Anwaltsverband Baden-Württemberg
im Deutschen **Anwalt**Verein e. V.

AnwaltsVerband BW, Kissinger Str. 49, 70372 Stuttgart

Ministerium des Inneren, für Digitalisierung und Kommunen
Baden-Württemberg
Referat 35 - Recht und Grundsatz
Herrn Marc Frank und Frau Sarah Schilling
Willy-Brandt-Straße 41
70173 Stuttgart

Geschäftsstelle beim Präsidenten:
RA Prof. Dr. jur. Peter Kothe
Johannes-Daur-Straße 10
70825 Korntal-Münchingen

Telefon 0711 / 2 36 59 63
Telefax 0711 / 2 55 26 55

E-Mail: sekretariat@av-bw.de
Internet: www.av-bw.de

Anschrift der Geschäftsführung:
Kathrin Eisenmann – Syndikusrechtsanwältin
Kissinger Straße 49
70372 Stuttgart

Telefon 0711 / 55 04 29 29
Telefax 0711 / 55 04 29 30
E-Mail: geschaeftsfuehrung@av-bw.de

19. August 2025

Per E-Mail: **poststelle@im.bwl.de; Agathe.Wer@im.bwl.de**

Az. IM3-1101-44/8/2
Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften
Hier: Stellungnahme des Anwaltsverbandes Baden-Württemberg

Sehr geehrter Herr Frank,

für die Übermittlung der Anhörungsunterlagen zum Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften vom 29.07.2025 danken wir Ihnen. Der Anwaltsverband nimmt die Gelegenheit zur Stellungnahme gern wahr.

Der Anwaltsverband Baden-Württemberg e. V. ist der freiwillige Zusammenschluss der 25 örtlichen Anwaltvereine in Baden-Württemberg, die Mitglied im Deutschen Anwaltverein (DAV) sind. Er repräsentiert damit mehr als die Hälfte aller Kolleginnen und Kollegen in Baden-Württemberg und vertritt so als größte freiwillige Anwaltsorganisation dieses Bundeslandes die Interessen der Anwaltschaft in unserem Bundesland und – in Zusammenarbeit mit dem DAV – auch auf nationaler und internationaler Ebene.

I. Allgemeine Bewertung

Mit dem Gesetzentwurf zur Änderung des Polizeigesetzes BW sollen Rechtsgrundlagen für eine automatisierte Datenanalyse, für die Nutzung der sog. Advanced-Mobile-Location-Technologie (AML-Technologie) zur Bestimmung des Standorts hilfesuchender Personen nach Anwahl der polizeilichen Notrufnummer sowie zur Entwicklung, zum Training, zum Testen, zur Validierung und zur Beobachtung, Überprüfung, Änderung und zum Trainieren von informationstechnischen Produkten geschaffen werden.

1. Zu den Kosten

Mit der Umsetzung der durch die Änderung des Polizeigesetzes geschaffenen Rechtsgrundlagen für die automatisierte Datenanalyse und zur Verarbeitung von Standortdaten bei Anwahl der Notrufnummer sollen Mehrausgaben für den Landeshaushalt in Höhe von **jährlich insgesamt rd. 10 Mio. EUR** verbunden sein.

Für die automatisierte Datenanalyse sei ein **Bedarf in Höhe von 9,25 Mio. EUR** für Personal- und Sachmittel veranschlagt. Neben den Kosten zur Beschaffung der Spezialsoftware seien für den Betrieb der technisch komplexen informationstechnischen Infrastruktur informationstechnische Spezialisten einzustellen.

Für den Betrieb der AML-Technologie sollen Finanzmittel in Höhe von rd. **550.000 EUR** benötigt werden. Im Staatshausplan 2025/2026 seien diese Mittelbedarfe bereits entsprechend berücksichtigt und im Bereich des Innenministeriums etatisiert.

Hinsichtlich der Schaffung einer Rechtsgrundlage für die Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO außerhalb von rein wissenschaftlichen Forschungsarbeiten sollen für Softwarebeschaffung, -entwicklung und -erprobung sächliche und personelle Aufwände entstehen, die in den Folgejahren von Anzahl und Ausgestaltung der Anwendungen abhängig sein würden und sich daher **noch nicht beziffern** lassen. Der Polizei stünden Mittel im Rahmen der informationstechnischen Budgetplanung im Staatshaushaltsplan zur Verfügung. Diese Mittel könnten in Teilen für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO genutzt werden.

Beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LFDI) könnten punktuell Mehraufwände im Rahmen seiner gesetzlichen Zuständigkeit durch Beratungsleistungen und die aufsichtliche Kontrolle zum Zwecke der Überprüfung der Einhaltung gesetzlicher Vorgaben entstehen, die angeblich im Rahmen vorhandener Mittel gedeckt werden.

2. Zur Transparenz

Aus den Medien ist zu entnehmen, dass es aktuell bei der Daten-Analyse-Software ausschließlich um den Einsatz der Software „Gotham“ des US-amerikanischen Unternehmens Palantir Technologies geht, für deren Beschaffung bereits im März 2025 ein Fünf-Jahres-Vertrag vom zuständigen Polizeipräsidium Technik abgeschlossen wurde. Hintergrund der Beschaffung dieser Software **vor** Schaffung der gesetzlichen Grundlage für deren Nutzung ist ein vom Freistaat Bayern im 2022 für alle Bundesländer geschlossener Rahmenvertrag und das Auslaufen der sich aus diesem ergebenden Preisbindung.

Bereits dieses Vorgehen weckt Bedenken, weil der Gesetzgeber hierdurch faktisch in Zugzwang gesetzt wird, weil anderenfalls erhebliche Finanzmittel in nicht nutzbringender Weise investiert würden. Die behauptete Alternativlosigkeit des Programms, mit der die Beschaffung (nachträglich) gerechtfertigt wird, besteht ersichtlich nicht, weil andere Programme, insbesondere das polnische DataWalk und das französische ChapVision zur Verfügung stehen, die drei Vorteile in sich vereinbaren : Sie sind verfassungskonform, transparent und in Europa gefertigt. Dass mit der Firma FSZ Computing Solutions, Metzingen, ein deutscher Anbieter vergleichbares bietet rundet das Bild nur ab.

Bezogen auf den Datenschutz, insbesondere die Verhinderung eines Datenabflusses in die USA, wird berichtet, dass das Fraunhofer-Institut die Ursprungsversion des Palantir-Programms geprüft und im vorstehenden Sinn für sicher befunden habe. Das vermag die begründeten Zweifel keineswegs auszuräumen. Keine Software kommt ohne Updates aus, die erfahrungsgemäß mindestens einmal, in der Regel jedoch mehrmals jährlich aufgespielt werden müssen. Zum einen ist nicht davon auszugehen, dass jedes Update einer entsprechenden Prüfung unterzogen würde. Zum anderen stellt sich die Frage, wie die weitere Nutzung der Software erfolgen soll, wenn ein solches Update nicht mehr die Gewähr dafür bietet, dass die Daten deutscher Ermittler auch in Deutschland bleiben. Bemerkenswert ist, dass an keiner Stelle vortragen wird, dass die anfänglich offenbar bestehende Sicherheit auch bei künftigen Updates weiterhin von Palantir gewährleistet wird.

Dies steht in krassem Gegensatz zu den Bedenken etwa der Kultusverwaltung gegen den Einsatz von Microsoft 365, die auf Einwände des Landesbeauftragten für den Datenschutz und Informationsfreiheit zurückgeht. Dieser hat dort zutreffend gerügt, dass besonders problematische Telemetrie- und Diagnosedaten im Rahmen des Pilotprojekts nicht vollständig deaktiviert, sondern nur reduziert werden konnten. Eine Übermittlung von Diagnose-, Telemetrie- oder anders genannten personenbezogenen Daten der Nutzer an Microsoft sowie die eigennützige Weiterverarbeitung dieser Daten durch Microsoft im Wege der Beobachtung, Aufzeichnung und Auswertung des Nutzer- und Geräteverhaltens ohne erkennbare Rechtsgrundlage findet nach den technischen Messungen des LfDI im Rahmen des Pilotbetriebs auch bei restriktiver Konfiguration weiterhin und in sehr großem sowie für die Diensterbringung nicht erforderlichen Umfang statt.

Außerdem bestehen zahlreiche Datentransfers in die USA, die nicht unterbunden werden können. Daraus ergeben sich auch vor dem Hintergrund der Entscheidung

EuGH, Urteil vom 16.07.2020 – C-311/18 („Schrems II"),

große Risiken. Die mit derartigen Übermittlungen zusammenhängenden Risiken konnten zwar durch die begrüßenswerten zusätzlichen Garantien von Microsoft gemindert, aber nicht abschließend ausgeräumt werden. Dies ist umso bedenklicher, als die Drittstaatentransfers auch in der geprüften Softwarevariante weiterhin einen großen Umfang haben.

Wenn aber bereits bei vergleichsweise einfachen Anwendungen wie derjenigen von Microsoft 365 in Schulen zutreffend derartige Bedenken erhoben werden, ist umso unverständlich, dass im Geschäftsbereich des Innenministeriums im Umgang mit weit sensibleren Daten keine hinreichenden Sicherheitsvorkehrungen auch für die Zukunft getroffen werden.

Sollten die zuvor beschriebenen Bedenken der Grund sein, weshalb in der Gesetzesbegründung die Software „Gotham" und deren Hersteller Palantir nicht genannt werden, würden den Abgeordneten und den Bürgern bestehende Risiken bewusst vorenthalten. Im Zentrum der aktuellen Diskussion um die Palantir-Software stehen weniger die allgemeinen Gefahren eines möglichen KI-Einsatzes als vielmehr der Umstand, dass deutsche Sicherheitsbehörden das System eines privaten Unternehmens mit Sitz in einem Nicht-EU-Staat verwenden wollen, in dem nicht nur geringere Datenschutzstandards gelten, sondern in dem seit Jahren hartnäckig Informationen verbreitet werden, dass dortige Software-Entwickler und –Hersteller verpflichtet seien dessen Geheimdiensten eine „Hintertür" einzubauen. Diese Informationen werden zwar regelmäßig mit Meldungen dementiert, aber nur in der Weise, dass eine solche gesetzliche Verpflichtung zugunsten US-amerikanische Geheimdienste (NSA) **noch** nicht begründet worden sei. Dies vermag in keiner Weise zur Beruhigung beizutragen.

3. Zum erforderlichen Personal und der Infrastruktur

Bereits im Rahmen der Expertenanhörung am 07.052025 im Landtag zur beabsichtigten Einführung der „elektronischen Fußfessel" für Fälle häuslicher Gewalt nach dem „spanischen Modell" im PolG BW wurde deutlich, dass Polizei und LKA derzeitig nicht über genügend fachkundiges Personal verfügen, um diese Technologien befriedigend beherrschen zu können. Schon mit der Überwachung von ehemaligen Sicherungsverwahrten und Terrorismus-Gefährdern auf diese Weise sind die beteiligten Bundesländer Hessen und Baden-Württemberg derzeit personell und von der Infrastruktur her weit überfordert. Es gebe kaum freie Kapazitäten für solche zusätzlichen Überwachungen. Personal müsse geschult und in mehreren Schichten eingesetzt werden.

Es fragt sich deshalb, woher die weiteren personellen Ressourcen kommen sollen, um die hier beabsichtigten Technologien der automatischen Datenanalyse und Entwicklung polizeieigener KI mit eigenen Mitarbeitern (IT-Experten) sinnvoll einführen und benutzen zu können und die Datensicherheit zu gewährleisten.

Die Gewerkschaft der Polizei bemängelt das Fehlen moderner und leistungsfähiger Basisausstattung. Wenn aber von Anfang an ein Vollzugsdefizit deutlich erkennbar ist, sollte man keine solche „Vorratsgesetzgebung“ machen.

Wenn in der Praxis die rechtlichen Möglichkeiten einer Befugnis nicht ausgeschöpft werden, nicht ausgeschöpft werden sollen und angesichts des aktuellen Stands der Technik derzeit auch nicht voll ausgeschöpft werden können, ändert dies nichts an den verfassungsrechtlichen Anforderungen,

> vgl. BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -.

4. Sicherheitsbedenken

Wie bei jeder Software ist mit Sicherheitslücken zu rechnen, die im Nachhinein geschlossen werden sollten. Wird nämlich – wie hier -

> „… Software privater Akteure … eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte (vgl. Wissenschaftlicher Dienst des Deutschen Bundestags, Datenbank-Analysen durch die Polizei. Grundrechte und Datenschutzrecht, 2. März 2020, WD3-3000-018/20, S. 8 m.w.N.).“
>
> (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, BVerfGE 165, 363 = juris (Rdnr. 100).

Wie aber wird sichergestellt, dass zwischenzeitlich nicht unbefugte Dritte durch Sicherheitslücken in der Zusammenführungs- und Analyse-Software auf die Datenbestände der deutschen Polizei zugreifen? Wie wird sichergestellt, dass - personenbezogene - Daten – in einem solchen Zeitraum nicht abfließen, insbesondere von Unbeteiligten? Diese drängenden Fragen werden vorliegend nicht beantwortet.

II. Zu den beabsichtigten Regelungen im Einzelnen

5. Zu Art. 1 - Änderung des Polizeigesetzes

a) Zu § 45a PolG BW-neu - Verarbeitung von Standortdaten bei Anwahl der Notrufnummer 110 - AML-Technologie

Durch die Nutzung der sog. Advanced-Mobile-Location-Technologie (AML-Technologie) sollen das Verfahren zur schnellen Standortbestimmung einer hilfesuchenden Person mittels einer **Web-Anwendung** digitalisiert und Medienbrüche reduziert werden. Zudem soll die Genauigkeit der Standortbestimmung durch die kombinierte Nutzung verschiedener technischer Positionsdienste erheblich verbessert werden. Hierfür kommt der auf mobilen Endgeräten vorinstallierte Systemdienst AML zum Einsatz.

§ 45a Abs. 1 regelt die Einrichtung eines „AML-Endpunktes“ beim **Präsidium Technik, Logistik, Service der Polizei.**

Bei AML handelt sich um einen Systemdienst, der fest in das Betriebssystem (i. d. R. Android oder iOS) der mobilen Endgeräte integriert ist. Dabei wird neben dem Rufaufbau zur Notrufabfragestelle zusätzlich (ohne Zutun der anrufenden Person) die Satellitennavigation, die GPS-Standortübertragung sowie das WLAN (zur Verbesserung der Standortgenauigkeit) des mobilen Endgerätes selbstständig aktiviert und gemäß technischem Bericht ETSI TR 103 393 V1.1.1 (2016-03) des Europäischen Instituts für Telekommunikationsnormen (ETSI) der Gerätestandort, Datum und Uhrzeit der Standortbestimmung, die Mobilfunkzellenidentifikationsnummer (Cell-ID), die internationale mobile Teilnehmerkennung (IMSI), die internationale Mobilgerätekennung (IMEI), der Mobilländercode (MCC), der Mobilnetzcode (MNC) sowie die Mobilfunknummer übermittelt.

Nach Satz 1 hält das Präsidium Technik, Logistik, Service der Polizei die von Betriebssystemherstellern übermittelten Daten zum Zwecke des dezentralen Abrufs durch die zuständigen Notrufabfragestellen der Polizeien der Länder vor.

Im Verhältnis zu den Polizeien der anderen Länder wird das Präsidium Technik, Logistik, Service der Polizei als **Auftragsverarbeiter** tätig. Hierzu sind separate Auftragsverarbeitungsvereinbarungen mit den einzelnen Ländern zu schließen.

Die Speicherdauer wird durch Satz 2 auf **60 Minuten** begrenzt.

AML dient ausschließlich der Rettung von Personen in Notlagen und wird nur bei Anwahl der Notrufnummer aktiviert. Satz 3 stellt sicher, dass eine Verarbeitung der Daten zu einem anderen Zweck als zur Übermittlung an die Notrufabfragestellen unzulässig ist.

Absatz 2 regelt die Erhebung, Verarbeitung und Speicherung von AML-Daten durch die zuständigen Notrufabfragestellen. In Baden-Württemberg ist dies der **Polizeivollzugsdienst.**

Die Verarbeitung ist ausschließlich zum Zweck der Abwehr einer Gefahr für Leib, Leben oder Freiheit möglich. Satz 2 begrenzt die Speicherdauer der Daten auf sechs Monate. Die Speicherung der AML-Daten erfolgt technisch im Einsatzleitsystem (derzeit Viadux). Die Löschfrist orientiert sich daher an dessen Löschkonzept.

Gegen Nutzung der AML-Technologie zur Bestimmung des Standorts hilfesuchender Personen nach Anwahl der polizeilichen Notrufnummer 110 hat der Anwaltsverband aus den im Gesetzentwurf angeführten Gründen keine Einwände.

b) Zu § 47a PolG BW – neu - Automatisierte Datenanalyse

Bisher unverbundene Daten und Datenquellen des Polizeivollzugsdienstes sollen in einer Analyseplattform zusammengeführt werden, um die vorhandenen Datenbestände durch **Suchfunktionen** systematisch erschließen zu können (automatisierte Datenanalyse). Die automatisierte Datenanalyse oder -auswertung ist darauf gerichtet, neues Wissen zu erzeugen. Die automatisierte Analyse oder Auswertung geht weiter, weil sie die **Verarbeitung großer und komplexer Informationsbestände** ermöglicht. Je nach der eingesetzten Analysemethode können zudem durch verknüpfende Auswertung vorhandener Daten neue persönlichkeitsrelevante Informationen gewonnen werden, die ansonsten so nicht zugänglich wären. Die Maßnahme erschließt die in den Daten enthaltenen Informationen damit intensiver als zuvor. Sie bringt nicht nur in den Daten angelegte, aber zunächst mangels Verknüpfung verborgene Erkenntnisse über Personen hervor, sondern kann sich bei entsprechendem Einsatz einem „Profiling“ annähern. Ein herkömmliches Verfahren, die nach dem Modell abgestufter Erkenntnisverdichtung erfolgende Ermittlungstätigkeit, wird hierdurch mit einer viel größeren Durchschlagskraft versehen. Mit der Überwindung der praktischen Erkenntnisgrenzen klassischer Polizeiarbeit gehen jedoch auch besondere Gefahren für die durch die Datenverarbeitung Betroffenen einher.

Für die **anlassbezogene** automatisierte Datenanalyse soll **eine ganzheitliche Plattform** zur Verfügung gestellt werden, um polizeiliche Datenbestände effizient und effektiv nach relevanten Informationen auswerten zu können, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu gewinnen wären.

Dabei soll das technische Verfahren aus zwei aufeinander aufbauenden, aber praktisch zeitgleich stattfindenden Schritten, nämlich dem Zusammenführen unterschiedlicher Dateisysteme und der

sich daran anschließenden Recherche innerhalb der zusammengeführten Datenbestände bestehen.

In der Entscheidung

> BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -,

hat das Bundesverfassungsgericht grundsätzlich geklärt, unter welchen Voraussetzungen eine automatisierte Datenanalyse verfassungskonform geregelt werden kann. Diese Anforderungen wurden in den jüngsten Entscheidungen zum sog. Staatstrojaner

> BVerfG, Beschluss vom 24.06.2025 – 1 BvR 2466/19 – (Staatstrojaner I) und BVerfG, Beschluss vom 24.06.2025 – 1 BvR 180/23 – (Staatstrojaner II),

nochmals aktuell konkretisiert, und zwar nicht nur bezogen auf die betroffenen Grundrechte, sondern auch und gerade hinsichtlich der Rechtsgüter, zu deren Schutz die Eingriffe erlaubt werden sollen.

Die Verarbeitung gespeicherter personenbezogener Daten im Rahmen einer automatisierten Datenanalyse greift in das **Grundrecht auf informationelle Selbstbestimmung** gemäß Art. 2 Abs. 1 i. V. mit Art. 1 Abs. 1 GG in zweifacher Weise ein.

Zum einen stellt die Nutzung der Daten über den ursprünglichen Anlass hinaus einen neuen Grundrechtseingriff dar, der nach dem **Grundsatz der Zweckbindung** gerechtfertigt sein muss. Zum anderen hat das Bundesverfassungsgericht ein potentielles **Eigengewicht** der automatisierten Datenanalyse festgestellt, das über das Eingriffsgewicht der weiteren Verwendung vormals getrennter Daten hinausgeht,

> vgl. BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 50, 67ff.).

Für eine verfassungskonforme Ausgestaltung der automatisierten Datenanalyse ist eine Bestimmung dieses Eigengewichts erforderlich, das je nach Art und Umfang der einzubeziehenden Daten und der Methode der Analyse sehr unterschiedlich sein kann,

> vgl. BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 72ff.).

Die gesetzlichen Anforderungen für eine verfassungskonforme Regelung bestimmen sich daher nach dem Eingriffsgewicht, das vom Gesetzgeber durch Vorkehrungen und Schutzmaßnahmen beeinflusst werden kann.

Die Rechtfertigung eines Grundrechtseingriffs setzt eine gesetzliche Ermächtigung voraus, die einen legitimen Zweck verfolgt und auch im Übrigen dem Grundsatz der Verhältnismäßigkeit genügt. Ein möglicher Zeitdruck allein, vermag derartige Grundrechtseingriffe wohl nicht zu rechtfertigen. Spezielle Anforderungen ergeben sich hier aus dem Gebot der Verhältnismäßigkeit im engeren Sinne. Wie streng diese Anforderungen im Einzelnen sind, bestimmt sich nach dem **Eingriffsgewicht der Maßnahme**,

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (269 Rdnr. 105); BVerfG, Beschluss vom 27.05.2020 – 1 BvR 1873/13 –, BVerfGE 155, 119 (178 Rdnr. 128) – Bestandsdatenauskunft II; BVerfG, Urteil vom 26.04.2022 – 1 BvR 1619/17 –, BVerfGE 162, 1 = juris (Rdnr. 152), st. Rspr.

Die Rechtfertigungsanforderungen an die weitere Nutzung staatlich erhobener Daten richten sich nach den **Grundsätzen der Zweckbindung und Zweckänderung,**

> grundlegend BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83 –, BVerfGE 65, 1 (46).

aa) Betroffene Datenbestände; 47a Abs. 3 PolG BW – neu

Im Gesetz selbst ist – laut Bundesverfassungsgericht - insbesondere zu regeln, **welche Datenbestände** einbezogen werden dürfen und inwiefern dies automatisiert erfolgen darf. Wenn der Gesetzgeber die verwendbaren Datenbestände nicht selbst abschließend aufzählt, muss er sicherstellen, dass dies untergesetzlich abstrakt-generell geregelt und veröffentlicht wird. Je größere Mengen personenbezogener Daten in die automatisierte Datenanalyse und -auswertung einbezogen werden können, je weniger der Gesetzgeber also die verwendbare Datenmenge begrenzt, umso schwerer wiegt der Grundrechtseingriff

> vgl. BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 76ff., 112ff.).

Soweit es aus der Gesetzesbegründung ersichtlich ist, können

- eigene polizeiliche Vorgangsdaten (z. B. Anzeigen, Ermittlungsberichte, Vermerke),
- Falldaten,
- Daten aus polizeilichen Auskunftssystemen (Kriminalakten, Personenfahndungen, Sachfahndungen, Haftdateien, erkennungsdienstliche Dateien, DNA-Analyse-Datei) und

- Daten aus dem polizeilichen Informationsaustausch (z. B. des webbasierten Fernschreibesystems EPOST 810) zusammengeführt werden.
- Außerdem sollen Verkehrsdaten nach § 70 TKG, wie Verbindungsdaten und Standort-Daten (§ 9 TDDDG),
- Daten aus Asservaten (USB-Sticks, Festplatten, Smartphones, Laptops),
- Daten aus landesfremden Datenbeständen,
- Daten aus staatlichen Registern (z. B. Melderegister, Zentrales Verkehrsinformationssystem – ZEWIS) sowie
- aus Internetquellen und damit offensichtlich auch aus Homepages und Sozialen Medien zusammengeführt werden können.

Hierbei handelt es sich fraglos um einen immensen Datenbestand. Der Gesetzentwurf sollte hierzu unbedingt mehr Angaben machen, damit sich allen Beteiligten die Tragweite erschließt. Aufgrund der erheblichen Bandbreite in Betracht kommender Daten ist der Einsatz von solcher Software für Zwecke der automatisierten Datenanalyse in hohem Maße grundrechtsrelevant für alle Betroffenen.

Die Funktionsweise beispielsweise der Palantir-Software ist nur eingeschränkt durchschaubar. Wie angesichts dessen sichergestellt werden soll, „dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden“ (§ 47a Abs. 2 Satz 2 PolG BW-neu), erschließt sich nicht, zumal eine etwaige Diskriminierung nicht das einzige Problem darstellt. Die Gesetzesbegründung macht keinerlei Angaben dazu, wie weit die Daten aus den einzubeziehenden Datenbeständen zurückreichen oder wie tief und effektiv gesucht werden kann. Angesichts der Menge der im Internet verfügbaren Daten, die abgefragt und verarbeitet werden können und sollen, ist nicht ersichtlich, wie den verfassungsrechtlichen Vorgaben Rechnung getragen werden kann.

Es ist vielmehr zu befürchten, dass die favorisierte Software nicht ausreichend gewichten kann, welche Daten wie relevant sind. In den zugrundeliegenden Datenbeständen können beispielsweise Rechtschreibfehler, Zahlendreher, Tarnbezeichnungen und Fehlinformationen enthalten sein, die die Suchergebnisse verfälschen. Fraglich ist, ob der Suchende erkennen kann, aus welcher verwendeten Datei eine Information stammt, wie alt sie etwa ist, wer sie eingestellt hat usw. Interessant ist deshalb stets der Kontext, der – so dürften die vorgesehenen Regelungen zu verstehen sein – nicht miterhoben wird.

Durch die mögliche Zusammenführung dieser immensen Datenbestände entsteht der Eindruck einer übermächtigen Überwachungsmöglichkeit, auch und gerade in Bezug auf un-

beteiligte Dritte. Daran ändern auch hehre gesetzlich vorgesehene Beschränkungen zunächst nichts. Je effektiver sie wirkt, desto größer sind ihre Gefahren im Falle des Missbrauchs.

Dabei stellt sich auch die Frage nach der Aktualität der Daten. Nicht deutlich wird, ob z. B. auch bereits geschlossene oder abgelegte polizeiliche Akten in die Suche einbezogen werden sowie solche die etwa wegen des Ablaufs gesetzlicher Tilgungsfristen nicht mehr zu verwerten sind. Die Bürger brauchen zur Herstellung von Rechtsfrieden Sicherheit, dass erledigte Fälle/Vorgänge auch erledigt bleiben.

Jemand, der aus banalen Gründen in einem polizeilichen Aktenvermerk oder einer E-Mail aufgeführt (Asservaten-Quelle?) wird, sollte sich nicht sorgen müssen, durch die Analyse-Software plötzlich in einen ganz anderen Kontext gesetzt zu werden.

bb) § 47a Abs. 1 PolG bW – neu - Zu schützende Rechtsgüter

Die Mehrzahl der Länder verzichtet bislang auf die Nutzung einer solchen Software, wie derjenigen von Palantir, ohne dass die dortige Sicherheitslage ernstlich beeinträchtigt erscheint. Der pauschale Verweis auf mögliche terroristische Anschläge oder sexuellen Missbrauch von Kindern verfängt nicht, solange er beispielsweise nicht mit aussagekräftigen Zahlen belegt ist. Deutschland erscheint bisher als vergleichsweise sicheres Land. Es ist nicht erkennbar, dass es ein sich stetig verschärfendes Sicherheitsgeschehen gibt, das zum Einsatz solcher Analyse-Software zwingen würde.

Es fragt sich daher, warum mit den bereits vorhandenen Mitteln nicht einfach weitergearbeitet oder diese verbessert werden könnten.

Bei der Anlage der bisher vorhandenen Datenbanken haben sich die Beteiligten doch etwas gedacht. Wenn es z. B. darum gehen soll, die Häufigkeit von Wohnungseinbrüchen in einem bestimmten Gebiet zu erkennen, kann die bisherige Datenbank dafür doch weitergenutzt werden. Sollten die Funktionalitäten dieser Datenbank nicht ausreichen, könnte man einfach diese verbessern, statt auf alle möglichen Datenbestände bei der Polizei zuzugreifen, die mit Wohnungseinbrüchen wahrscheinlich gar Nichts zu tun haben oder veraltet sind.

Im Gesetzentwurf ist nicht dargelegt, warum ein derartiges Vorgehen nicht grundrechtsschonender sein soll.

Aus der Gesetzesbegründung erschließt sich die gebotene **Erforderlichkeit** der automatisierten Datenanalyse, so wie hier angedacht, nicht. Vor diesem Hintergrund lässt sich der Einsatz der Analyse-Software verfassungsrechtlich allenfalls dann rechtfertigen, wenn und soweit er durch **überragende Sicherheitsinteressen** des Landes zwingend geboten ist. Nicht Alles was technisch möglich ist, muss auch umgesetzt werden.

(1) Zu Nr. 1

> *„… zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist, …“*

Heimliche Überwachungsmaßnahmen, wie eine automatische Datenanalyse, bei der die Betroffenen nicht zugegen sind, die tief in das Privatleben hineinreichen, sind nur zum Schutz **besonders gewichtiger Rechtsgüter** zulässig,

> vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (270 Rdnr. 108).

Zu den besonders gewichtigen Rechtsgütern zählen vor allem Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes,

> vgl. BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277 (365 Rdnr. 203); BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (270 Rdnr. 108); BVerfG, Urteil vom 19.05.2020 – 1 BvR 2835/17 –, BVerfGE 154, 152 (269 Rdnr. 221); BVerfG, Beschluss vom 10.11.2020 – 1 BvR 3214/15 –, BVerfGE 156, 11(55 Rdnr. 116); BVerfG, Urteil vom 26.04.2022 - 1 BvR 1619/17 -, juris (Rdnr. 243).

Vergleichbares Gewicht entfalten kann der Schutz von **Sachen von bedeutendem Wert**, deren Erhaltung im öffentlichen Interesse geboten ist, sofern darunter einem engen Verständnis folgend etwa **wesentliche Infrastruktureinrichtungen** oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen gefasst werden,

> vgl. BVerfG, Urteil vom 26.04.2022 - 1 BvR 1619/17 -, juris (Rdnr. 243f.) unter Hinweis auf BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (296 Rdnr. 183) sowie BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277 (365 Rdnr. 203).

Der Anwaltsverband vermisst in der Gesetzesbegründung eine Erläuterung, was mit Sachen von bedeutendem Wert gemeint sein soll. In seiner Entscheidung zur zentralen Antiterrordatei führte das Bundesverfassungsgericht insoweit aus:

> „Gemeint sind im Zusammenhang mit der Terrorismusabwehr etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen. Auch enthält die Vorschrift hohe Eingriffsschwellen. Es bedarf für die Schutzgüter einer gegenwärtigen Gefahr, die sich nicht nur auf tatsächliche Anhaltspunkte stützt, sondern durch bestimmte Tatsachen unterlegt sein muss. Dabei sind Zugriff und Nutzung der Daten nur erlaubt, wenn dies unerlässlich ist und die Datenübermittlung aufgrund eines Ersuchens nicht rechtzeitig erfolgen kann. Der Zugriff auf die Daten ist überdies verfahrensrechtlich gesichert. Die weitere Verwendung der Daten steht weiterhin unter Zustimmungsvorbehalt der jeweils informationsführenden Behörden, über deren Erteilung - wie der Zusammenhang der Norm nahelegt - nach Maßgabe des jeweiligen Fachrechts zu entscheiden ist."
>
> BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277 = juris (Rdnr. 203).

Dem vorliegenden Entwurf ist nicht zu entnehmen, dass der Begriff „Sachen von bedeutendem Wert" in derselben Weise zu verstehen sein soll. Ebenso wenig werden vergleichbar Eingriffsschwellen definiert oder die Zustimmung der informationsführenden Behörde vorausgesetzt. Gleichwohl sollen „gezielte Abfragen in landesfremden Datenbeständen" ermöglicht und „Daten in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Daten aus Internetquellen" herangezogen werden können (§ 47a Abs. 3 Satz 2 PolG BW-neu). Dies lässt eine völlige Entgrenzung der Datenverarbeitung befürchten.

(2) Zu Nr. 2

Das Erfordernis einer hinreichend konkretisierten Gefahrenlage oder eines qualifizierten Tatverdachts bestimmt den **Anlass**, aus dem entsprechende Daten erhoben werden dürfen, nicht aber die erlaubten Zwecke, für die die Daten der Behörde dann zur Nutzung offenstehen. Für die Wahrung der **Zweckbindung** kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt. Ausdrücklich geregelt wird dies nicht.

Vorausgesetzt wird eine konkrete Gefahr für ein besonders gewichtiges Rechtsgut, wie bei „Straftaten von erheblicher Bedeutung".

Der Begriff der **konkreten Gefahr** setzt eine Sachlage voraus, die bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens im Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einer Verletzung des geschützten Rechtsguts führt.

Eine **hinreichend konkretisierte Gefahr** kann schon vorliegen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen darauf hinweisen, dass eine entsprechende **Straftat** begangen werden wird.

Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann,

> vgl. BVerfG, BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 106).

Da zu den Straftaten von erheblicher Bedeutung auch Vorfeldstraftaten wie die §§ 129a und 129b Strafgesetzbuch (StGB) sowie die §§ 89a, 89b und 89c StGB gehören, wird in der Nummer 2 zusätzlich verlangt, dass mit der konkretisierten Gefahr der Begehung einer **Straftat von erheblicher Bedeutung** auch bereits eine Gefahr für das durch den Straftatbestand geschützte Rechtsgut verbunden ist,

> vgl. BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 170); BVerfG, Beschluss vom 09.12.2022 - 1 BvR 1345/21 -, juris (Rdnr. 95).

Je geringere Anforderungen der Gesetzgeber an den Anlass einer Datenanalyse oder -auswertung stellt, umso genauer und enger muss er die Methode der Suche regeln.

(3) Zu Nr. 3

Will der Gesetzgeber der Polizei eine Befugnis zur automatisierten Datenanalyse oder -auswertung – wie hier – bereits für die **vorbeugende Bekämpfung von**

Straftaten, also im Vorfeld einer konkretisierten Gefahr einräumen, muss er zur Wahrung der Verhältnismäßigkeit die Eingriffsintensität der Maßnahme reduzieren. Bei den hierfür bestehenden Möglichkeiten zur Begrenzung insbesondere von Art und Umfang der Daten und der Verarbeitungsmethoden sind die Anforderungen des **Gesetzesvorbehalts** zu beachten. Der Gesetzgeber muss die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben.

Die Eingriffsschwelle in der Nummer 3 betrifft die Verhütung von Straftaten. Dies ist bei weniger gewichtigen Eingriffen zulässig, wenn sie dem Schutz besonders gewichtiger Rechtsgüter dienen,

> vgl. BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 107).

Dabei muss der Gesetzgeber das erforderliche Rechtsgut nicht zwingend unmittelbar benennen, sondern kann auch an entsprechende Straftaten anknüpfen.

Maßgeblich für die Schwere des tatbestandlichen Unrechts sind der Rang des verletzten Rechtsguts und andere tatbestandlich umschriebene, gegebenenfalls auch in einem Qualifikationstatbestand enthaltene Begehungsmerkmale und weitere Tatfolgen. Sie allein müssen die besondere, deutlich über dem Durchschnitt liegende Schwere des jeweiligen Straftatbestandes begründen,

> vgl. BVerfG, Urteil vom 03.03.2004 – 1 BvR 2378/98 –, BVerfGE 109, 279 (344 Rdnr. 238).

Dabei gibt der Strafrahmen einer Deliktsnorm einen maßgebenden Anhaltspunkt dafür, ob es sich abstrakt um eine - wie hier erforderliche - besonders schwere Straftat handelt. Ausgehend vom Strafrahmen einer Strafnorm liegt die besondere Schwere einer Straftat jedenfalls dann vor, wenn sie mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht ist,

> vgl. BVerfG, Beschluss vom 24.06.2025 – 1 BvR 180/23 –, juris (Rdnr. 134); BVerfG, Beschluss vom 24.06.2025 – 1 BvR 2466/19 –, juris (Rdnr. 137); BVerfG, Beschluss vom 17.07.2024 – 1 BvR 2133/22 –, BVerfGE 169, 130 (219 Rdnr. 203); BVerfG, Beschluss vom 09.12.2022 – 1 BvR 1345/21 –, BVerfGE 165, 1 (93 Rdnr. 179); BVerfG, Urteil vom 03.03.2004 – 1 BvR 2378/98 –, BVerfGE 109, 279 (347f., 349).

cc) Diskriminierungsschutz – Einsatz welcher Systeme?

Die Analyseplattform darf keine Prognosesoftware in dem Sinne sein, dass sie eigenständig kriminelles Verhalten vorhersagt und die von einem Menschen zu treffende abschließende Bewertung ersetzt. Sie darf lediglich ein technisches Hilfsmittel sein.

Welche Systeme - mit oder ohne KI-Funktionalität - letztlich in eine verfahrensübergreifende Recherche- und Analyseplattform integriert werden, kann – laut der derzeitigen Gesetzesbegründung – angeblich aufgrund der fortschreitenden technischen Entwicklungen im Einzelnen nicht konkret abgesehen werden.

Das ist inakzeptabel. Das Gesetz soll jetzt erlassen und angewendet werden. Es muss dem verfassungsrechtlichen Grundsatz der Normenklarheit genügen. Die in Betracht kommenden Systeme sind deshalb zumindest ihrer Art und Funktionalität nach zu beschreiben. Ein nur negative Abgrenzung, was die Systeme nicht können bzw. ermöglichen dürfen – und dies auch nur beschränkt auf ein einzelnes Kriterium -, genügt diesen Anforderungen nicht.

Sollten sich die technischen Möglichkeiten zukünftig wesentlich ändern, wird das Gesetz entsprechend zu ändern oder neu zu fassen sein.

dd) Ausschluss von Verkehrsdaten aus Funkzellenabfragen sowie Telekommunikationsdaten

Die Datenmenge wird auch durch Regelungen über Aufbewahrungsfristen und Löschungspflichten bestimmt. Dies wird jedoch in der vorliegenden Entwurfsfassung nicht hinreichend deutlich.

Soweit mit der Einbeziehung von Verkehrsdaten, insbesondere den aus Funkzellenabfragen gewonnenen Daten (vgl. etwa § 100g Abs. 3 StPO), in den für die automatisierte Datenanalyse oder -auswertung bereitstehenden Datenpool eine breitere bevorratende Speicherung von Verkehrsdaten möglich ist, müssen jedenfalls die erfassbaren Datenmengen substantiell begrenzt und eine Höchstspeicherungsdauer geregelt sein,

> vgl. für die nachrichtendienstliche Ausland-Ausland- Telekommunikationsaufklärung BVerfG, Urteil vom 19.05.2020 – 1 BvR 2835/17 –, BVerfGE 154, 152 (259 Rdnr. 191).

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat gegenüber dem Bundesverfassungsgericht erklärt, bei der Funkzellenabfrage enthalte eine Lieferung ungefähr 100.000 Daten,

> vgl. BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 142).

Da bei der Verkehrsdatenerhebung aus Funkzellenabfragen insbesondere im Hinblick auf die Standortdaten häufig eine Vielzahl unbeteiligter Personen betroffen ist, führt der Ausschluss der Einbeziehung von Verkehrsdaten aus Funkzellenabfragen zu einer deutlichen Reduzierung der Eingriffsintensität. Dies dient sowohl dem Schutz unbeteiligter Personen als auch der Wahrung der Verhältnismäßigkeit.

Darüber hinaus dürfen auch Telekommunikationsdaten nicht in die automatisierte Datenanalyse gemäß Absatz 1 Nummer 3 einbezogen werden, weil der **zusätzliche Eingriff in das Fernmeldegeheimnis nach Artikel 10 Absatz 1 des Grundgesetzes** – gerade im Hinblick auf die gegebenenfalls betroffenen Inhaltsdaten bei der Telekommunikation – eine Abstufung der Eingriffsintensität erforderlich macht.

ee) § 47a Abs. 7 PolG BW-neu – schriftlicher Anordnungsvorbehalt mit Begründungszwang

Für eine effektive Kontrolle unerlässlich ist, dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden.

Hier ist zu fordern, dass derartige Anordnungen nicht zu bloßen Floskeln verkommen. Der Gesetzentwurf sollte zur Orientierung der Bürger, aber auch der Verantwortlichen die Konsequenzen anführen, die eintreten, wenn dem Begründungszwang nicht ausreichend genüge getan wird. Eine nur formelhafte Begründung hätte datenschutzrechtlich keinen Bestand.

ff) Ausschluss von personenbezogenen Daten aus einer Wohnraumüberwachung oder einer Online-Durchsuchung

Zur Verringerung der Eingriffsintensität der automatisierten Datenanalyse trägt schließlich bei, dass nach Absatz 3 Satz 6 personenbezogene Daten, die aus den **besonders schwerwiegenden Grundrechtseingriffen** der Wohnraumüberwachung und der Online-Durchsuchung stammen, nicht einbezogen werden dürfen.

Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall hinreichend konkretisierten Gefahr kommt hier – laut Bundesverfassungsgericht - nicht in Betracht.

gg) Zu § 47a Abs. 4 PolG BW-neu - Technisch-organisatorische Vorkehrungen – zu veröffentlichende Verwaltungsvorschrift

Zur Regelung von Aspekten, die nicht unmittelbar vom Gesetzgeber selbst zu normieren sind, kommt zunächst eine Verordnungsermächtigung in Betracht. Darüber hinaus kann der Gesetzgeber hier die Verwaltung verpflichten, die im Gesetz oder in Rechtsverordnungen geregelten Vorgaben in abstrakt-genereller Form weiter zu konkretisieren. In jedem Fall bedarf die Konkretisierung durch Verwaltungsvorschriften aber einer **gesetzlichen Grundlage**. Dabei müssen Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz selbst bestimmt werden. Hierbei hat der Gesetzgeber sicherzustellen, dass die für die Anwendung der Bestimmungen im Einzelfall maßgebliche Konkretisierung und Standardisierung seitens der Behörden nachvollziehbar dokumentiert und **veröffentlicht** wird,

> vgl. auch BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277 (357 Rdnr. 183); BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 123).

Denn die Dokumentation und Offenlegung der von der Verwaltung festgelegten Kriterien versetzt insbesondere die **Datenschutzbeauftragten** in die Lage, die Anwendung der Befugnis durch die Exekutive zu kontrollieren,

> vgl. BVerfG, Urteil vom 24.04.2013 – 1 BvR 1215/07 –, BVerfGE 133, 277 (357f. Rdnr. 184 m. w. N.).

Technisch-organisatorische Vorkehrungen, die die **Einhaltung der Zweckbindung** sicherstellen, können etwa in der technischen Trennung von Datenbeständen nach unterschiedlichen Verarbeitungszwecken oder einer zweckabhängigen Verteilung von Zugriffsrechten auf Datenbestände bestehen,

> vgl. BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 -, juris (Rdnr. 140).

(1) Nr. 1 - Rollen- und Rechtekonzept – Zugriffsrechte

> Je weniger Personen Zugriff auf das Analyseinstrument haben und je zielgenauer der Zugriff erfolgt, umso weniger Analyse- oder Auswertungsvorgänge dürften tendenziell in Gang gesetzt werden und umso weniger Daten werden verarbeitet.

Sofern die für die automatisierte Datenanalyse oder -auswertung verwendbaren Datenbestände nicht von vornherein inhaltlich und mengenmäßig sehr eng begrenzt sind, muss der Gesetzgeber zur Begrenzung der automatisierten Anwendung zudem sicherstellen, dass nur einzelne, entsprechend qualifizierte Mitarbeiterinnen und Mitarbeiter der Polizei Zugriff auf die Einrichtung haben und davon nur in dem durch den gesetzlich zu regelnden Eingriffsanlass erforderlichen Zusammenhang Gebrauch machen können. Die Begrenzung der Zugriffsmöglichkeiten ist über die rechtliche Begrenzung hinaus durch organisatorische und technische Vorkehrungen sicherzustellen. Technische Einzelheiten können in zu veröffentlichenden Verwaltungsvorschriften geregelt werden.

(2) Nr. 2 - Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten

Das Bundesverfassungsgericht verlangt in seiner Entscheidung vom 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20 zur Reduzierung der Eingriffsintensität beispielsweise eine Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen.

Datenbestände, die zukünftig in eine automatisierte Datenanalyse einbezogen werden sollen, sind daher bereits jetzt entsprechend anzulegen und zu pflegen.

(3) Nr. 3 – Konzept zur Zugriffskontrolle, § 47a Abs. 4 PolG BW – neu

Protokollierung der einzelnen Arbeitsschritte gemäß § 74 PolG BW. Die gesetzlich vorgeschriebene Protokollierung soll die nachträgliche aufsichtliche Kontrolle sichern und ist gleichzeitig Voraussetzung für die Gewährleistung effektiven Rechtsschutzes gemäß Artikel 19 Absatz 4 GG.

(4) Nr. 4 – Begründung für längere Speicherdauer auf Analyseplattform und bei Gefahr im Verzug

Einzelfallbezogene auf der Analyseplattform gespeicherte Daten sollen grundsätzlich nach zwei Jahren gelöscht werden müssen. Es fragt sich, warum die Analyse-Ergebnisse auf der Plattform gespeichert werden sollen. Sicherer wäre doch die getrennte Ablage für den Fall, dass die eingesetzte Software Sicherheitslücken aufweist, gerade auch dann, wenn sie von ausländischen Lieferanten stammt, der nicht hiesigen Datenschutzbestimmungen unterliegt und bei dem –

wie eingangs angemerkt – keine absolute Sicherheit gegen einen Datenabfluss in die USA besteht.

hh) § 47a Abs. 8 PolGB-neu - Beteiligung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LFDI)

Der Verhältnismäßigkeitsgrundsatz stellt Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle,

vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 (282 Rdnr. 134) m. w. N., st. Rspr.

Insbesondere einer sachgerechten Ausgestaltung der Kontrolle kommt große Bedeutung zu. Richtig ist, den LfDI vor dem Einsatz oder einer wesentlichen Änderung solcher Analyse-Software anzuhören. Dazu sollte ihm nicht nur ausreichend Zeit eingeräumt werden, sondern ihm gegenüber auch die Funktionsweise der Software im Detail offengelegt werden, damit er seine Beratungs- und Kontrollfunktion ordnungsgemäß ausüben kann. Eine solche Offenlegung wird – soweit bekannt – bezogen auf die Software „Gotham" von Palantir abgelehnt.

c) Zu § 57a PolG BW – neu - Weitere Verarbeitung zu Zwecken der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten

Mit der Regelung in § 57a soll eine Grundlage für die Verarbeitung von personenbezogenen Daten für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von informationstechnischen Produkten einschließlich **KI-Systemen** und KI-Modellen im Sinne der KI-VO für Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst geschaffen werden, unabhängig von der Durchführung wissenschaftlicher Forschungsarbeiten.

„Informationstechnische Produkte" sind entsprechend der Legaldefinition in **§ 2 Abs. 9a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)** Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten. Zu den informationstechnischen Produkten zählen insbesondere auch KI-Systeme, also maschinengestütze Systeme, die für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt sind und die nach ihrer Betriebsaufnahme anpassungsfähig sein können und aus den erhaltenen Eingaben für explizite oder implizite Ziele ableiten, wie Ausgaben - wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen - erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können (KI-Systeme gem. Art. 3 Nr. 1 VO KI-VO) sowie

diesen Systemen zugrundeliegende KI-Modelle mit oder ohne allgemeinen Verwendungszweck i. S. des der KI-VO.

Hier fragt sich, wieso eine solche polizeiinterne Entwicklung für **erforderlich** gehalten wird und die Ergebnisse von wissenschaftlichen Einrichtungen, wie bisher, nicht mehr ausreichend sein sollen. Der Gesetzentwurf gibt keine Antwort auf die Frage, woher die erforderlichen IT-Fachkräfte innerhalb der Polizei dafür kommen sollen. Wie gesagt, werden innerhalb der Polizei bisher ein großer Personalnotstand und unzureichende technische Infrastruktur beklagt.

Der Anwaltsverband BW hält externe Forschung und Entwicklung an **geeigneten** wissenschaftlichen Einrichtungen für zielführender, weil gerade sie eine gewisse Unabhängigkeit gewährleisten und deren objektivierter Blick von außen gewiss hilfreich ist. In anderen Lebensbereichen wird wissenschaftlichen Einrichtungen vertraut; nicht nachvollziehbar ist, weshalb dies im Bereich der inneren Sicherheit nicht gelten soll. Ebenso bleibt unklar, warum wissenschaftliche Einrichtungen nicht in der Lage sein sollen, realitätsnahe Trainingsdaten zu verwenden.

Soweit Datenbestände der Polizei nicht anonymisiert verwendet werden sollen, hat der Anwaltsverband BW große Bedenken. Insbesondere muss das begründete **Erfordernis** bestehen, Daten unverändert zu verarbeiten, oder eine **Anonymisierung oder Pseudonymisierung** der Daten muss entweder nicht oder nur mit unverhältnismäßigem Aufwand möglich sein.

Soweit der Gesetzentwurf in § 57a Abs. 1 Nr. 2 PolG BW-neu auf einen „unverhältnismäßigen Aufwand“ abstellt, verweist der Anwaltsverband auf die Entscheidung zu Art. 15 DSGVO

BFH, Urteil vom 14.01.2025 – IX R 25/22 –;

danach darf ein Verantwortlicher den Auskunftsanspruch nach Art. 15 DSGVO nicht mit dem Argument ablehnen, dass die Erteilung der Auskunft angeblich einen unverhältnismäßigen Aufwand verursache. Die Rechte Betroffener können nicht ohne weiteres durch organisatorische oder logistische Herausforderungen der verantwortlichen Stelle eingeschränkt werden.

Dies bedeutet für Behörden eine erhöhte Sorgfaltspflicht im Umgang mit personenbezogenen Daten. Insbesondere in komplexen Datenbeständen sollten verantwortliche Stellen **frühzeitig** geeignete Maßnahmen zur effizienten Erfüllung datenschutzrechtlicher Vorgaben implementieren. D.h. bei der Anlage und beim Betreiben von Datenbanken, auf die später zugegriffen werden soll, ist schon darauf zu achten, dass sie bei einem möglichen Training von „informationstechnischen Produkten“ nicht zu unerwünschten Konfrontationen führen.

Die Gesetzesbegründung gibt auch keinerlei Hinweise, wann so ein „unverhältnismäßiger Aufwand“ anzunehmen sein soll und wie und von wem er festgestellt werden soll. Unstreitig dürfte sein, dass hierbei der Aufwand für eine Anonymisierung und/oder Pseudonymisierung zu deren Schutzzweck ins Verhältnis zu setzen sein werden. Angesichts des hohen Stellenwertes des Schutzes persönlicher Daten vermag somit allenfalls ein immenser Aufwand geeignet, eine Anwendung der Regelung zu rechtfertigen. Der Anwaltsverband weist in diesem Zusammenhang erneut auf verfassungsrechtliche Gebot der Normenklarheit und -bestimmtheit hin.

Insbesondere beim Einsatz von Techniken, bei denen KI-Modelle mit Daten trainiert werden, besteht die Gefahr, dass darauf aufbauende Systeme **Diskriminierungen fortschreiben** oder verstärken, wenn unvollständige, fehlerhafte oder nicht repräsentative Trainingsdaten verwendet werden oder auch wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen (Rückkopplungsschleifen). Es muss also unter anderem sichergestellt werden, dass die Trainings-, Validierungs- und Testdatensätze im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sind.

d) Zu § 74 PolG BW-neu – Protokollierung eingriffsintensiver Maßnahmen

Der Anwaltsverband begrüßt die Erweiterung der Protokollierungspflicht in § 74 PolG BW wegen der hohen Eingriffsintensität auf Maßnahmen nach dem neuen § 47a PolG BW (automatisierte Datenanalyse).

e) Zu § 86 PolG BW – neu – Informationspflicht

Der Anwaltsverband begrüßt die Erweiterung der Informationspflicht in § 86 PolG BW wegen der hohen Eingriffsintensität auf Maßnahmen nach dem neuen § 47a PolG BW (automatisierte Datenanalyse).

f) Zu § 90 PolG BW – neu - Parlamentarische Kontrolle, Unterrichtung der Öffentlichkeit

aa) Parlamentarisches Kontrollgremium – vierteljährliche Unterrichtung

Im Rahmen der Unterrichtung ist darzustellen, in welchem Umfang von den aufgeführten Maßnahmen aus Anlass welcher Art von Gefahrenlagen Gebrauch gemacht wurde und betroffene Personen benachrichtigt wurden. Damit wird den Anforderungen des Bundesverfassungsgerichts in seinem Urteil zum BKA-Gesetz Rechnung getragen,

BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09 –, BVerfGE 141, 220 = juris (Rdnr. 142ff.).

bb) Jährliche Unterrichtung der Öffentlichkeit

Absatz 2 normiert die vom Bundesverfassungsgericht ebenfalls geforderte Pflicht zur Unterrichtung der Öffentlichkeit und sieht insoweit ein jährliches Intervall vor. Hier ist zu fordern, dass ein ausführlicher und aussagekräftiger Bericht vorgelegt wird, der für die Bürger verständlich ist.

6. Artikel 2 - Änderung der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes – Anordnungsbefugnis bei Gefahr in Verzug

Gegen die beabsichtige Regelung bestehen keine Einwände.

Wir würden uns freuen, wenn unsere Hinweise und Vorschläge Berücksichtigung finden würden. Für etwaige Rückfragen oder auch Gespräche stehen wir selbstverständlich gerne zur Verfügung. Sollte im Laufe des weiteren Verfahrens eine weitere Anhörung durchgeführt werden, so bitten wir um Unterrichtung und erneute Gelegenheit zur Äußerung.

Mit freundlichen Grüßen

Prof. Dr. Peter Kothe
Präsident