Ermittlungsverfahren fallen Bild-, Video- und Audiodaten inzwischen in einem Umfang an, der mit manuellen Recherchemitteln kaum noch sinnvoll bewältigt werden kann. Der automatisierte biometrische Abgleich beschleunigt daher nicht lediglich herkömmliche Ermittlungsarbeit, sondern kann öffentlich zugängliche Datenbestände überhaupt erst in einer praktisch nutzbaren Größenordnung für die Strafverfolgung erschließen. Gerade in umfangreichen und komplexen Verfahren kann er damit zu einem unverzichtbaren Ermittlungsinstrument werden.

Bereits der Gesetzentwurf zur Verbesserung der Terrorismusbekämpfung aus dem Jahr 2024 sah einen automatisierten biometrischen Internetabgleich vor, war jedoch enger gefasst.⁵ Er beschränkte die Maßnahme auf die Identitätsfeststellung und Aufenthaltsermittlung und setzte eine

⁴ § 98d Abs. 1 StPO-E; BT-Drs. 21/6806, S. 15.

⁵ BT-Drs. 20/12806, S. 14 f., 25 f.

schwere Straftat nach § 100a Abs. 2 StPO voraus, die auch im Einzelfall schwer wiegen musste; zudem war grundsätzlich eine richterliche Anordnung vorgesehen.⁶ Nach der Sachverständigenanhörung, in deren Rahmen teilweise grundsätzliche verfassungsrechtliche Bedenken geäußert wurden⁷, wurde die Befugnis in der Ausschussfassung nochmals enger ausgestaltet: Erforderlich sollte eine besonders schwere Straftat nach § 100b Abs. 2 StPO sein; Zeugen wurden aus dem Kreis der Zielpersonen herausgenommen und zusätzliche technische und institutionelle Sicherungen vorgesehen.⁸

Der nunmehr vorliegende Entwurf geht gegenüber dieser Fassung in mehreren für das Eingriffsgewicht wesentlichen Punkten weiter. Er erweitert den Ermittlungszweck um die Sachverhaltserforschung, bezieht Zeugen wieder ausdrücklich ein und senkt die Tatgewichtsschwelle auf eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine im Katalog des § 100a Abs. 2 StPO bezeichnete Straftat, ab.⁹ Zugleich entfällt der Richtervorbehalt zugunsten einer grundsätzlich staatsanwaltschaftlichen Anordnung.¹⁰ Die in der Ausschussfassung 2024 vorgesehenen besonderen technischen Kontroll- und Evaluierungsregelungen finden sich in § 98d StPO-E nicht wieder. Dem stehen insbesondere die qualifizierte Subsidiarität, der nunmehr medienneutral formulierte Ausschluss von Echtzeitdaten sowie Protokollierungs- und Löschungspflichten gegenüber.¹¹

2. Kritik an Reichweite und Ausgestaltung des § 98d StPO-E

Insbesondere die gegenüber dem Entwurf 2024 vorgesehenen Erweiterungen – namentlich die (Wieder-)Einbeziehung von Zeugen, die Öffnung für die Sachverhaltserforschung, die Absenkung der Eingriffsschwelle sowie der Wegfall des Richtervorbehalts – haben teils erhebliche Kritik ausgelöst. **Die vorgeschlagene Befugnis wird dementsprechend unterschiedlich beurteilt:** Während die Schaffung einer ausdrücklichen Rechtsgrundlage und auch die konkrete Ausgestaltung teilweise ausdrücklich begrüßt werden¹², wird § 98d StPO-E von anderer Seite teilweise grundsätzlich abgelehnt¹³ oder als zu weitreichend¹⁴ angesehen. Weitere Bedenken betreffen insbesondere die Reichweite der einbeziehenden Vergleichsdaten, die automatisierte Verarbeitung großer Datenbestände sowie Fehler- und Diskriminierungsrisiken biometrischer Systeme.¹⁵ Zudem wird den vorgesehenen materiellen und verfahrensrechtlichen Sicherungen, insbesondere der Subsidiaritätsklausel und der staatsanwaltschaftlichen Anordnung, teilweise keine hinreichend begrenzende Wirkung beigemessen.¹⁶

⁶ BT-Drs. 20/12806, S. 14 f., 25 f.

⁷ Vgl. Deutscher Bundestag, Ausschuss für Inneres und Heimat, Protokoll-Nr. 20/86, Wortprotokoll der öffentlichen Anhörung v. 23.9.2024, S. 12 ff.

⁸ BT-Drs. 20/13413, S. 58.

⁹ § 98d Abs. 1 StPO-E; BT-Drs. 21/6806, S. 15.

¹⁰ § 98d Abs. 4 StPO-E; BT-Drs. 21/6806, S. 17.

¹¹ BT-Drs. 21/6806, S. 16 f.

¹² Deutscher Richterbund (DRB), Stellungnahme Nr. 9/2026, S. 1 ff.; Gewerkschaft der Polizei (GdP), Stellungnahme v. 1.4.2026, S. 2, 4; Deutsche Polizeigewerkschaft (DPoIG), Stellungnahme v. 31.3.2026, S. 2.

¹³ AG KRITIS/AlgorithmWatch/Amnesty International u.a., Gemeinsame Stellungnahme im Rahmen der Verbändebeteiligung v. 1.4.2026, S. 1 ff.; Gesellschaft für Freiheitsrechte (GFF), Stellungnahme v. 2.4.2026, S. 2 ff.; AlgorithmWatch, Stellungnahme v. 2.4.2026, S. 1 ff.

¹⁴ Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Stellungnahme v. 2.6.2026, S. 2 ff.; Strafverteidigervereinigungen, Stellungnahme v. 6.4.2026, S. 2 ff.; Bundesrechtsanwaltskammer (BRAK), Stellungnahme Nr. 21/2026, S. 8 ff.; Zöller, ZRP 2026, 128 ff.

¹⁵ BRAK, Stellungnahme Nr. 21/2026, S. 10 ff.

¹⁶ Deutscher Anwaltverein (DAV), Stellungnahme Nr. 26/2026, S. 8 f.; BRAK, Stellungnahme Nr. 21/2026, S. 9.

Im Kern steht damit der Vorwurf, dass § 98d StPO-E angesichts des Erkenntnispotentials und der Streubreite des automatisierten biometrischen Abgleichs keine hinreichenden materiellen und verfahrensrechtlichen Begrenzungen vorsieht und deshalb in seiner vorgesehenen Ausgestaltung den verfassungsrechtlichen Anforderungen nicht genügt.

3. Verfassungsrechtliche Bewertung

a) Verfassungsrechtliche Grundsätze

Der automatisierte biometrische Abgleich nach § 98d StPO-E greift in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein, weil er personenbezogene biometrische Daten automatisiert erhebt und verarbeitet, mit weiteren Datenbeständen verknüpft und zusätzliche personenbezogene Erkenntnisse erzeugen kann.¹⁷ Verfassungsrechtlich gerechtfertigt sind diese Eingriffe insbesondere dann, wenn sie den Anforderungen der Verhältnismäßigkeit genügen.¹⁸ Zudem sind die Grundsätze von Zweckbindung und -änderung zu berücksichtigen.¹⁹

aa) Grundrechtlich relevante Verarbeitungsschritte

Grundrechtlich relevant sind drei aufeinanderfolgende Verarbeitungsschritte: die Verwendung der bereits vorhandenen biometrischen Ausgangsdaten, die Erhebung der öffentlich zugänglichen Vergleichsdaten und deren anschließender automatisierter biometrischer Abgleich.

Für die **Ausgangsdaten** gelten, soweit sie nicht im nämlichen Strafverfahren erhoben worden sind, die Grundsätze der Zweckbindung und die Hürden der Zweckänderung.²⁰ Eine zweckändernde Weiterverwendung von Daten setzt grundsätzlich voraus, dass diese für den neuen Zweck mit vergleichbar eingriffsintensiven Mitteln erhoben werden dürften und ein hinreichend spezifischer Ermittlungsansatz besteht.²¹

Hiervon zu unterscheiden ist die dem Abgleich vorgelagerte Erhebung der Vergleichsdaten aus dem Internet. Technisch setzt der biometrische Abgleich voraus, dass die im Internet verfügbaren Bild-, Audio- oder Videoinhalte zunächst erfasst, biometrisch aufbereitet und über numerische Vektoren und einen Wahrscheinlichkeits-Score in eine für den automatisierten Vergleich geeignete Datenrepräsentation überführt werden.²² Erst auf dieser Grundlage kann ein Abgleich mit den biometrischen Ausgangsdaten des Strafverfahrens erfolgen.²³ Dabei ist allerdings zu berücksichtigen, dass die bloße Kenntnisnahme öffentlich zugänglicher Daten durch staatliche Stellen grundsätzlich noch keinen Eingriff in das Recht auf informationelle Selbstbestimmung begründet.²⁴ Der Staat darf von allgemein zugänglichen Informationsquellen grundsätzlich unter denselben Bedingungen wie jeder Dritte Gebrauch machen.²⁵ Anderes gilt jedoch, wenn diese Informationen gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und dadurch einen zusätzlichen Aussagewert erhalten.²⁶

¹⁷ Vgl. grundlegend BVerfGE 65, 1, 43 ff. (Volkszählung); zur grundrechtlichen Relevanz automatisierter Verarbeitung und Verknüpfung personenbezogener Daten BVerfGE 150, 244 Rn. 36 ff. (Kfz-Kennzeichenkontrollen 2); BVerfGE 165, 363 Rn. 55 ff. (Automatisierte Datenanalyse).

¹⁸ BVerfGE 172, 106 Rn. 177 (Trojaner II).

¹⁹ BVerfGE 165, 363 Rn. 55 (Automatisierte Datenanalyse).

²⁰ BVerfGE 165, 363 Rn. 55 ff. (Automatisierte Datenanalyse).

²¹ BVerfGE 165, 363 Rn. 62 (Automatisierte Datenanalyse).

²² Hahn, VerfBlog v. 31.3.2026, unter Verweis auf Hahn, GA 2025, 440 (444 f.); Zöller, ZRP 2026, 128, 129.

²³ Zöller, ZRP 2026, 128, 129.

²⁴ BVerfGE 142, 234 Rn. 31 (Cybercrime Convention); BVerfGE 120, 274 Rn. 308 (Online-Durchsuchung).

²⁵ BVerfGE 142, 234 Rn. 31 (Cybercrime Convention).

²⁶ BVerfGE 142, 234 Rn. 31 (Cybercrime Convention).

Ein Eingriff liegt dabei allerdings nicht schon bei jeder technisch vermittelten Erfassung personenbezogener Daten vor. Insbesondere fehlt es daran, wenn Daten Dritter im Rahmen elektronischer Datenverarbeitung lediglich zufällig am Rande miterfasst und unmittelbar anschließend technisch anonym, spurenlos und ohne behördliches Erkenntnisinteresse gelöscht werden.²⁷ Maßgeblich ist, ob sich das behördliche Interesse an den betreffenden Daten unter Berücksichtigung von Überwachungs- und Verwendungszweck bereits in einer Weise verdichtet hat, die eine grundrechtlich relevante Betroffenheit begründet.²⁸ **Werden öffentlich zugängliche Daten dagegen gezielt automatisiert erfasst, um sie einer weiteren staatlichen Verarbeitung zuzuführen, kann bereits hierin ein eigenständiger Grundrechtseingriff liegen;** ihre öffentliche Zugänglichkeit lässt den grundrechtlichen Schutz nicht entfallen.²⁹

Als dritter – eigentlicher – Verarbeitungsschritt ist von der Erhebung der Vergleichsdaten deren anschließender biometrischer Abgleich mit den Ausgangsdaten des Strafverfahrens zu unterscheiden. **Auch dieser bildet aufgrund seines eigenständigen Verarbeitungs- und Erkenntnisgehalts einen selbständigen Eingriff in das Recht auf informationelle Selbstbestimmung.**³⁰

bb) Bestimmung des Eingriffsgewichts

Das Gewicht der einzelnen Eingriffe bestimmt sich nach den allgemeinen Grundsätzen nach Art, Umfang und Verwendungsmöglichkeiten der Daten, der Zahl der Betroffenen und der Intensität ihrer individuellen Beeinträchtigung.³¹ Von Bedeutung ist ferner, ob die Betroffenen einen zurechenbaren Anlass für die Verarbeitung gegeben haben, welche weiteren staatlichen Maßnahmen an die gewonnenen Erkenntnisse anknüpfen können, ob die Verarbeitung heimlich erfolgt und insbesondere, welches neue persönlichkeitsrelevante Wissen durch sie erzeugt werden kann.³²

Für den automatisierten biometrischen Abgleich sind die vom Bundesverfassungsgericht für die automatisierte Datenanalyse entwickelten Maßstäbe heranzuziehen, weil auch hier große personenbezogene Datenbestände automatisiert verarbeitet, miteinander verknüpft und dadurch zusätzliche persönlichkeitsrelevante Erkenntnisse erzeugt werden können. Sein Eingriffsgewicht bestimmt sich neben dem Gewicht der vorausgegangenen Datenerhebungseingriffe nach dem eigenständigen Gewicht der automatisierten Verarbeitung. **Besonderes Gewicht kommt dabei Art und Umfang der verarbeitbaren Daten** zu.³³ Je größer, sensibler und weniger begrenzt der einbeziehbare Datenbestand ist, desto höher ist grundsätzlich das Eingriffsgewicht.³⁴ Eingriffsmindernd wirken demgegenüber normative, technische und organisatorische Begrenzungen, insbesondere hinsichtlich Herkunft und Ersterhebung der Daten, ihres Sach- und Personenbezugs zum Ermittlungsanlass, der einbeziehbaren Datenarten und -quellen, ihrer Aufbewahrung und Löschung sowie der Zugriffs- und Verwendungsmöglichkeiten.³⁵ Umgekehrt erhöhen eine weitreichende Einbeziehung nicht tatbezogener

²⁷ BVerfGE 150, 244 Rn. 43 (Kfz-Kennzeichenkontrollen 2).

²⁸ BVerfGE 150, 244 Rn. 43 (Kfz-Kennzeichenkontrollen 2).

²⁹ BVerfGE 150, 244 Rn. 39, 43 (Kfz-Kennzeichenkontrollen 2).

³⁰ BVerfGE 165, 363 Rn. 50 ff. (Automatisierte Datenanalyse).

³¹ BVerfGE 165, 363 Rn. 76 f. (Automatisierte Datenanalyse); vgl. auch BVerfGE 120, 378 Rn. 76 (Automatisierte Kennzeichenerfassung).

³² BVerfGE 165, 363 Rn. 76 f. (Automatisierte Datenanalyse).

³³ BVerfGE 165, 363 Rn. 78 (Automatisierte Datenanalyse).

³⁴ BVerfGE 165, 363 Rn. 78 ff. (Automatisierte Datenanalyse).

³⁵ BVerfGE 165, 363 Rn. 79 ff. (Automatisierte Datenanalyse).

oder unbeteiligter Personen und die Möglichkeit einer automatisierten Erschließung zusätzlicher Datenbestände die Streubreite und das Eingriffsgewicht.³⁶

Neben der Datenbasis ist die Methode der Verarbeitung relevant. Je stärker diese einem einfachen, durch konkrete Suchkriterien gesteuerten Abgleich auf vorgegebene Übereinstimmungen angenähert ist, desto geringer ist grundsätzlich ihr Gewicht; es steigt dagegen mit Komplexität, Offenheit und Erkenntnistiefe der Verarbeitung.³⁷ Zu berücksichtigen sind insbesondere Zahl und Art der Verarbeitungsschritte, die Bindung an konkrete Personen oder Sachverhalte, Art und Aussagegehalt der erzeugten Ergebnisse sowie deren weitere Verwendung. Eingriffssteigernd können zudem mangelnde Nachvollziehbarkeit sowie Fehler- und Diskriminierungsrisiken automatisierter oder KI-gestützter Systeme wirken.³⁸

cc) Korrespondierende verfassungsrechtliche Anforderungen

Dem Gewicht des jeweiligen Grundrechtseingriffs müssen entsprechend gewichtige materielle Eingriffsvoraussetzungen gegenüberstehen. Die verfassungsrechtlichen Anforderungen richten sich bei repressiven strafprozessualen Ermittlungsmaßnahmen an die Eingriffsschwelle und an das Gewicht der Straftaten, die den Anlass der Überwachung bilden.³⁹ Für den Eingriff bedarf es zudem einer gesicherten Tatsachenbasis.⁴⁰ Dies gilt nicht nur für die Annahme des Tatverdachts, sondern auch und insbesondere für die Erstreckung der Maßnahmen auf Dritte und deren Einbeziehung, für die es ebenfalls „bestimmte Tatsachen“ braucht.⁴¹

Aus diesem Korrespondenzverhältnis zwischen Eingriffs- und Tatgewicht folgt eine abgestufte Zuordnung. Für Ermittlungsmaßnahmen von erheblichem, aber noch begrenztem Eingriffsgewicht kann eine Straftat von erheblicher Bedeutung ausreichen. Das Merkmal kann in dieser Eingriffskategorie auch ohne abschließenden Straftatenkatalog eine hinreichend bestimmte Begrenzung gewährleisten. So hat das Bundesverfassungsgericht dies für die längerfristige technische Observation mittels GPS angenommen.⁴² Auch die automatisierte Kraftfahrzeugkennzeichenkontrolle hat es – allerdings im präventiven Bereich – als Eingriff von erheblichem Gewicht eingeordnet.⁴³ Maßnahmen mit hohem Eingriffsgewicht setzen demgegenüber grundsätzlich die Verfolgung schwerer Straftaten voraus; dies gilt etwa für die klassische Telekommunikationsüberwachung.⁴⁴ Besonders oder sehr schwerwiegende Eingriffe sind auf besonders schwere Straftaten zu beschränken, wie dies insbesondere für die akustische Wohnraumüberwachung und besonders eingriffsintensive Zugriffe auf informationstechnische Systeme gilt.⁴⁵ Bei Maßnahmen höheren Eingriffsgewichts, die schwere oder besonders schwere Straftaten voraussetzen, bedarf es – anders als bei Maßnahmen mit begrenztem Gewicht – einer näheren gesetzlichen Konkretisierung der erfassten Straftatbestände.⁴⁶

³⁶ BVerfGE 165, 363 Rn. 84 (Automatisierte Datenanalyse).

³⁷ BVerfGE 165, 363 Rn. 90 ff. (Automatisierte Datenanalyse).

³⁸ BVerfGE 165, 363 Rn. 90 ff. (Automatisierte Datenanalyse).

³⁹ BVerfGE 172, 106 Rn. 178 (Trojaner II); BVerfGE 165, 363 Rn. 54 (Automatisierte Datenanalyse).

⁴⁰ BVerfGE 172, 106 Rn. 178 (Trojaner II); BVerfGE 129, 208 Rn. 202 (TKÜ-Neuregelung).

⁴¹ BVerfGE 129, 208 Rn. 202 (TKÜ-Neuregelung); vgl. BVerfGE 172, 106 Rn. 178 (Trojaner II).

⁴² BVerfGE 112, 304 Rn. 48 (GPS-Überwachung).

⁴³ BVerfGE 150, 244 Rn. 96, 99 (Kfz-Kennzeichenkontrollen 2).

⁴⁴ BVerfGE 129, 208 Rn. 203 f. (TKÜ-Neuregelung).

⁴⁵ BVerfGE 172, 106 Rn. 196 ff. (Trojaner II).

⁴⁶ BVerfGE 125, 260 Rn. 228 (Vorratsdatenspeicherung); BVerfGE 172, 106 Rn. 208 ff. (Trojaner II).

Welche Straftaten der danach erforderlichen Gewichtskategorie zuzurechnen sind, bestimmt sich nach ihrem materiellen Gewicht. Maßgeblichen Anhaltspunkt bildet der gesetzliche Strafrahmen; ergänzend können Begehungsmerkmale und Tatfolgen berücksichtigt werden.⁴⁷ Ein fehlendes abstraktes Tatgewicht lässt sich für strafprozessuale Maßnahmen hingegen nicht durch eine ergänzende Rechtsgutsbetrachtung oder eine besondere Qualifizierung etwa als terroristische Straftat kompensieren.⁴⁸ Von der besonderen Schwere einer Straftat ist auszugehen, wenn sie der Gesetzgeber jedenfalls mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt hat.⁴⁹ Eine Höchstfreiheitsstrafe von fünf Jahren qualifiziert eine Straftat für sich genommen weder als schwer noch als besonders schwer; entsprechende Tatbestände können allenfalls dem mittleren Kriminalitätsbereich zuzuordnen sein.⁵⁰ Straftaten, die lediglich mit einer Höchstfreiheitsstrafe von bis zu drei Jahren oder mit Geldstrafe bedroht sind, ordnet das Bundesverfassungsgericht demgegenüber dem Bereich einfacher Kriminalität zu.⁵¹

b) Anwendung auf § 98d StPO-E

Bei Anwendung dieser Grundsätze genügt § 98d StPO-E den verfassungsrechtlichen Anforderungen nicht in jeder Hinsicht. Verfassungsrechtlich unbedenklich sind die Nutzung der bereits im Strafverfahren vorhandenen Ausgangsdaten sowie im Grundsatz die Erhebung öffentlich zugänglicher Vergleichsdaten als solche. Hinsichtlich der Datenerhebung dürfte sich allerdings mit Blick auf die Wesentlichkeitstheorie eine ausdrückliche gesetzliche Regelung empfehlen. Bedenken bestehen demgegenüber insbesondere hinsichtlich der Reichweite des automatisierten Abgleichs, soweit dieser auf Zeugen erstreckt und zur Sachverhaltserforschung zugelassen wird.

aa) Ausgangsdaten

Die Verwendung der bereits in einem Strafverfahren erhobenen biometrischen Ausgangsdaten ist verfassungsrechtlich unbedenklich. Maßgeblich sind die aus der ursprünglichen Erhebung fortwirkenden Zweck- und Verwendungsbindungen; soweit eine Zweckänderung vorliegt, treten die Anforderungen der hypothetischen Datenneuerhebung hinzu. § 98d StPO-E löst die Ausgangsdaten nicht von den Anforderungen ihrer ursprünglichen Erhebung, sondern setzt deren rechtmäßige Verfügbarkeit voraus. Die Formulierung „Daten aus einem Strafverfahren“ beseitigt diese fortwirkenden Bindungen nicht.

Einer zusätzlichen pauschalen Beschränkung nach dem strafrechtlichen Gewicht des Vorwurfs im Ausgangsverfahren bedarf es dementsprechend nicht.⁵² Das Tatgewicht bildet insoweit schon für sich genommen keinen hinreichenden Maßstab für die weitere Verwendbarkeit der Daten. Entscheidend sind vielmehr die konkrete Grundlage und das Gewicht ihrer ursprünglichen Erhebung sowie die hieraus fortwirkenden Zweck- und Verwendungsbindungen. Die Forderung, biometrische Ausgangsdaten nur aus Verfahren wegen nicht lediglich geringfügiger Straftaten zuzulassen, greift daher zu kurz.

Gleichwohl könnte – gerade mit Blick auf § 98e Abs. 6 StPO-E – erwogen werden, auch für § 98d StPO-E ausdrücklich klarzustellen, dass die für die Ausgangsdaten geltenden Übermittlungs- und

⁴⁷ BVerfGE 172, 106 Rn. 208 (Trojaner II).

⁴⁸ BVerfGE 172, 106 Rn. 216 (Trojaner II).

⁴⁹ BVerfGE 172, 106 Rn. 209 (Trojaner II).

⁵⁰ BVerfGE 172, 106 Rn. 210 (Trojaner II).

⁵¹ BVerfGE 172, 106 Rn. 211 (Trojaner II).

⁵² Andere Ansicht Zöller, ZRP 2026, 128, 129.

Verwendungsbeschränkungen unberührt bleiben. Zwar finden die allgemeinen strafprozessualen Vorgaben, insbesondere die §§ 474 ff. StPO und die jeweiligen besonderen Verwendungsregelungen, unabhängig von einer solchen Klarstellung Anwendung. Die Entwurfsbegründung weist für die Datenverarbeitung nach §§ 98d StPO-E und 98e StPO-E allgemein auf die Fortgeltung der §§ 474 ff. StPO hin.⁵³ Während § 98e Abs. 6 StPO-E die Fortgeltung der Übermittlungs- und Verwendungsregelungen jedoch ausdrücklich normiert, fehlt für § 98d StPO-E eine entsprechende Bestimmung. **Systematische Gründe sprechen deshalb dafür, diese Klarstellung auch dort aufzunehmen.**

bb) Erhebung der Vergleichsdaten

Auch die automatisierte Erhebung öffentlich zugänglicher biometrischer Vergleichsdaten ist verfassungsrechtlich grundsätzlich unbedenklich. Sie stellt zwar einen eigenständigen Eingriff in das Recht auf informationelle Selbstbestimmung dar, ihr Eingriffsgewicht bleibt jedoch begrenzt.

Eingriffsmindernd wirkt zunächst, dass ausschließlich öffentlich zugängliche Daten erfasst werden. Soweit die betroffenen Personen entsprechende Bilder, Videos oder sonstige biometrisch auswertbare Inhalte selbst öffentlich zugänglich gemacht haben, ist ihre Vertraulichkeitserwartung zusätzlich reduziert. Insoweit unterscheidet sich die Konstellation von der automatisierten Kraftfahrzeugkennzeichenkontrolle, bei der die öffentliche Wahrnehmbarkeit des Kennzeichens nicht auf einer freiwilligen Veröffentlichung personenbezogener Informationen beruht. Eingriffssteigernd wirken demgegenüber die erhebliche Streubreite der Maßnahme und die Einbeziehung potentiell sehr großer Datenbestände mit einer Vielzahl von Personen, die keinerlei Bezug zum Ermittlungsverfahren aufweisen. Auch Nichttreffer werden zunächst gezielt in den staatlichen Verarbeitungsvorgang einbezogen. Ihre Erfassung ist daher nicht lediglich zufällige oder technisch unvermeidbare Begleiterscheinung.

Erschwerend tritt hinzu, dass § 98d StPO-E – anders als die Kennzeichenerfassung – unmittelbar personenbezogene biometrische Merkmale betrifft. Das Gewicht dieser Belastungen wird jedoch dadurch begrenzt, dass die Erhebung für sich genommen noch keine neuen Erkenntnisse über die Betroffenen erzeugt, sondern zunächst lediglich den Datenbestand bereitstellt, der anschließend auf eine Übereinstimmung mit dem konkreten Suchdatum überprüft wird. Für die ganz überwiegende Zahl der erfassten Personen bleibt die Maßnahme zudem folgenlos, wenn Nichttreffer unmittelbar ausgesondert werden und weder gespeichert noch zum Anlass weiterer staatlicher Maßnahmen genommen werden.⁵⁴

Die Erhebung erreicht danach zwar ein nennenswertes Eingriffsgewicht; dieses steht jedoch zu den in § 98d StPO-E vorgesehenen Eingriffsschwellen, insbesondere zum Erfordernis einer Straftat von auch im Einzelfall erheblicher Bedeutung, in einem angemessenen Verhältnis. Eine weitergehende materielle Beschränkung der Datenerhebung ist deshalb verfassungsrechtlich nicht geboten.

⁵³ BT-Drs. 21/6806, S. 15.

⁵⁴ Vgl. insoweit BVerfGE 150, 244 Rn. 98 (Kfz-Kennzeichenkontrollen 2).

Allerdings sollte die Erhebung der Vergleichsdaten ausdrücklich gesetzlich geregelt werden.

Sie bildet nach den vorstehenden Grundsätzen einen eigenständigen Grundrechtseingriff und unterliegt damit dem Vorbehalt des Gesetzes und den Anforderungen der Wesentlichkeitstheorie.⁵⁵ Dies würde zugleich Unklarheiten im Verhältnis zu Abs. 3 vermeiden und klarstellen, dass die Vorschrift nicht nur den Abgleich bereits anderweitig vorhandener Daten, sondern auch deren vorgelagerte automatisierte Erhebung und Zusammenstellung erfasst.⁵⁶

cc) Gewicht des biometrischen Abgleichs

Die im Ausgangspunkt aufgezeigten verfassungsrechtlichen Bedenken gegen § 98d StPO-E betreffen nicht den biometrischen Abgleich als solchen, sondern dessen Ausgestaltung in einzelnen Einsatzkonstellationen. Für die Identitätsfeststellung und Aufenthaltsermittlung eines Beschuldigten genügen die vorgesehenen Eingriffsvoraussetzungen; bei der Einbeziehung von Zeugen bedarf es einer zusätzlichen personenbezogenen Tatsachenschwelle, während die Sachverhaltserforschung wegen ihres weitergehenden Erkenntnispotentials eine höhere Tatgewichtsschwelle erfordert.

(1) Identitätsfeststellung und Aufenthaltsermittlung des Beschuldigten

Der automatisierte biometrische Abgleich weist ein erhebliches Eingriffspotential auf, bleibt jedoch in seiner auf die Identitätsfeststellung oder Aufenthaltsermittlung eines Beschuldigten gerichteten Ausgestaltung methodisch begrenzt. Belastungserhöhend wirken insbesondere die Heimlichkeit der Maßnahme, die Verarbeitung biometrischer Merkmale, der potentiell außerordentlich große Internetvergleichsraum sowie die technische Einbeziehung einer Vielzahl unbeteiligter Personen. Dem steht gegenüber, dass der einzelne Verarbeitungsvorgang an ein konkretes biometrisches Suchmerkmal anknüpft und auf die Feststellung einer vorgegebenen Übereinstimmung gerichtet ist. Eine offene algorithmische Suche nach bislang unbekannten Auffälligkeiten, Risikomustern oder Zusammenhängen eröffnet diese Einsatzform nicht; ebenso wenig werden eigenständige Gefährlichkeits- oder Wahrscheinlichkeitsaussagen über Personen erzeugt.

Das datenbezogene Eingriffsgewicht ist gleichwohl erheblich. Die Vergleichsdaten stammen zwar ausschließlich aus öffentlich zugänglichen Internetquellen; der hierdurch erschließbare Datenraum ist jedoch potentiell außerordentlich groß und mengenmäßig nicht näher begrenzt. Eingriffsverstärkend wirkt zudem, dass biometrische Daten verarbeitet werden und sich unter den Vergleichsdaten auch solche befinden können, die nicht von den Betroffenen selbst, sondern durch Dritte veröffentlicht wurden. Hinzu kommt die erhebliche Streubreite, weil technisch eine große Zahl vollständig unbeteiligter Personen in den Abgleich einbezogen werden kann. Eingriffsmindernd wirken demgegenüber die Beschränkung auf öffentlich zugängliche Quellen, der Ausschluss individuell oder gruppenbezogen zugangsbeschränkter Inhalte, die grundsätzlich folgenlose Aussonderung von Nichttreffern sowie der Ausschluss von Echtzeitdaten.

Methodisch bleibt der Abgleich demgegenüber grundsätzlich in der Nähe eines klassischen automatisierten Such- und Vergleichsvorgangs. Ausgangspunkt ist ein bestimmtes biometrisches Merkmal, dessen Übereinstimmung mit den Vergleichsdaten überprüft wird. Der Abgleich ist nicht auf eine freie algorithmische Analyse unbekannter Zusammenhänge gerichtet und erzeugt als

⁵⁵ BVerfGE 165, 363 Rn. 110 ff., 120 f. (Automatisierte Datenanalyse); so auch Zöller, ZRP 2026, 128, 129.

⁵⁶ Zöller, ZRP 2026, 128, 129 f.

unmittelbares Ergebnis grundsätzlich lediglich Treffer und die zugehörigen Fundstellen. Eingriffssteigernd können allerdings Fehler-, Diskriminierungs- und Nachvollziehbarkeitsrisiken biometrischer Systeme wirken, zumal § 98d StPO-E insoweit bislang keine näheren gesetzlichen Mindestanforderungen an Zuverlässigkeit und Transparenz der eingesetzten Verfahren enthält.

Für die Identitätsfeststellung und Aufenthaltsermittlung eines Beschuldigten führt die Zusammenschau dieser Faktoren zu einem erheblichen, aber noch begrenzten Eingriffsgewicht. Das Erkenntnisziel ist eng umrissen, die Verarbeitung an ein konkretes biometrisches Suchdatum gebunden und der Beschuldigte aufgrund des durch bestimmte Tatsachen begründeten Tatverdachts dem Ermittlungsansatz zurechenbar. Das so bestimmte Eingriffsgewicht steht mit der in § 98d Abs. 1 StPO-E vorgesehenen Schwelle einer Straftat von auch im Einzelfall erheblicher Bedeutung in einem angemessenen Verhältnis.

Zur Absicherung dieser Schwelle verlangt § 98d Abs. 1 StPO-E, dass die Straftat auch im Einzelfall von erheblicher Bedeutung ist, und nennt hierfür „insbesondere eine in § 100a Absatz 2 bezeichnete Straftat“. Dieser – in gleicher Form auch in §§ 100g Abs. 1, 100i Abs. 1 und 100k Abs. 1 StPO verwendete – Verweis erscheint im Lichte der jüngeren Rechtsprechung des Bundesverfassungsgerichts⁵⁷ allerdings bedenklich. Denn nicht jede in § 100a Abs. 2 StPO aufgeführte Straftat ist aufgrund ihrer Katalogzugehörigkeit bereits von erheblicher Bedeutung.⁵⁸ Der Katalog enthält Tatbestände, die lediglich mit einer Höchstfreiheitsstrafe von drei Jahren oder weniger bedroht sind und damit dem Bereich einfacher Kriminalität zuzuordnen sind. Für repressive Ermittlungsmaßnahmen kommt es jedoch allein auf das materielle Gewicht der verfolgten Straftat an; ein unzureichendes abstraktes Tatgewicht kann weder durch die Aufnahme in einen gesetzlichen Katalog noch durch eine ergänzende Rechtsgutsbetrachtung oder eine besondere Qualifizierung der Tat kompensiert werden.⁵⁹

Die Bezugnahme auf § 100a Abs. 2 StPO ist zudem aus systematischen Gründen missverständlich. Dieselbe Vorschrift dient innerhalb der Strafprozessordnung als Anknüpfungspunkt für unterschiedliche Tatgewichtsschwellen: § 100a Abs. 1 StPO bezeichnet die Katalogtaten als „schwere Straftaten“ und verlangt zusätzlich, dass die Tat auch im Einzelfall schwer wiegt; § 100f Abs. 1 StPO setzt eine „in § 100a Abs. 2 bezeichnete, auch im Einzelfall schwerwiegende Straftat“ voraus. Demgegenüber verwenden §§ 100g Abs. 1, 100i Abs. 1 und 100k Abs. 1 StPO denselben Katalog lediglich als Beispiel für Straftaten von auch im Einzelfall erheblicher Bedeutung. Auch § 98e StPO-E knüpft an § 100a Abs. 2 StPO an, verlangt dort aber – entsprechend seinem höheren Eingriffsgewicht – eine schwere Straftat. Der Katalog des § 100a Abs. 2 StPO bezeichnet damit keine einheitliche verfassungsrechtliche Gewichtskategorie.

Für § 98d StPO-E wäre daher ungeachtet der derzeitigen Reformbestrebungen zu § 100a Abs. 2 StPO⁶⁰ zu erwägen, auf den Zusatz „insbesondere eine in § 100a Absatz 2 bezeichnete Straftat“ zu verzichten und allein auf eine Straftat von auch im Einzelfall erheblicher Bedeutung abzustellen. Denn auch eine Überarbeitung des Katalogs ändert nichts daran, dass § 100a

⁵⁷ BVerfGE 172, 106 Rn. 214 ff. (Trojaner II).

⁵⁸ BVerfGE 172, 106 Rn. 215 f. (Trojaner II).

⁵⁹ BVerfGE 172, 106 Rn. 214 ff. (Trojaner II).

⁶⁰ Vgl. etwa BT-Drs. 21/3205, S. 3.

Abs. 2 StPO innerhalb der Strafprozessordnung als Anknüpfungspunkt für unterschiedliche Tatgewichtsschwellen dient und deshalb keine eigenständige, einheitliche verfassungsrechtliche Gewichtskategorie bezeichnet. Eine eigenständige Anknüpfung an die materielle Schwelle der „Straftat von erheblicher Bedeutung“ entspricht bereits der Regelungstechnik der §§ 100h Abs. 1 Satz 2, 163e Abs. 1 Satz 1 und 163f Abs. 1 Satz 1 StPO und vermeidet die durch den § 100a-Katalog hervorgerufene Vermischung unterschiedlicher Tatgewichtskategorien. Dem steht nicht entgegen, dass das Bundesverfassungsgericht bei Maßnahmen höheren Eingriffsgewichts eine gesetzliche Konkretisierung der schweren oder besonders schweren Anlasstaten verlangt. Für Maßnahmen von erheblichem, aber noch begrenztem Eingriffsgewicht hat es die Anknüpfung an eine Straftat von erheblicher Bedeutung auch ohne abschließenden Straftatenkatalog als hinreichend bestimmt angesehen.⁶¹

(2) Einbeziehung von Zeugen

Der biometrische Abgleich eines Zeugen weist gegenüber der entsprechenden Maßnahme bei einem Beschuldigten ein zwar erhöhtes – die nächsthöhere Tatgewichtsstufe jedoch noch nicht erforderndes – Eingriffsgewicht auf. Eingriffssteigernd wirkt insbesondere, dass es regelmäßig an einem dem Zeugen zurechenbaren Tat- oder Ermittlungsansatz fehlt.⁶² Datenbasis, Verarbeitungsmethode und Erkenntnispotential der Maßnahme bleiben demgegenüber unverändert, sodass das erhöhte Eingriffsgewicht noch innerhalb derselben Tatgewichtsstufe aufgefangen werden kann. Dies entspricht auch der Systematik der Strafprozessordnung: Bei einer Reihe heimlicher Ermittlungsmaßnahmen bleibt die für die Maßnahme geltende Tatgewichtsschwelle gegenüber Dritten unverändert.⁶³

Erforderlich ist aber – wie auch bei anderen heimlichen Ermittlungsmaßnahmen gegenüber nicht tatverdächtigen Dritten⁶⁴ – eine entsprechend qualifizierte personenbezogene Eingriffsschwelle.⁶⁵ Die bloße Zeugenstellung genügt hierfür nicht. Sie beschreibt lediglich die prozessuale Rolle der betroffenen Person und gewährleistet angesichts der Weite des strafprozessualen Zeugenbegriffs keinen hinreichend qualifizierten Bezug zu dem konkreten Ermittlungsansatz. Zeuge ist nach dem strafprozessualen Begriffsverständnis grundsätzlich, wer in einem nicht gegen sich selbst gerichteten Verfahren über die Wahrnehmung von Tatsachen Auskunft geben soll; eine besondere Nähe zur Tat oder zum Beschuldigten ist hierfür nicht erforderlich.⁶⁶ Die Entwurfsbegründung erkennt das Erfordernis eines besonderen Sachbezugs des Zeugen zwar insoweit an, als sie als typischen Anwendungsfall auf einen „relevanten Zeugen“ abstellt⁶⁷; weder der Gesetzestext noch die Begründung bestimmen jedoch, aufgrund welcher tatsächlichen Umstände diese Relevanz gegeben sein muss.

⁶¹ BVerfGE 112, 304 Rn. 48 (GPS-Überwachung).

⁶² BVerfGE 165, 363 Rn. 76 f. (Automatisierte Datenanalyse).

⁶³ Vgl. § 100h Abs. 2 Nr. 2 StPO (Einsatz sonstiger besonderer technischer Observationsmittel außerhalb von Wohnungen), § 100f Abs. 2 StPO (akustische Überwachung außerhalb von Wohnraum), § 163e Abs. 1 Satz 3 StPO (Ausschreibung zur Beobachtung bei polizeilichen Kontrollen), § 163f Abs. 1 Satz 3 StPO (längerfristige Observation), § 163g Abs. 2 Satz 1 Nr. 2 StPO (automatische Kennzeichenerfassung).

⁶⁴ Vgl. § 100a Abs. 3, § 100f Abs. 2, § 100h Abs. 2 Nr. 2, § 100i Abs. 3 Satz 1 i.V.m. § 100a Abs. 3, § 163e Abs. 1 Satz 3, § 163f Abs. 1 Satz 3 und § 163g Abs. 2 Satz 1 Nr. 2 StPO.

⁶⁵ Vgl. BVerfGE 172, 106 Rn. 178 (Trojaner II); BVerfGE 129, 208 Rn. 202 (TKÜ-Neuregelung).

⁶⁶ RGSt 52, 289; Meyer-Goßner/Schmitt, StPO, vor § 48 Rn. 1.

⁶⁷ BT-Drs. 21/6806, S. 16.

(3) Sachverhaltserforschung

Eine andere Qualität erreicht der biometrische Abgleich, soweit er zur Sachverhaltserforschung eingesetzt wird. Zwar bleibt auch hier der einzelne Verarbeitungsvorgang an ein konkretes biometrisches Suchmerkmal gebunden und damit methodisch enger als eine offene automatisierte Datenanalyse. Das Erkenntnisziel geht jedoch deutlich über die bloße Identitätsfeststellung oder Aufenthaltsermittlung hinaus. Der Abgleich dient nunmehr gerade dazu, bislang unbekannte tatbezogene Erkenntnisse zu gewinnen. Das Eingriffsgewicht erhöht sich insbesondere dadurch, dass § 98d StPO-E Zahl und Abfolge aufeinander aufbauender Abgleiche nicht näher begrenzt. Ein Treffer kann damit zum Ausgangspunkt weiterer Abgleiche werden, durch die schrittweise neue Sach- und Personenzusammenhänge sichtbar gemacht werden. Der Abgleich bleibt zwar formal auf biometrische Übereinstimmungen beschränkt; funktional nähert sich die Sachverhaltserforschung damit aber der automatisierten Datenanalyse an, weil Zusammenhänge und weitere Ermittlungsansätze durch die Verarbeitung erst erzeugt werden können. Verstärkt wird dieses Erkenntnispotential durch den potentiell außerordentlich großen und mengenmäßig kaum begrenzten Internetvergleichsraum.

Dieses gegenüber der bloßen Identitätsfeststellung und Aufenthaltsermittlung gesteigerte Erkenntnispotential verlangt eine entsprechend höhere materielle Eingriffsschwelle. Für die qualitative Sonderstellung der Sachverhaltserforschung spricht ergänzend die Systematik des § 9a BKAG-E. Zwar erlaubt § 9a Abs. 1 Satz 1 Nr. 2 BKAG-E den biometrischen Abgleich im Rahmen der Zentralstellenaufgabe auch zur ergänzenden Erforschung des Sachverhalts. Gegen die in § 9a Abs. 2 Nr. 2 BKAG-E erfassten Personen, also insbesondere Zeugen, Opfer, Kontaktpersonen und Auskunftspersonen, ist die Maßnahme jedoch ausdrücklich auf Identifizierung und Aufenthaltsermittlung beschränkt. Eine Sachverhaltserforschung gegenüber diesem Personenkreis ist insoweit nicht vorgesehen.

Dass auch andere strafprozessuale Maßnahmen der Sachverhaltserforschung dienen können, ohne dass hierfür gegenüber ihrer sonstigen Anwendung eine erhöhte Eingriffsschwelle vorgesehen ist, steht dem nicht entgegen. §§ 100h, 163e und 163f StPO eröffnen keine vergleichbare automatisierte Erschließung eines bereits vorhandenen, potentiell sehr großen Datenbestands; auch die Rasterfahndung nach § 98a StPO ist hinsichtlich Datenbasis, Suchmerkmalen und gesetzlicher Struktur enger begrenzt. Aus dem Umstand, dass die Sachverhaltserforschung bei diesen Maßnahmen innerhalb der allgemeinen Eingriffsschwelle zulässig ist, lässt sich daher für die deutlich erkenntnisintensivere Ausgestaltung des § 98d StPO-E nichts Gegenteiliges herleiten. Die Sachverhaltserforschung sollte danach auf schwere Straftaten beschränkt und diese Tatgewichtsschwelle gesetzlich näher konkretisiert werden. Eine bloße generalklauselartige Anknüpfung an „schwere Straftaten“ genügt für eine Maßnahme dieser Eingriffsintensität nicht.⁶⁸

4. Ausgewählte weitere Regelungsfragen

a) Reichweite des Abgleichs und unionsrechtliche Erforderlichkeit

Die in § 98d Abs. 1 StPO-E vorgesehene Reichweite des biometrischen Abgleichs ist nach Maßgabe der vorstehenden Ausführungen im Grundsatz sachgerecht. Dies gilt insbesondere für die Einbeziehung der Sachverhaltserforschung und von Zeugen. Beide Erweiterungen sind prak-

⁶⁸ BVerfGE 125, 260 Rn. 228 (Vorratsdatenspeicherung); vgl. BVerfGE 172, 106 Rn. 208 ff. (Trojaner II).

tisch sinnvoll, bedürfen jedoch der vorstehend aufgezeigten zusätzlichen Begrenzungen. Ein Änderungsbedarf hinsichtlich der lediglich „aus einem Strafverfahren“ stammenden biometrischen Ausgangsdaten besteht nach hiesiger Ansicht nicht.

Auch die Bestimmung der öffentlich zugänglichen Internetdaten erscheint sachgerecht. Dies gilt, soweit nach der Entwurfsbegründung auch Angebote erfasst werden können, die erst nach Registrierung, Genehmigung oder Entgeltzahlung zugänglich sind.⁶⁹ Allein eine Registrierung oder Entgeltzahlung macht einen grundsätzlich jedermann eröffneten Informationsraum jedoch nicht zu einem individuell geschützten Kommunikationsbereich. Entscheidend ist, dass Inhalte mit individuell oder gruppenbezogen kontrolliertem Zugang sowie Privatkommunikation ausgeschlossen bleiben. Auch der Umstand, dass Bilder oder andere biometrische Daten teilweise ohne Willen oder Zutun der Betroffenen in das Internet gelangt sind, rechtfertigt keinen generellen Ausschluss dieser Daten.⁷⁰ Die erhebliche Größe des damit verbleibenden Vergleichsraums ist, auch soweit Drittveröffentlichungen betroffen sind, nach Maßgabe der vorstehenden Einordnung verfassungskonform und für die effektive Strafverfolgung gerade erwünscht.

Soweit gegen § 98d StPO-E eingewandt wird, Art. 5 Abs. 1 Buchst. e KI-VO stehe der hierfür erforderlichen Gesichtserkennungsdatenbank grundsätzlich entgegen⁷¹, greift jedenfalls in dieser Allgemeinheit nicht durch. Die Vorschrift verbietet nicht die Erstellung oder Verwendung von Gesichtserkennungsdatenbanken als solche, sondern das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die solche Datenbanken durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern.⁷² Nach den Leitlinien der Europäischen Kommission liegt ein solches ungezieltes Auslesen gerade nicht vor, wenn anhand des Bildes einer bestimmten Person gezielt nach Übereinstimmungen im Internet gesucht wird.⁷³ KI-generierte Datenbanken sieht § 98d StPO-E nicht vor. Soweit ein praktikabler biometrischer Abgleich mit umfangreichen Internetbeständen aus technischen Gründen eine Vorverarbeitung und Indexierung der Vergleichsdaten und damit die Vorhaltung einer datenbankartigen Struktur erfordern sollte, wäre zudem fraglich, ob darin ein „ungezieltes Auslesen“ im Sinne des Art. 5 Abs. 1 Buchst. e KI-VO liegt. Wird ein solcher Bestand ausschließlich geschaffen oder vorgehalten, um konkrete strafprozessuale Abgleichsvorgänge technisch zu ermöglichen, fehlt es nicht an der erforderlichen Zielgerichtetheit; mit dem in den Leitlinien beschriebenen „Staubsauger“-Prinzip⁷⁴ eines wahllosen Erfassens möglichst vieler Gesichtsbilder wäre ein anderes Verständnis auch nicht ohne Weiteres zu vereinbaren.

Zu begrüßen sind schließlich die qualifizierte Subsidiaritätsklausel und der Ausschluss des Abgleichs mit Echtzeitdaten. Soweit der Subsidiaritätsklausel teilweise keine hinreichend begrenzende Wirkung beigemessen wird⁷⁵, vermag dies nicht zu überzeugen. Dass der automatisierte Abgleich lediglich schneller, kostengünstiger oder einfacher durchzuführen ist, genügt nach dem Wort-

⁶⁹ BT-Drs. 21/6806, S. 16; kritisch hierzu etwa Zöller, ZRP 2026, 128, 129

⁷⁰ Andere Ansicht Zöller, ZRP 2026, 128, 131.

⁷¹ BfDI, Stellungnahme v. 2.6.2026, S. 4; BRAK, Stellungnahme Nr. 21/2026, S. 12; vgl. auch Teichmann, ZRP 2026, 207 f.

⁷² Vgl. Hahn, VerBlog v. 31.3.2026.

⁷³ Europäische Kommission, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, C(2025) 5052 final v. 29.7.2025, Rn. 228 f.

⁷⁴ Europäische Kommission, Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, C(2025) 5052 final v. 29.7.2025, Rn. 228.

⁷⁵ Vgl. etwa Strafverteidigervereinigungen, Stellungnahme vom 6. April 2026, S. 3 f.; BRAK, Stellungnahme Nr. 21/2026, S. 8 ff.

laut der Vorschrift gerade nicht. **Ein zwingender Änderungsbedarf folgt auch nicht aus der unionsrechtlichen Vorgabe der „unbedingten Erforderlichkeit“ nach Art. 10 RL (EU) 2016/680.** Nach der Rechtsprechung des Gerichtshofs setzt die „unbedingte Erforderlichkeit“ insbesondere voraus, dass der mit der Verarbeitung verfolgte Zweck nicht in zumutbarer Weise ebenso wirksam mit weniger eingriffsintensiven Mitteln erreicht werden kann.⁷⁶ Die in § 98d Abs. 1 Satz 1 Nr. 2 StPO-E vorgesehene qualifizierte Subsidiaritätsklausel trägt diesem Maßstab grundsätzlich Rechnung. Der Begriff der „wesentlichen Erschwerung“ ist dabei unionsrechtskonform dahin auszulegen, dass auf die biometrische Verarbeitung nur zurückgegriffen werden darf, wenn der konkrete Ermittlungszweck nicht ebenso wirksam mit weniger eingriffsintensiven Mitteln erreicht werden kann.⁷⁷

b) Dokumentation, Löschung und weitere Verwendung

Die Protokollierungs- und Lösungsregelungen der Absätze 2 und 3 sind grundsätzlich sachgerecht.⁷⁸ Ergänzungsbedarf ergibt sich jedoch aus Art. 10 RL (EU) 2016/680. Nach der jüngeren Rechtsprechung des EuGH muss die zuständige Behörde begründen, aus welchen Gründen die Verarbeitung biometrischer Daten im konkreten Fall unbedingt erforderlich ist; eine nachträgliche gerichtliche Kontrolle kann diese behördliche Begründung nicht ersetzen.⁷⁹ Die Dokumentationspflicht nach § 98d Abs. 2 StPO-E sollte sich deshalb auch auf die Gründe für die Erforderlichkeit erstrecken. Eine vollständige technische Reproduzierbarkeit des Abgleichs oder gar die Speicherung sämtlicher erfolglos verarbeiteter Vergleichsdaten ist dagegen nicht geboten und stünde mit der Löschungspflicht des Abs. 3 in Spannung.

Nicht überzeugend ist ferner die Forderung, automatisiert erzeugte Treffer generell von einer späteren Beweisverwertung auszuschließen und lediglich als Spurenansatz zuzulassen.⁸⁰ Ein automatisierter Treffer bedarf vielmehr der fachlichen Überprüfung durch die Ermittlungsbehörden und unterliegt im gerichtlichen Verfahren der freien Beweiswürdigung. Fehlerwahrscheinlichkeit und mangelnde Nachvollziehbarkeit können den Beweiswert mindern; ein generelles gesetzliches Verwertungsverbot folgt daraus nicht.

Auch die weitere Verwendung relevanter Treffer ist hinreichend eingeeht. § 98d Abs. 3 StPO-E erlaubt zwar, von einer sofortigen Löschung abzusehen, wenn sich ein konkreter Ermittlungsansatz für ein anderes Strafverfahren ergibt. Eine voraussetzungslose Weiterverwendungsmöglichkeit wird dadurch aber nicht eröffnet: Über § 479 Abs. 2 Satz 1 i.V.m. § 161 Abs. 3 StPO gilt der Grundsatz der **hypothetischen Datenneuerhebung**. Daneben bleibt § 101 Abs. 8 StPO anwendbar; auch zunächst relevante Daten sind zu löschen, sobald sie für Strafverfolgung und gerichtliche Kontrolle nicht mehr erforderlich sind.⁸¹

c) Anordnung, Benachrichtigung und Rechtsschutz

Nach § 98d Abs. 4 StPO-E wird der biometrische Abgleich grundsätzlich durch die Staatsanwaltschaft und bei Gefahr im Verzug deren Ermittlungspersonen angeordnet. Anders als der Entwurf von 2024 sieht die Vorschrift damit keinen Richtervorbehalt mehr vor.

⁷⁶ EuGH, Urt. v. 26.1.2023 – C-205/21 – Ministerstvo na vatreshnite raboti, Rn. 121 ff., 135; EuGH, Urt. v. 19.3.2026 – C-371/24 – Comdribus, Rn. 23 ff., insb. Rn. 35 f.

⁷⁷ Zur unionsrechtskonformen Auslegung allgemein BVerfG, Beschl. v. 26.9.2011 – 2 BvR 2216/06 u.a. –, Rn. 46 f.

⁷⁸ DRB, Stellungnahme Nr. 9/2026, S. 3.

⁷⁹ EuGH, Urt. v. 19.3.2026 – C-371/24 – Comdribus, Rn. 68, 72 ff.

⁸⁰ DAV, Stellungnahme Nr. 26/2026, S. 3, 10.

⁸¹ BT-Drs. 21/6806, S. 25.

Dieser Verzicht auf eine vorherige richterliche Entscheidung wird in den Stellungnahmen teilweise kritisch gesehen.⁸² **Auch unter Berücksichtigung des vorstehend bestimmten und in Bezug auf die Sachverhaltserforschung erhöhten Eingriffsgewichts ist eine vorherige richterliche Entscheidung verfassungsrechtlich nicht zwingend.** Nach der Rechtsprechung des Bundesverfassungsgerichts hängt das Erfordernis einer unabhängigen Vorabkontrolle maßgeblich vom Eingriffsgewicht ab.⁸³ Erst bei schwerwiegenden heimlichen Grundrechtseingriffen ist eine vorbeugende Kontrolle durch eine unabhängige Instanz erforderlich; bei Eingriffen von besonders hohem Gewicht verdichtet sich diese Anforderung grundsätzlich zu einem Richtervorbehalt.⁸⁴ Maßgeblich ist neben der Heimlichkeit insbesondere, ob besonders geschützte Bereiche der Privatheit berührt werden oder typischerweise mit der Erfassung höchstprivater Informationen zu rechnen ist.⁸⁵ Bei weniger eingriffsintensiven heimlichen Maßnahmen besteht demgegenüber kein generelles Erfordernis einer unabhängigen Vorabkontrolle; maßgeblich bleibt die konkrete Eingriffsintensität.⁸⁶

Diese Schwelle erreicht der biometrische Abgleich nach § 98d StPO-E auch unter Berücksichtigung der vorstehend unterschiedenen Einsatzkonstellationen nicht. Bei der Identitätsfeststellung und Aufenthaltsermittlung eines Beschuldigten ist der Erkenntniszweck eng begrenzt; verarbeitet werden ausschließlich öffentlich zugängliche Vergleichsdaten, und ein Echtzeitabgleich ist ausgeschlossen. Auch die weitergehende Sachverhaltserforschung erhöht zwar das Eingriffsgewicht, führt aber nicht typischerweise zur Erfassung höchstprivater Informationen oder zum Eindringen in besonders geschützte Bereiche der Privatheit. Dem erhöhten Erkenntnispotential ist – wie vorstehend ausgeführt – durch die Beschränkung auf schwere Straftaten Rechnung zu tragen; ein Richtervorbehalt könnte deren Fehlen ohnehin nicht kompensieren.⁸⁷ Dieser ist nicht dazu geeignet, die Mängel einer zu unbestimmt geregelten oder zu niedrig angesetzten Eingriffsschwelle auszugleichen, da auch die unabhängige Prüfungsinstanz nur sicherstellen kann, dass die geregelten Eingriffsvoraussetzungen eingehalten werden.⁸⁸ Auch Art. 26 Abs. 10 KI-VO fordert bei nachträglicher biometrischer Fernidentifizierung eine bindende und justiziell überprüfbare Entscheidung einer Justiz- oder Verwaltungsbehörde, nicht zwingend einen Richtervorbehalt.

II. Einführung des § 98e StPO-E – Automatisierte verfahrensübergreifende Datenanalyse

1. Regelungskonzept und praktische Bedeutung

Mit § 98e StPO-E soll erstmals eine ausdrückliche strafprozessuale Rechtsgrundlage für die automatisierte verfahrensübergreifende Datenanalyse geschaffen werden. Bei Verdacht einer in § 100a Abs. 2 StPO bezeichneten schweren Straftat, die auch im Einzelfall schwer wiegt, dürfen rechtmäßig gespeicherte und bereits für eine polizeiliche Analyseplattform zusammengeführte personenbezogene Daten automatisiert zur Aufklärung der Tat oder zur Aufenthaltsermittlung weiterverarbeitet werden.

⁸² Zöller, ZRP 2026, 128, 130 f.; DAV, Stellungnahme Nr. 26/2026, S. 9 f.; BRAK, Stellungnahme Nr. 21/2026, S. 9; Strafverteidigervereinigungen, Stellungnahme v. 6.4.2026, S. 3 f.; eco, Stellungnahme v. 2.4.2026, S. 2.

⁸³ BVerfGE 162, 1 Rn. 217 (Bayerisches Verfassungsschutzgesetz).

⁸⁴ BVerfGE 162, 1 Rn. 214, 217 (Bayerisches Verfassungsschutzgesetz); BVerfGE 120, 274 Rn. 259 (Online-Durchsuchung); BVerfGE 165, 1 Rn. 149 (Polizeiliche Befugnisse nach SOG MV).

⁸⁵ BVerfGE 162, 1 Rn. 217 f. (Bayerisches Verfassungsschutzgesetz); BVerfGE 155, 119 Rn. 253 (Bestandsdatenauskunft II).

⁸⁶ BVerfGE 162, 1 Rn. 217, 219 (Bayerisches Verfassungsschutzgesetz).

⁸⁷ BVerfGE 120, 274 Rn. 258 (Online-Durchsuchung); BVerfGE 110, 33 Rn. 149 f. (Zollkriminalamt).

⁸⁸ BVerfGE 110, 33 Rn. 149 f. (Zollkriminalamt).

Konzeptionell baut § 98e StPO-E auf bereits bestehenden polizeilichen Analyseplattformen auf. Die Vorschrift ermächtigt nicht selbst zur erstmaligen Zusammenführung sämtlicher Polizeidaten, sondern gestattet die automatisierte Auswertung bereits rechtmäßig gespeicherter und zusammengeführter Daten für ein konkretes Strafverfahren. Für Daten aus besonders eingriffsintensiven Maßnahmen sieht § 98e Abs. 2 StPO-E zusätzliche Begrenzungen vor: Die in Satz 2 bezeichneten Daten dürfen nur ergänzend und bei Erforderlichkeit einbezogen werden; Daten aus Online-Durchsuchungen und akustischen Wohnraumüberwachungen anderer Verfahren sind nach Satz 3 von der Analyse ausgeschlossen. Eine unmittelbare Anbindung an nichtpolizeiliche Register oder Internetdienste ist unzulässig.⁸⁹

Für die Schaffung einer solchen Befugnis besteht ein erhebliches praktisches Bedürfnis. Die operative IT-Infrastruktur der Polizeibehörden beruht teilweise noch auf einem unverbundenen Nebeneinander zahlreicher Dateien und Datenquellen, die bislang einzeln abgefragt und ausgewertet werden müssen. Eine Analyseplattform kann demgegenüber vorhandene Datenbestände systematisch erschließen und insbesondere in komplexen Verfahren Zusammenhänge sichtbar machen, die durch isolierte Einzelabfragen nur mit erheblichem Aufwand erkannt würden.⁹⁰ **Die Schaffung einer solchen Ermächtigung für die automatisierte verfahrensübergreifende Datenanalyse ist daher uneingeschränkt zu begrüßen.**

2. Kritiklinien in Literatur und Stellungnahmen

Wegen ihres eigenständigen Erkenntnispotentials und der Breite der einbezieharen Datenbestände wird die automatisierte verfahrensübergreifende Datenanalyse aber teilweise erheblich kritisiert.⁹¹ Beanstandet wird insbesondere, dass die Analyse auf umfangreiche, bereits verfahrensübergreifend zusammengeführte Polizeidaten zugreifen kann und dabei auch Daten von Zeugen, Geschädigten und unbeteiligten Dritten sowie Ergebnisse eingriffsintensiver Ermittlungsmaßnahmen einbezogen werden können.⁹² Die vorgelagerte, vom Einzelfall unabhängige Zusammenführung solcher Daten auf einer Analyseplattform wird als unzulässige „Superdatenbank“ angesehen; insbesondere werden fehlende eigenständige Speicherschwellen, Zweckbegrenzungen und Speicherfristen beanstandet.⁹³ Daneben werden die Eingriffsschwelle des § 98e Abs. 1 StPO-E, insbesondere die Anknüpfung an den Straftatenkatalog des § 100a Abs. 2 StPO, das Fehlen einer besonderen Anordnungsregel sowie die Anforderungen an Dokumentation, Nachvollziehbarkeit und Kontrolle beanstandet.⁹⁴

Im Kern konzentriert sich die Kritik damit auf die Frage, ob die in § 98e Abs. 1 bis 6 StPO-E vorgesehenen Begrenzungen dem erheblichen Erkenntnispotential der verfahrensübergreifenden automatisierten Datenanalyse verfassungsrechtlich hinreichend Rechnung tragen.

⁸⁹ § 98e Abs. 3 StPO-E; BT-Drs. 21/6806, S. 20 f.

⁹⁰ BT-Drs. 21/6806, S. 1 f.

⁹¹ BfDI, Stellungnahme v. 2.6.2026, S. 14 ff.; BRAK, Stellungnahme Nr. 21/2026, S. 17 ff.; eco, Stellungnahme v. 2.4.2026, S. 2 f.; AG KRITIS/AlgorithmWatch/Amnesty International u.a., Gemeinsame Stellungnahme v. 1.4.2026, S. 2 ff. Kritisch auch Botta, Verfassungsblog v. 1.9.2026; Brüning, Verfassungsblog v. 3.9.2026. Zustimmung dagegen DRB, Stellungnahme Nr. 9/2026, S. 4 f.; GdP, Stellungnahme v. 1.4.2026, S. 4 f.; DPoIG, Stellungnahme v. 31.3.2026, S. 2.

⁹² BfDI, Stellungnahme v. 2.6.2026, S. 18 f.; DAV, Stellungnahme Nr. 26/2026, S. 4, 12 ff.; eco, Stellungnahme v. 2.4.2026, S. 3.

⁹³ BfDI, Stellungnahme v. 2.6.2026, S. 15 f.; Botta, Verfassungsblog v. 1.9.2026.

⁹⁴ BfDI, Stellungnahme v. 2.6.2026, S. 20 f.; DAV, Stellungnahme Nr. 26/2026, S. 4, 12 ff.; AG KRITIS/AlgorithmWatch/Amnesty International u.a., Gemeinsame Stellungnahme v. 1.4.2026, S. 4 f.; BRAK, Stellungnahme Nr. 21/2026, S. 18.

3. Verfassungsrechtliche Bewertung

a) Verfassungsrechtliche Grundsätze

Den maßgeblichen verfassungsrechtlichen Ausgangspunkt bildet das Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 zu § 25a HSOG a.F. und § 49 HmbPolDVG a.F., in dem das Gericht die automatisierte Datenanalyse als solche nicht beanstandete, die angegriffenen Regelungen aber für verfassungswidrig erachtete, weil sie angesichts ihrer nur geringen Begrenzung Eingriffe von sehr hohem Gewicht ermöglichten, ohne diese an entsprechend qualifizierte Eingriffsvoraussetzungen zu binden.⁹⁵ Hinsichtlich der maßgeblichen Kriterien kann auf die vorstehenden Ausführungen verwiesen werden.⁹⁶

Nicht Gegenstand dieser Entscheidung war allerdings die verfassungsrechtliche Rechtfertigung einer vorgelagerten, vom konkreten Analyseanlass unabhängigen Zusammenführung und Vorhaltung eines Analysedatenbestands.⁹⁷ An einen solchen Datenbestand knüpft § 98e StPO-E nunmehr aber ausdrücklich an. **Die vorgelagerte Speicherung und die spätere automatisierte Analyse stellen eigenständige Verarbeitungsschritte und Grundrechtseingriffe dar, die jeweils gesondert zu rechtfertigen sind.**⁹⁸ Die vorgelagerte Speicherung ist für die Bewertung des § 98e StPO-E gleichwohl von unmittelbarer Bedeutung: Sie bestimmt, welche Daten in welchem Umfang für spätere Analysen verfügbar sind. Da vor allem Art und Umfang der verarbeitbaren Daten das Eingriffsgewicht prägen⁹⁹, wirkt die Ausgestaltung der vorgelagerten Speicherung unmittelbar auf das Gewicht der späteren automatisierten Analyse zurück.

Die verfassungsrechtlichen Anforderungen an eine vorgelagerte Speicherung personenbezogener Daten für eine erst künftig mögliche Nutzung hat das Bundesverfassungsgericht in einer jüngeren Entscheidung näher präzisiert.¹⁰⁰ Dabei behandelt das Gericht bereits diese vorsorgende Speicherung als Zweckänderung.¹⁰¹ Sie ist nur zulässig, wenn Speicherzweck, Speicherschwelle und Speicherdauer gesetzlich hinreichend bestimmt sind. **Unzulässig ist insbesondere ein offener Datenvorrat, der lediglich deshalb vorgehalten wird, weil die Daten künftig noch benötigt werden könnten.**¹⁰²

b) Anwendung auf § 98e StPO-E

Bei Anwendung dieser Grundsätze genügt § 98e StPO-E den verfassungsrechtlichen Anforderungen nicht in jeder Hinsicht. Bedenken bestehen zum einen hinsichtlich der **zweckändernden Einbeziehung bereits erhobener Daten**, weil die Vorschrift nicht durchgängig einen hinreichend spezifischen Bezug der verwendeten Daten zum konkreten Ermittlungsverfahren verlangt. Zum anderen trägt die in § 98e Abs. 1 StPO-E vorgesehene Eingriffsschwelle dem eigenständigen Gewicht der automatisierten verfahrensübergreifenden Datenanalyse in der derzeitigen Ausgestaltung ohne Begrenzung des Datenraums nicht hinreichend Rechnung.

⁹⁵ BVerfGE 165, 363 Rn. 123 ff., 149 ff. (Automatisierte Datenanalyse).

⁹⁶ Siehe oben B. I. 3. a).

⁹⁷ Vgl. Botta, VerfBlog v. 1.9.2026.

⁹⁸ BVerfGE 169, 332 Rn. 90, 152 ff. (BKAG II).

⁹⁹ BVerfGE 165, 363 Rn. 78 (Automatisierte Datenanalyse).

¹⁰⁰ BVerfGE 169, 332 Rn. 90, 155 ff. (BKAG II).

¹⁰¹ BVerfGE 169, 332 Rn. 181 (BKAG II); hierzu etwa Thiel, JR 2025, 62, 66.

¹⁰² BVerfGE 169, 332 Rn. 183 (BKAG II).

aa) Zweckänderung und konkreter Ermittlungsansatz

§ 98e StPO-E genügt den verfassungsrechtlichen Anforderungen an die Zweckänderung aus zwei Gründen nicht vollständig.

Zum einen fehlt für die Verwendung der nach § 98e Abs. 2 Satz 1 StPO-E einbezogenen Daten ein hinreichend spezifischer Ermittlungsansatz. Soweit bereits erhobene personenbezogene Daten für die automatisierte Analyse in einem anderen Strafverfahren oder nach einem Wechsel vom gefahrenabwehrrechtlichen zum repressiven Verwendungszweck genutzt werden, liegt regelmäßig eine Zweckänderung vor.¹⁰³ Für diese genügt nicht allein, dass die Daten rechtmäßig gespeichert sind. Vielmehr muss sich aus den weiterzuverarbeitenden Daten selbst oder in Verbindung mit weiteren Erkenntnissen ein konkreter Ermittlungsansatz für das betreffende Verfahren ergeben.¹⁰⁴ Der nach § 98e Abs. 1 StPO-E erforderliche qualifizierte Tatverdacht hinsichtlich der Anlasstat ersetzt diesen auf die zweckändernd einbezogenen Daten bezogenen Ermittlungsansatz nicht. Einen solchen setzt § 98e Abs. 2 Satz 1 StPO-E nicht voraus. Die Analyse könnte insoweit ohne einen konkreten Ermittlungsansatz aus den einbezogenen Daten erfolgen und diene dann aber erst dazu, einen solchen Ansatz zu generieren. Dies genügt verfassungsrechtlich gerade nicht.

Zum anderen sieht der Entwurf in Absatz 2 Satz 2 für die dort näher bezeichneten besonders sensiblen Daten zwar eine zusätzliche Begrenzung vor; auch diese bleibt jedoch mit dem gesetzlichen Erfordernis bloßer Erforderlichkeit hinter den Anforderungen an einen hinreichend spezifischen Bezug zum konkreten Ermittlungsverfahren zurück. Daten aus den dort bezeichneten eingriffsintensiven Maßnahmen und aus Asservaten dürfen zwar ergänzend einbezogen werden, „soweit dies im Einzelfall erforderlich ist“. Die Entwurfsbegründung konkretisiert dies dahin, dass bereits vor Kenntnis des Dateninhalts tatsächliche Anhaltspunkte dafür bestehen müssen, dass die betreffenden Daten mit dem konkreten Suchanlass in Verbindung stehen könnten.¹⁰⁵ Diese Begrenzung genügt den verfassungsrechtlichen Anforderungen jedoch nicht. Das Bundesverfassungsgericht hat in seiner BKAG-II-Entscheidung, wenn auch in einem anderen Zusammenhang¹⁰⁶, festgestellt, dass eine „nicht näher angeleitete Prüfung der Erforderlichkeit“ wegen ihrer Offenheit nicht den verfassungsrechtlich gebotenen Differenzierungsgrad gewährleistet.¹⁰⁷ Auch die nach der Entwurfsbegründung vorgesehene, an kriminalistischen Kriterien orientierte Vorauswahl der einzubeziehenden Datenbestände¹⁰⁸ beseitigt dieses Regelungsdefizit nicht. Es bleibt unklar, anhand welcher gesetzlichen Kriterien diese Vorauswahl vorzunehmen ist und wie sichergestellt wird, dass nur solche Daten in die Analyse einbezogen werden, die den verfassungsrechtlich erforderlichen Bezug zum konkreten Ermittlungsansatz aufweisen.

bb) Eingriffsgewicht und Anforderungen an die Eingriffsschwelle

§ 98e StPO-E unterscheidet sich in wesentlichen Punkten von den vom Bundesverfassungsgericht beanstandeten § 25a HSOG a.F. und § 49 HmbPolDVG a.F. Deren entscheidendes Defizit bestand

¹⁰³ Vgl. BVerfGE 165, 363 Rn. 60 ff. (Automatisierte Datenanalyse).

¹⁰⁴ BVerfGE 165, 363 Rn. 62 (Automatisierte Datenanalyse); BVerfGE 169, 332 Rn. 138 f. (BKAG II); grundlegend zur hypothetischen Datenerhebung BVerfGE 141, 220 Rn. 284 ff. (BKAG I).

¹⁰⁵ BT-Drs. 21/6806, S. 20.

¹⁰⁶ Dort ging es um die vorsorgende Speicherung von Grunddaten Beschuldigter; das Bundesverfassungsgericht beanstandete, dass die Beschuldigteneigenschaft in Verbindung mit einer bloßen Erforderlichkeitsprüfung keinen hinreichend bestimmten tatsächlichen Bezug zu künftig zu verhütenden oder zu verfolgenden Straftaten gewährleistete, BVerfGE 169, 332 Rn. 195 ff. (BKAG II).

¹⁰⁷ BVerfGE 169, 332 Rn. 198 (BKAG II).

¹⁰⁸ BT-Drs. 21/6806, S. 21 f.

darin, dass sie Art und Umfang der für die konkrete Analyse verwendbaren Daten kaum begrenzten und zugleich rechtlich nahezu unbegrenzte Analysemethoden ermöglichten.¹⁰⁹

Insbesondere sind die zulässigen Analysemethoden deutlich stärker begrenzt. § 98e Abs. 4 StPO-E enthält eine abschließende Beschreibung der zulässigen Verarbeitungsvorgänge. Zwar können datei- und informationssystemübergreifend Beziehungen und Zusammenhänge identifiziert, klassifiziert, strukturell analysiert und visualisiert, Informationen gefiltert, Erkenntnisse bekannten Sachverhalten zugeordnet, Suchkriterien gewichtet und Daten statistisch ausgewertet werden. Anders als die vom Bundesverfassungsgericht beurteilten landespolizeirechtlichen Regelungen eröffnet § 98e StPO-E jedoch keine allgemeine Befugnis zum Einsatz beliebiger technisch verfügbarer Analysemethoden. Jeder Analysevorgang muss anlassbezogen und manuell ausgelöst werden und anhand von Suchkriterien erfolgen, die sich aus einem konkreten Sachverhalt ergeben. Die Analyse dient der Aufbereitung und Bereitstellung von Daten für eigene Bewertungen und Entscheidungen der Strafverfolgungsbehörden; eine ausschließlich auf der automatisierten Datenanalyse beruhende Entscheidung mit unmittelbar nachteiliger Rechtsfolge oder erheblicher Beeinträchtigung ist ausgeschlossen. Hinzu treten das Verbot diskriminierender Algorithmen sowie die Begründungs- und Protokollierungspflichten nach Absatz 5. Damit werden wesentliche der vom Bundesverfassungsgericht als eingriffsrelevant bezeichneten Gesichtspunkte der Offenheit, Nachvollziehbarkeit und Kontrollierbarkeit automatisierter Analyse normativ begrenzt. Der Einsatz künstlicher Intelligenz oder selbstlernender Systeme wird allerdings nicht generell ausgeschlossen; nach der Entwurfsbegründung können KI-Systeme und Sprachmodelle innerhalb der in Absatz 4 gezogenen methodischen Grenzen eingesetzt werden.

Auf der Datenseite verbleibt demgegenüber ein außerordentlich weitreichendes Eingriffspotential. Absatz 2 erfasst neben Daten aus polizeilichen Informationssystemen und dem polizeilichen Informationsaustausch insbesondere auch Vorgangs- und Falldaten. Vorgangsbearbeitungssysteme können dabei Daten von Geschädigten, Zeugen, Hinweisgebern und sonstigen Personen enthalten, die selbst keinen Anlass für strafrechtliche Ermittlungsmaßnahmen gegeben haben und teilweise lediglich zu Zwecken der Vorgangsverwaltung oder Dokumentation gespeichert werden. Der hierdurch eröffnete Datenraum kann dementsprechend erheblich sein.

Zwar bestehen für Teile der von § 98e StPO-E erfassten Daten durchaus materielle Begrenzungen. So ist die vorsorgende Speicherung im polizeilichen Informationsverbund an die Voraussetzungen der §§ 29 ff. BKAG gebunden. § 30 BKAG begrenzt die Verbundrelevanz, § 30a Abs. 2 BKAG stellt für die vorsorgende Speicherung von Daten Beschuldigter und Tatverdächtiger zusätzliche Anforderungen, und § 77 Abs. 7 und 8 BKAG sehen besondere Aussonderungsprüffristen vor. Der für Analysen verfügbare polizeiliche Datenbestand ist deshalb nicht schlechthin rechtlich unbegrenzt, auch wenn nicht zweifelsfrei erscheint, ob die zwischenzeitlich eingeführten Regelungen die Anforderungen aus der BKAG II-Entscheidung vollständig umsetzen.¹¹⁰ **Eine entsprechende Einhegung ist jedoch für den gesamten von § 98e StPO-E eröffneten Datenraum nicht gewährleistet, weil die vorgenannten Regelungen nur für Daten im polizeilichen Informationsverbund gelten.** Soweit für einzelne Datenbestände lediglich allgemeine Aussonderungsprüffristen greifen, gewährleisten

¹⁰⁹ BVerfGE 165, 363 Rn. 123 ff., 152 ff. (Automatisierte Datenanalyse).

¹¹⁰ Vgl. kritisch etwa Rossi, Stellungnahme zu BT-Drs. 21/324 und 21/325, Ausschussdrucks. 21(4)013 F, S. 3 f.; Arzt, Stellungnahme zu BT-Drs. 21/324 und 21/325, Ausschussdrucks. 21(4)013 C, S. 5 ff., 8 ff.; ferner BfDI, Stellungnahme zu BT-Drs. 21/324 und 21/325, Ausschussdrucks. 21(4)013 A; demgegenüber etwa Moldenhauer, Ausschussdrucks. 21(4)013 B.

auch diese für sich genommen keine hinreichende Begrenzung. Zu § 77 Abs. 1 BKAG hat das Bundesverfassungsgericht ausdrücklich festgestellt, dass gesetzliche Höchstfristen für die Prüfung der Löschungspflichten kein hinreichend ausdifferenziertes Regelungskonzept ersetzen, wenn die nähere Konkretisierung der Prüfungs- und Aussonderungsfristen innerbehördlichen Vorgaben überlassen bleibt.¹¹¹ Hinzu kommt, dass § 98e StPO-E auf Datenbestände unterschiedlicher Polizeibehörden und damit auf Daten zugreifen kann, deren Speicherung unterschiedlichen gesetzlichen Regelungen unterliegt.

Soweit § 98e StPO-E im Ausgangspunkt voraussetzt, dass die Daten „rechtmäßig gespeichert“ und bereits für eine polizeiliche Analyseplattform zusammengeführt worden sind, führt dies nicht weiter. Die bloße Rechtmäßigkeit der jeweiligen Ausgangsspeicherung gewährleistet nicht, dass der hieraus zusammengeführte Gesamtbestand seinerseits in einer Weise begrenzt ist, die seiner späteren verfahrensübergreifenden automatisierten Nutzung Rechnung trägt. Entscheidend ist, ob der hieraus für künftige Analysen vorgehaltene Gesamtbestand den verfassungsrechtlichen Anforderungen an eine solche vorsorgende Datenhaltung genügt.

Auch § 98e Abs. 6 StPO-E führt insoweit zu keiner durchgreifenden zusätzlichen Begrenzung. Zwar bleiben danach „im Übrigen“ das für die speichernde Stelle geltende Datenverarbeitungsrecht einschließlich der Übermittlungs- und Verwendungsregelungen unberührt und ist dessen Einhaltung technisch und organisatorisch sicherzustellen. Soweit § 98e StPO-E selbst die Einbeziehung bestimmter Datenbestände gestattet, lässt sich daraus jedoch keine einheitliche materielle Begrenzung des für die Analyse verfügbaren Gesamtbestands ableiten.¹¹²

Damit ist nicht für den gesamten Analysedatenbestand gewährleistet, dass die vom Bundesverfassungsgericht geforderten Anforderungen an einen hinreichend bestimmten Speicherzweck, eine den Zusammenhang zwischen Daten und Speicherzweck sichernde Speicherschwelle sowie eine angemessene Speicherdauer eingehalten werden. Unzulässig ist insbesondere ein „seiner Zwecksetzung nach offene[r] Datenvorrat“, dessen spätere Nutzung erst nach Bedarf bestimmt wird.¹¹³

Da das Eingriffsgewicht der automatisierten Analyse vor allem durch Art und Umfang der verarbeitbaren Daten bestimmt wird,¹¹⁴ kann die nach § 98e StPO-E zugelassene Datenanalyse bei Ausschöpfung des eröffneten Datenraums ein sehr hohes eigenständiges Eingriffsgewicht erreichen. In der Gesamtschau vermögen auch die erheblichen methodischen Begrenzungen des § 98e Abs. 4 und 5 StPO-E dieses Gewicht nur begrenzt zu mindern. Sie begrenzen, wie die vorhandenen Daten ausgewertet werden dürfen, nicht aber entscheidend, welche und wie viele personenbezogenen Daten der Analyse zugänglich sind. Bei einer solchen Ausschöpfung des eröffneten Datenraums genügt die vorgesehene Eingriffsschwelle nicht.

¹¹¹ BVerfGE 169, 332 Rn. 202 f. (BKAG II).

¹¹² BfDI, Stellungnahme v. 2.6.2026, S. 17 f.

¹¹³ BVerfGE 169, 332 Rn. 182 f. (BKAG II).

¹¹⁴ BVerfGE 165, 363 Rn. 78 (Automatisierte Datenanalyse).

c) Folgerungen

aa) Erforderliche Nachbesserungen

Aus den Anforderungen an die Zweckänderung folgt zunächst ein Nachbesserungsbedarf bei der Auswahl der einbeziehbaren Daten. § 98e StPO-E muss gesetzlich hinreichend bestimmt vorgeben¹¹⁵, dass zweckändernd verwendete Daten einen hinreichend spezifischen Bezug zu dem konkreten Strafverfahren aufweisen. Für § 98e StPO-E bietet es sich daher an, die Einbeziehung zweckändernd verwendeter Daten davon abhängig zu machen, dass bestimmte Tatsachen einen konkreten Bezug der betreffenden Daten zur Anlasstat, zum Beschuldigten oder zu einem sonstigen aufklärungsrelevanten Sachverhalt begründen. Für die besonders sensiblen Daten des Abs. 2 Satz 2 sollte die bislang lediglich verlangte Erforderlichkeit entsprechend konkretisiert werden. Die erforderliche Begrenzung wirkt zugleich auf das Eingriffsgewicht der Analyse zurück, weil sie den Kreis der im konkreten Verfahren einbeziehbaren Daten reduziert.

Daneben bedarf der für spätere Analysen vorgehaltene Grunddatenbestand einer eigenständigen normativen Einhegung. Eine erst nach Eintritt der Voraussetzungen des § 98e StPO-E erfolgende Zusammenführung der Daten wäre zwar grundrechtsschonender, entspräche jedoch nicht dem Regelungskonzept des Entwurfs und würde den mit der vorgelagerten Zusammenführung bezweckten Effizienzgewinn weitgehend verfehlen. § 98e StPO-E setzt deshalb gerade auf einen bereits vorhandenen und technisch aufbereiteten Analysebestand auf.

Soll das dem Entwurf zugrunde liegende Konzept eines bereits zusammengeführten und technisch aufbereiteten Datenbestands beibehalten werden, müssen Speicherzweck, Speicherschwelle und Speicherdauer hinreichend bestimmt geregelt sein.

Dies betrifft insbesondere die Frage, welche Datenarten und Personengruppen unter welchen tatsächlichen Voraussetzungen in den Analysebestand aufgenommen und wie lange sie dort vorgehalten werden dürfen. Der verfassungsrechtliche Nachbesserungsbedarf liegt daher nicht in einem Verzicht auf die vorgelagerte Speicherung, sondern in ihrer hinreichenden gesetzlichen Begrenzung. Konkrete Anhaltspunkte, wie eine solche Differenzierung gesetzlich ausgestaltet werden kann, lassen sich der BKAG-II-Entscheidung selbst entnehmen. Das Bundesverfassungsgericht nennt dort für die von ihm beurteilte vorsorgende Speicherung als mögliche Kriterien der Speicherschwelle insbesondere Art, Schwere und Begehungsweise der früheren Tat, die Persönlichkeit und das bisherige strafrechtliche Erscheinungsbild des Betroffenen, Häufigkeit und Ausmaß früherer Straffälligkeit sowie die Dauer zwischenzeitlicher Straffreiheit. Die erforderliche Wahrscheinlichkeit kann danach personen-, phänomen- oder tatbezogen begründet werden; auch eine Ausrichtung an bestimmten Delikts- oder Phänomenbereichen kommt in Betracht.¹¹⁶

Werden sowohl die vorgelagerte Speicherung als auch die zweckändernde Einbeziehung der Daten hinreichend eingegregelt, reduziert sich zugleich das Eingriffsgewicht der automatisierten Analyse. **Unter dieser Voraussetzung erscheint die in § 98e Abs. 1 StPO-E vorgesehene Eingriffsschwelle grundsätzlich tragfähig.** Sie verlangt den Verdacht einer in § 100a Abs. 2 StPO bezeichneten Straftat, die auch im Einzelfall schwer wiegt. Bei einem durch die beschriebenen datenbezogenen

¹¹⁵ Vgl. BVerfGE 165, 363 Rn. 61 f., 118 (Automatisierte Datenanalyse); BVerfGE 169, 332 Rn. 138 f. (BKAG II).

¹¹⁶ BVerfGE 169, 332 Rn. 186 (BKAG II).

Begrenzungen verminderten Eingriffsgewicht erscheint eine generelle Beschränkung auf den engen Katalog des § 100b Abs. 2 StPO nicht erforderlich.

Nachbesserungsbedarf verbleibt jedoch innerhalb des Katalogs des § 100a Abs. 2 StPO. Der Katalog erfasst auch Straftatbestände, die ihrem abstrakten Gewicht nach dem Bereich einfacher Kriminalität zuzurechnen sind. Das Bundesverfassungsgericht hat zuletzt hervorgehoben, dass ein unzureichendes abstraktes Tatgewicht nicht dadurch kompensiert werden kann, dass die Tat im Einzelfall schwer wiegen muss.¹¹⁷ Soll § 100a Abs. 2 StPO als Ausgangspunkt beibehalten werden, sind deshalb jedenfalls diejenigen Katalogtaten auszunehmen, die bereits abstrakt kein hinreichendes Gewicht für die automatisierte verfahrensübergreifende Datenanalyse aufweisen.

bb) Weiterentwicklung zu einem abgestuften Eingriffsmodell

Die Rechtsprechung des Bundesverfassungsgerichts begrenzt die Ausgestaltung automatisierter Datenanalysen auf mehreren, aufeinander bezogenen Ebenen. Bereits der für spätere Analysen vorgehaltene Datenbestand muss auf einer hinreichend bestimmten gesetzlichen Grundlage beruhen und insbesondere nach Speicherzweck, Speicherschwelle und Speicherdauer begrenzt sein. Auf einer zweiten Stufe muss die Einbeziehung der gespeicherten Daten in den konkreten Analysevorgang den Anforderungen der Zweckbindung und Zweckänderung genügen; zweckändernd verwendete Daten dürfen danach nur bei einem hinreichend spezifischen Bezug zum konkreten Ermittlungsverfahren herangezogen werden. Auf einer dritten Stufe greifen die Begrenzungen der eigentlichen automatisierten Analyse, insbesondere hinsichtlich der zulässigen Analysemethoden sowie der verfahrensrechtlichen und technisch-organisatorischen Sicherungen.

Diese auf den verschiedenen Ebenen ansetzenden Begrenzungen sind verfassungsrechtlich geboten; sie beschränken bei einem undifferenzierten Einstufenmodell aber zugleich die Leistungsfähigkeit der Analyse, nicht zuletzt deshalb, weil für die verfassungsrechtliche Beurteilung das durch die gesetzliche Ermächtigung eröffnete potentielle Eingriffsgewicht maßgeblich ist. Je geringer das Gewicht der Anlasstat ist, desto stärker muss das zulässige Eingriffsgewicht der Maßnahme begrenzt werden; insbesondere müssen Datenbestand und Analysemethoden entsprechend enger gefasst sein. Je stärker bereits die für die Ausgangsdaten geltenden Speicherregime den verfügbaren Datenbestand nach Speicherzweck, Speicherschwelle und Speicherdauer begrenzen, desto enger ist der für die Analyse erschließbare Datenraum.

Soll das Potential der automatisierten Datenanalyse ausgeschöpft werden, spricht deshalb viel für ein abgestuftes Regelungsmodell. Neben einer ersten, in Datenbestand und Methoden enger begrenzten Analysestufe könnten eine oder mehrere qualifizierte weitere Analysestufen vorgesehen werden, für die bei entsprechend höheren materiellen Voraussetzungen weitergehende Datenbestände einbezogen oder leistungsfähigere Analysemethoden zugelassen werden. Ein solches Modell würde das verfassungsrechtliche Wechselverhältnis zwischen Eingriffsgewicht und Eingriffsvoraussetzungen unmittelbar im Regelungskonzept abbilden.

Denkbar wäre insbesondere, eine der qualifizierten Analysestufen der Aufklärung schwerster Straftaten vorzubehalten. Als Anknüpfungspunkt könnte dienen, dass die Straftat überragend wichtige

¹¹⁷ BVerfGE 172, 106 Rn. 213 ff. (Trojaner II).

Rechtsgüter betrifft. Hierzu zählen insbesondere Leib, Leben und Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen menschlicher Existenz berührt.¹¹⁸ **Bei einer derart erhöhten Eingriffsschwelle könnten verfassungsrechtlich weitergehende Datenbestände oder leistungsfähigere Analysemethoden zulässig sein.**

4. Ausgewählte weitere Regelungsfragen

a) Zusammenführung und Einbeziehung der Daten

Der Bundesrat schlägt vor, § 98e Abs. 1 StPO-E um eine eigenständige strafprozessuale Befugnis zur Zusammenführung der Daten zu erweitern.¹¹⁹ Eine solche Ergänzung änderte das Regelungskonzept grundlegend. Der Entwurf erlaubt derzeit die strafprozessuale Weiterverarbeitung eines anderweitig bereits vorhandenen Datenbestands; eine eigenständige Befugnis zur Zusammenführung würde demgegenüber selbst die Grundlage für dessen Herstellung schaffen. Soll der so geschaffene Grunddatenbestand dauerhaft für spätere Analysen vorgehalten werden, bedürfte diese vorsorgende Speicherung nach den Maßstäben von „BKAG II“ einer hinreichenden gesetzlichen Begrenzung insbesondere nach Speicherzweck, Speicherschwelle und Speicherdauer. Zudem müsste bestimmt werden, welche Datenarten und Personengruppen unter welchen Voraussetzungen in den Bestand aufgenommen werden dürfen.¹²⁰ Der Vorschlag kann daher nicht lediglich als Ergänzung der Analysebefugnis umgesetzt werden, sondern müsste mit einem entsprechend ausgestalteten Speicherregime verbunden werden.

Nicht überzeugend ist die Auffassung der BfDI, bereits § 98e Abs. 3 StPO-E könne als Rechtsgrundlage für die dauerhafte Speicherung der dort genannten Daten auf einer Analyseplattform verstanden werden.¹²¹ Die Vorschrift regelt, welche zusätzlich erhobenen Datensätze in einen Analysevorgang einbezogen werden dürfen, und schließt insbesondere die unmittelbare Anbindung nichtpolizeilicher Register und von Internetdiensten aus. Eine Befugnis zur dauerhaften Speicherung dieser Daten lässt sich daraus nicht ableiten. Die daran anknüpfenden Fragen eines Eingriffs in landesrechtliche Speicherregime und der Gesetzgebungskompetenz stellen sich daher insoweit nicht.

Nicht zu folgen ist der Forderung der Bundesrechtsanwaltskammer, die Datenanalyse auf solche Daten zu beschränken, die in einem strafrechtlichen Ermittlungsverfahren in zulässiger Weise hätten erhoben werden dürfen.¹²² Das geltende Strafprozessrecht lässt die Verwendung auf präventiv-polizeilicher Grundlage gewonnener Daten im Strafverfahren zu. § 161 Abs. 3 StPO knüpft hierfür an die materiellen Voraussetzungen des hypothetischen Ersatzeingriffs an; der Bundesgerichtshof hat die Verwendung präventiv-polizeilich gewonnener Erkenntnisse im Strafverfahren auf dieser Grundlage dementsprechend ausdrücklich für zulässig erachtet.¹²³ Das verfassungsrechtliche Problem liegt auch nicht in der präventiven Herkunft der Daten, sondern in der hinreichenden Begrenzung des für die Analyse verfügbaren Datenbestands und der zweckändernden Einbeziehung der Daten in den konkreten Analysevorgang. Dies ist durch die vorstehend dargestellten Anforderungen an Speicherzweck, Speicherschwelle und Speicherdauer sowie an den konkreten Ermittlungsansatz aufzufangen.

¹¹⁸ BVerfGE 120, 274 Rn. 247 f. (Online-Durchsuchung); BVerfGE 165, 1 Rn. 179 (Polizeiliche Befugnisse nach SOG MV).

¹¹⁹ BT-Drs. 21/6806, S. 26 ff.

¹²⁰ BVerfGE 169, 332 Rn. 180–190 (BKAG II); vgl. auch Botta, VerfBlog v. 1.9.2026.

¹²¹ BfDI, Stellungnahme v. 2.6.2026, S. 17 f.

¹²² BRAK, Stellungnahme Nr. 21/2026, S. 16.

¹²³ BGHSt 62, 123 Rn. 38.

b) Besonders sensible Daten, § 98e Abs. 2 Satz 2 und 3 StPO-E

Zu begrüßen ist, dass § 98e Abs. 2 Satz 3 StPO-E Daten aus Online-Durchsuchungen und akustischen Wohnraumüberwachungen (§§ 100b, 100c StPO) anderer Verfahren vollständig von der Analyse ausschließt.¹²⁴ Keiner zusätzlichen Sonderregelung in § 98e StPO-E bedarf es grundsätzlich zum Schutz kernbereichsrelevanter Daten und solcher Daten, die dem Schutz von Berufsgeheimnisträgern unterliegen.¹²⁵ Entscheidend ist allerdings, dass die bereits für Erhebung, Speicherung und weitere Verwendung geltenden Schutz-, Verwendungs- und Löschungsregelungen tatsächlich durchgreifen. Daten, deren Speicherung oder weitere Verwendung unzulässig ist, dürfen auch nicht in die Analyse einbezogen werden.

c) Analysemethoden und Einsatz künstlicher Intelligenz

Die in § 98e Abs. 4 StPO-E vorgesehenen methodischen Begrenzungen sind im Grundsatz sachgerecht. Insbesondere muss jeder Analysevorgang anlassbezogen und manuell ausgelöst werden; die abschließende Bewertung der gewonnenen Erkenntnisse verbleibt bei den Strafverfolgungsbehörden, und diskriminierende Algorithmen dürfen weder herausgebildet noch verwendet werden.¹²⁶ Das Verbot ausschließlich automatisierter Entscheidungen darf allerdings nicht rein formal verstanden werden. Auch bei einer menschlichen Letztentscheidung besteht die Gefahr eines faktischen Automatisierungseffekts, wenn die vom System erzeugte Auswahl, Gewichtung oder Priorisierung den weiteren Entscheidungsprozess praktisch vorprägt.¹²⁷ Entscheidend bleibt deshalb, dass die gewonnenen Ergebnisse eigenständig fachlich bewertet und – soweit sie Grundlage weiterer Ermittlungsmaßnahmen werden sollen – hinreichend verifiziert werden.

Ein genereller Ausschluss künstlicher Intelligenz oder selbstlernender Systeme ist weder erforderlich noch wünschenswert. Es sollte jedoch sichergestellt sein, dass ein im operativen Einsatz befindliches System nicht anhand der jeweils analysierten personenbezogenen Echt Daten selbständig fortlaufend weiterlernt. Andernfalls können aus personenbezogenen Daten gewonnene Informationen im Modell fortwirken, obwohl die zugrunde liegenden Daten später zu löschen sind.¹²⁸

d) Dokumentation, Rechtsschutz und Anordnung

Die Begründungs- und Protokollierungspflichten des § 98e Abs. 5 StPO-E sind ein wesentliches Element der Nachvollziehbarkeit und Kontrolle automatisierter Datenanalysen. Sie sollten so ausgestaltet werden, dass der konkrete Analysevorgang nachträglich tatsächlich rekonstruiert werden kann. Neben den einbezogenen Datenbeständen sollten deshalb jedenfalls die verwendeten Suchbegriffe und -parameter, Analysefunktionen und wesentlichen Gewichtungen sowie gegebenenfalls die eingesetzte System- oder Modellversion dokumentiert werden. Nur so lässt sich nachvollziehen, auf welchem Weg ein für das weitere Ermittlungsverfahren relevanter Treffer zustande gekommen ist. Das Bundesverfassungsgericht misst einer eigenständigen Begründung und nachvollziehbaren Dokumentation für die Kontrolle automatisierter Datenanalysen besondere Bedeutung bei.¹²⁹

¹²⁴ DRB, Stellungnahme Nr. 9/2026, S. 4 f.; BRAK, Stellungnahme Nr. 21/2026, S. 19.

¹²⁵ BRAK, Stellungnahme Nr. 21/2026, S. 19.

¹²⁶ Vgl. DRB, Stellungnahme Nr. 9/2026, S. 5; GdP, Stellungnahme v. 1.4.2026, S. 5; DPoIG, Stellungnahme v. 31.3.2026, S. 2.

¹²⁷ Vgl. BRAK, Stellungnahme Nr. 21/2026, S. 19 f.; AG KRITIS, Stellungnahme v. 2.4.2026, S. 7, 14; AG KRITIS/AlgorithmWatch/Amnesty International u.a., Gemeinsame Stellungnahme v. 1.4.2026, S. 6; eco, Stellungnahme v. 2.4.2026, S. 2 f.

¹²⁸ Vgl. Bergemann/Kinz, VerBlog v. 1.9.2026.

¹²⁹ BVerfGE 165, 363 Rn. 109, 113 (Automatisierte Datenanalyse).

Eine darüber hinausgehende individuelle Benachrichtigung sämtlicher Personen, deren Daten in einen Analysevorgang einbezogen wurden, erscheint demgegenüber weder praktisch sachgerecht noch verfassungsrechtlich geboten.¹³⁰ Die verfahrensübergreifende Analyse kann Daten einer großen Zahl von Personen erfassen, ohne dass diese zum Gegenstand weiterer Ermittlungen werden. Eine Benachrichtigung allein aufgrund der technischen Einbeziehung ihrer Daten wäre deshalb kaum praktikabel. Soweit hierfür bislang nicht individualisierte Betroffene zunächst identifiziert werden müssten, könnte sie zudem zusätzliche Datenverarbeitungen und damit weitere Grundrechtseingriffe auslösen. Das Bundesverfassungsgericht verlangt für automatisierte Datenanalysen wirksame Transparenz-, Rechtsschutz- und Kontrollmechanismen, schreibt hierfür aber keine unterschiedslose individuelle Benachrichtigung sämtlicher technisch erfasster Personen vor.¹³¹

Schließlich ist auch ein **genereller Richtervorbehalt verfassungsrechtlich nicht zwingend**.¹³² Insofern kann auf die Ausführungen zu § 98d StPO-E verwiesen werden. Auch aus der Entscheidung zur automatisierten Datenanalyse ergibt sich kein allgemeines Erfordernis richterlicher Vorabkontrolle; maßgeblich sind vielmehr das Eingriffsgewicht, die materielle Einhegung der Befugnis und die Wirksamkeit der vorgesehenen Kontrollmechanismen. Eine richterliche Anordnung jedenfalls für Analysen unter Einbeziehung der besonders sensiblen Daten des § 98e Abs. 2 Satz 2 StPO-E wäre als zusätzliche rechtspolitische Sicherung erwägenswert, verfassungsrechtlich zwingend erscheint sie jedoch nicht.

III. Anpassung der Benachrichtigungs- und Rechtsschutzregelungen

Die vorgesehene Einbeziehung des § 98d StPO-E in das Benachrichtigungs- und Rechtsschutzregime des § 101 StPO trägt den verfassungsrechtlichen Anforderungen jedenfalls hinsichtlich der Zielperson der Maßnahme Rechnung. Bei heimlichen Datenverwendungen ist grundsätzlich sicherzustellen, dass diejenigen Personen nachträglich benachrichtigt werden, auf die sich die Maßnahme unmittelbar bezogen hat; andernfalls wäre effektiver Rechtsschutz regelmäßig nicht gewährleistet.¹³³ Dies betrifft bei § 98d StPO-E insbesondere die Person, deren biometrische Ausgangsdaten gezielt für den Abgleich verwendet werden. Ergänzend eröffnet § 101 Abs. 7 StPO die nachträgliche gerichtliche Überprüfung der Rechtmäßigkeit der Maßnahme und der Art und Weise ihres Vollzugs.

Eine weitergehende Benachrichtigung sämtlicher Personen, deren öffentlich zugängliche biometrische Daten erfolglos als Vergleichsmaterial verarbeitet wurden, wie sie teilweise gefordert wird¹³⁴, ist dagegen nicht verfassungsrechtlich geboten. Zwar werden deren Daten technisch gezielt in den Abgleich einbezogen; die betreffenden Personen sind jedoch nicht Ziel des behördlichen Erkenntnisinteresses und die Verarbeitung bleibt bei einem Nichttreffer folgenlos. Für lediglich mitbetroffene Personen lässt das Bundesverfassungsgericht abgestufte Benachrichtigungspflichten zu und berücksichtigt insbesondere, dass eine Benachrichtigung den Grundrechtseingriff vertiefen kann, wenn

¹³⁰ A.A. etwa AG KRITIS, Stellungnahme v. 2.4.2026, S. 7, 14.

¹³¹ Vgl. BVerfGE 165, 363 Rn. 109, 113 (Automatisierte Datenanalyse).

¹³² Für einen Richtervorbehalt BRAK, Stellungnahme Nr. 21/2026, S. 18; DAV, Stellungnahme Nr. 26/2026, S. 4; AG KRITIS/Algorithm-Watch/Amnesty International u.a., Gemeinsame Stellungnahme v. 1.4.2026, S. 4; Brüning, VerfBlog v. 3.9.2026.

¹³³ BVerfGE 125, 260 Rn. 244 f. (Vorratsdatenspeicherung); BVerfGE 129, 208 Rn. 229 (Neuregelung der Telekommunikationsüberwachung)

¹³⁴ Vgl. BRAK, Stellungnahme Nr. 21/2026, S. 10.

die betroffene Person hierfür erst identifiziert werden müsste.¹³⁵ **Eine generelle Benachrichtigungspflicht für erfolglos abgegliche Vergleichspersonen erscheint daher weder verfassungsrechtlich geboten noch sachgerecht.**

C. Änderungen des Bundeskriminalamtgesetzes

I. Automatisierter biometrischer Abgleich als Zentralstellenbefugnis (§ 9a BKAG-E)

1. Regelungskonzept und praktische Bedeutung

§ 9a BKAG-E überträgt den automatisierten biometrischen Internetabgleich auf die **Zentralstellen-**aufgabe des Bundeskriminalamts. Das BKA soll öffentlich zugängliche personenbezogene Daten mit biometrischen Merkmalen aus dem Internet erheben und automatisiert mit Daten abgleichen dürfen, auf die es zur Erfüllung seiner Aufgaben zugreifen darf. Die Maßnahme dient der Ergänzung bereits vorhandener Sachverhalte und kann insbesondere zur Identifizierung und Aufenthaltsermittlung, zur Sachverhaltserforschung sowie zur Ermittlung von Zusammenhängen mit anderen Straftaten oder Gefahren eingesetzt werden; eine erstmalige Gewinnung von Verdachts- oder Gefahrenmomenten soll dagegen nicht ermöglicht werden.¹³⁶

Anders als § 98d StPO-E erfasst § 9a BKAG-E repressive und präventive Sachverhalte und begrenzt den einbeziehenden Personenkreis näher. Für Zeugen, Opfer, Kontakt- und Auskunftspersonen ist der Abgleich nach § 9a Abs. 2 Nr. 2 BKAG-E auf Identifizierung und Aufenthaltsermittlung beschränkt. Für die verwendeten polizeilichen Ausgangsdaten gelten aufgrund des Abs. 3 Satz 1 die Anforderungen des § 12 Abs. 2 BKAG an die hypothetische Datenneuerhebung; Daten aus besonders eingriffsintensiven Maßnahmen nach § 12 Abs. 3 BKAG sind ausgeschlossen. Nicht relevante Daten sind grundsätzlich nach § 9a Abs. 4 Satz 1 BKAG-E unverzüglich zu löschen. Eine weitere Besonderheit besteht darin, dass der Abgleich unter zusätzlichen Voraussetzungen auch durch andere öffentliche oder nichtöffentliche Stellen sowie durch Stellen in Drittstaaten durchgeführt werden kann, § 9a Abs. 5 BKAG-E.

Der Befugnis kommt gerade im Rahmen der Zentralstellenaufgabe besondere praktische Bedeutung zu. Das Bundeskriminalamt hat die für diese Aufgabe erforderlichen Informationen zu sammeln und auszuwerten und die Polizeien des Bundes und der Länder bei der Kriminalitätsbekämpfung zu unterstützen. Die Entwurfsbegründung hebt deshalb zutreffend hervor, dass eine moderne Wahrnehmung dieser Aufgabe auch Informationen aus dem Internet einbeziehen muss.¹³⁷ Für die grundsätzliche praktische Bedeutung des biometrischen Internetabgleichs im Übrigen kann auf die Ausführungen zu § 98d StPO-E verwiesen werden.¹³⁸

2. Kritiklinien in Literatur und Stellungnahmen

Die gegen § 9a BKAG-E erhobene Kritik überschneidet sich in wesentlichen Punkten mit den Einwänden gegen § 98d StPO-E. Dies gilt insbesondere für die Streubreite des Internetabgleichs, die Verarbeitung ohne Zutun der Betroffenen veröffentlichter biometrischer Daten, Fehler- und Diskriminierungsrisiken sowie die Anforderungen an Subsidiarität, Transparenz und Kontrolle. Insoweit kann

¹³⁵ BVerfGE 125, 260 Rn. 245 (Vorratsdatenspeicherung); BVerfGE 129, 208 Rn. 227 (Neuregelung der Telekommunikationsüberwachung).

¹³⁶ BT-Drs. 21/6132, S. 24.

¹³⁷ Vgl. § 2 Abs. 1 und 2 Nr. 1, § 13 Abs. 2 Nr. 4 BKAG; BT-Drs. 21/6132, S. 23.

¹³⁸ Vgl. oben B. I. 1.

auf die dort dargestellten Kritiklinien verwiesen werden.¹³⁹ Eigenständige Bedenken betreffen daneben den Aufgabenbezug sowie die Durchführung durch externe Stellen. Kritisiert werden insbesondere die Anknüpfung an die „Ergänzung vorhandener Sachverhalte“ im Rahmen der Zentralstellenaufgabe als zu offen sowie die Übermittlung biometrischer Daten an private Unternehmen und Stellen in Drittstaaten wegen damit verbundener Kontroll-, Zweckbindungs- und Datensicherheitsrisiken.¹⁴⁰

3. Verfassungsrechtliche Bewertung

Bei Anwendung der vorstehend dargestellten verfassungsrechtlichen Grundsätze zum automatisierten biometrischen Internetabgleich¹⁴¹ bestehen hinsichtlich der Ausgangsdaten keine durchgreifenden Bedenken. § 9a Abs. 3 BKAG-E ordnet für die beim BKA vorhandenen und als Grundlage des Abgleichs verwendeten Daten die Anwendung des § 12 Abs. 2 BKAG an und bindet ihre Weiterverarbeitung damit ausdrücklich an die Anforderungen der hypothetischen Datenerhebung. Daten aus den besonders eingriffsintensiven Maßnahmen des § 12 Abs. 3 BKAG sind vom Abgleich ausgeschlossen. Die aus der ursprünglichen Erhebung fortwirkenden Zweck- und Verwendungsbindungen werden damit ausdrücklich abgesichert.

Im Ergebnis bestehen auch im Übrigen keine durchgreifenden verfassungsrechtlichen Bedenken gegen § 9a BKAG-E. Anders als bei § 98d StPO-E ergibt sich insbesondere für die Sachverhaltserforschung kein grundsätzlicher Bedarf für eine weitere Anhebung der materiellen Eingriffsschwelle.

Für die Identifizierung und Aufenthaltsermittlung bleibt es bei einem erheblichen, aber noch begrenzten Eingriffsgewicht. Zwar weisen die Sachverhaltserforschung und die Ermittlung von Zusammenhängen mit anderen Straftaten oder Gefahren ein erhöhtes Eingriffsgewicht auf, weil diese Einsatzformen über die Feststellung einer vorgegebenen biometrischen Übereinstimmung hinaus auf die Gewinnung zusätzlicher, bislang unbekannter Erkenntnisse gerichtet sind. § 9a BKAG-E begrenzt dieses weitergehende Erkenntnispotential jedoch deutlich stärker als § 98d StPO-E. Gegenüber den in Absatz 2 Nummer 2 erfassten Personen – insbesondere Zeugen, Opfern sowie Kontakt- und Auskunftspersonen – darf der Abgleich ausschließlich zur Identifizierung und Aufenthaltsermittlung eingesetzt werden; eine weitergehende Sachverhalts- oder Zusammenhangserforschung ist ausgeschlossen. Hinzu kommt die Abwägung mit entgegenstehenden schutzwürdigen Interessen. Damit wird gerade gegenüber Personen, die selbst keinen oder nur einen verminderten zurechenbaren Anlass für die Maßnahme gesetzt haben, das Erkenntnispotential erheblich begrenzt. Das bei § 98d StPO-E aufgezeigte höhere Eingriffsgewicht der Sachverhaltserforschung stellt sich bei § 9a BKAG-E deshalb insgesamt deutlich abgeschwächt dar. Grundsätzliche verfassungsrechtliche Bedenken gegen die gewählte materielle Eingriffsschwelle bestehen danach nicht.

Dies gilt auch für die präventive Variante. § 9a Abs. 1 BKAG-E verlangt bestimmte Tatsachen, die die Annahme rechtfertigen, dass eine bestimmte Person innerhalb eines übersehbaren Zeitraums auf zumindest ihrer Art nach konkretisierte Weise eine Straftat von auch im Einzelfall erheblicher

¹³⁹ Siehe Seite 5.

¹⁴⁰ Vgl. BfDI, Stellungnahme v. 2.6.2026, S. 5 f.; AG KRITIS, Stellungnahme v. 2.4.2026, S. 8; zur Durchführung durch externe Stellen ferner BRAK, Stellungnahme Nr. 21/2026, S. 14 f.; GFF, Stellungnahme v. 2.4.2026, S. 7 f.; AG KRITIS/AlgorithmWatch/Amnesty International u.a., Gemeinsame Stellungnahme v. 1.4.2026, S. 6.

¹⁴¹ Siehe oben B. I. 3. a).

Bedeutung begehen wird. Die Befugnis knüpft damit nicht an eine lediglich abstrakte Gefahr an, sondern setzt einen individualisierten und tatsächengestützten Gefahrenbezug voraus. **Eine darüber hinausgehende generelle Beschränkung auf den Schutz besonders gewichtiger Rechtsgüter erscheint angesichts der personellen und zweckbezogenen Begrenzungen des § 9a BKAG-E auch für die Sachverhalts- und Zusammenhangserforschung nicht erforderlich.**

Auch die Einbettung in die Zentralstellenaufgabe führt zu keiner anderen Bewertung. Gerade im Rahmen der Zentralstellenaufgabe kommt dem biometrischen Internetabgleich besondere praktische Bedeutung zu. Das Bundeskriminalamt unterstützt als Zentralstelle die Polizeien des Bundes und der Länder und hat hierfür die erforderlichen Informationen zu sammeln und auszuwerten.¹⁴² Der automatisierte Abgleich öffentlich zugänglicher Internetdaten fügt sich in diese Informations- und Schnittstellenfunktion ein. Die „Ergänzung vorhandener Sachverhalte“ beschreibt dabei lediglich den Aufgabenbezug der Maßnahme, nicht deren materielle Eingriffsschwelle. Hinzutreten müssen die tatbestandlichen repressiven oder präventiven Voraussetzungen des § 9a Abs. 1 BKAG-E; insbesondere muss der Abgleich nach Nr. 2 zur Ergänzung vorhandener Sachverhalte im Rahmen der Zentralstellenaufgabe erforderlich sein. Eine erstmalige Gewinnung von Verdachts- oder Gefahrenmomenten soll gerade nicht ermöglicht werden.¹⁴³ Die gegen die Bestimmtheit des Aufgabenbezugs erhobenen Bedenken greifen daher nicht durch.¹⁴⁴

§ 9a BKAG-E ist danach in seinem Regelungskonzept verfassungsrechtlich tragfähig. Anders als bei § 98d StPO-E ergibt sich insbesondere aus der Sachverhaltserforschung kein grundsätzlicher Bedarf für eine weitere Anhebung der materiellen Eingriffsschwelle, weil der Entwurf das weitergehende Erkenntnispotential bereits durch die personellen und zweckbezogenen Begrenzungen des Absatzes 2 wesentlich einhegt.

4. Ausgewählte weitere Regelungsfragen

a) Datenbasis, technische Sicherungen und Kontrollanforderungen

Die in § 9a BKAG-E vorgesehenen datenbezogenen Begrenzungen sind sachgerecht. Die BfDI fordert einen ausdrücklichen Verweis auf § 22 Abs. 2 BKAG, um Daten auszuschließen, die lediglich zur Vorgangsverwaltung oder befristeten Dokumentation gespeichert sind.¹⁴⁵ Einer solchen Ergänzung bedarf es rechtlich nicht. § 22 Abs. 2 BKAG erlaubt die Weiterverarbeitung der dort erfassten Daten ausdrücklich ausschließlich zu diesen Zwecken; eine hiervon abweichende Zweckänderungsbefugnis enthält § 9a BKAG-E nicht. Hinsichtlich Fehler-, Diskriminierungs- und Nachvollziehbarkeitsrisiken sowie der fachlichen Überprüfung automatisiert erzeugter Treffer gelten die zu § 98d StPO-E dargestellten Erwägungen entsprechend.

Soweit die KI-Verordnung für die eingesetzten Systeme zusätzliche Anforderungen an die menschliche Kontrolle vorsieht, gelten diese unmittelbar; einer Wiederholung im BKAG bedarf es nicht.¹⁴⁶

¹⁴² § 2 Abs. 1 und 2 Nr. 1 BKAG.

¹⁴³ BT-Drs. 21/6132, S. 24.

¹⁴⁴ BfDI, Stellungnahme v. 2.6.2026, S. 5 f.; vgl. auch AG KRITIS, Stellungnahme v. 2.4.2026, S. 8.

¹⁴⁵ BfDI, Stellungnahme v. 2.6.2026, S. 2 f.

¹⁴⁶ Vgl. BfDI, Stellungnahme v. 2.6.2026, S. 10 f.

b) Durchführung durch andere Stellen und Drittstaaten

Die Möglichkeit, den biometrischen Abgleich unter den Voraussetzungen des § 9a Abs. 5 und 6 BKAG-E durch andere Stellen durchführen zu lassen, ist sachgerecht. Die Regelung hat erkennbar Auffangcharakter. Nach § 9a Abs. 5 Nr. 2 BKAG-E kommt die Durchführung durch eine andere Stelle nur in Betracht, wenn sie dem Bundeskriminalamt selbst technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand möglich ist. Der Rückgriff auf externe Stellen ist damit nicht als Regel-, sondern als subsidiäre Ausweichlösung ausgestaltet.

Die hiergegen erhobenen Bedenken hinsichtlich Kontrollverlust, Datensicherheit, Zweckbindung und Löschung¹⁴⁷ verfangen nicht. Die für die externe Durchführung vorgesehenen Abweichungen von allgemeinen Zweckbindungsregelungen eröffnen dem Empfänger keine eigenständige Nutzungsbefugnis, sondern sollen die technische Durchführung des gesetzlich zugelassenen Abgleichs ermöglichen. Entscheidend bleibt, dass die Verarbeitung funktional auf diesen Zweck beschränkt wird und die übermittelten Daten nicht für eigene Zwecke des Empfängers weiterverarbeitet werden dürfen. Das Gewicht der hierfür erforderlichen Datenübermittlung bleibt regelmäßig begrenzt. Übermittelt werden dürfen nur die für den konkreten Abgleich erforderlichen Daten. Deren Umfang wird deshalb typischerweise überschaubar sein; im Einzelfall kann bereits die Übermittlung eines einzelnen Lichtbilds oder eines sonstigen biometrischen Ausgangsdatums genügen. Eine Weitergabe umfassender Ermittlungs- oder Polizeidatenbestände ist damit nicht verbunden. Für Drittstaaten treten zusätzliche Anforderungen hinzu, sodass dem erhöhten Risiko einer Verarbeitung außerhalb der Europäischen Union Rechnung getragen wird. Die Übermittlungsbefugnisse der Absätze 5 und 6 erweitern schließlich nicht die unionsrechtlichen Grenzen der eingesetzten technischen Systeme. Insbesondere kann die Einschaltung eines externen Anbieters den Einsatz eines nach Art. 5 Abs. 1 Buchst. e KI-VO unzulässigen Systems nicht legitimieren.

c) Gesetzgebungskompetenz bei Drittstaatenübermittlungen

Die gegen § 9a Abs. 6 BKAG-E erhobenen kompetenzrechtlichen Bedenken¹⁴⁸ überzeugen nicht. Zwar macht die Vorschrift die Durchführung des Abgleichs durch eine Stelle in einem Drittstaat zusätzlich davon abhängig, dass dies „zum Zwecke des Schutzes der nationalen Sicherheit“ erforderlich ist. Hieraus ergeben sich jedoch keine Auswirkungen auf das Zustimmungserfordernis des Art. 73 Abs. 2 GG i.V.m. Art. 73 Abs. 1 Nr. 9a GG. § 9a Abs. 6 BKAG-E begründet keine eigenständige Aufgabe zur Abwehr von Gefahren für die nationale Sicherheit, sondern regelt eine besondere Form der Durchführung der Zentralstellenbefugnis nach Absatz 1. Die Maßnahme bleibt an deren Voraussetzungen und damit an die Zentralstellenaufgabe nach § 2 Abs. 2 Nr. 1 BKAG gebunden; der Schutz der nationalen Sicherheit tritt lediglich als zusätzliche Voraussetzung für die besonders sensible Drittstaatenkonstellation hinzu. Für die Zentralstellenfunktion folgt die Gesetzgebungskompetenz aus Art. 73 Abs. 1 Nr. 10 Buchst. a GG. Das Bundesverfassungsgericht hat diesen Kompetenztitel auch für Datenverarbeitungsbefugnisse des BKA im Rahmen seiner Zentralstellenfunktion herangezogen; zutreffend stützt sich die Entwurfsbegründung hierauf.¹⁴⁹ Die zusätzliche Beschränkung der Drittstaatenübermittlung auf Zwecke des Schutzes der nationalen Sicherheit führt danach nicht zu einem Wechsel der Kompetenzgrundlage.

¹⁴⁷ Vgl. BRAK, Stellungnahme Nr. 21/2026, S. 14 f.; AG KRITIS/AlgorithmWatch/Amnesty International u.a., Gemeinsame Stellungnahme v. 1.4.2026, S. 6.

¹⁴⁸ BfDI, Stellungnahme v. 2.6.2026, S. 9 f.

¹⁴⁹ BT-Drs. 21/6132, S. 26.

d) Anordnung, Benachrichtigung und Kontrolle

Eines allgemeinen Richtervorbehalts bedarf es auch für § 9a BKAG-E nicht.¹⁵⁰ Für die besonders sensible Durchführung des Abgleichs durch Stellen in Drittstaaten sieht § 9a Abs. 8 BKAG-E bereits grundsätzlich eine gerichtliche Anordnung vor; bei Gefahr im Verzug ist die gerichtliche Entscheidung unverzüglich nachzuholen und die Anordnung tritt außer Kraft, wenn sie nicht binnen drei Tagen bestätigt wird.

Ergänzungsbedarf besteht dagegen bei der Benachrichtigung der Zielperson. Der biometrische Abgleich erfolgt regelmäßig verdeckt. Für § 98d StPO-E wird dem durch die Einbeziehung in das Benachrichtigungs- und Rechtsschutzregime des § 101 StPO Rechnung getragen. Eine entsprechende Regelung fehlt für § 9a BKAG-E. § 74 Abs. 1 BKAG sieht eine aktive Benachrichtigung für die dort im Einzelnen bezeichneten Maßnahmen vor, erfasst § 9a BKAG-E jedoch nicht; auch der Entwurf enthält insoweit keine Ergänzung.¹⁵¹ Anders als für § 98d StPO-E, der ausdrücklich in das Benachrichtigungsregime des § 101 StPO einbezogen werden soll, fehlt für die Zielperson des § 9a BKAG-E eine besondere Benachrichtigungsregelung. Eine Benachrichtigung sämtlicher Personen, deren öffentlich zugängliche Daten lediglich als Vergleichsmaterial verarbeitet wurden, ist demgegenüber – entsprechend der Bewertung zu § 98d StPO-E – nicht erforderlich.

II. Automatisierte Datenanalyse als Zentralstellenbefugnis (§ 9b BKAG-E)

1. Regelungskonzept und praktische Bedeutung

Mit § 9b BKAG-E soll für das Bundeskriminalamt im Rahmen seiner Zentralstellenaufgabe eine ausdrückliche Rechtsgrundlage für die automatisierte Datenanalyse geschaffen werden. Das BKA darf Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, nach Maßgabe des § 12 BKAG automatisiert zusammenführen und analysieren, wenn die in Absatz 1 bezeichneten repressiven oder präventiven Voraussetzungen vorliegen.

Anders als § 98e StPO-E setzt § 9b BKAG-E nicht lediglich auf einer bereits bestehenden Analyseplattform auf, sondern erfasst auch die vorgelagerte Zusammenführung der Daten zu einem analysfähigen Grunddatenbestand. Nach der Entwurfsbegründung soll dieser bereits zusammengeführt, aktualisiert und in einem einheitlichen Datenformat vorliegen; die technische Zusammenführung soll insoweit „vom Einzelfall und weiteren Eingriffsschwellen unabhängig“ erfolgen.¹⁵² Eine unmittelbare Anbindung der Analyseanwendung an Internetdienste oder nicht vom Anwendungsbereich der Richtlinie (EU) 2016/680 erfasste Register ist ausgeschlossen.¹⁵³ Die zusammengeführten Daten können zugleich für strafprozessuale Analysen nach Maßgabe des § 98e StPO-E genutzt werden.¹⁵⁴

Für eine automatisierte Erschließung umfangreicher polizeilicher Datenbestände besteht das bereits zu § 98e StPO-E dargestellte praktische Bedürfnis. § 9b BKAG-E soll hierfür im Bereich der Zentralstellenaufgabe des BKA die erforderliche Analysebefugnis und zugleich die technische Grundlage für eine gemeinsame Analyseplattform schaffen.

¹⁵⁰ Siehe oben B. I. 4. c).

¹⁵¹ Vgl. zur Kritik etwa BRAK, Stellungnahme Nr. 21/2026, S. 13.

¹⁵² BT-Drs. 21/6132, S. 28.

¹⁵³ § 9b Abs. 3 Satz 1 BKAG-E.

¹⁵⁴ § 9b Abs. 1 Satz 2 BKAG-E; BT-Drs. 21/6132, S. 27 f.

2. Kritiklinien in Literatur und Stellungnahmen

Die gegen die konkrete automatisierte Datenanalyse nach § 9b BKAG-E erhobenen Einwände entsprechen weitgehend der bereits zu § 98e StPO-E dargestellten Kritik. Beanstandet werden insbesondere Breite und Sensibilität der einbeziehbaren Daten, die Möglichkeit zur Gewinnung bislang unbekannter Zusammenhänge, die Einbeziehung von Daten nicht verantwortlicher Personen sowie Fehler-, Diskriminierungs- und Intransparenzrisiken komplexer Analyseverfahren. Kritik richtet sich ferner gegen die materiellen Eingriffsschwellen und die verfahrensrechtlichen Sicherungen.¹⁵⁵ Insofern kann auf die Ausführungen zu § 98e StPO-E verwiesen werden.¹⁵⁶ Ein eigenständiger Schwerpunkt der Kritik betrifft die vorgelagerte Zusammenführung und Vorhaltung des analysefähigen Grunddatenbestands. Beanstandet wird, dass dieser bereits unabhängig von einem konkreten Analyseanlass zusammengeführt werden soll, ohne dass die Vorschrift eigenständig bestimmt, welche Daten unter welchen Voraussetzungen und für welche Dauer in diesem Bestand vorgehalten werden dürfen.¹⁵⁷

3. Verfassungsrechtliche Bewertung

Für die verfassungsrechtliche Bewertung der automatisierten Datenanalyse gelten die unter B. II. 3 entwickelten Maßstäbe entsprechend. **Verfassungsrechtlicher Nachbesserungsbedarf besteht vor allem hinsichtlich der vorgelagerten, vom konkreten Analysefall unabhängigen Zusammenführung und Vorhaltung eines analysefähigen Grunddatenbestands.** Insofern stellt sich bei § 9b BKAG-E ein dem § 98e StPO-E entsprechendes Grundproblem: **Ein für künftig mögliche Analysen vorgehaltener Datenbestand bedarf einer eigenständigen gesetzlichen Begrenzung nach Speicherzweck, Speicherschwelle und Speicherdauer.** Zugleich schlägt die fehlende Einhegung unmittelbar auf das Eingriffsgewicht der späteren automatisierten Analyse aus. Solange Art und Umfang des für die Analyse verfügbaren Datenbestands nicht hinreichend begrenzt sind, tragen die in § 9b Abs. 1 BKAG-E vorgesehenen Eingriffsschwellen dem dadurch eröffneten Eingriffsgewicht nicht hinreichend Rechnung.

Hinsichtlich der zweckändernden Einbeziehung vorhandener Daten ist § 9b BKAG-E demgegenüber enger ausgestaltet als § 98e StPO-E. Die Verarbeitung erfolgt nach Absatz 1 ausdrücklich „nach Maßgabe von § 12“. Für eine zweckändernde Weiterverarbeitung verlangt § 12 Abs. 2 BKAG nicht nur eine hinreichende Gleichgewichtigkeit des neuen Verwendungszwecks, sondern ausdrücklich, dass sich im Einzelfall konkrete Ermittlungsansätze zur Verhütung, Aufdeckung oder Verfolgung der betreffenden Straftaten beziehungsweise zur Abwehr entsprechender Gefahren ergeben. Der für eine Zweckänderung erforderliche konkrete Ermittlungsansatz ist damit gesetzlich bereits vorgegeben.

Bei hinreichender Einhegung des zugrunde liegenden Datenbestands bestehen gegen die konkrete automatisierte Analyse im Übrigen keine grundsätzlichen verfassungsrechtlichen Bedenken. Wie weit diese Einhegung reichen muss, lässt sich auf Grundlage des vorliegenden Regelungskonzepts allerdings nicht abschließend bestimmen. Maßgeblich ist das Wechselverhältnis zwischen Art und Umfang des für die Analyse verfügbaren Datenbestands und den hierfür geltenden Eingriffsschwel-

¹⁵⁵ Vgl. BfDI, Stellungnahme v. 2.6.2026, S. 13 ff.

¹⁵⁶ Siehe oben B. II. 2.

¹⁵⁷ Etwa BfDI, Stellungnahme v. 2.6.2026, S. 15 f.; vgl. auch Botta, VerfBlog v. 1.9.2026.

len: Je weiter der Datenbestand reicht, desto höher müssen die Anforderungen an den Eingriffsanlass sein. Für die Ausgestaltung der erforderlichen Speicherschwelen bietet die BKAG-II-Entscheidung die bereits dargestellten konkreten Anhaltspunkte. Vorzugswürdig erscheint deshalb ein abgestuftes Regelungsmodell, das unterschiedliche Datenbestände und gegebenenfalls Analyseintensitäten an entsprechend unterschiedliche materielle Eingriffsvoraussetzungen knüpft.

Anders als die vom Bundesverfassungsgericht 2023 beanstandeten weitgehend offenen Analysebefugnisse enthält § 9b BKAG-E erhebliche materielle, personenbezogene und methodische Begrenzungen. Die Datenverarbeitung erfolgt nach Maßgabe des § 12 BKAG; Absatz 2 begrenzt den einbeziehbaren Personenkreis, Absatz 3 schließt eine unmittelbare Anbindung an Internetdienste und bestimmte externe Register aus und Absatz 4 zählt die zulässigen Analyseformen abschließend auf. Hinzu treten die Zweck- und Verwendungsbindungen des Absatzes 5, das Verbot diskriminierender Algorithmen und ausschließlich automatisierter belastender Entscheidungen sowie organisatorische und verfahrensrechtliche Sicherungen in den Absätzen 6 und 7.

4. Ausgewählte weitere Regelungsfragen

a) Datenbasis und Verwendungsbindungen

Sachgerecht ist auch die Begrenzung externer Datenquellen in Absatz 3. Eine unmittelbare Anbindung der Analyseanwendung an Internetdienste und an Register außerhalb des Anwendungsbereichs der Richtlinie (EU) 2016/680 ist ausgeschlossen; Daten aus solchen Quellen können nur einbezogen werden, wenn sie aufgrund einer eigenständigen Befugnis rechtmäßig erhoben worden sind. § 9b BKAG-E schafft damit keine allgemeine Befugnis zur unmittelbaren Erschließung externer Datenbestände.

Anders als § 98e StPO-E schließt § 9b BKAG-E Daten aus besonders eingriffsintensiven Erhebungsmaßnahmen nicht generell von der Analyse aus. Ein solcher kategorischer Ausschluss erscheint jedoch nicht zwingend. Entscheidend ist, dass die aus der ursprünglichen Erhebung folgenden erhöhten Verwendungsanforderungen und besonderen Schutzbindungen über § 12 BKAG fortgelten und auch innerhalb der Analyseplattform technisch zuverlässig abgebildet werden. Die Zusammenführung darf bestehende Kennzeichnungen und Verwendungsbeschränkungen insbesondere bei besonders sensiblen Daten nicht nivellieren.

Sachgerecht ist schließlich auch, dass die nach § 9b BKAG-E zusammengeführten Daten nach Absatz 1 Satz 2 für strafprozessuale Analysen nur „nach Maßgabe von § 98e der Strafprozessordnung“ genutzt werden dürfen.

b) Analysemethoden und Einsatz künstlicher Intelligenz

Von der operativen Datenanalyse nach § 9b BKAG-E ist die Entwicklung, Änderung und das Training der eingesetzten Systeme zu unterscheiden. Hierfür schafft § 22 Abs. 3 BKAG-E eine eigenständige Rechtsgrundlage. § 9b BKAG-E kann deshalb insbesondere nicht als Grundlage dafür dienen, ein selbstlernendes System während des operativen Einsatzes anhand der jeweils analysierten personenbezogenen Echtdata fortlaufend weiterzutrainieren. Soweit die Verarbeitung der Daten der Entwicklung, Änderung oder dem Training des Systems dient, richten sich ihre Voraussetzungen nach § 22 Abs. 3 BKAG-E.

c) Dokumentation und Anordnung

§ 9b Abs. 6 BKAG-E enthält bereits wesentliche organisatorische und verfahrensrechtliche Sicherungen. Die Analyse darf nur durch besonders geschultes Personal durchgeführt werden; Zugriffe und Verarbeitungsschritte sind nach Maßgabe des § 82 Abs. 1 BKAG zu protokollieren, zusätzlich ist die Zielperson festzuhalten. Diese Vorkehrungen bilden eine geeignete Grundlage für die nachträgliche fachliche, datenschutzrechtliche und gerichtliche Kontrolle. **Erwägenswert ist eine weitergehende Konkretisierung der Dokumentationspflichten.** Bei komplexen automatisierten Analysen sollte insbesondere nachvollziehbar bleiben, welche Datenbestände und Analysefunktionen einbezogen, welche wesentlichen Suchparameter oder Gewichtungen verwendet und welche System- oder Modellversion eingesetzt wurden. Nur so lässt sich nachträglich hinreichend rekonstruieren, auf welchem Analyseweg ein für weitere Maßnahmen relevantes Ergebnis zustande gekommen ist. Insoweit gelten die zu § 98e StPO-E entwickelten Erwägungen entsprechend.

Ein allgemeiner Richtervorbehalt ist demgegenüber auch für § 9b BKAG-E verfassungsrechtlich nicht zwingend. Insoweit kann ebenfalls auf die Ausführungen zu § 98e StPO-E verwiesen werden. § 9b Abs. 7 BKAG-E sieht bereits einen qualifizierten behördlichen Anordnungsvorbehalt vor. Entscheidend bleiben hinreichende materielle Voraussetzungen sowie eine wirksame Dokumentation und nachträgliche Kontrolle; ein Richtervorbehalt kann Defizite auf diesen Ebenen nicht ersetzen.

III. Entwicklung, Überprüfung, Änderung und Training von IT-Produkten, § 22 Abs. 3 und 4 BKAG-E

Die Schaffung einer ausdrücklichen Rechtsgrundlage für die Entwicklung, Überprüfung, Änderung und das Training von IT-Produkten einschließlich selbstlernender Systeme mit beim Bundeskriminalamt vorhandenen personenbezogenen Daten ist zu begrüßen. Polizeiliche IT-Systeme müssen unter realitätsnahen Bedingungen entwickelt und überprüft werden können; zugleich stellt die Verwendung vorhandener personenbezogener Daten zu diesen Zwecken eine eigenständige Zweckänderung dar, die einer gesetzlichen Grundlage bedarf. § 22 Abs. 3 BKAG-E knüpft die Verarbeitung an ihre Erforderlichkeit für die Aufgabenerfüllung und schließt Daten aus den in § 12 Abs. 3 BKAG bezeichneten besonders eingriffsintensiven Maßnahmen jedenfalls vom Training aus. Absatz 4 ermöglicht unter zusätzlichen Voraussetzungen auch die Einbeziehung externer Stellen.¹⁵⁸

Soweit eingewendet wird, die Vorschrift eröffne einen zu weitreichenden Zugriff auf personenbezogene Echtdaten¹⁵⁹, verfängt dies nicht. Die in § 22 Abs. 3 Satz 1 Nr. 1 und 2 BKAG-E genannten Fallgruppen treten nicht an die Stelle der übergreifenden Voraussetzung, dass die Verarbeitung personenbezogener Daten zur Aufgabenerfüllung erforderlich sein muss. Können anonymisierte oder pseudonymisierte Daten den verfolgten Zweck mit vertretbarem Aufwand ebenso erfüllen, fehlt es an dieser Erforderlichkeit. Der Begriff des unverhältnismäßigen Aufwands eröffnet daher keine voraussetzungslose Verwendung unveränderter Echtdaten.

¹⁵⁸ BT-Drs. 21/6132, S. 30 f.

¹⁵⁹ Vgl. GFF, Stellungnahme v. 2.4.2026, B. 3. a), insb. cc).

Auch der Einwand, bei selbstlernenden Systemen könnten personenbezogene Trainingsinformationen im Modell fortwirken oder später rekonstruiert werden¹⁶⁰, rechtfertigt keinen generellen Ausschluss personenbezogener Trainingsdaten. Er unterstreicht allerdings die Notwendigkeit einer restriktiven Erforderlichkeitsprüfung sowie wirksamer technischer und organisatorischer Schutzmaßnahmen. Keine durchgreifenden Bedenken bestehen schließlich gegen die Einbeziehung externer Stellen nach Absatz 4. Soweit insoweit Kontroll-, Sicherheits- und Zweckentfremdungsrisiken geltend gemacht werden¹⁶¹, enthält die Vorschrift bereits erhebliche Begrenzungen: Die Voraussetzungen des Absatzes 3 gelten fort; Daten nach § 12 Abs. 3 BKAG dürfen nicht übermittelt werden, die mit den Daten befassten Personen unterliegen besonderen Geheimhaltungspflichten und der Empfänger darf sie ausschließlich für die in Absatz 3 bezeichneten Zwecke weiterverarbeiten. Eine Nutzung der übermittelten Polizeidaten für eigene Zwecke des Empfängers wird damit nicht eröffnet.

IV. Biometrischer Abgleich und automatisierte Datenanalyse zur Abwehr von Gefahren des internationalen Terrorismus, §§ 39a, 39b BKAG-E

Die Übertragung des biometrischen Internetabgleichs und der automatisierten Datenanalyse auf die Aufgabe des Bundeskriminalamtes zur Abwehr von Gefahren des internationalen Terrorismus ist sachgerecht. §§ 39a und 39b BKAG-E entsprechen in ihrer Regelungsstruktur weitgehend den bereits behandelten §§ 9a und 9b BKAG-E, knüpfen den Einsatz der Maßnahmen jedoch an die besondere Aufgabe nach § 5 Abs. 1 Satz 2 BKAG und damit an terroristische Gefahren. Der Entwurf begrenzt die Befugnisse zusätzlich durch qualifizierte Gefahrenlagen und den Schutz besonders gewichtiger Rechtsgüter.

§ 39a BKAG-E unterscheidet sich von § 9a BKAG-E vor allem hinsichtlich der personellen und materiellen Eingriffsstruktur. Während § 9a BKAG-E den biometrischen Abgleich gegenüber bestimmten nicht verantwortlichen Personen auf die Identifizierung und Aufenthaltsermittlung beschränkt, knüpft § 39a Abs. 1 Nr. 1 Buchst. a) BKAG-E die Maßnahme unmittelbar an qualifizierte Gefahrenlagen im Bereich des internationalen Terrorismus. Dies begegnet bei Anwendung der vorstehend dargestellten verfassungsrechtlichen Maßstäbe keinen durchgreifenden Bedenken, weil bei terroristischen Straftaten deren hinreichende Qualifikation den erforderlichen Schutz besonders gewichtiger Rechtsgüter gewährleisten kann.

Für § 39b BKAG-E gelten die zu § 9b BKAG-E entwickelten Anforderungen an die vorgelagerte Zusammenführung und Vorhaltung eines analysefähigen Grunddatenbestands uneingeschränkt fort. Auch die besondere Bedeutung der Terrorismusabwehr rechtfertigt keine in ihren gesetzlichen Grenzen offene vorsorgende Datenhaltung. Erforderlich bleiben hinreichend bestimmte Regelungen zu Speicherzweck, Speicherschwelle und Speicherdauer sowie dazu, welche Personen und Daten unter welchen tatsächlichen Voraussetzungen in den Grunddatenbestand aufgenommen werden dürfen. Ein offener Datenvorrat darf insbesondere nicht allein deshalb vorgehalten werden, weil die Daten künftig für sicherheitsbehördliche Zwecke benötigt werden könnten. Auch zur Terrorismusabwehr darf daher keine in ihren Grenzen offene „Superdatenbank“ entstehen, deren konkrete Nutzung erst auf der Ebene des späteren Analysevorgangs eingeeht wird. Je weiter der Speicherzweck und

¹⁶⁰ GFF, Stellungnahme v. 2.4.2026, B. 3. a) bb), cc).

¹⁶¹ Vgl. GFF, Stellungnahme v. 2.4.2026, B. 3.

je länger die Vorhaltung reichen, desto größere Bedeutung kommt der Begrenzung des Datenbestands, einer tatsächengestützten Speicherschwelle und einer angemessenen Speicherdauer zu. Wird die vorgelagerte Datenhaltung entsprechend gesetzlich eingeghegt, bestehen gegen die konkrete automatisierte Analyse nach § 39b BKAG-E im Übrigen keine eigenständigen durchgreifenden Bedenken; insoweit kann auf die Bewertung zu § 9b BKAG-E verwiesen werden.

V. Sicherung von Verkehrsdaten, §§ 10b, 52 Abs. 3 bis 8 BKAG-E

Die Einführung einer Befugnis zur vorläufigen Sicherung von Verkehrsdaten ist zu begrüßen.

Verkehrsdaten sind regelmäßig nur für begrenzte Zeit verfügbar; ihre Löschung kann eine spätere rechtmäßige Erhebung endgültig vereiteln. Unter den Bedingungen moderner elektronischer Kommunikation bedarf es deshalb hinreichender Befugnisse, vorhandene Verkehrsdaten vorläufig zu sichern, damit gesetzlich zulässige Ermittlungsmaßnahmen nicht allein deshalb ins Leere laufen, weil die hierfür benötigten Daten zwischenzeitlich gelöscht worden sind. Die Sicherungsanordnung bildet insoweit eine notwendige Ergänzung der mit BT-Drs. 21/6581 vorgesehenen IP-Adressspeicherung, deren Einführung ebenfalls uneingeschränkt zu begrüßen ist.

§ 10b BKAG-E ermöglicht dem Bundeskriminalamt deshalb in seiner Zentralstellenfunktion, vorhandene Verkehrsdaten beim Telekommunikationsanbieter vorläufig zu sichern, solange die zuständige Strafverfolgungs- oder Polizeibehörde noch nicht feststeht. § 52 Abs. 3 bis 8 BKAG-E schafft eine entsprechende Befugnis für die Terrorismusabwehr, wenn tatsächliche Anhaltspunkte für eine spätere Erhebungsbefugnis bestehen, deren Voraussetzungen aber noch nicht vollständig geklärt sind. Die Sicherungsanordnung vermittelt dem Bundeskriminalamt noch keinen Zugriff auf die Daten; sie erhält lediglich den vorhandenen Datenbestand für eine mögliche spätere Erhebung. Für diese müssen die jeweils geltenden eigenständigen Voraussetzungen erfüllt sein.

Die Eingriffsschwelle ist auch nicht unzulässig in das Vorfeld verlagert, auch wenn sie insbesondere die vorsorgliche Sicherung von Daten noch nicht verantwortlicher Kontaktpersonen ermöglicht. Gerade weil die Sicherungsanordnung noch keine Kenntnisaufnahme oder Auswertung der Daten ermöglicht, ist ihr Eingriffsgewicht gegenüber der späteren Erhebung deutlich vermindert. Aus dem gleichen Grund ist auch ein Richtervorbehalt nicht erforderlich. Es wäre deshalb zudem nicht sachgerecht, bereits die Sicherung an sämtliche materiellen Voraussetzungen des späteren Datenzugriffs zu binden; damit könnte sie ihren Zweck, den Verlust der Daten bis zur Klärung dieser Voraussetzungen zu verhindern, vielfach nicht erfüllen.

VI. Biometrischer Abgleich und automatisierte Datenanalyse im Personenschutz, §§ 63b, 63c BKAG-E

Auch die Einführung entsprechender Befugnisse für den Personenschutz nach § 6 BKAG ist im Grundsatz sachgerecht. §§ 63b und 63c BKAG-E übertragen den biometrischen Internetabgleich und die automatisierte Datenanalyse auf den Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts und knüpfen die Maßnahmen an qualifizierte Gefahrenlagen für besonders gewichtige Rechtsgüter.¹⁶²

¹⁶² BT-Drs. 21/6132, S. 31 f.

Soweit § 63b Abs. 1 Nr. 3 BKAG-E den biometrischen Abgleich bereits dann zulässt, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine einschlägige Straftat begehen wird, ohne dass bereits ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen feststehen muss, bestehen keine durchgreifenden Bedenken. Die Entwurfsbegründung greift insoweit auf die vom Bundesverfassungsgericht für die Terrorismusabwehr anerkannte personenbezogene Gefahrenprognose zurück und verweist auf die vergleichbare Bedrohungs- und Destabilisierungswirkung möglicher Angriffe auf nach § 6 BKAG geschützte Personen.¹⁶³ Diese Übertragung ist tragfähig. Auch soweit der Abgleich gegenüber nicht verantwortlichen Personen über die bloße Identifizierung und Aufenthaltsermittlung hinaus zur Sachverhaltserforschung eingesetzt werden kann, bestehen aus den zu § 39a BKAG-E dargestellten Gründen keine durchgreifenden Bedenken. Entscheidend sind auch hier die qualifizierte Gefahrenlage und der Schutz besonders gewichtiger Rechtsgüter.

Für § 63c BKAG-E bestehen gegen die konkrete automatisierte Datenanalyse ebenfalls keine eigenständigen durchgreifenden Bedenken. Die Vorschrift knüpft an Gefahren für Leib, Leben oder Freiheit geschützter Personen und damit an besonders gewichtige Rechtsgüter an; § 63c Abs. 1 Satz 2 BKAG-E übernimmt zudem die vom Bundesverfassungsgericht entwickelten Anforderungen an eine konkretisierte Gefahrenlage.¹⁶⁴ Gleichwohl bedarf auch die vorgelagerte Datenhaltung einer eigenständigen gesetzlichen Einhegung. Soweit § 63c BKAG-E eine vom konkreten Analyseanlass unabhängige Zusammenführung und Vorhaltung eines analysefähigen Grunddatenbestands ermöglichen soll, gelten die zu §§ 9b und 39b BKAG-E entwickelten Anforderungen entsprechend. Auch der Personenschutz rechtfertigt keine in ihren gesetzlichen Grenzen offene vorsorgende Datenhaltung.

D. Änderungen des Bundespolizeigesetzes

Die für die Bundespolizei vorgesehenen Befugnisse zur Entwicklung und zum Training von IT-Produkten (§ 46 Abs. 3 und 4 BPolG-E), zum biometrischen Internetabgleich (§ 58a BPolG-E) und zur automatisierten Datenanalyse (§ 58b BPolG-E) entsprechen in ihrer Grundstruktur weitgehend den bereits für das Bundeskriminalamt untersuchten Regelungen. Eigenständige verfassungsrechtliche Fragen stellen sich daher nur hinsichtlich der aufgabenspezifischen Eingriffsschwellen.

Gegen § 46 Abs. 3 und 4 BPolG-E bestehen aus den zu § 22 BKAG-E dargestellten Gründen keine durchgreifenden Bedenken. Auch hier ist die Verwendung personenbezogener Daten für Entwicklung und Training an die Erforderlichkeit gebunden, das Training mit Daten aus den in § 12 Abs. 3 BKAG bezeichneten besonders eingriffsintensiven Maßnahmen ausgeschlossen und die Übermittlung an externe Stellen besonderen Zweck- und Geheimhaltungsbindungen unterworfen.¹⁶⁵

Auch § 58a BPolG-E ist im Ausgangspunkt verfassungsrechtlich tragfähig. Die Vorschrift übernimmt die wesentlichen Begrenzungen des biometrischen Internetabgleichs – insbesondere den Ausschluss von Echtzeitdaten, die qualifizierte Subsidiarität sowie personenbezogene und datenbezogene Beschränkungen – und knüpft die Maßnahme zusätzlich an die besonderen Aufgaben der

¹⁶³ BT-Drs. 21/6132, S. 32; BVerfGE 141, 220 Rn. 112 (BKAG I).

¹⁶⁴ BT-Drs. 21/6132, S. 32; BVerfGE 141, 220 Rn. 105 f., 165 (BKAG I).

¹⁶⁵ BT-Drs. 21/6132, S. 13 f.

Bundespolizei und gewichtige Gefahren beziehungsweise näher bezeichnete Straftaten. Soweit gegen die Reichweite der in § 58a Abs. 1 Nr. 3 BPolG-E erfassten Straftaten eingewandt wird, dass diese teilweise nur vergleichsweise niedrige Strafraumen aufweisen¹⁶⁶, ist zu berücksichtigen, dass die Vorschrift zusätzlich voraussetzt, dass die konkretisierte Straftat eine nicht unerhebliche Schädigung eines der in Nummer 1 genannten Rechtsgüter erwarten lässt. Die Eingriffsschwelle wird damit nicht allein durch die abstrakte Strafandrohung des jeweiligen Delikts bestimmt und erscheint deshalb ausreichend. Im Übrigen gelten die zu § 39a BKAG-E entwickelten Erwägungen entsprechend.

Entsprechendes gilt für die automatisierte Datenanalyse nach § 58b BPolG-E. Die Norm begrenzt ihren Einsatz auf gewichtige Gefahren beziehungsweise näher konkretisierte Straftaten im besonderen Aufgabenbereich der Bundespolizei und übernimmt die personellen, methodischen und organisatorischen Sicherungen des § 9b BKAG-E.¹⁶⁷ Soweit auch hier eine vom konkreten Analyseanlass unabhängige Zusammenführung und Vorhaltung eines analysefähigen Grunddatenbestands ermöglicht werden soll, gelten allerdings die zu § 9b BKAG-E dargestellten Anforderungen entsprechend. Darüber hinaus besteht kein eigenständiger Nachbesserungsbedarf.

E. Änderung des Asylgesetzes

Auch gegen die Neufassung des § 15b AsylG bestehen keine Bedenken. Die Vorschrift ermöglicht den automatisierten Abgleich des nach § 16 Abs. 1 AsylG erhobenen Lichtbilds mit öffentlich zugänglichen biometrischen Daten aus dem Internet, wenn der Ausländer keinen gültigen Pass oder Passersatz besitzt und der Abgleich zur Feststellung seiner Identität oder Staatsangehörigkeit erforderlich ist. Echtzeitdaten sind ausgeschlossen; die für den Abgleich erhobenen Daten sind zu löschen, sobald sie für die Identitäts- oder Staatsangehörigkeitsfeststellung nicht mehr erforderlich sind, und dürfen nicht zu anderen Zwecken weiterverarbeitet werden.¹⁶⁸

Soweit gegen die Regelung insbesondere wegen der Breite des biometrischen Internetabgleichs bei einer lediglich verwaltungsrechtlichen Identitätsfeststellung erhöhte Verhältnismäßigkeitsbedenken erhoben werden¹⁶⁹, greifen diese nicht durch. Denn dem Fehlen eines Straftatverdachts oder einer Gefahr steht ein deutlich engerer Verwendungszweck gegenüber: § 15b AsylG-E erlaubt ausschließlich die Feststellung von Identität oder Staatsangehörigkeit bei fehlendem gültigen Identitätspapier; eine Sachverhalts- oder Zusammenhangserforschung ist nicht eröffnet. Hinzu kommen eine strikte Zweckbindung, Löschungspflichten sowie besondere organisatorische und technische Vorkehrungen, die insbesondere verhindern sollen, dass der Herkunftsstaat oder ein Verfolgerstaat Kenntnis von der Maßnahme erlangt.¹⁷⁰

Die vorgesehene Eingriffsschwelle ist daher nicht zu beanstanden, zumal sie an die Erforderlichkeit anknüpft und eine weitergehende Verwendung der gewonnenen Erkenntnisse durch Absatz 2 ausdrücklich ausgeschlossen ist.

¹⁶⁶ BRAK, Stellungnahme Nr. 21/2026, S. 9.

¹⁶⁷ BT-Drs. 21/6132, S. 33.

¹⁶⁸ BT-Drs. 21/6132, S. 34.

¹⁶⁹ DAV, Stellungnahme Nr. 27/2026, S. 20 f.

¹⁷⁰ § 15b Abs. 2 und 3 AsylG-E.

Sachgerecht ist ferner, dass eine Durchführung durch Dritte nach Absatz 4 auf inländische Stellen und Stellen in Mitgliedstaaten der Europäischen Union begrenzt bleibt. Anders als bei den polizeilichen Regelungen ist eine Beauftragung von Stellen in Drittstaaten nicht vorgesehen.¹⁷¹ Weitergehender Änderungsbedarf ist daher nicht ersichtlich.

¹⁷¹ § 15b Abs. 4 AsylG-E.