



Ausschussdrucksache 21(4)179

vom 2. Juni 2026

Schriftliche Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Bonn vom 2. Juni 2026

zu dem

Gesetzentwurf der Bundesregierung

**Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit
BT-Drucksache 21/6132**

und dem

Gesetzentwurf der Bundesregierung

**Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von
Gefahren des internationalen Terrorismus des Bundesministeriums des Innern
BT-Drucksache 21/6131**

sowie dem

Gesetzentwurf der Bundesregierung

**Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungs-
maßnahmen“ des Bundesministeriums der Justiz und für Verbraucherschutz
BT-Drucksache 21/...**

Deutscher Bundestag
Vorsitzender des Innenausschusses
Herrn MdB Josef Oster
Platz der Republik 1
11011 Berlin
innenausschuss@bundestag.de

Deutscher Bundestag
Vorsitzender des Ausschusses für Recht und
Verbraucherschutz
Herrn MdB Carsten Müller
Platz der Republik 1
11011 Berlin
rechtsausschuss@bundestag.de

Deutscher Bundestag
Vorsitzender des Ausschusses für Digitales
und Staatsmodernisierung
Herrn MdB Hansjörg Durz
Platz der Republik 1
11011 Berlin
adi@bundestag.de

Digitale Ermittlungsbefugnisse

Sehr geehrte Herren Vorsitzende,

anlässlich Ihrer anstehenden Befassung mit dem „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ und dem „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“ des Bundesministeriums des Innern (BMI) sowie dem „Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“ des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) wende ich mich an Sie,

**Prof. Dr. Louisa
Specht-Riemenschneider**
Die Bundesbeauftragte

Telefon: +49 228 997799 5000

E-Mail: bfdi@bfdi.bund.de

Aktenz.: SI2-642/041#1777
(**bitte immer angeben**)

Dok.: 50904/2026

Anlage: 1

Bonn, 02.06.2026

um mich nachdrücklich für eine grundlegende Überarbeitung der vorgesehenen Regelungen dieses sogenannten „Sicherheitspakets“ einzusetzen.

Zu diesem Zweck möchte ich Ihnen zum einen meine erheblichen verfassungsrechtlichen Bedenken hierzu darlegen. Andererseits unterbreite ich konkrete Vorschläge, die geeignet sind, die Entwürfe praktisch tragfähiger auszugestalten und gleichzeitig einen angemessenen Ausgleich zwischen polizeilichen Praxisbedarfen und dem Grundrechtsschutz zu finden.

Ich bitte Sie, diese Stellungnahme an die Mitglieder Ihrer Ausschüsse zu verteilen.

Mit freundlichen Grüßen

Prof. Dr. Louisa Specht-Riemenschneider

Bonn, den 02.06.2026

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

**zum Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit
und dem Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr
von Gefahren des internationalen Terrorismus des Bundesministeriums des Innern (BMI)
sowie dem Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermitt-
lungsmaßnahmen“ des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV)**

Die vorliegenden Entwürfe enthalten Vorschriften zum biometrischen Datenabgleich (I.) und zur automatisierten Datenanalyse (II.).

Diese sind nach meiner Auffassung in der aktuell geplanten Form nicht mit höherrangigem Recht vereinbar. Aus meiner Sicht sollten, soweit möglich, alternative Lösungsmöglichkeiten stärker in den Fokus genommen werden.

I. Zum Biometrischen Datenabgleich

Durch die geplanten §§ 9a, 39a, 63b BKAG-E sowie § 98d StPO-E sollen Befugnisse der Polizei- und Ermittlungsbehörden zum biometrischen Datenabgleich eingeführt werden. Im Wesentlichen sollen dabei öffentlich zugängliche personenbezogene Daten, die biometrische Merkmale enthalten, aus dem Internet erhoben und mittels einer automatisierten Anwendung zur Datenverarbeitung unter bestimmten Voraussetzungen mit den Daten der jeweiligen Behörde biometrisch abgeglichen werden dürfen.

Insgesamt handelt es sich bei den Befugnissen um **intensive Grundrechtseingriffe**. Diese sind nach meiner Ansicht verfassungsrechtlich nicht in dieser Form gerechtfertigt und nicht vollständig mit europäischem Recht vereinbar.

Bewertung der Befugnisse

1. Datenbestand

Die geplanten BKAG-Vorschriften ermöglichen den Abgleich sämtlicher beim BKA verfügbarer biometrischer Daten mit Daten aus dem Internet. Das Bundeskriminalamt darf in diesen Abgleich einen in doppelter Hinsicht **maximal weitgehenden Datenbestand** einbeziehen. Zum einen sind dies alle (!) Daten, auf die das BKA zur Erfüllung seiner Aufgaben zugreifen darf. Dies sind nicht nur die Daten, die das BKA selbst in seinen Beständen gespeichert hat, sondern auch Daten anderer Behörden, auf die es zugreifen kann. Dies sind nicht notwendig polizeiliche Datenbestände, wie zum Beispiel der polizeiliche Informationsverbund, sondern potentiell alle Dateien, zu denen ein Gesetz eine Zugriffsmöglichkeit einräumt, beispielsweise das Ausländerzentralregister. Umfasst sind auch innerhalb des BKA nicht nur Daten, die zum Zwecke der Vorsorge – unter den entsprechend hohen in §§ 18 f. BKAG geregelten Voraussetzungen – gespeichert sind, sondern alle Daten. Dies umfasst auch die Daten zu Opfern und Zeugen im Vorgangsbearbeitungssystem, auch soweit diese dort nur zu Zwecken der Dokumentation polizeilichen Handelns gespeichert sind (z.B. Daten und Bilder des Opfers einer länger zurückliegenden Sexualstraftat, ggf. sogar

Tat- und Tatortbilder). Hier wäre mindestens ein Verweis auf die Geltung des **§ 22 Abs. 2 BKAG** erforderlich.

Entsprechendes gilt für die geplante StPO-Norm. Grundlage des Datenabgleichs gemäß § 98d Absatz 1 StPO-E sind biometrische Daten „aus einem Strafverfahren“. Damit ist nicht festgelegt, dass diese aus dem „bestimmten Strafverfahren“ stammen. Der Wortlaut lässt insofern den Zugriff auf alle bei Polizeibehörden oder Staatsanwaltschaften gespeicherten Daten aus (irgend)einem Strafverfahren zu. Dazu gehören nicht nur vereinzelte Lichtbilder, Stimmprofile oder andere biometrische Einzeldaten. Darüber hinaus können zum Beispiel umfangreiche Sammlungen von sichergestellten Videoaufnahmen herangezogen werden, die z.B. in einem weiten Umkreis um Tatorte in Ladengeschäften, öffentlichen Verkehrsmitteln etc. aufgenommen wurden.¹ Es ist nicht festgelegt, dass nur nach einer oder wenigen Personen gesucht werden darf, die als „Hauptverdächtige“ in Betracht kommen. Vielmehr kann eine Vielzahl von Personen abgeglichen werden, die in der Nähe eines Tatorts oder nach einer Versammlung z.B. öffentliche Verkehrsmittel benutzt haben. Vor allem in der Kombination mit anderen Vorschriften zur Datenanalyse wie § 98e StPO-E, § 9b BKAG-E oder § 25a HSOG ergeben sich hier weitreichende Möglichkeiten. Denn es sind auch biometrische Daten „aus einem Strafverfahren“ erfasst, die eine Künstliche Intelligenz zuvor aus einer Vielzahl von weiteren Datenbeständen als mögliche Beschuldigte, Zeugen oder sonst für das Verfahren oder einen Sachverhalt relevante Person vorgeschlagen hat. Diese Datenbestände können ihrerseits zahlreiche Videoaufnahmen enthalten.

Diese jeweils ihrerseits weitgehenden Datenbestände können mit sämtlichen im Internet verfügbaren Daten abgeglichen werden, auch bei kostenpflichtigen Diensten. Dass dies ein maximal weitgehender Eingriff insbesondere mit Blick auf die Streubreite ist, bedarf keiner Erläuterung.

2. Analysemethode

Durch den biometrischen Abgleich – dessen Technik nicht näher eingegrenzt ist – ist nicht nur der einzubeziehende Datenbestand, sondern auch die **Analysemethode für sich betrachtet eingriffsintensiv**. Umfangreiche **Bewegungs- und Verhaltensprofile** sind nicht

¹ Vgl. dazu etwa den Bericht des Hamburgischen Datenschutzbeauftragten über die „Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, abrufbar unter: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/Pruefbericht_Gesichtserkennungsoftware.pdf, zuletzt abgerufen am 18.05.2026, 14:29 Uhr.

ausgeschlossen, sondern sind durch die Formulierungen „zur Ergänzung vorhandener Sachverhalte“² bzw. „zur Erforschung des Sachverhalts“³ offenbar sogar beabsichtigt.

Ferner lassen die Gesetzentwürfe eine Darstellung vermissen, wie der Einsatz der Gesichtserkennungstechnologie technisch ermöglicht werden soll.

Nach der Begründung zu § 98d Absatz 1 StPO-E soll auch die Erhebung und temporäre Speicherung öffentlich zugänglicher Daten aus dem Internet von der Norm umfasst sein.⁴ Der vorgeschlagene Wortlaut des § 98d StPO-E erlaubt hingegen lediglich den Abgleich mit diesen Daten und bietet somit keine taugliche Erlaubnis für eine solche Erhebung und Speicherung.

Die KI-Verordnung verbietet unter anderem die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsmaterial erstellen oder erweitern.⁵ Da die Polizeibehörden demnach keine eigene umfassende Datenbank zur Gesichtserkennung anlegen dürfen, müssten sie für jeden Abgleich von Gesichtsbildern den aktuellen Lichtbildbestand des Internets erheben. Dies ist unter den heutigen technischen Gegebenheiten unrealistisch.

Bezüglich der Nutzung von Gesichtserkennungssoftware allgemein wird auf die Entschliessung der DSK vom 20. September 2024 Bezug genommen, in der es u.a. heisst:

„Sofern nach der KI-Verordnung und dem Verfassungsrecht Regelungsspielraum für den nationalen Gesetzgeber verbleibt und er den entsprechenden Einsatz als zwingend erforderlich betrachtet, muss er spezifische, verhältnismäßige Rechtsgrundlagen für den Einsatz von Gesichtserkennungssystemen schaffen. Hierin sind in Abhängigkeit von der Eingriffsintensität hinreichende Eingriffsschwellen, ausreichende Anforderungen an den Rechtsgüterschutz und zusätzliche Schutzmechanismen festzulegen.“⁶

² Siehe § 9a Abs. 1 Satz 1 Nr. 2 BKAG-E.

³ Siehe § 9a Abs. 1 Satz 1 Nr. 2, 39a Abs. 1 Satz 1 Nr. 1, 63 Abs. 1 Satz 1 BKAG-E sowie § 98d Abs. 1 Satz 1 StPO-E.

⁴ Siehe Gesetzesbegründung S. 13.

⁵ Art. 5 Abs. 1 lit. e) KI-Verordnung.

⁶ https://www.datenschutzkonferenz-online.de/media/en/2024-09-20_Entschliessung_DSK_Gesichtserkennung.pdf (letzter Abruf: 12.05.2026 17:00 Uhr).

3. Eingriffsschwellen

In der Gesamtschau ergibt sich also, dass die geplanten Befugnisse zum biometrischen Datenabgleich schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung ermöglichen.

Für gefahrenabwehrende Befugnisse hat das Bundesverfassungsgericht entschieden, dass Datenanalysen, die einen schwerwiegenden Grundrechtseingriff darstellen, nur zum Schutz besonders gewichtiger Rechtsgüter zulässig sind.⁷ Auf der repressiven Seite teilt das Bundesverfassungsgericht dabei die Anlasstaten in vier Kategorien. Dies sind einfache, erhebliche, schwere und besonders schwere Straftaten. Zwischen den Abstufungen auf repressiver und präventiver Seite ist ein Gleichlauf anzunehmen.⁸ Der Schutz besonders gewichtiger Rechtsgüter auf der präventiven Seite entspricht insofern der Verfolgung besonders schwerer Straftaten auf der repressiven Seite.⁹

a) § 9a BKAG-E

Die dargelegten Schwellen sieht der BKAG-Entwurf jedoch nicht vor. Anlass ist bei § 9a BKAG-E weder eine konkrete Gefahrenabwehr noch eine konkrete Strafverfolgungshandlung, sondern vielmehr nach Absatz 1 Satz 1 Nummer 2 allgemein die „Ergänzung vorhandener Sachverhalte“ als Zentralstelle. Voraussetzung für ein Tätigwerden ist laut der Begründung diesbezüglich lediglich, „dass bereits Ermittlungsunterlagen vorliegen“.¹⁰

Auf **welche Zentralstellenaufgabe** in § 9a Absatz 1 Satz 1 Nummer 2 BKAG-E genau verwiesen wird, **ist unklar** formuliert. Der Verweis auf § 2 Absatz 2 Nummer 1 BKAG umfasst lediglich allgemein das Sammeln und die Auswertung von Informationen und bezieht sich seinerseits auf die Generalklausel in Absatz 1, nach der das BKA die Polizeien der Länder unterstützt. Es müsste hier viel deutlicher herausgearbeitet werden, wofür der Datenabgleich konkret genutzt werden soll.

Der Kreis der in § 9a Absatz 1 Satz 1 Nummer 1 BKAG-E genannten Straftaten ist zu wenig eingegrenzt. Die Norm bewegt sich weit im Vorfeld einer Straftat, weil auch die allgemeine Prognose ausreichend ist, dass eine Person eine relevante Straftat begehen könnte.

Die in § 9a Absatz 1 Satz 1 Nummer 3 BKAG-E genannte **Subsidiaritätsklausel** führt als verbleibende tatbestandliche Grenze nicht zu einer nennenswerten Anhebung der Ein-

⁷ BVerfG, Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1206), Rn. 105.

⁸ BVerfG, Urteil vom 26.4.2022 – 1 BvR 1619/17, NJW 2022, 1583 (1598), Rn. 244 unter Verweis auf Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1807f.), Rn. 347.

⁹ Vgl. BVerfG, Beschluss v. 28.9.2022 – 1 BvR 2354/13, GSZ 2022, 299 (305) Rn. 136; Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1807f.), Rn. 347.

¹⁰ Siehe Begründung zu § 9a BKAG-E, S. 24 des Entwurfs.

griffsschwelle. Mit der Formulierung „wesentlich erschwert“ enthält sie einen unbestimmten Rechtsbegriff. Es wird zur Anhebung der Eingriffsschwelle empfohlen, eine Formulierung wie „**unbedingt erforderlich**“ zu verwenden. Vorsorglich weise ich darauf hin, dass eine Änderung dieses Merkmals nicht dazu führt, die oben genannten Mängel – insbesondere den Verweis auf die wenig konkrete Zentralstellenaufgabe – zu beheben.

b) § 98d StPO-E

Als Eingriffsschwelle ist in § 98d Absatz 1 StPO-E lediglich vorgesehen, dass Anlass eine Straftat von erheblicher Bedeutung sein muss. Nicht gefordert werden schwere bzw. besonders schwere Straftaten. Der Verweis auf den Katalog des § 100a Absatz 2 StPO ist irreführend. Dieser Katalog soll zwar formal „schwere Straftaten“ umfassen, doch verweist Absatz 1 auf diesen nur „insbesondere“ und lässt im Übrigen niedrigschwellig „Straftaten von erheblicher Bedeutung“ genügen.

Nach der dargelegten Systematik des Bundesverfassungsgerichts wäre mindestens ein Verweis auf den Katalog des § 100b Absatz 2 StPO erforderlich. In der vorherigen Version dieses Gesetzesentwurfs wurde der § 100b Absatz 2 StPO als Schwelle zugrunde gelegt.¹¹ Warum diese Schwelle im aktuellen Entwurf wieder abgesenkt wurde, ist für mich nicht nachvollziehbar. Ein Verweis auf den Katalog des **§ 100b Absatz 2 StPO oder aber des § 138 StGB** wäre erforderlich. Wie oben dargelegt entspricht die im präventiven Bereich geltende Schwelle der besonders wichtigen Rechtsgüter im repressiven Bereich der besonders schweren Straftat. Diese ist nicht im Katalog des § 100a Abs. 2 StPO abgebildet, sondern im Katalog des § 100b Abs. 2 StPO. Als weitere alternative Lösung könnte der Gesetzgeber auch an die **Öffentlichkeitsfahndung gemäß § 131b StPO** anknüpfen. Diese Anknüpfung würde auch thematisch am nächsten liegen.¹²

4. Adressatenkreis

a) Geplante Änderungen im BKAG

Der jeweils in Absatz 2 der geplanten BKAG-Vorschriften definierte **Personenkreis** Betroffener ist zu weit gefasst. Bei § 9a BKAG-E sind neben den nach Bundespolizeigesetz (BPolG) polizeipflichtigen Personen explizit Tatverdächtige, Beschuldigte sowie Personen nach § 18 Absatz 1 Nummer 4 BKAG umfasst. In §§ 39a, 63b BKAG-E ist der Kreis der Be-

¹¹ Vgl. Drucksache 20/14704, Seite 29, Zu Nummer 1.

¹² Siehe hierzu weiter unten bei „5. Übermittlungsbefugnisse“.

troffenen noch weiter. Damit ist der Personenkreis schon für sich genommen sehr weit gefasst. Das Bundesverfassungsgericht hat entschieden, dass bereits die vorsorgende Speicherung personenbezogener Daten der hier genannten Personen zur Erfüllung der Zentralstellenaufgaben des BKA allein aufgrund der Beschuldigteneigenschaft nicht verhältnismäßig ist.¹³ In Anbetracht dieser Entscheidung begegnet die dargestellte Eingriffsschwelle zum – in seiner Eingriffsintensität über die Vorsorgespeicherung hinausgehenden – Datenabgleich verfassungsrechtlichen Bedenken.

b) § 98d StPO-E

Der Adressatenkreis des § 98d StPO-E ist noch weniger eingegrenzt. Der biometrische Datenabgleich soll hier „zur Erforschung des Sachverhalts“ bereits möglich sein, wenn der Verdacht besteht, jemand habe als Täter oder Teilnehmer eine Straftat nach § 100a Absatz 2 StPO durch eine Straftat vorbereitet. Unter den Wortlaut der Norm ist somit bereits die Beihilfe zum einfachen Diebstahl an einem Kennzeichen zu subsumieren, wenn der Verdacht besteht, dass dieses Kennzeichen später bei der Einfuhr von Betäubungsmitteln verwendet werden soll – unabhängig davon, ob dieser mutmaßliche Plan je in die Tat umgesetzt wird. Dies stellt eine **übermäßige Vorverlagerung des Anknüpfungspunktes der Strafbarkeit** dar, die mit der Eingriffstiefe der Befugnis nicht in Einklang zu bringen ist. Hier ist unbedingt eine Eingrenzung vorzunehmen. Möglich wäre etwa eine **Beschränkung auf Beschuldigte bei Verdacht einer Tat nach § 100b Absatz 2 StPO**.

5. Übermittlungsbefugnisse

a) Geplante Änderungen im BKAG

Die in den Absätzen 5 und 6 der geplanten BKAG-Normen geregelten **Übermittlungsbefugnisse gehen deutlich zu weit**. Das Bundesverfassungsgericht hat entschieden, dass die Übermittlung von Daten an staatliche Stellen im Ausland den allgemeinen verfassungsrechtlichen Grundsätzen von Zweckänderung und Zweckbindung unterliegt.¹⁴ Insofern besteht für die sich sowohl auf öffentliche als auch nicht-öffentliche Stellen beziehenden Absätze 5 und 6 jedenfalls erheblicher weitergehender Klärungsbedarf hinsichtlich einer möglichen verfassungskonformen Ausgestaltung.

¹³ BVerfG Urteil vom 01.10.2024 – 1 BvR 1160/19, NVwZ 2024, 1736 (1749 ff.), Rn. 174 ff.

¹⁴ BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1799 f.) Rn 276 f.

Die verantwortlichen Stellen sollen danach personenbezogene Daten an nichtöffentliche Stellen übermitteln dürfen, ohne dass diese verpflichtet sind, die zulässigen Verarbeitungszwecke zu beachten. Das eröffnet es gleichzeitig, die Dienste jeglicher privater Dienstleister zu nutzen. Dies umfasst auch sämtliche KI-Systeme und ist unabhängig davon, wer das System betreibt, welchem Datenschutzregime die Verarbeitung unterliegt und wie fehleranfällig diese ist. Die Nutzung von kommerziellen Anbietern wie PimEyes oder Clearview AI ist durch die Ausgestaltung der jeweiligen Absätze 6 der Normen erkennbar beabsichtigt.

Hintergrund der geplanten Regelung ist die Identifizierung von Daniela Klette, die durch einen Journalisten mit Hilfe von PimEyes erfolgte.¹⁵ Es ist nachvollziehbar, dass es aus Sicht der Ermittlungsbehörden nicht akzeptabel ist, wenn Privatpersonen Ermittlungserfolge mit öffentlich verfügbaren Werkzeugen herbeiführen, die den Ermittlungsbehörden untersagt sind. Datenbanken wie jene von PimEyes und Clearview AI sind datenschutzrechtlich jedoch höchst bedenklich und kaum mit der KI-VO sowie der DSGVO vereinbar.¹⁶ Die Datenverarbeitung ist zudem intransparent und nicht kontrollierbar. Die eingriffsintensive Nutzung solcher Services durch deutsche Ermittlungsbehörden ist daher äußerst kritisch zu sehen.¹⁷ Der Gesetzentwurf lässt zudem eine entscheidende Tatsache außer Betracht: Daniela Klette war zur Öffentlichkeitsfahndung ausgeschrieben, die abgeglichenen Lichtbilder von ihr waren also ohnehin weltweit für jedermann verfügbar. Mit einiger Wahrscheinlichkeit waren die Lichtbilder bereits bei PimEyes gespeichert, bevor der Journalist sie zum Zwecke des Abgleichs dort hochlud. Diese Tatsache senkt die Eingriffsintensität der geplanten Datenübermittlung erheblich. Es wird daher dringend empfohlen, die Anwendbarkeit der jeweiligen **Absätze 5 und 6 der geplanten BKAG-Normen auf Personen zu beschränken, die zur Öffentlichkeitsfahndung ausgeschrieben sind**. Für die Fälle, die der Gesetzgeber hier im Blick hat, ist die Verhältnismäßigkeit der Normen aus hiesiger Sicht ohne Öffentlichkeitsfahndung ausgeschlossen. Dabei ist festzuhalten, dass auch die

¹⁵ Vgl. <https://www.zeit.de/gesellschaft/zeitgeschehen/2024-03/daniela-klette-fahndung-polizei-raf-terroristin> (letzter Abruf: 22.05.2026, 07: 45 Uhr); <https://verfassungsblog.de/klette-und-die-frucht-der-vergifteten-maschine/> (letzter Abruf: 22.05.2026, 07:48 Uhr).

¹⁶ Vgl. Art. 5 Abs. 1 Satz 1 lit. e) KI-VO; LfDI Baden-Württemberg, Pressemitteilung vom 21. Dezember 2022 <https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/> (letzter Abruf: 18.05.2026, 11:23 Uhr); <https://noyb.eu/de/no-action-taken-against-pimeyes-noyb-lawsuit-against-hamburg-dpa> (letzter Abruf: 19.05.2026, 14:52 Uhr).

¹⁷ Vgl. hierzu auch den Beschluss des AG Reutlingen vom 11.02.2026 (Az.: 5 Gs 19/26). Dort wird ein dringender Tatverdacht und damit auch der beantragte Haftbefehl insbesondere aus dem Grund abgelehnt, dass sich das Ermittlungsergebnis der Polizei allein auf das Ergebnis einer „Gesichtserkennungssoftware“ stützt, „deren Funktionsweise, Algorithmus, Referenzdaten und Qualitätsparameter nicht nachvollziehbar dokumentiert sind“ <https://www.landesrecht-bw.de/bsbw/document/NJRE001637569> (letzter Abruf: 19.05.2026, 14:54 Uhr).

Schwellen des § 131b StPO in der Praxis teilweise überstrapaziert werden¹⁸ und daher aus unserer Sicht ebenfalls einer Schärfung bedürften.

b) § 15b AsylG-E

Auch in § 15b Absatz 4 Satz 2 AsylG-E ist nunmehr die Übermittlung der biometrischen Daten zum Abgleich mit öffentlich zugänglichen Daten aus dem Internet an nichtöffentliche Stellen im Inland und in das europäische Ausland vorgesehen. Eine Übermittlung an nicht-öffentliche Stellen ist in dem geltenden § 15b Absatz 9 Satz 4 AsylG ausdrücklich ausgeschlossen.¹⁹ Die Gesetzesbegründung macht zur Abkehr von der bisherigen Regelung keine Ausführungen, es wird lediglich ausgeführt, dass „zur Durchführung des biometrischen Internetabgleichs nach Absatz 1 eine Übermittlung an andere öffentliche oder nichtöffentliche Stellen erforderlich sein [kann]“²⁰. Das ist in Anbetracht der Eingriffsintensität in das Grundrecht auf informationelle Selbstbestimmung unzureichend. Die Erforderlichkeit dieser Regelung ist bereits nicht dargelegt. Zur Verhältnismäßigkeit der Regelung wird in der Gesetzesbegründung ebenfalls nichts ausgeführt.

Des Weiteren ist es widersprüchlich, wenn das BMI selbst in der Gesetzesbegründung ausführt, dass Art. 14 KI-VO (Menschliche Aufsicht) zu beachten ist²¹, ergo davon ausgeht, dass die Anwendung zum Abgleich der biometrischen Daten eine Hochrisiko-KI sein wird, aber die Möglichkeit einräumt, die mit der KI zu bewältigende Aufgabe an andere öffentliche oder nichtöffentliche Stellen im Inland oder in der EU übertragen zu können, wenn der Abgleich technisch unmöglich ist oder mit unverhältnismäßigem Aufwand verbunden ist. Zudem das BKA dem BAMF gemäß § 16 Absatz 3 AsylG Amtshilfe leistet.

6. Fragliche Gesetzgebungskompetenz

Teilweise ist die **Gesetzgebungskompetenz** zu den BKAG-Normen **fraglich**. Aus hiesiger Sicht ist nicht klar, inwieweit die Gesetzesbegründung zu § 9a Absatz 6 BKAG-E²² in Bezug auf den Zweck des Schutzes der nationalen Sicherheit sich mit der in § 9a Absatz 1 Nummer 2 BKAG-E festgelegten Erfüllung der Aufgabe als Zentralstelle vereinbaren lässt. Für den Schutz der nationalen Sicherheit, insbesondere in Form der Abwehr terroristischer Aktivitäten, findet sich in dem Gesetzentwurf „zur Stärkung digitaler Ermittlungsbefugnisse

¹⁸ Zur vermehrten Nutzung der Öffentlichkeitsfahndung in Bagatelldfällen vgl. <https://www.heise.de/news/Digitale-Rasterfahndung-Wenn-Bilder-im-Netz-Leben-zerstoeren-11305596.html> (letzter Aufruf 27.05.2026, 10:50 Uhr).

¹⁹ Vgl. den Wortlaut der Norm: „Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind.“

²⁰ Siehe Begründung zu § 15b AsylG-E, S. 37 des Entwurfs.

²¹ Siehe Begründung zu § 15b AsylG-E, S. 37 des Entwurfs.

²² Siehe Gesetzesbegründung zu § 9a BKAG-E, Seite 26 unter „Zu Absatz 6“.

zur Abwehr von Gefahren des internationalen Terrorismus“ der § 39a BKAG-E, der den zustimmungsbedürftigen Teil des Gesetzespakets darstellt. Insofern ist hier nicht verständlich, wieso die Regelung der § 9a Absatz 6 Nummer 1 und § 63b Absatz 6 Nummer 1 BKAG-E, die nach dem Wortlaut ebenso zum Schutz der nationalen Sicherheit geschaffen werden sollen, sich im nicht zustimmungsbedürftigen Teil des Gesetzespakets befindet. Insoweit muss bereits die Gesetzgebungskompetenz in Frage gestellt werden. Die jeweiligen Absätze 6 der Regelungen dürften unter Artikel 73 Absatz 1 Nummer 9a GG fallen und bedürfen somit nach Artikel 73 Absatz 2 GG der **Zustimmung des Bundesrats**.

Darüber hinaus sind auch die **Regelungen der geplanten Übermittlungsbefugnisse im Zusammenhang mit dem Schutz der nationalen Sicherheit**²³ aus hiesiger Sicht **nicht mit dem europäischen Recht vereinbar**. Entgegen der Begründung zu § 39a Absatz 6 BKAG-E²⁴ sind aus Sicht der BfDI sämtliche Datenverarbeitungen der Strafverfolgungsbehörden den verschiedenen Zwecken der Richtlinie (EU) 2016/680 zuzuordnen. Sie haben insofern im Anwendungsbereich des Unionsrechts zu erfolgen und dessen Grenzziehungen sowie materielle Vorgaben insbesondere zum Grundsatz der Zweckbindung zu respektieren. Eine Neuorientierung ist daher abzulehnen.

7. Unzureichende Schutzmechanismen

Neben den bereits dargelegten Bedenken zu den unzureichenden Eingriffsschwellen ist festzuhalten, dass zusätzliche **Schutzmechanismen** für den Einsatz des biometrischen Abgleichs fehlen.

Für die Fälle, die nicht von Artikel 26 Absatz 10 Unterabsatz 1 KI-VO erfasst werden, sieht der Gesetzentwurf keinerlei Schutzmechanismen vor. Dies betrifft vor allem den biometrischen Abgleich zur erstmaligen Identifizierung eines potenziellen Verdächtigen.

Systeme zum biometrischen Abgleich und insbesondere zur Gesichtserkennung besitzen eine spezifische **Fehleranfälligkeit**.²⁵ Ich empfehle daher eine Klarstellung in allen Gesetzesentwürfen oder zumindest in deren Begründung hinsichtlich der regelhaften Anwendbarkeit des **Vieraugenprinzips nach Artikel 14 Absatz 5 Unterabsatz 1 KI-VO**. Die Unverhältnismäßigkeit im Sinne von Unterabsatz 2 der Vorschrift ist aus hiesiger Sicht in der Praxis restriktiv zu handhaben.

a) Geplante Änderungen im BKAG

²³ Vgl. §§ 9a Absatz 6 Nr. 1, 39a Absatz 6, § 63 b Absatz 6 BKAG-E sowie § 58a Absatz 6 BPolG, §§ 18a Absatz 7, 36a Absatz 7 ZollKrimBG-E.

²⁴ Siehe Gesetzesbegründung zu den digitalen Ermittlungsbefugnissen in der Polizeiarbeit Seite 26.

²⁵ Vgl. Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 1. A. 2025, S. 32 f., 309 ff.

Ich empfehle für die geplanten BKAG-Normen zumindest eine **alleinige Anordnungskompetenz der Präsidentin oder des Präsidenten des BKA** festzulegen. Die in den BKAG-Regelungen jeweils in Absatz 8 Satz 5 enthaltene Übertragung der Anordnungskompetenz auf potentiell alle Bedienstete des BKA mit Befähigung zum Richteramt geht deutlich zu weit.

Auch fehlt im BKAG-Entwurf eine explizite Regelung entsprechend § 45 Absatz 7 BKAG zur Unzulässigkeit der Maßnahme, wenn anzunehmen ist, dass allein **Erkenntnisse aus dem Kernbereich privater Lebensgestaltung** erlangt würden und eine entsprechende **Anordnung der Löschung** dieser Erkenntnisse. Die KI-VO trifft keine speziellen Regelungen zum Kernbereichsschutz, ich empfehle diese zu ergänzen.

b) § 98d StPO-E

Ebenso sollte bei § 98d StPO-E die **Anordnung allein durch die Staatsanwaltschaft** erfolgen dürfen. Die Möglichkeit zur Eilanordnung durch Ermittlungsbeamte kann nicht nachvollzogen werden. Es handelt sich um eine aufwendige und komplexe Maßnahme, die für Eilanordnungen in der Sache ungeeignet ist. Hier sollte eine entsprechende **Anordnung des § 131c StPO** vorgesehen werden, insbesondere wenn die Vorschrift meinem oben dargestellten Lösungsvorschlag angepasst wird.

§ 98d Absatz 3 StPO-E bezieht sich nur auf die unverzügliche Löschung von Daten ohne konkreten Ermittlungsgrundsatz. Überwiegende schutzwürdige Interessen der betroffenen Person im Einzelfall werden nicht mehr berücksichtigt. Das steht nicht im Verhältnis zur Eingriffsintensität der Maßnahme. Auch hier sollte zumindest eine Regelung zum Kernbereichsschutz eingefügt werden.

§ 98d Absatz 1 Satz 2 StPO-E schließt zwar einen Abgleich mit Echtzeitdaten aus. Nach der Begründung sollen insbesondere keine Live-Streams und -Videos sowie Echtzeit-Lichtbild-Sequenzen verwendet werden.²⁶ Die Norm regelt allerdings nicht, wie im Einzelfall **sicher-gestellt** werden soll, dass es sich bei den zum Abgleich verwendeten Daten **nicht um Echtzeitdaten handelt**. Diese Beschränkung des Ausschlusses auf „live“ bzw. in Echtzeit übertragene Daten ist ungenügend. Echtzeitdaten im Sinne der KI-VO sind Daten, die „ohne erhebliche Verzögerung“ verarbeitet werden (vgl. Erwägungsgrund 17 der KI-VO). Ob eine solche „erhebliche Verzögerung“ vorliegt, muss im Einzelfall geprüft werden.²⁷ Eine solche **Pflicht zur Prüfung im Einzelfall** sollte normiert werden, um zu gewährleisten, dass keine (grundsätzlich unzulässige) biometrische Echtzeit-Fernidentifizierung im Sinne von Artikel 5 Buchstabe h KI-VO stattfindet.

²⁶ Siehe Gesetzesbegründung zu § 98d StPO-E, Seite 13.

²⁷ Vgl. Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung) (abrufbar unter <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>; letzter Abruf 18.05.2026, 16:48 Uhr), Rn. 310.

Die in § 98d Absatz 2 StPO-E vorgesehene Protokollierung umfasst zudem nicht die abgeglichenen Daten und ermöglicht deshalb keine **datenschutzrechtliche Kontrolle**. Es fehlt darüber hinaus die Angabe, auf welche Personen oder Daten sich die Datenabgleiche beziehen.

c) § 15b AsylG-E

Speziell bei § 15b AsylG war bisher in dessen Absatz 3 geregelt, dass die Treffer des Abgleichs durch Inaugenscheinnahme zu überprüfen sind. Dies wurde mit der Einführung des § 15b AsylG 2024 eingeführt, um der KI-VO Rechnung zu tragen. Dies ist nunmehr im § 15b AsylG-E ersatzlos weggefallen. Der Verweis auf Art. 14 KI-VO in der Gesetzesbegründung fängt den Wegfall dieser Regelung nicht auf. Die Klarstellung sollte nach meinem Dafürhalten nicht aus dem Normtext gestrichen werden.

Des Weiteren ist die in § 15b Absatz 10 AsylG vorgesehene **Pflichtkontrolle** der BfDI im Entwurf ersatzlos weggefallen. Diese war als Kompensation für den Eingriff in die Grundrechte der Betroffenen aufgenommen worden. Zur geplanten Streichung wird in der Gesetzesbegründung gar nichts ausgeführt. Die Pflichtkontrolle sollte beibehalten werden.

Ebenso sollte nach § 15b Absatz 11 AsylG die BfDI bei der von der Bundesregierung zu erarbeitenden Rechtsverordnung für das technische Verfahren des automatisierten Abgleichs der biometrischen Daten angehört werden. Auch diese Regelung ist im Gesetzentwurf ersatzlos und ohne Begründung entfallen. Die Regelung sollte wieder aufgenommen werden.

Insgesamt ist eine Befristung der Gesetze und eine vorzusehende **Evaluierung** anzuregen.

II. Zur Automatisierten Datenanalyse

Die Bundesregierung beabsichtigt, durch die geplanten Regelungen der §§ 9b, 39b, 63c BKAG-E, § 58b BPolG-E sowie § 98e StPO-E Befugnisse zur automatisierten Datenanalyse zu verschiedenen polizeilichen und ermittlungstechnischen Zwecken einzuführen. Im Wesentlichen handelt es sich hierbei jeweils um die Befugnis, bestimmte Daten unter bestimmten Voraussetzungen mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenzuführen und darüber hinaus zum Zwecke der Analyse weiterzuverarbeiten.

1. Die Befugnisse im Licht der aktuellen verfassungsrechtlichen Vorgaben

Das Bundesverfassungsgericht hat in seiner Entscheidung zur automatisierten Datenanalyse ein zweistufiges Vorgehen des Gesetzgebers vorgezeichnet.²⁸ Auf der ersten Stufe kann der Gesetzgeber die Eingriffsintensität der Datenanalyse steuern. In der zweiten Stufe kann er anschließend daran angepasste Eingriffsschwellen festlegen. Begrenzt er die Tiefe des mit der Analyse verbundenen Grundrechtseingriffs, kann er Analysen unter niedrigeren Schwellen zulassen. Tut er das nicht, sind automatisierte Datenanalysen auf der Gefahrenabwehrseite nur zum Schutz höchstrangiger Rechtsgüter zulässig. Daraus folgt für repräsentative Befugnisse, dass die Ermittlungsbehörden damit nur besonders schwere Straftaten verfolgen dürfen.

Maßgebend für die Eingriffsintensität der Datenanalyse an sich sind unter anderem die Streubreite, der von den betroffenen Personen gegebene – oder eben nicht gegebene – zu-rechenbare Anlass, die Möglichkeit der Bildung von Bewegungs-, Verhaltens- oder Persönlichkeitsprofilen sowie potentielle Diskriminierungsrisiken. Ganz maßgeblich wird die Eingriffsintensität dabei vor allem durch Art und Umfang der einzubeziehenden Daten bestimmt.²⁹

Ergänzend ist dabei zu beachten, dass das Bundesverfassungsgericht in seiner Entscheidung vom 1. Oktober 2024 klargestellt hat, dass innerhalb der polizeilichen Datenverarbeitung **nach verschiedenen internen Zwecken zu differenzieren** ist. Es hat betont, dass die Speicherung zu Zwecken der Vorsorge ein eigenständiger Grundrechtseingriff ist.³⁰ Dadurch unterliegen die Daten, die nicht zu Zwecken der Vorsorge gespeichert sind, zugleich anderen Verwendungsregeln. Insbesondere darf diese Zwecktrennung prinzipiell nicht dadurch unterlaufen werden, dass Daten aus abgeschlossenen Fällen, die lediglich zu Zwecken der Dokumentation gespeichert sind, über den Umweg der Datenanalyse zu Zwecken der Vorsorge verwendet werden. Dasselbe gilt in besonderer Weise für Daten zu Personen, die selbst keinen ihnen zurechenbaren Anlass für polizeiliche Maßnahmen gegeben haben, wie insbesondere Zeugen und Opfer von Straftaten. Das Bundesverfassungsgericht hat auf diesen Zusammenhang, der auch – aber nicht nur – Daten aus den Vorgangsbearbeitungssystemen betrifft, besonders hingewiesen.³¹

Auffällig ist, dass in allen bislang vorliegenden Vorschlägen der „Sicherheitspakete“ **weitgehend darauf verzichtet wird, den vom Gericht vorgezeichneten und aus meiner Sicht äußerst sinnvollen, differenzierten und lösungsorientierten Weg** zu gehen. Stattdessen werden pauschal sehr weitreichende Datenanalysen vorgesehen, die zu intensiven Grundrechtseingriffen führen. Auf ein gestuftes Vorgehen wird verzichtet, obwohl dies mit einer moderneren Datenverarbeitung möglich wäre.

²⁸ BVerfG, Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1202), Rn. 71.

²⁹ Ebd., Rn. 76.

³⁰ BVerfG, Urteil vom 01.10.2024 – 1 BvR 1160/19, NVwZ 2024, 1736 (1740), Rn. 90.

³¹ BVerfG Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1208), Rn. 126.

So könnten etwa Datenanalysen auf die Daten beschränkt werden, die in den polizeilichen Systemen für Zwecke der Vorsorge gespeichert sind. Für bestimmte Fälle könnte der Gesetzgeber den Kreis der Daten stufenweise und in verhältnismäßiger Weise erweitern.

Statt auf einzelne und grundrechtlich fragwürdige Analysesysteme zu setzen, wäre es **ziel-führender, die polizeiliche Datenverarbeitung grundlegend zu modernisieren**. Analysesysteme, wie sie mit den vorgeschlagenen Befugnissen propagiert werden, sind nur dann notwendig, wenn die vorliegenden polizeilichen Daten in geringer Qualität und unstrukturiert vorliegen. Gerade dieses Problem wird aber mit dem **Programm P20** angegangen. Dies bietet aufgrund der besseren Datenstruktur die Chance, stärkere Rücksicht auf die Zweckbindung der Daten zu nehmen. Dann wäre keine Vorschrift notwendig, die pauschal die Analyse einer Vielzahl von Daten erlaubt, auch zu Zeugen, Opfern und Unbeteiligten. Vielmehr könnten mit stärker begrenzten Befugnissen ebenfalls gute Ergebnisse erzielt werden, die dann nur in bestimmten Fällen gestuft erweitert werden müssten.

Umgekehrt können allerdings Befugnisse, die die datenschutzrechtliche Zweckbindung in polizeilichen Dateien weitgehend aushebeln, die polizeiliche Datenverarbeitung in einem modernisierten Datenhaus in weiten Teilen unverhältnismäßig werden lassen. Das **gefährdet dann sogar solch wichtige Projekte** wie das genannte Programm P20. Denn die Modernisierung der polizeilichen Datenverarbeitung und die – auch grundrechtliche – Rechtsbindung der Verwaltung müssen Hand in Hand gehen. Im BKAG-Entwurf wurde allerdings durch die Bezugnahme auf § 22 Absatz 2 BKAG jedenfalls in die richtige Richtung gegengesteuert.

2. Bewertung der Befugnisse

Alle hier geplanten Eingriffsnormen zur automatisierten Datenanalyse weisen zu unscharfe Tatbestandsmerkmale auf und ermöglichen erhebliche Eingriffe in die Rechte unbeteiligter Personen.

a) Dauerhafte Speicherung der Daten in der Analyseplattform

Von vornherein nicht verfassungsrechtlich tragfähig ist die vorgesehene dauerhafte Speicherung der Daten in einer neuen „**Super-Datenbank**“.³²

³² Vgl. BVerfG, Urteil v. 1.10.2024 – 1 BvR 1160/19, NVwZ 2024, 1736 (1750), Rn. 183.

Auch wenn die sprachliche Fassung der geplanten BKAG-Befugnisse zur automatisierten Datenanalyse dies auf den ersten Blick nicht nahelegten, ist der Aufbau einer solchen Datenbank ausweislich der Begründung das ausdrückliche Ziel der Regelung.³³ Bei der geplanten StPO-Norm setzt die Begründung eine solche polizeiliche Analyseplattform explizit voraus.³⁴

Möglich werden soll – dauerhaft und unabhängig von einem konkreten Vorgang – die Zusammenführung aller Daten aus dem Informationssystem des BKA und dem polizeilichen Informationsverbund aller deutschen Polizeibehörden. Dies umfasst eine Vielzahl von Daten Beschuldigter, Opfer, Zeugen oder sogar gänzlich unbeteiligter Personen. Zudem handelt es sich um Daten sehr unterschiedlicher Sensibilität, von bloßen Adressen über medizinische Gutachten bis hin zu Namen von Vergewaltigungsopfern und Angaben über Details solcher Taten.

Das Bundesverfassungsgericht hat in seiner Entscheidung zur automatisierten Datenanalyse keine Aussagen über eine dauerhaft zugrundeliegende Datenbank getroffen. Es ging anscheinend davon aus, dass jeweils im Zeitpunkt der automatisierten Datenanalyse der dafür zu verarbeitende Datenbestand zusammengestellt wird. Die hier beabsichtigte, dauerhaft angelegte Datenbank stellt einen darüber hinaus gehenden, äußerst schwerwiegenden Eingriff dar, welcher nicht mit dem Grundgesetz vereinbar ist:

„Der Staat darf nicht etwa alle Daten, die er rechtmäßig erhoben oder geschaffen hat, über den primären Zweck hinaus mit der Begründung vorsorgend speichern, die Daten könnten künftig noch einmal benötigt werden und der gebotene Schutz könne in die Ausgestaltung der zulässigen künftigen Nutzung verlagert werden. Unzulässig wäre es daher, unabhängig von solchen Zweckbestimmungen einen Datenvorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt. Die Bereitstellung eines solchen seiner Zwecksetzung nach offenen Datenvorrats würde den notwendigen Zusammenhang zwischen Speicherung und Speicherungszweck aufheben und

³³ Siehe Begründung zu § 9b BKAG-E, Seite 29 des Entwurfs: „Der Vorgang der Zusammenführung und Formatierung ist aufgrund der Masse der Daten aufwändig, so dass eine Zusammenführung lediglich im Einzelfall dem gewünschten Zweck der schnellen und effektiven Straftatenverhütung und -verfolgung nicht gerecht werden könnte. Die technische Zusammenführung der Daten sichert die Verarbeitbarkeit der Daten im Rahmen der automatisierten Datenanalyse. Die Zusammenführung muss daher aus technischen Gründen vom Einzelfall und weiteren Eingriffsschwellen unabhängig sein.“

³⁴ Siehe Begründung zu § 98e StPO-E, Seite 16 des Entwurfs: „Absatz 1 regelt die grundsätzliche Befugnis der Strafverfolgungsbehörden [...] in Datei- und Informationssystemen der Polizei rechtmäßig gespeicherte und für eine polizeiliche Analyseplattform zusammengeführte, personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung weiter zu verarbeiten [...]“.

damit auch die zentrale datenschutzrechtliche Freiheitssicherung durch die Zweckbindung. Auch wäre die Tragweite für die Bürgerinnen und Bürger nicht vorhersehbar“.³⁵

Nicht geregelt ist, wie lange die Daten in dieser Super-Datenbank vorgehalten werden dürfen. Das erhöht die Eingriffstiefe nochmals. Selbst wenn § 98e StPO-E nicht als eigene Rechtsgrundlage für den Betrieb der Analyseplattformen angesehen würde, bliebe dieses Problem. Denn darunter leidet auch etwa der § 25a HSOg, auf den die Gesetzesbegründung verweist³⁶, ebenso wie § 9b BKAG-E.

b) Polizeiliche Zwecktrennung und polizeilicher Regelungsbereich

Wie bereits dargestellt stellt die vorsorgende Speicherung personenbezogener Daten einen eigenständigen Grundrechtseingriff von erheblichem Gewicht dar, sodass eine solche Speicherung im polizeilichen Informationsverbund nur unter engen Bedingungen und nur befristet möglich ist.³⁷

Es ist eine polizeiinterne Zwecktrennung vorzusehen. Diese muss differenzieren zwischen primärer Aufgabenerfüllung, Dokumentation polizeilichen Handelns und vorsorgender Speicherung.

Insbesondere die Vorgangsbearbeitungssysteme der Polizeibehörden müssen deshalb die Daten nach den oben genannten Zwecken trennen.³⁸ Die Zugriffsregeln müssen dann so gestaltet werden, dass die Daten nur für ihren jeweiligen Zweck genutzt werden können.

Speichert man jedoch alle Daten pauschal in einer Analyseplattform, dann unterläuft dies die Grenzen, die für die vorsorgende Speicherung gelten. Einbezogen sind dann nicht nur Beschuldigte, sondern ebenso Zeuginnen und Zeugen sowie unbeteiligte Dritte. Dies schließt biometrische Daten oder besonders sensible Inhalte von Zeugenaussagen ein, etwa der Opfer von Sexualstraftaten. Zudem kann dies dann etwa Daten aus Ordnungswidrigkeitenverfahren betreffen, allgemeine Verkehrsunfallaufnahmen und alle sonstigen niedrigschwellig erhobenen polizeilichen Informationen.

Die geplante StPO-Vorschrift will jedoch diese Daten nicht nur für die Analyse im Einzelfall freigeben, sondern für die dauerhafte Speicherung in einer „Analyseplattform“. **Damit greift die Vorschrift unmittelbar in den polizeirechtlichen Regelungsbereich ein.**

³⁵ BVerfG, Urteil v. 1.10.2024 – 1 BvR 1160/19, NVwZ 2024, 1736 (1750), Rn. 183.

³⁶ Siehe Begründung zu § 98e StPO-E, Seite 16 des Entwurfs.

³⁷ BVerfG, Urteil v. 1.10.2024 – 1 BvR 1160/19, NVwZ 2024, 1736 (1748 ff.), Rn. 155 ff., 181, 183.

³⁸ BfDI, 28. Tätigkeitsbericht 2019, Nr. 6.7.3, Seite 55 f. (zu den in der Folge erreichten Lösungen siehe BfDI, 32. Tätigkeitsbericht 2023, Nr. 12.2, S. 152 f.).

Zwar ist auf den ersten Blick unklar, ob § 98e Absatz 1 StPO-E als eigenständige Befugnis zu verstehen ist, eine solche Analyseplattform einzurichten. Nach der Begründung ist offenbar gemeint, dass eine für die Gefahrenabwehr nach anderen Rechtsgrundlagen geschaffene Plattform hier für Zwecke der Strafverfolgung genutzt werden kann.³⁹

Diese Lesart verbietet sich aber mit Blick auf Absatz 3. Wenn die Befugnis der Analyseplattform sich nur auf das Polizeirecht stützen würde, dann könnte die Strafprozessordnung nicht deren Inhalt regeln. § 98e Absatz 3 StPO-E regelt aber explizit, welche – nach Polizeirecht (!) – verfügbaren Daten in die Analyseplattform aufgenommen werden dürfen und bestimmt dabei ausdrücklich, dass auch die Daten aus den Vorgangsbearbeitungssystemen für Zwecke der Analyse in einer „Analyseplattform“ – offenbar dauerhaft – gespeichert werden dürfen.

Damit kann § 98e Absatz 3 StPO-E in der Weise verstanden werden, dass er eine ausdrückliche Rechtsgrundlage schaffen will, alle verfügbaren polizeilichen Vorgangsdaten für Zwecke der („Analyse-“) Vorsorge zu speichern. Allein dies ist ein tiefgreifender Grundrechtseingriff, der kaum rechtfertigungsfähig ist.

Erschwerend kommt hinzu, dass die Regelung dabei nicht nach einzelnen Ländern differenziert. Damit wäre begrifflich sogar eine länderübergreifende Speicherung aller Vorgangsdaten in einer Analyseplattform umfasst. Das aber ist aufgrund der verfassungsrechtlichen Vorgaben undenkbar.

Soweit das Bundesrecht Landesrecht bricht, führt der Eingriff in die polizeirechtliche Regelungshoheit der Länder durch § 98e StPO-E ggf. zu **Fragen der Gesetzgebungskompetenz**. Dies gilt etwa, wenn ein Land – was vorzuziehen wäre – eine Analyseplattform schafft, die einem vom Bundesverfassungsgericht vorgezeichneten gestuften Regelungsmodell folgt. Der in Absatz 6 enthaltene Verweis auf das für die speichernde Stelle geltende Recht über die Verarbeitung personenbezogener Daten ist nicht ausreichend, um die Weite der einbezogenen Daten zu reduzieren. Dies ergibt sich schon aus der einleitenden Formulierung „im Übrigen“. Da Absatz 2 alle „Vorgangsdaten“⁴⁰ einbezieht, sind nicht nur Daten zur konkreten Aufgabenerfüllung umfasst – was für sich schon sehr weit wäre –, sondern auch alle zur Dokumentation gespeicherten Daten. Es fehlt eine Regelung, die die zur Dokumentation gespeicherten Daten von der Analyse ausschließt. Damit sind zum Beispiel sensible Daten der Opfer von Straftaten sogar dann erfasst, wenn der jeweilige Fall längst

³⁹ Siehe Begründung zu § 98e StPO-E, Seite 16 des Entwurfs.

⁴⁰ Diesen Begriff enthalten die Polizeigesetze nicht. Der Begriff „Vorgangsbearbeitungssystem“ ist zumeist nur ein polizeifachlicher Begriff, kein polizeirechtlicher. Die Polizeigesetze sprechen von „Vorgangsverwaltung und Dokumentation“ als einen Zweck, z.B. § 22 Absatz 2 BKAG. Dieser ist von „Aufgabenerfüllung“ zu trennen, z.B. § 16 Absatz 1 BKAG. Die Vorgangsbearbeitungssysteme können meist beides, müssen dies aber trennen. Siehe dazu den Prüfbericht der BfDI zum VBS des BKA, dazu 28. Tätigkeitsbericht 2019, Nr. 6.7.3, S. 55 f. Das VBS des BKA wird in begrüßenswerter Weise neu aufgestellt. Zu den erreichten Lösungen siehe BfDI, 32. Tätigkeitsbericht 2023, Nr. 12.2, Seite 152 f.

abgeschlossen ist. In dieser Hinsicht wurde – was ich ausdrücklich begrüße – der geplante § 9b BKAG-E zumindest insoweit ergänzt, als er nunmehr vorschreibt, dass § 22 Absatz 2 BKAG unberührt bleibt. Damit sind dort zwar weiterhin Zeugen und Opfer umfasst, aber wenigstens nicht im Bereich der reinen Dokumentation nach Abschluss der jeweiligen Aufgabe.

c) Fehlende Begrenzung der einzubeziehenden Daten

Der geplante **Analyseumfang** führt für sich genommen zu einer **sehr hohen Eingriffsintensität**.

Für die Eingriffsintensität des § 98e StPO-E ist hier insbesondere maßgeblich, dass gemäß Absatz 2 Satz 1 Daten aus den Vorgangsbearbeitungssystemen in die Analyse einbezogen werden dürfen.⁴¹ Ausgeschlossen sind gemäß § 98e Absatz 2 Satz 3 StPO-E lediglich Daten, die mit den in §§ 100b, 100c StPO – bzw. entsprechenden – Maßnahmen zur Verfolgung besonders schwerer Straftaten erhoben wurden. Daten aus anderen eingriffsintensiven Ermittlungsmaßnahmen, die zur Verfolgung schwerer Straftaten zulässig sind, dürfen hingegen grundsätzlich verwendet werden. Das betrifft etwa Daten aus der Telekommunikationsüberwachung oder Verkehrsdaten.

Gerade die nach § 100g StPO erhobenen Verkehrsdaten können zu einer sehr hohen Eingriffsintensität führen, wie etwa die vom Bundesverfassungsgericht als Beispiel angeführten Funkzellendateien zeigen.⁴²

Sogar Daten aus Asservaten können einbezogen werden. Diese können ihrerseits eine Vielzahl von Daten unbeteiligter Dritter enthalten. Denkbar wäre es beispielsweise, auch beschlagnahmte größere Datenbestände von Unternehmen oder Anwaltskanzleien einzubeziehen. Soweit die Begründung ausführt, dass elektronische Akten ausgeschlossen seien⁴³, trifft dies nur den Teil, der bei den Staatsanwaltschaften vorhanden ist. Die Vorgangsbearbeitungssysteme der Polizeibehörden werden hingegen eindeutig einbezogen (§ 98e Absatz 2 Satz 1 StPO-E). Sie dienen dazu, die elektronische Akte zu befüllen und enthalten daher seitens der Polizei alle Daten, die auch in die offizielle Ermittlungsakte überführt werden. Der Umfang der im Vorgangsbearbeitungssystem vorhandenen Daten ist in der Regel sogar eher größer. Zu Absatz 6 siehe oben.

⁴¹ Vgl. BVerfG Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1209 f.), Rn. 134 ff.

⁴² BVerfG Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1210), Rn. 142; siehe dazu BfDI, 30. Tätigkeitsbericht 2021, Nr. 8.2.4, Seite 90.

⁴³ Siehe Begründung zu § 98e StPO-E, S. 18 des Entwurfs.

Notwendig wäre zudem eine Regelung, nach der im konkreten Fall die Strafverfolgungsbehörde verpflichtet ist, die für die Analyse verwendeten Daten zumindest für den konkreten Einzelfall näher einzugrenzen.⁴⁴

Gemäß § 98e Absatz 2 Satz 2 StPO-E findet sich eine solche eingrenzende Pflicht nur sehr allgemein und bezogen auf den dortigen Katalog von Daten, die aus bestimmten Ermittlungsmaßnahmen oder Asservaten stammen („soweit erforderlich“).

Der Entwurf sieht also eine Gesamtmenge an einzubeziehenden Daten vor, die zu einer sehr hohen Eingriffsintensität der Analyse führen.

Entsprechendes gilt für die geplanten BKAG-Normen zur automatisierten Datenanalyse. Mit Ausnahme des Hinweises auf § 12 und § 22 Abs. 2 BKAG erfolgt keine nennenswerte Eingrenzung der einzubeziehenden Daten.

d) Umfassende Analysemethoden

Ob die in den geplanten Befugnissen vorhandene tatbestandliche Umschreibung der Analysemethoden zu einer wesentlichen Minderung der Eingriffsintensität führt, ist zweifelhaft.

In der Gesamtschau scheinen sämtliche Regelungen auf einen **„big data“-Ansatz** hinzuweisen, d.h. alle einbezogenen Daten werden zusammengeführt und automatisiert ausgewertet. Bei diesem Ansatz wird keine Vorselektion im Einzelfall vorgenommen, welche Daten für ein konkretes Verfahren relevant sind, d.h. es wird sich im Allgemeinen nicht vermeiden lassen, auch für den Einzelfall nicht erhebliche Daten mitzuverarbeiten. Es wird vermutlich so sein, dass bei jeder Suche alle vorhandenen Daten und Dateien nach den Suchbegriffen durchsucht und somit verarbeitet werden.

Sämtliche geplanten Befugnisse zur automatisierten Datenanalyse erlauben jeweils in Absatz 4 eine Vielzahl von Analysevorgängen, die nicht zwingend als einfache Datenabgleiche zu verstehen sind. Das gilt bereits für die jeweils in Abs. 4 Satz 1 Nr. 5 der Normen genannte Methode der statistischen Auswertung.⁴⁵

Der Entwurf macht keinen Gebrauch von der Möglichkeit, die Eingriffsintensität der Maßnahme durch den ausdrücklichen Ausschluss des Einsatzes selbstlernender Systeme zu verringern⁴⁶.

Dass der Einsatz von KI nicht ausgeschlossen ist, ergibt sich bereits aus der jeweiligen Verpflichtung sicherzustellen, dass sich diskriminierende Algorithmen nicht „herausbilden“

⁴⁴ Vgl. BVerfG Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1213), Rn. 162.

⁴⁵ Vgl. BVerfG Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1211), Rn. 147.

⁴⁶ Vgl. BVerfG Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1211), Rn. 120 f.

dürfen⁴⁷. Damit ist offensichtlich ein „lernendes“ System gemeint, da das Verb „herausbilden“ einen dynamischen Entwicklungsprozess impliziert, in dessen Verlauf diskriminierende Muster erst durch Training oder selbstlernende Mechanismen entstehen können. Dies entspricht auch der Aussage des Bundesverfassungsgerichts, wonach die Verhinderung der „Herausbildung und Verwendung diskriminierender Algorithmen“ als eine spezifische Herausforderung im Zusammenhang mit lernfähigen Systemen bezeichnet wird.⁴⁸

§ 98e Absatz 4 Satz 2 StPO-E sieht zusätzlich vor, dass das Analysesystem die Daten nur aufbereiten und bereitstellen darf, um den Strafverfolgungsbehörden eine eigene Entscheidung zu ermöglichen. Dies schließt den Einsatz von Künstlicher Intelligenz aber nicht aus. Denn die KI kann ohnehin keine abschließende Entscheidung der Ermittlungsbehörde treffen, diese ist der Anklageschrift vorbehalten. Absatz 4 Satz 3 der Norm gibt vor, dass der Einsatz der Anwendung anlassbezogen und anhand von Suchbegriffen ausgelöst wird, die sich aus dem zugrundeliegenden Sachverhalt ergeben. Darunter können auch an die KI gerichtete Eingaben verstanden werden (prompts). Die Vorgaben von § 98e Absatz 4 StPO-E mindern deshalb die Eingriffsintensität ebenfalls nicht wesentlich.

e) An die Eingriffsintensität nicht ausreichend angepasste Eingriffsschwellen

In der Gesamtschau ergibt sich also, dass die geplante Datenanalyse einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung ermöglicht. Dies folgt aus den wenig begrenzten, zum Teil sehr sensiblen einzubeziehenden Daten und aus den möglichen weitreichenden und an big data orientierten Analysemethoden.

Für gefahrenabwehrende Befugnisse hat das Bundesverfassungsgericht entschieden, dass solche Maßnahmen nur zum Schutz besonders gewichtiger Rechtsgüter zulässig sind.⁴⁹ Der **Schutz besonders gewichtiger Rechtsgüter** auf der präventiven Seite entspricht wie oben dargelegt der **Verfolgung besonders schwerer Straftaten** auf der repressiven Seite.⁵⁰

Angesichts der beschriebenen Eingriffsintensität ist daher die Schwelle des § 98e StPO-E sowie § 9b BKAG-E zur Verfolgung schwerer Straftaten unter Verweis auf den Katalog des § 100a Absatz 2 StPO zu niedrig angesetzt. Dies würde selbst dann gelten, wenn der Katalog

⁴⁷ Siehe §§ 9b Absatz 5 Satz 1, 39b Absatz 5 Satz 1, 63c Absatz 5 Satz 1 BKAG-E, § 98e Absatz 4 Satz 5, § 58b Absatz 5 Satz 1 BPolG-E.

⁴⁸ Vgl. BVerfG Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1205), Rn. 100.

⁴⁹ BVerfG Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1206), Rn. 105.

⁵⁰ Vgl. BVerfG, Beschluss v. 28.9.2022 – 1 BvR 2354/13, GSZ 2022, 299 (305) Rn. 136; Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1807f.), Rn. 347; siehe zum Gleichlauf auch Urteil vom 26.4.2022 – 1 BvR 1619/17, NJW 2022, 1583 (1598), Rn. 244 unter Verweis auf Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1807f.), Rn. 347.

bereinigt würde, wie ich dies nunmehr schon vielfach in Gesetzgebungsverfahren gefordert habe.

Als Schwelle angemessen wäre es vielmehr, die im Entwurf beschriebene Datenanalyse nur zur Verfolgung besonders schwerer Straftaten zuzulassen und entsprechend auf den **Katalog des § 100b Absatz 2 StPO bzw. den des § 138 StGB** zu verweisen. Praktikabler ist in Bezug auf § 9b BKAG-E die enge Begrenzung auf **Personen, nach denen gemäß § 131b StPO öffentlich gefahndet wird**.

Bei der Bundespolizei verbleibt auch nach Vorlage des Gesetzesentwurfes im repressiven Bereich ein Manko an Rechtsgrundlagen für teilautomatisierte KI-basierte Bildabgleiche außerhalb des Internets. Wie mir aus meiner Kontroll- und Beratungspraxis bekannt ist, setzt die Bundespolizei derzeit ein teilautomatisiertes KI-System zum massenhaften biometrischen Abgleich von Daten zu repressiven Zwecken ein. § 98c StPO stellt dafür bisher keine geeignete Rechtsgrundlage dar, da sie keinerlei Eingriffsschwellen für schwere Grundrechtseingriffe vorsieht.

Massenhafte Abgleiche und Analysen von Videodateien mit einem KI-System stellen keinen einfachen Abgleich dar. Deshalb bedarf es auch hier der Einschränkung auf schwere Taten. BMI und Bundespolizei haben in der Praxis mittels der einschlägigen EAO selbst bereits eine Einschränkung auf den Bereich schwerer Straftaten vorgenommen. Gemäß dem Wesentlichkeitsgebot hat diese Entscheidung jedoch der Parlamentsgesetzgeber zu treffen. Eine Kontrolle hat außerdem gezeigt, dass eine abstrakte Beschränkung auf schwere Straftaten teilweise in Einzelfällen dazu führt, dass der Abgleich unverhältnismäßig erscheint. Es sollte daher auch hier eine Einschränkung auf Straftaten, die auch im Einzelfall schwer wiegen, vorgesehen werden.

f) Fehlende Verfahrensvorkehrungen

Es fehlen jegliche Vorschriften zur **Transparenz der eingesetzten Verfahren** und der konkreten Datenverarbeitung im Einzelfall. Aus § 98e Absatz 4 Satz 2 StPO-E ist abzulesen, dass der Entwurf die Frage als sensibel ansieht, in welcher Form das System den Behörden Daten aufbereiten und bereitstellen kann. Diese aufbereiteten Daten sollen dann Grundlage für Entscheidungen der Strafverfolgungsbehörden im Strafverfahren sein.

Für die betroffene Person im Strafverfahren ist es jedoch essentiell zu erfahren, wie diese Entscheidungsgrundlage zusammengestellt wurde. Dies setzt zum einen die umfassende Kenntnis der eingesetzten Verfahren voraus. Zum anderen lässt sich diese durch den Einsatz von big data, Algorithmen und KI zusammengestellte Entscheidungsgrundlage nur prüfen, wenn auch die ausgewerteten Datenbestände bekannt und überprüfbar sind. In einem rechtsstaatlichen Verfahren folgen daraus umfassende **Einsichtsrechte der Betroffenen** und der Strafverteidigerinnen und Strafverteidiger.

Wie diese Einsichtsrechte mit den Datenschutzrechten aller Drittbetroffenen in Ausgleich gebracht werden sollen, ist im Gesetzentwurf nicht geregelt. Diese haben ebenfalls ein Recht auf Transparenz.

Eine **Benachrichtigungspflicht in § 101 StPO** fehlt, obwohl es sich um einen besonders tiefgreifenden Grundrechtseingriff handelt.