



Ausschussdrucksache 21(4)214 B
vom 17. September 2026

Schriftliche Stellungnahme

von Prof. Dr. Markus Löffelmann, Hochschule des Bundes für
öffentliche Verwaltung vom 17.9.2026

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
- d) Antrag der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Dr. Lena Gumnior, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
Rechtsstaat stärken, Grundrechte schützen – Moderne Polizeiarbeit gestalten
BT-Drucksache 21/6913
- e) Antrag der Abgeordneten Clara Bünger, Donata Vogtschmidt, Luke Hoß, weiterer Abgeordneter und der Fraktion Die Linke
Nein zu biometrischen Massenerkennungssystemen
BT-Drucksache 21/6917



Hochschule des Bundes
für öffentliche Verwaltung

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

Herrn Vorsitzenden

des Innenausschusses des Deutschen
Bundestags

Prof. Dr. Markus Löffelmann

HAUSANSCHRIFT Habersaathstr. 51, 10115 Berlin

POSTANSCHRIFT Postfach 40527, 10063 Berlin

TEL 030 – 22 00 89 – 85513

E-MAIL markus.loeffelmann@hsbund-nd.de

DATUM Berlin, 17.09.2026

- ausschließlich per E-Mail -

BETREFF Stellungnahme zu BT-Drs. 21/6131 u.a.

Sehr geehrter Herr Vorsitzender,

anliegend übersende ich die erbetene Stellungnahme zu den

Gesetzentwürfen der Bundesregierung und den

Anträgen der Fraktionen BÜNDNIS 90/DIE GRÜNEN und Die Linke zur

Stärkung digitaler Ermittlungsbefugnisse

BT-Drucksachen 21/6131, 21/6132 und 21/6511, 21/6806, 21/6913 und 21/6917



A. Vorbemerkung

Die drei Gesetzentwürfe dienen der Schaffung von polizeilichen Befugnissen für den Abgleich gespeicherter und öffentlich zugänglicher biometrischer Daten und die automatisierte Auswertung von Datenbeständen. Es handelt sich dabei um eine in technischer und regulatorischer Hinsicht sehr anspruchsvolle Materie. Im Folgenden wird zunächst in Kürze der maßgebliche rechtliche Rahmen für solche Befugnisse aufgezeigt (B.), bevor die beabsichtigten Regelungen kritisch gewürdigt (C.) und Regelungsperspektiven aufgezeigt werden (D.). Angesichts der Kürze der für die Begutachtung zur Verfügung stehenden Zeit kann nur auf zentrale Gesichtspunkte des Vorhabens eingegangen werden.

B. Rechtlicher Rahmen

I. Verfassungsrechtliche Maßstäbe

In seiner Entscheidung vom 16. Februar 2023 hat das BVerfG zahlreiche Gesichtspunkte aufgezeigt, die der Gesetzgeber bei einer Regelung der automatisierten Datenanalyse zu berücksichtigen habe. Die wichtigsten Aussagen der Entscheidung sind¹:

1. Maßnahmen der automatisierten Datenanalyse können eine große Bandbreite von Eingriffsintensitäten aufweisen. Maßgeblich hierfür sind vor allem Art und Umfang der verarbeiteten Daten und die verwendete Analyseverfahren.²
2. Die automatisierte Datenanalyse weist eine selbständige, über den Primäreingriff (Datenerhebung) hinausgehende Eingriffsqualität auf. Bei einer hohen Eingriffsintensität der Analyse reicht die Anwendung des Prinzips der hypothetischen Datenneuerhebung zur Bildung der Eingriffsschwelle nicht aus.³
3. Es obliegt dem Gesetzgeber, in Relation zur Eingriffsintensität für eine präzise rechtliche Einhegung zu sorgen. Teilaspekte der Regulierung kann er auf die Exekutive

¹ BVerfGE 165, 363; dazu näher *Löffelmann*, Stellungnahme vom 17.4.2024, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdr. 20(4)418 F, S. 3 ff.; *ders.* JR 2023, 331, 341 ff.

² BVerfGE 165, 363, 398 ff. (Rn. 71 ff.).

³ BVerfGE 165, 363, 392 ff., 395, 398 (Rn. 60 ff., 66, 72) und Leitsatz 2.



delegieren, muss aber die Voraussetzungen hierfür schaffen und die wesentlichen Entscheidungen selbst treffen.⁴

4. Erforderlich sind „in jedem Fall auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle“.⁵

Zu berücksichtigen ist dabei, dass das BVerfG mehrere rechtlich relevante Fragestellungen ausdrücklich offenlässt, weil insoweit die Zulässigkeitsvoraussetzungen seiner Befassung nicht gegeben waren. Das BVerfG äußert sich insbesondere nicht oder nicht abschließend

- zur Zulässigkeit des Vorhaltens aller in eine automatisierte Analyse einzubeziehenden Daten in einer gemeinsamen Datenbank⁶,
- zu den verfassungsrechtlich gebotenen Anforderungen an verfahrensrechtliche Sicherungen,
- zu den zu schützenden Rechtsgütern, die eine automatisierte Analyse legitimieren können,
- zur Verarbeitung von Daten, die aus Primäreingriffen in Art. 10 und 13 GG stammen
- und zu etwaig erforderlichen Einschränkungen hinsichtlich Art und Umfang der zu verarbeitenden Daten und der Analysemethode im Falle einer hohen gesetzlichen Eingriffsschwelle.⁷

Das macht es erforderlich, die Entscheidung des BVerfG zur automatisierten Datenanalyse weiterzudenken.

Zur Verarbeitung biometrischer Daten hat sich das BVerfG bislang nur im Zusammenhang mit der DNA-Analyse verhalten und die Verarbeitung von DNA-Identifizierungsmustern an mittlere Eingriffsschwellen (Straftaten von erheblicher Bedeutung) geknüpft.⁸

⁴ BVerfGE 165, 363, 414, 416 ff. (Rn. 112, 115 ff.).

⁵ BVerfGE 165, 363, 410, 412 (Rn. 103, 109).

⁶ Vgl. auch Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Deutscher Bundestag, Innenausschuss, Ausschussdr. 21(4)2179, S. 15; zur Unzulässigkeit des Schaffens eines hoheitlichen „Datenvorrats“ auch BVerfGE 169, 332, 404; Thiel, JR 2025, 62, 68 erachtet „die Berücksichtigung der umfassenden und vielschichtigen Vorgaben hinsichtlich der »vorsorgenden Speicherung« im »polizeilichen Informationsverbund« als hochkomplexe Aufgabe“.

⁷ BVerfGE 165, 363, 387, 413, 431 (Rn. 48, 109, 111, 152); vgl. dazu auch Bäuerte in: Möstl/Bäuerte, BeckOK Polizei- und Ordnungsrecht Hessen, HSOG § 25a Rn. 12 f.



II. Europarechtliche Maßstäbe

Beim Abgleich biometrischer Daten handelt es sich um eine Maßnahme der Massendatenverarbeitung (*bulk surveillance*). Für solche Maßnahmen hat der EGMR in seiner jüngeren Rechtsprechung anspruchsvolle gesetzliche Vorgaben definiert. Ob ein Staat sich bei der Schaffung von Instrumenten der Massendatenverarbeitung im Rahmen seines konventionsrechtlich eröffneten Ermessensspielraums bewegt, untersucht der Gerichtshof anhand von acht Kriterien.⁹ Dabei kommt unter anderem der angemessenen Einhegung des Kreises betroffener Personen, der präventiven Kontrolle solcher Maßnahmen durch eine unabhängige Stelle und einer wirksamen *ex post facto*-Kontrolle eine zentrale Bedeutung zu.¹⁰ Auf Formen der automatisierten Analyse von Massendatenbeständen dürften diese Vorgaben übertragbar sein.

Wird für den Datenabgleich ein KI-System i.S.d. Art. 3 Nr. 1 der Verordnung (EU) 2024/1689 (kurz: KI-VO) verwendet, unterliegt dessen Einsatz deren Anforderungen (s. Art. 2 KI-VO). Auf die heute gebräuchlichen KI-Gesichtserkennungsprogramme zur nachträglichen biometrischen Fernidentifikation (s. Art. 3 Nr. 1, Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1 lit. a KI-VO) dürfte das zutreffen. Zu beachten ist hier insbesondere, dass nach Art. 26 Abs. 10 UAbs. 3 S. 2 KI-VO ein Gesichtstreffer nicht die alleinige Grundlage für eine spätere Maßnahme mit nachteiliger Rechtsfolge bilden darf und nach Art. 14 Abs. 5 UAbs. 1 KI-VO stets eine menschliche Überprüfung des Treffers notwendig ist. Allgemein ergibt sich aus Art. 14 Abs. 1 KI-VO, dass jede Ausgabe eines Hochrisiko-KI-Systems von einer natürlichen Person ausreichend zu beaufsichtigen ist. Unzulässig ist nach Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO das Erstellen einer Datenbank zur Gesichtserkennung durch das ungezielte Auslesen von Ge-

⁸ Vgl. BVerfGE 103, 21, 37 ff.; zur daran anschließenden Kammerrechtsprechung ausf. *Krehl* in: Jahn/Krehl/Löffelmann/Güntge, Die Verfassungsbeschwerde in Strafsachen, 3. Aufl. 2025, Rn. 817 ff.

⁹ EGMR, *Big Brother Watch u.a. ./.* Vereinigtes Königreich [GK], 25. Mai 2021, Nr. 58170/13 u.a., Rn. 361; EGMR, 25. Mai 2021, *Centrum för Rättvisa ./.* Schweden, Nr. 35252/08, Rn. 275.

¹⁰ Vgl. auch zur unabhängigen nachträglichen Kontrolle in Fällen des Racial Profiling EGMR, 18. Oktober 2022, B. ./. Deutschland, Nr. 215/19, Rn. 33 ff.



sichtsbildern aus dem Internet.¹¹ Darüber hinaus sind die Vorgaben der Richtlinie (EU) 2016/680 (JI-RL) zur Verarbeitung personenbezogener Daten zu beachten.¹²

C. Kritische Würdigung

I. Abgleich von biometrischen Daten

Die in allen Gesetzentwürfen vorgesehenen Befugnisse zum Abgleich biometrischer Daten erlauben in großem Umfang die Verarbeitung besonders sensibler personenbezogener Daten. Hervorzuheben ist, dass

- die Art der biometrischen Daten nicht eingeschränkt ist, sondern jedwede Art biometrischer Daten und deren Kombinationen umfasst¹³;
- der Abgleich auch solche Daten einschließen kann, die unter – ggf. sogar strafbarer – Verletzung von Persönlichkeitsrechten ins Internet eingestellt wurden;
- der Abgleich auch mittels bearbeiteter biometrischer Daten (etwa künstliche Alterung des Gesichts oder Schärfung des Bildmaterials) erfolgen kann¹⁴;
- der Abgleich nicht nur zum Zweck der Identifizierung oder Ermittlung des Aufenthaltsorts erfolgen darf, sondern generell zur Aufklärung des in Rede stehenden Sachverhalts;

¹¹ Vgl. zu diesen Anforderungen auch BT-Drs. 21/6806 S. 14; *Elsner/Müller*, Vom Gesicht zum Gericht KI-gestützte Verdachtskonkretisierung am Beispiel von KI-Systemen zur nachträglichen biometrischen Fernidentifikation, JR 2026 Heft 11 (im Erscheinen; ahead of print online abrufbar unter: <https://www.degruyterbrill.com/de/document/doi/10.1515/JURU-2026-3027/html>); *Martini/Botta*, DÖV 2025, 1033, 1036 ff.

¹² Näher dazu *Adam*, Unionsrechtliche und grundgesetzliche Grenzen des Data Mining durch die Sicherheitsbehörden des Bundes, 2025, S. 126 ff.; *Martini/Botta*, DÖV 2025, 1033, 1035 f.

¹³ In diesem Zusammenhang ist darauf hinzuweisen, dass § 81e Abs. 2 S. 2 StPO und manche Polizeigesetze eine erweiterte DNA-Spurenanalyse u.a. zum Zweck der Feststellung der Augen-, Haar- und Hautfarbe und des biologischen Alters des Spurenverursachers – also das Erstellen eines „genetischen Phantombilds“ (*Petri* in: Möstl/Schwabenbauer, Polizei- und Sicherheitsrecht Bayern, 2. Aufl. 2025, PAG, Art. 32a Rn. 5 m.w.N. zur an der Regelung geübten Kritik) – erlauben (Art. 32a BayPAG). Die Ergebnisse einer solchen Analyse können dann wiederum Gegenstand eines Abgleichs biometrischer Merkmale sein. Das gilt auch für Mischprofile und Trugs Spuren, wodurch sich die Wahrscheinlichkeit falscher Treffer bedeutend erhöhen dürfte.

¹⁴ Vgl. zu solchen Aspekten näher *Schindler*, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdr. 20(4)493 K, S. 6 f.



- der Abgleich auch zur Verdachtsbegründung und -konkretisierung erfolgen darf, wobei die rechtlichen Anforderungen an einen Anfangsverdacht generell niedrig sind¹⁵;
- der Abgleich nicht auf Beschuldigte oder Störer beschränkt ist, sondern auch bei Dritten wie Zeugen und anderen nicht verantwortlichen Personen angewendet werden darf.¹⁶

Zugleich werden bei einem solchen Abgleich die Daten einer Vielzahl von drittbetroffenen Personen automatisiert verarbeitet. Angesichts der besonderen Schutzbedürftigkeit biometrischer Daten liegt die Eingriffsintensität einer solchen Maßnahme oberhalb derjenigen anderer Arten der Massendatenverarbeitung wie etwa der Videoüberwachung öffentlicher Räume¹⁷, der automatisierten Kfz-Kennzeichenanalyse¹⁸ oder einer automatisierten Verarbeitung von Telekommunikations-Verkehrsdaten.¹⁹ Der Eingriff dürfte deshalb in der verfassungsgerichtlichen Taxonomie als schwer zu qualifizieren sein.²⁰

Die vorgesehenen Eingriffsschwellen und verfahrensrechtlichen Sicherungen tragen dem nicht durchgehend Rechnung:

1. Zu § 98d StPO-E

Die Vorschrift bezieht sich zwar in Absatz 1 auf die schweren Straftaten nach § 100a Abs. 2 StPO, die grundsätzlich eine geeignete Schwelle darstellen, verknüpft diese aber mit dem Begriff der Straftat von erheblicher Bedeutung. Straftaten von erheblicher Bedeutung sind nach gefestigter Rechtsprechung solche der mittleren Kriminalität.²¹ Der Katalog des § 100a

¹⁵ Dazu eingehend *Elsner/Müller* (Fn. 11); allg. zur Unschärfe „tatsächlicher Anhaltspunkte“ *Löffelmann/Pfundmair/Lutsch*, GSZ 2025, 264 ff.

¹⁶ Vgl. zu diesen Kritikpunkten näher *Zöller*, ZRP 2026, 128 ff.; den weiten Adressatenkreis beanstandete auch bereits die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdr. 20(4)493 H, S. 3, 4, 5 zum damaligen Gesetzentwurf unter BT-Drs. 20/12806; aktuell dies., Ausschussdr. 21(4)2179, S. 2 f.; ebenso Bundesrechtsanwaltskammer, Stellungnahme Nr. 21 April 2026, S. 8.

¹⁷ BVerfG NVwZ 2007, 688, 691.

¹⁸ BVerfGE 150, 244, 283 ff.

¹⁹ BVerfGE 107, 299, 318 ff.

²⁰ In diese Richtung auch *Schindler*, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdr. 20(4)493 K, S. 2 ff. m.w.N. zur Rspr. des BVerfG.

²¹ Vgl. auch die entsprechende Kritik an § 25a Abs. 2 S. 1 Nr. 2 HSOG von *Bäuerle* in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, HSOG § 25a Rn. 34 ff. und an § 47a Abs. 1 Nr. 2 lit. a) BWPoIG von *Trurnit* in: Möstl/Trurnit, BeckOK Polizeirecht Baden-Württemberg, BWPoIG § 47a Rn. 11.



Abs. 2 StPO kann zwar als einengende Auslegungshilfe dienen („insbesondere“). Dennoch liegt hier ein verfassungsrechtliches Risiko, insbesondere, wenn der Abgleich zu Personen erfolgen soll, bei denen es sich nicht um Beschuldigte handelt. Wenn der Grundrechtseingriff als schwer einzuordnen ist, müsste die Maßnahme zudem durch eine unabhängige Vorabkontrolle prozessual flankiert sein. Der Anordnungsvorbehalt der Staatsanwaltschaft nach § 98d Abs. 4 StPO-E reicht dann nicht aus. Positiv hervorzuheben ist, dass die unmittelbar betroffene Person nach § 101 Abs. 4 S. 1 Nr. 1a StPO-E zu benachrichtigen ist.

2. Zu § 9a BKAG-E

Auch die entsprechende Befugnis des BKA in seiner Funktion als Zentralstelle knüpft – sowohl für präventive als auch repressive Zwecke – an den Begriff der Straftat von erheblicher Bedeutung an. Auf die Ausführungen zu 1. wird Bezug genommen. Eine Besonderheit der Regelung in § 9a BKAG-E ist, dass der Abgleich auch durch öffentliche oder nicht-öffentliche Stellen in einem Mitgliedstaat der EU (Absatz 5) und sogar in einem Drittstaat (Absatz 6) durchgeführt werden darf. Für den letztgenannten Fall gilt ein Richtervorbehalt (Absatz 8). Diese Auslagerung des Abgleichs ist ausgesprochen kritisch zu sehen, denn damit geht eine beträchtliche Erhöhung für die Betroffenen nachteiliger und missbräuchlicher Datenverwendungen einher. Im Bereich des nachrichtendienstlichen Informationsaustausches hat das BVerfG für die Übermittlung von personenbezogenen Daten an ausländische Stellen besondere Schutzvorkehrungen gefordert, um die Einhaltung von datenschutzrechtlichen und rechtsstaatlichen Mindeststandards zu gewährleisten.²² Absatz 7 erklärt zwar die Übermittlungsvorschriften nach §§ 25 bis 28 BKAG für anwendbar, diese enthalten jedoch keine vergleichbaren Sicherungen. Auch hier liegt ein verfassungsrechtliches Risiko.

3. Zu § 39a und § 63b BKAG-E und § 58a BPolG

Angesichts des hohen Rangs der nach § 39a BKAG-E zu schützenden Rechtsgüter sind die vorgesehenen Schwellen – auch bei einem Abgleich der Daten von Personen, die nicht Beschuldigte oder Störer sind – nicht zu beanstanden. Die auch hier zulässige (Absatz 5 und 6) Datenverarbeitung im Ausland ist unter Verhältnismäßigkeitsgesichtspunkten weniger kri-

²² BVerfGE 154, 152, 273 ff.; BVerfGE 162, 1, 121 ff.



tisch zu sehen, zumal die Anwendungshäufigkeit deutlich geringer sein dürfte. Für die Anwendung der Maßnahme im Rahmen der Aufgabe des Personenschutzes durch das BKA (§ 63b BKAG-E) und die Aufgabenerfüllung der Bundespolizei (§ 58a BPolG) können vergleichbare Überlegungen angestellt werden. Im letztgenannten Fall dürfte die Anwendungsbreite allerdings wiederum deutlich größer sein, weshalb einer Datenverarbeitung im Ausland Bedenken begegnen.

Die Anforderungen nach der KI-VO (s. oben B.II.) werden durch die beabsichtigten Regelungen erfüllt. Insbesondere tragen die Löschungspflichten in § 98d Abs. 3 StPO-E dem Verbot des Errichtens von Datenbanken zur Gesichtserkennung Rechnung. Um eine Maßnahme auf diese Weise nach dem derzeitigen Stand der Technik umgesetzt werden kann²³, vermag der Unterzeichnende nicht zu beurteilen.

II. Automatisierte Datenanalyse

1. Eingriffsschwelle

Die Gesetzentwürfe verfehlen die anspruchsvollen verfassungsrechtlichen Anforderungen an eine gesetzliche Einhegung automatisierter Datenanalysen. Ein kohärentes regulatorisches Konzept fehlt bislang.²⁴ Die beabsichtigten Regelungen (wie auch die bereits auf Landesebene in den Polizeigesetzen geschaffenen) orientieren sich durchgehend an der verfassungsgerichtlichen Formulierung von Mindestanforderungen für schwerwiegende Eingriffe durch automatisierte Datenanalysen. Solche Eingriffe seien „nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten“ und erforderten eine hinreichend konkretisierte Gefahr für ein beson-

²³ Das wird u.a. bezweifelt von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Deutscher Bundestag, Ausschuss für Inneres und Heimat, Ausschussdr. 20(4)493 H, S. 3 zum damaligen Gesetzentwurf unter BT-Drs. 20/12806; aktuell dies., Ausschussdr. 21(4)2179, S. 4; ebenso Bundesrechtsanwaltskammer, Stellungnahme Nr. 21 April 2026, S. 12; *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung. Technisches Gutachten, September 2025, abrufbar unter: <https://algorithmwatch.org/de/wp-content/uploads/2025/10/2025-AW-Gutachten-V9.pdf>.

²⁴ In diese Richtung auch Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Deutscher Bundestag, Innenausschuss, Ausschussdr. 21(4)2179, S. 13: „pauschal sehr weitreichende Datenanalysen“.



ders gewichtiges Rechtsgut.²⁵ Die Entwurfsverfasser ziehen daraus den Schluss, dass bei dieser Eingriffsschwelle eine gesetzliche Einhegung der Analyse nach Art und Umfang der verarbeiteten Daten und der verwendeten Analysemethode nicht erforderlich sei. Mit der grundsätzlichen dogmatischen Weichenstellung, dass bei schwerwiegenden Eingriffen durch eine Analyse die Anwendung des Grundsatzes der hypothetischen Datenneuerhebung nicht ausreichend sei²⁶, ist das nicht zu vereinbaren. Denn gerade bei der Weiterverarbeitung von Daten, die aus schwerwiegenden Primäreingriffen gewonnen wurden, würde nach dieser Logik der *selbständigen* Eingriffsqualität der automatisierten Analyse nicht Rechnung getragen. Mit anderen Worten: Wenn besonders sensible Daten verarbeitet werden, wären danach an eine automatisierte Analyse *keine* gegenüber dem Primäreingriff erhöhten Anforderungen zu stellen. Das ist widersprüchlich und wird so vom BVerfG nicht judiziert, das sich zu dieser Konstellation nicht abschließend geäußert hat. Im Schrifttum werden vor diesem Hintergrund für jede Form der automatisierten Datenanalyse gesetzliche Vorgaben zu Art und Umfang der Daten und der Methoden gefordert.²⁷

Vor diesem Hintergrund begegnen die beabsichtigten Regelungen folgenden Einwänden:

a) Zu § 98e StPO-E

- Die in § 98e Abs. 1 StPO-E vorgesehene Schwelle des qualifizierten Verdachts einer schweren Straftat nach § 100a Abs. 2 StPO liegt (bei einem übergreifenden Vergleich zwischen einem straftat- und einem rechtsgutbezogenen Regelungsmodell) unterhalb derjenigen eines besonders gewichtigen Rechtsguts. Die vergleichbare Schwelle wären hier besonders schwere Straftaten, wie sie etwa § 100b Abs. 2 StPO definiert.²⁸ Erforderlich wären bei einem Unterschreiten dieser Schwelle besondere Einhegungen der Analyse insbesondere nach Art und Umfang der verarbeiteten Daten und der verwendeten Methode.

²⁵ BVerfGE 165, 363, 410 f. (Rn. 104 ff.).

²⁶ BVerfGE 165, 363, 397 (Rn. 70).

²⁷ Vgl. nur Kugelman/Buchmann, GSZ 2024, 1, 7; Bäuerle in: Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen, HSO § 25a Rn. 40 ff.; Teichmann, HRRS, 2026, 13, 26; diff. Adam, Unionsrechtliche und grundgesetzliche Grenzen des Data Mining durch die Sicherheitsbehörden des Bundes, 2025, S. 179: nur Vorgaben zur Methode, nicht zu Art und Umfang der Daten.

²⁸ Vgl. BVerfGE 162, 1, 118; BVerfGE 163, 43, 95; BVerfGE 169, 130, 183, 217 ff.; jeweils zur Übermittlungsschwelle für nachrichtendienstliche Informationen.



- Nach § 98e Abs. 2 S. 1 StPO-E dürfen in die Analyse „Vorgangsdaten, Falldaten, Daten aus den polizeilichen Informationssystemen und aus dem polizeilichen Informationsaustausch einbezogen werden“. Das stellt keine Einhegung nach Art und Umfang der verarbeiteten Daten dar. Es handelt sich um eine bloße Nennung von Speicherorten oder Dateitypen, die eine unbestimmte Vielzahl von personenbezogenen Daten unterschiedlicher Qualität beinhalten. Dies umfasst auch Daten von Zeugen, Opfern und dritten Personen.
- Insbesondere enthält die Norm keinen Ausschluss der Verarbeitung von Daten Unbeteiligter. Zumindest im Bereich der Vorgangsdaten müssten die auszuwertenden Daten unter Ausschluss von Zeugen und anderen Unbeteiligten auf die Daten von verurteilten, beschuldigten, verdächtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen begrenzt werden. Im Bereich weiterer Datenquellen sollte eine Einschränkung auf Daten Unbeteiligter „wenn möglich“ erfolgen.²⁹
- § 98e Abs. 2 S. 2 StPO-E stellt die Verarbeitung von Daten aus eingriffsintensiven Primärmaßnahmen wie etwa der Telekommunikationsüberwachung oder Überwachung des gesprochenen Worts unter den Vorbehalt der Erforderlichkeit. Das ist keine qualifizierte Schwelle. Alle Grundrechtseingriffe stehen unter dem Vorbehalt der Erforderlichkeit. Hier wird deutlich, dass dem gegenüber dem Primäreingriff selbständigen Gewicht der Analyse nicht Rechnung getragen wird.
- Daten aus Maßnahmen nach den §§ 100b und 100c StPO dürfen nach § 98e Abs. 2 S. 3 StPO-E in die Analyse einbezogen werden, wenn sie im selben Strafverfahren erhoben wurden. Gerade bei Umfangsverfahren gegen eine Vielzahl von Beschuldigten können auf diese Weise sogar Daten aus besonders eingriffsintensiven Maßnahmen automatisiert mit anderen Datenbeständen abgeglichen werden. Das wäre zwar zweckwahrend, würde aber dennoch die Eingriffsintensität der Analyse stark erhöhen.
- Nach § 98e Abs. 3 S. 2 StPO-E können Datensätze aus automatisierten Registerabfragen in die Analyse einbezogen werden. Darin liegt ein erhebliches Potenzial, die automatisierte Analyse auch auf nicht-polizeiliche hoheitliche Datenbestände zu er-

²⁹ Hintergrund dieser Einschränkung ist, dass dort die Rollen der betroffenen Personen nicht immer festgelegt sind.



strecken. Insbesondere bei künftigen Erweiterungen automatisierter Abfragen ist das im Auge zu behalten.

- § 98e Abs. 4 S. 1 StPO-E beschreibt die zulässigen Zwecke der Analyse. Damit dürften sämtliche polizeilichen Bedarfe abgedeckt sein. Unzulässige Zwecke werden hingegen nicht ausgeschlossen. So lässt die Norm z.B. nicht erkennen, ob auch die Erstellung von Persönlichkeitsprofilen das Ergebnis einer Klassifizierung nach Nr. 1 sein kann.
- § 98e Abs. 4 S. 2 und 3 StPO-E beschränken die Vorgaben zur Methodik auf eine manuelle Veranlassung mittels Suchbegriffen. Das ist wichtig (und vermutlich im Rahmen einer strafprozessualen Anwendung allein zielführend), schließt aber bewusst die Verwendung von Künstlicher Intelligenz und statistische Analysen, denen nach der Rechtsprechung des BVerfG eine erhöhte Eingriffsintensität zukommt, nicht aus (BT-Drs. 21/6806 S. 22). Zulässig wäre auch eine agentische Analyse. Mangels Vorgaben zu den zu verwendenden Selektoren können diese sehr weit gefasst sein.

Bei einer Gesamtbetrachtung wird die Eingriffsintensität der ermöglichten Analysen daher nicht so stark eingeeht, dass ein Unterschreiten der vom BVerfG für schwerwiegende Eingriffe formulierten Schwelle gerechtfertigt ist. Hinzu kommt, dass bei einer kritischen Lesart der zugrunde liegenden Entscheidung des BVerfG einschränkende gesetzliche Vorgaben zu Art und Umfang der verarbeiteten Daten und der verwendeten Analysemethode auch bei einer hohen Schwelle erforderlich sind.

b) Zu § 9b BKAG-E

Die Vorschrift betrifft die Funktion des BKA als Zentralstelle i.S.d. § 2 BKAG.

- Für Zwecke der Strafverfolgung etabliert § 9b Abs. 1 S. 1 Nr. 1 BKAG-E ebenfalls die Schwelle der schweren Straftat. Auf die Ausführungen unter a) zu § 98e Abs. 1 StPO-E wird Bezug genommen. Anders als dort ist kein qualifizierter Tatverdacht erforderlich, wodurch die Anforderungen nochmals hinter denen nach der StPO zurückbleiben. § 9b Abs. 1 S. 1 Nr. 2 BKAG-E ist nicht zu beanstanden.



- Nach § 9b Abs. 2 Nr. 2 BKAG-E darf die Maßnahme auch gegen mögliche künftige Zeugen und Opfer einer Straftat, Kontaktpersonen der verantwortlichen Person, Hinweisgeber und Auskunftspersonen durchgeführt werden. Die in Bezug genommene Norm des § 19 Abs. 1 S. 1 BKAG steht im Kontext der Verhütung künftiger Straftaten und der Vorsorge für die Verfolgung künftiger Straftaten. Eine automatisierte Analyse zu diesen Zwecken wäre eine Form des *predictive policing* und nur in sehr engen Grenzen verfassungsrechtlich zu rechtfertigen.³⁰ Allerdings ist nach § 9b Abs. 1 BKAG-E die Maßnahme nur zur Verfolgung begangener Straftaten oder bei konkretisierter Gefahr zulässig. Die Bezugnahme auf den Kontext der Straftatenverhütung und Verfolgungsvorsorge ist demnach regelungstechnisch unglücklich und irreführend.
- Auch hier gilt, dass die Norm keine gesetzlichen Vorgaben zu Art und Umfang der zu verarbeitenden Daten und zulässigen Analysemethoden enthält. Auf die Ausführungen unter a) wird Bezug genommen. Anders als in § 98e Abs. 4 S. 2 und 3 StPO-E ist hier auch keine einschränkende Maßgabe zu einer ausschließlich manuellen Veranlassung und Analyse anhand von Suchbegriffen enthalten.

c) Zu § 39b BKAG-E

Die Vorschrift schließt an die Aufgabe des BKA zur Abwehr von Gefahren des internationalen Terrorismus an. Angesichts des hohen Rangs der zu schützenden Rechtsgüter und des großen Ausmaßes der abzuwehrenden Gefahren begegnet die automatisierte Datenanalyse hier keinen Einwänden unter Verhältnismäßigkeitsgesichtspunkten. Allerdings sind auch hier – schon aus Gründen der Transparenz – gesetzliche Vorgaben zu Art und Umfang der zu verarbeitenden Daten und der zulässigen Analysemethoden erforderlich. Auf die Ausführungen zu a) wird insoweit Bezug genommen. Anders als in § 98e Abs. 4 S. 2 und 3 StPO-E ist hier ebenfalls keine einschränkende Maßgabe zu einer ausschließlich manuellen Veranlassung und Analyse anhand von Suchbegriffen enthalten.

³⁰ BVerfGE 165, 363, 407 f. (Rn. 98, 100).



d) Zu § 63c BKAG-E

Die Vorschrift betrifft die Funktion des BKA als zuständige Stelle für den Personenschutz.

- Die Schwelle der konkreten Gefahr für Leib, Leben und Freiheit zu schützender Personen in § 63c Abs. 1 S. 1 BKAG-E ist unter Verhältnismäßigkeitsgesichtspunkten nicht zu beanstanden. Das gilt auch für die Fälle des § 63c Abs. 1 S. 2 BKAG-E, die die Art und Weise der Gefahr für diese Rechtsgüter als Straftaten von erheblicher Bedeutung konkretisieren. Die subtile Differenzierung zwischen den drei Fallgruppen erscheint allerdings verzichtbar. Als Eingriffsschwelle könnte auch generell eine konkretisierte Gefahr für die genannten Rechtsgüter herangezogen werden.
- Auch hier enthält die Norm allerdings keine gesetzlichen Vorgaben zu Art und Umfang der zu verarbeitenden Daten und zulässigen Analysemethoden. Auf die Ausführungen unter a) wird Bezug genommen. Eine einschränkende Maßgabe zu einer ausschließlich manuellen Veranlassung und Analyse anhand von Suchbegriffen ist hier ebenfalls nicht vorgesehen.

e) Zu § 58b BPolG-E

Die Vorschrift regelt die automatisierte Datenanalyse im Zuständigkeitsbereich der Bundespolizei. Die Schwellen in § 58b Abs. 1 S. 1 BPolG-E sind nicht zu beanstanden. Hinsichtlich der fehlenden Ausformung zu Art und Umfang der Daten und zur zulässigen Methode wird auf die vorstehenden Ausführungen Bezug genommen.

2. Verfahrenssicherungen

Für jede Form der automatisierten Datenanalyse sind gesetzliche Regelungen zu Transparenz, individuellem Rechtsschutz und Kontrolle erforderlich.³¹ Das BVerfG fordert insoweit explizit

³¹ Vgl. dazu *Kugelman/Buchmann*, GSZ 2024, 1, 9.



- die Pflicht zur Begründung für die Veranlassung der automatisierten Analyse im Einzelfall³²,
- schützende Regelungen für die Nachvollziehbarkeit der Verarbeitung bei allen eingriffsintensiven Formen des Datenabgleichs³³,
- Vorkehrungen zur Entdeckung und Korrektur von Fehlern³⁴,
- Formen der wirksamen aufsichtlichen Kontrolle.³⁵

Dem dogmatischen Ansatz des BVerfG zufolge, wonach die automatisierte Datenanalyse einen selbständigen Eingriff begründet, wäre es zudem schlüssig, den Einsatz solcher Maßnahmen von einer Präventivkontrolle durch eine unabhängige und neutrale Stelle, etwa in Gestalt eines Richtervorbehalts abhängig zu machen, sofern der durch die Analyse vermittelte Eingriff als schwer zu gewichten ist. Hinzu kommen weitere denkbare Verfahrenssicherungen wie etwa regelmäßige externe Audits durch Sachverständige und unabhängige Prüfstellen.³⁶

Die beabsichtigten Normen enthalten solche prozeduralen Sicherungen nur teilweise.

a) Zu § 98e StPO-E

§ 98e Abs. 5 S. 1 StPO-E enthält eine Begründungspflicht, § 98e Abs. 5 S. 2 i.V.m. § 98d Abs. 2 StPO-E eine Protokollierungspflicht. Im Übrigen verweist § 98e Abs. 6 StPO-E auf die allgemeinen Regelungen über die Verarbeitung personenbezogener Daten und die Rechte Betroffener. Das damit in Bezug genommene Regelungsregime (vgl. BT-Drs. 21/6806 S. 23 f.) ist allerdings selbst sehr unübersichtlich und reformbedürftig.³⁷ Eine Pflicht zur Benach-

³² BVerfGE 165, 363, 413 (Rn. 109).

³³ BVerfGE 165, 363, 409 (Rn. 101).

³⁴ BVerfGE 165, 363, 409 (Rn. 102).

³⁵ BVerfGE 165, 363, 412 f., 414 f. (Rn. 109, 113).

³⁶ Vgl. *Teichmann*, HRRS 2026, 13, 27 f., der einen prä-operativen Audit-Report über Trainingsdaten, Modellarchitektur und Validierungsmetriken, laufende halbjährliche Bias-Prüfungen und ex post eine öffentliche Fehler- und Beschwerdestatistik vorschlägt; in diese Richtung argumentiert auch der Antrag unter BT-Drs. 21/6913.

³⁷ Insbesondere enthält die StPO noch keine Regelung zur hypothetischen Datenneuerhebung, die zwingend, insbesondere vor dem Hintergrund des Auslegungsspielraum eröffnenden Wortlautes des § 161 Abs. 3 i.V.m. § 479 Abs. 2 StPO, auch bei einer automatisierten Analyse zu beachten ist; vgl. hierzu auch Bundesrechtsanwalts-



richtung betroffener Personen ist nicht vorgesehen. Möglichkeiten des nachträglichen Rechtsschutzes sind somit faktisch weitgehend ausgeschlossen, weshalb einer – ebenfalls nicht vorgesehenen – unabhängigen Vorabkontrolle eine wichtige kompensatorische Funktion zukäme. Eine aufsichtliche ex post facto-Kontrolle kann durch den für die Strafverfolgungsorgane jeweils zuständigen Datenschutzbeauftragten des Landes oder Bundes erfolgen. Aus Transparenzgründen sollte das klargestellt werden. Eine Verpflichtung zur Etablierung eines Rechte- und Rollenkonzepts für den Zugriff auf die automatisierten Analysesysteme ist ebenfalls nicht vorgesehen.

b) Zu § 9b, 39b und 63c BKAG-E

Die verfahrensrechtlichen Sicherungen der Normen decken sich. Keine der Normen enthält eine Pflicht zur Begründung der Maßnahme im Einzelfall. Für die erforderliche Protokollierung verweisen alle Normen auf § 82 Abs. 1 BKAG, was nicht zu beanstanden ist. Eine Benachrichtigung betroffener Personen ist nicht vorgesehen. In allen Fällen gilt für die Anordnung ein Behördenleitervorbehalt bzw. das Erfordernis der Anordnung durch einen Mitarbeitenden mit Befähigung zum Richteramt, d.h. einen Mitarbeitenden, der ein rechtswissenschaftliches Studium an einer Universität mit der ersten Prüfung und einen anschließenden Vorbereitungsdienst mit der zweiten Staatsprüfung abgeschlossen hat (§ 5 Abs. 1 Hs. 1 DRiG). Mit einem Richtervorbehalt ist das nicht vergleichbar. Hinsichtlich der Zugriffsberechtigungen verweisen die Normen auf § 15 BKAG, was ebenfalls nicht zu beanstanden ist. Außerdem fordern alle Normen organisatorische und technische Vorkehrungen gegen unbefugte Kenntnisnahme.

c) Zu § 58b BPolG

Eine Begründungs- und Protokollierungspflicht werden hier nicht geregelt. Für die Anordnung gilt ein erweiterter Behördenleitervorbehalt. Im Übrigen ist die Norm parallel zu den Regelungen im BKAG ausgestaltet.



D. Regelungsperspektiven

I. Kategorisierung

Zwingend erforderlich für eine präzise und kohärente gesetzliche Regelung automatisierter Datenanalysen ist die Bildung von Kategorien der hierfür zulässigen Daten und Analysemethoden. Eine solche Kategorisierung kann nur im interdisziplinären Zusammenwirken von Datenanalysten, Informatikern, Psychologen und Juristen erfolgen und müsste regelmäßig mit dem Fortschreiten der technischen Entwicklung überprüft und revidiert werden. Die folgenden Einteilungen können daher nur die grobe Richtung andeuten, in die weitergedacht werden sollte und sind lediglich exemplarisch zu verstehen.

Hinsichtlich der Analysemethoden müsste anhand von technischen und teleologischen Kriterien gewichtet werden, in welchem Maße die Leistungsfähigkeit der Systeme (und damit die durch sie vermittelte spezifische Gefährdung von Persönlichkeitsrechten) über die Fähigkeiten eines humanen Agenten hinausgehen. Beispiel:

Kat.	Intensität	Art	Ziel	Zweck	Beispiele
1	niedrig	computer-gestützte Suchverfahren	effizientes Erzeugen von Ergebnissen, die auch mittels manueller Auswertung erzeugt werden können	Ressourcenschonung, Fehlervermeidung	Indexierung großer Datenbestände; Durchsuchen anhand von Selektoren; inhaltliche Zusammenfassungen
2	erhöht	automatisierte statistische Analyse	Erzeugen von Ergebnissen, die zwingend eine mathematisch-statistische Analyse erfordern und nicht durch einen humanen Akteur substituiert werden können	Erkennen neuer Zusammenhänge, Ausschalten humaner Biases	statistische Analyse, z.B. t-Test, Chi ² -Test; explorative Analyse; Graph-Analyse
3	mittel	machine learning	Erzeugen von Ergebnissen, die nicht durch eine konkrete Suche	Erkennen neuer Zusammenhänge innerhalb eines Datenbe-	Unsupervised Learning, z.B. Clustering (DBSCAN, k-means), Dimensi-



			vorgegeben sind; Suche nach bis dahin unbekannten Strukturen	standes und Vorhersage an- hand von Indika- toren, Klassifika- tion, Regression	onsreduktion (PCA); Supervised Learn- ing, z.B. SVM, RandomForest, XGBoost, Deep Learning Modelle
4	hoch	agenti- sche KI	Erzeugen von Er- gebnissen durch Nutzung von mul- tiplen Tools, die vom System selb- ständig kombiniert und korrigiert wer- den können	gezieltes Über- schreiten huma- ner kreativer Wissensgene- rierung	LLM-basierte Ana- lyse außerhalb der Stufen 1, 2 und 3; agentische Analyse
5	beson- ders hoch	predictive policing	Erzeugen einer Vorhersage indivi- duellen personen- oder gruppenbezo- genen Verhaltens	möglichst früh- zeitiges Erken- nen künftiger Rechtsgutsver- letzungen	Gefährdereinstu- fung; individuelle Risikoscores; Le- galbewährungs- prognose

Die für eine Analyse zulässigen Arten von Daten lassen sich entlang der bereits etablierten Rechtsprechungslinien hinsichtlich ihrer Schutzbedürftigkeit kategorisieren, wobei die Herkunft der Daten (also die Intensität des Primäreingriffs) nur ein relevantes Kriterium unter anderen darstellt.³⁸ Denn auch aus sehr eingriffsintensiven Erhebungsmaßnahmen können wenig schutzwürdige Daten resultieren. Umgekehrt können durch niedrighschwellige Primäreingriffe (z.B. offene Befragungen) hoch schutzwürdige Daten erhoben werden. Für das Erkennen und Kennzeichnen der jeweiligen Datenkategorie könnten wiederum Anwendungen Künstlicher Intelligenz eingesetzt werden. Anhaltspunkte für Datenkategorien unterschiedlicher Schutzwürdigkeit ergeben sich aus der Rechtsprechung des BVerfG und dem Datenschutzrecht. So haben sich etwa die Mitgliedstaaten der Europäischen Union in Art. 9 Abs. 1 DS-GVO und Art. 10 der JI-Richtlinie auf besondere Kategorien personenbezogener Daten verständigt, bei denen ein erhöhtes Schutzniveau greift. Der EuGH fordert in seiner jüngsten Judikatur zur „Vorratsdatenspeicherung“ von IP-Adressen eine „wirksame strikte Trennung der verschiedenen Kategorien auf Vorrat gespeicherter Daten“.³⁹ Teilweise finden sich be-

³⁸ Näher *Löffelmann*, GSZ 2024, 215 ff.; die folgende Tabelle ist dieser Publikation entnommen.

³⁹ EuGH (Plenum), La Quadrature du Net 2, Urteil vom 30.4.2024, C-470/21, Rn. 84 = EuGRZ 2024, 246 (255).



reits in den deutschen Sicherheitsgesetzen Kategorien verschiedener Daten.⁴⁰ Die Daten-Verordnung des BKA (BKADV) differenziert in Anknüpfung an Regelungen im BKAG zwischen acht verschiedenen Datenkategorien mit insgesamt rund 100 verschiedenen Datenarten.⁴¹

Kat.	Schutzbedürftigkeit	Sammelbezeichnung	Beispiele für Datenarten
0	keine	offene Daten	Daten ohne Personenbezug; öffentlich zugängliche Daten zu Personen der Zeitgeschichte; von der betroffenen Person selbst öffentlich gemachte Daten; rein hoheitliche Daten
1	leicht	Grunddaten	Name, Geburtsdatum, Wohnort; TK-Bestandsdaten; Konto-Stammdaten; Kfz-Daten; Vorstrafen
2	mittel	Verkehrsdaten	TK-Verkehrsdaten; einzelne Kontoein- und -ausgänge; Kontaktdaten; einzelne Standortdaten; Reisedaten; Daten betreffend das Verhalten einer Person im öffentlichen Raum
3	hoch	Inhaltsdaten	TK-Inhaltsdaten; Telemedien-Nutzungsdaten; verbundene Standortdaten (Bewegungsprofile); Konto-Bewegungsdaten; verbundene Daten der Kategorie 2
4	besonders hoch	höchstpersönliche Daten	biometrische Daten; Gesundheitsdaten; Persönlichkeitsprofile; Tagebuchaufzeichnungen mit Bezug zu strafbaren Handlungen; Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen; genetische Daten; Daten zum Sexualleben oder zur sexuellen Orientierung
5	absolut	Kernbereichsdaten	Austausch mit Personen des engsten Vertrauens; intime Äußerungen; Gebete, Beichte

⁴⁰ Vgl. etwa § 20 I Nr. 2 HSOG und § 50 III POG RP (Grunddaten); § 2 XII (genetische Daten), XIII (biometrische Daten), XIV (Gesundheitsdaten), XV Nr. 1 (Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen) und Nr. 5 (Daten zum Sexualleben oder zur sexuellen Orientierung), IXX (Grunddaten) SPoLDVG.

⁴¹ BKADV vom 4.6.2010 (BGBl. I S. 716); die BKADV wurde mittlerweile an die Neuregelungen in den §§ 16, 18 und 19 BKAG angepasst, ist in dieser Version aber noch nicht veröffentlicht und in Kraft getreten.



Beide Parameter (Methode und Datenart) müssten im Verbund durch den Gesetzgeber gewichtet und den durch die Datenanalyse verfolgten Zielen gegenübergestellt werden.⁴² Dabei würde es sich anbieten, auf der Ebene des Gesetzes die jeweiligen Kategorien nur abstrakt zu beschreiben und eine nähere Ausformung (auch unter Verwendung spezifisch technischer Begriffe) auf untergesetzlicher Ebene zu erlauben (vgl. sogleich unter II.).

II. Gesetzgebungstechnik

Das BVerfG fordert zwar eine präzise Einhegung von Maßnahmen der automatisierten Datenanalyse durch den Gesetzgeber, lässt aber durchaus Spielraum für eine Verlagerung konkretisierender Normen auf die untergesetzliche Ebene, etwa in Rechtsverordnungen und Dienstvorschriften.⁴³ Hierfür muss der Gesetzgeber dann eine Ermächtigung schaffen. Vergleichbare Regelungsansätze auf Landesebene nutzen zum Teil bereits diese Möglichkeit.⁴⁴

So dürfte sich eine nähere Ausgestaltung im Wege der Rechtsverordnung anbieten für

- die Konkretisierung von Art und Umfang der zu verarbeitenden Daten und der zulässigen Analysemethoden,
- organisatorische und technische Sicherungen der Systeme vor Missbrauch,
- Vorgaben zum Monitoring der eingesetzten Software.

Durch Verwaltungsvorschrift könnten näher geregelt werden

- Vorgaben zur Kennzeichnung und Löschung von Daten und zur Protokollierung von Zugriffen,
- ein Rechte- und Rollenkonzept für Zugriffsberechtigungen,
- Vorgaben zur Schulung von Mitarbeitenden.

⁴² S. bereits *Löffelmann*, BT-Innenausschuss Prot-Nr. 20/74 v. 22.4.2024, S. 79.

⁴³ BVerfGE 165, 363, 414 f. (Rn. 113).

⁴⁴ Vgl. § 25a Abs. 3 S. 2 HSOG; § 47a Abs. 4 S. 1 BWPolG; § 65a Abs. 4 S. 2 POG RP.



Sowohl für die Regelungen zur automatisierten Datenanalyse als auch zum Abgleich biometrischer Daten vermag der gesetzgebungstechnische Ansatz, Verfahrensregelungen wortgleich in verschiedenen Regelungskontexten zu wiederholen, nicht zu überzeugen. Allein im BKAG werden auf diese Weise identische Regelungen an drei verschiedenen Stellen geschaffen. Der Gesetzestext wird dadurch unnötig aufgebläht. Eine Zentralnorm zu der jeweiligen Maßnahme würde für mehr Übersichtlichkeit sorgen.

III. Harmonisierung

Mit dem Projekt „Polizei 20/20“ sollen die dislozierten polizeilichen Datenbestände in einem gemeinsamen „Datenhaus“ zusammengeführt werden. Hierfür ist eine Rechtsgrundlage erforderlich. Im Zuge ihrer Schaffung wäre es ausgesprochen sinnvoll, auch gemeinsame Rechtsgrundlagen für den Abgleich biometrischer Daten und vor allem für die Verwendung von Systemen der automatisierten Datenanalyse zu schaffen. Bislang fehlt ein gemeinsames Regelungskonzept. Die bisher Gesetz gewordenen Regelungen zur automatisierten Datenanalyse weisen beträchtliche Unterschiede auf.⁴⁵ Wie bei diesem Befund eine Bündelung der Datenverwaltung erfolgen kann, ist völlig offen. Eine enge Abstimmung zwischen Bund und Ländern wäre dringend erforderlich.

Zentraler Regelungsort für eine Vorschrift, die Kategorien von Datenarten jeweils zulässigen Analysemethoden zuordnet und einheitliche gesetzliche Grundlagen für verfahrensrechtliche Sicherungen enthält, könnte das BKAG sein. In seiner Funktion als Zentralstelle für den polizeilichen Informationsverbund ist das BKA prädestiniert dafür, für verbindliche normative Vorgaben zur Datenanalyse und deren technische Rahmenbedingungen Sorge zu tragen. In den Befugnissen zur automatisierten Analyse in den einzelnen Fachgesetzen und in einem

⁴⁵ Etwa bei den Eingriffsschwellen (z.B. § 47a Abs. 1 Nr. 2 BWPoIG, § 25a Abs. 2 S. 1 Nr. 2 HSOg, § 65a Abs. 1 Nr. 2 POG RP; auch bei Straftaten von erheblicher Bedeutung; Art. 61a Abs. 1 BayPAG; auch bei drohender Gefahr), gesetzlichen Vorgaben zur Abwägung (§ 47a Abs. 6 BWPoIG; u.a. Status der Person; § 25a Abs. 3 HSOg, § 65a Abs. 6 POG RP: Veranlassungszusammenhang und Grundrechtsrelevanz), der Art der zulässigen Daten (z.B. § 47a Abs. 3 S. 2 BWPoIG, § 65a Abs. 3 S. 1 POG RP; auch Daten aus Asservaten; § 47a Abs. 2 S. 1 ASOG Bln, § 25a Abs. 2 S. 2 HSOg; auch Daten aus Asservaten und Telekommunikationsdaten; Art. 61a Abs. 2 S. 3, 4 BayPAG: keine biometrischen Daten, Audio- und Videodateien), den Verfahrenssicherungen (z.B. § 47a Abs. 4 bis 6 BWPoIG, § 25a Abs. 3, 4 HSOg, § 65a Abs. 4 bis 6 POG RP: Rechte- und Rollenkonzept; § 47a Abs. 3 S. 6 ASOG Bln: Benachrichtigung) und der aufsichtlichen Kontrolle (z.B. § 47a Abs. 8 BWPoIG; § 47a Abs. 5 S. 2, Abs. 6, 7 ASOG Bln; § 25a Abs. 4 S. 6, Abs. 5 S. 2 HSOg; § 65a Abs. 8 POG RP); vgl. zu einer (nicht ganz aktuellen) vergleichenden Bestandsaufnahme auch *Martini/Botta*, DÖV 2025, 1033, 1039 ff.



etwaig erforderlichen Staatsvertrag zum Informationsverbund könnte auf diese Zentralnorm Bezug genommen werden.

E. Schlussbemerkung

Die beabsichtigten Regelungen zum Abgleich biometrischer Daten sind sehr weitreichend. Ob sie verfassungsrechtlichen Anforderungen genügen, ist schwer einzuschätzen, weil einschlägige verfassungsrechtliche Judikatur insoweit bislang nicht vorliegt. Nicht den verfassungsrechtlichen Anforderungen entsprechen die beabsichtigten Regelungen zur automatisierten Datenanalyse. Sie entbehren weitgehend der erforderlichen gesetzlichen Vorgaben zu Art und Umfang der zu verarbeitenden Daten und den zulässigen Analysemethoden. Gerade bei der Verarbeitung von Daten, die aus eingriffsintensiven Primärmaßnahmen stammen, wird der Regelungszweck verfehlt, weil die erforderlichen Schwellen nicht höher liegen als bei den Erhebungseingriffen. Umgekehrt werden der Polizei durch die Orientierung an der Schwelle der konkretisierten Gefahr für besonders gewichtige Rechtsgüter Analyseanwendungen abgeschnitten, die den Schutz weniger gewichtiger Rechtsgüter bezwecken könnten.⁴⁶ Der (weitgehende) Verzicht auf die Eingriffsintensität einschränkende Maßgaben reduziert also in beträchtlichem Maße die verfassungsrechtlich zulässige Anwendungsbreite automatisierter Datenanalysen. Das ist unverständlich. Das aktuell größte Defizit in diesem Bereich ist jedoch das Fehlen eines kohärenten Regelungskonzepts für die Polizeien in Bund und Ländern. Es ist nicht zu erkennen, wie bei der gegebenen Heterogenität der Regelungen die polizeiliche Datenverwaltung zukunftsfest aufgestellt werden könnte. Auch für die im Sinne digitaler Souveränität wünschenswerte Entwicklung eigener Analysetools wäre ein schlüssiges technisch-normatives Konzept, welches das technisch Machbare mit dem normativ Zulässigen verknüpft, ein unverzichtbarer Ausgangspunkt. Bei alledem bleibt zu betonen, dass die Digitalisierung der Polizeiarbeit die mit Abstand wichtigste Weichenstellung für eine moderne, ressourcenbewusste, effektive und auch grundrechtsschonende Polizeiarbeit darstellen dürfte.

gez. Prof. Dr. Markus Löffelmann

⁴⁶ Vgl. BVerfGE 165, 363, 399, 411 f. (Rn. 74, 107).