Landtag von Baden-Württemberg **Drucksache 17 / 9478**

17. Wahlperiode **23.9.2025**

Gesetzentwurf

der Landesregierung

Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

A. Zielsetzung

Das Gesetz verfolgt im Wesentlichen drei Ziele. Zunächst soll eine Rechtsgrundlage dafür geschaffen werden, bisher unverbundene Daten und Datenquellen des Polizeivollzugsdienstes in einer Analyseplattform zusammenzuführen, um die vorhandenen Datenbestände durch Suchfunktionen systematisch erschließen zu können (automatisierte Datenanalyse). Zudem soll eine Rechtsgrundlage zur Erhebung, Verarbeitung und Übermittlung von Standortdaten geschaffen werden, die nach Anwahl der Notrufnummer mittels eines mobilen Endgerätes automatisiert und ohne Interaktion der anrufenden Person generiert und übermittelt wurden. Dies ermöglicht dem Polizeivollzugsdienst unter Nutzung der sogenannten Advanced-Mobile-Location-Technologie (AML-Technologie) die schnelle Ortung einer hilfesuchenden Person. Schließlich sollen die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst mit Befugnissen zur Entwicklung, zum Training, zum Testen, zur Validierung und zur Beobachtung von informationstechnischen Produkten ausgestattet werden, um die eigenständige Entwicklung von informationstechnischen Produkten zu ermöglichen und die Abhängigkeit von ausländischen, insbesondere außereuropäischen Produkten zu verringern. Durch rechtliche, technische und organisatorische Maßgaben wird dabei ein hohes Schutzniveau für personenbezogene Daten gewährleistet und gleichzeitig die Entwicklung und Nutzung von diskriminierungsfreien informationstechnischen Produkten sichergestellt.

B. Wesentlicher Inhalt

Der Gesetzentwurf sieht im Wesentlichen die Schaffung von Rechtsgrundlagen zur Einführung einer automatisierten Datenanalyse, zur Erhebung, Verarbeitung und Übermittlung von Standortdaten, die nach Anwahl der Notrufnummer mittels eines mobilen Endgerätes automatisiert generiert und übermittelt wurden, sowie zur Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von informationstechnischen Produkten vor.

Eingegangen: 23.9.2025 / Ausgegeben: 6.10.2025

C. Alternativen

Keine.

D. Kosten für die öffentlichen Haushalte

Die Umsetzung der durch die Änderung des Polizeigesetzes geschaffenen Rechtsgrundlagen führt nach einer ersten Grobabschätzung zu Mehrausgaben für den Landeshaushalt in Höhe von jährlich rund 10 Millionen Euro. Es handelt sich dabei um Personal- und Sachmittel für die Beschaffung von Software und für den Betrieb der zum Teil komplexen informationstechnischen Infrastruktur. Diese Mehrausgaben sind bereits im Staatshaushaltsplan 2025/2026 im Bereich des Innenministeriums vollständig 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 außerhalb von rein wissenschaftlichen Forschungsarbeiten können der Polizei Kosten im Rahmen von Softwarebeschaffung, -entwicklung und -erprobung, die sich derzeit noch nicht beziffern lassen, entstehen. Die Deckung dieser Kosten erfolgt jedoch im Rahmen der vorhandenen Mittel der Polizei. Über eventuell zukünftig entstehende Mehrbedarfe entscheidet der Haushaltsgesetzgeber.

E. Bürokratievermeidung, Prüfung Vollzugstauglichkeit

Der Gesetzentwurf verursacht keine erheblichen Auswirkungen für Unternehmen, Verwaltung und Bürgerinnen und Bürger oder aufwendige Verwaltungsverfahren. Von der Durchführung eines Praxis-Checks und einer Bürokratielastenschätzung wurde daher abgesehen. Gleichwohl können punktuell Mehraufwände beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen seiner gesetzlichen Zuständigkeit entstehen, die im Rahmen vorhandener Mittel gedeckt werden.

F. Nachhaltigkeits-Check

Es ergeben sich positive Auswirkungen auf den Zielbereich IV. Wohl und Zufriedenheit.

G. Digitaltauglichkeits-Check

Die automatisierte Datenanalyse ermöglicht es dem Polizeivollzugsdienst, vorhandene Datenbestände durch Suchfunktionen systematisch zu erschließen. Dadurch werden Medienbrüche reduziert und manuelle Abfragen verschiedener Datenquellen entbehrlich, die aufgrund großer Datenmengen aus unterschiedlichen Quellen sowie unterschiedlicher Dateiformate bislang zeitaufwendig und komplex sind. Durch Nutzung der AML-Technologie werden das Verfahren zur schnellen Standortbestimmung einer hilfesuchenden Person mittels einer Web-Anwendung digitalisiert und Medienbrüche reduziert. Zudem wird die Genauigkeit der Standortbestimmung durch die kombinierte Nutzung verschiedener technischer Positionsdienste erheblich verbessert. Durch die Einführung entsprechender elektronischer Fachverfahren ist daher sowohl bezogen auf die Analyse von polizeilichen Datenbeständen als auch bezogen auf die Standortbestimmung von notrufenden Personen eine Vereinfachung und Beschleunigung polizeilicher Abläufe zu erwarten.

H. Sonstige Kosten für Private

Keine.

Staatsministerium
Baden-Württemberg
Ministerpräsident

Stuttgart, 23. September 2025

An die
Präsidentin des Landtags
von Baden-Württemberg

Sehr geehrte Frau Landtagspräsidentin,

als Anlage übersende ich Ihnen gemäß Artikel 59 Absatz 1 der Verfassung des Landes Baden-Württemberg den von der Landesregierung beschlossenen Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften. Ich bitte Sie, die Beschlussfassung des Landtags herbeizuführen. Die federführende Zuständigkeit liegt beim Ministerium des Inneren, für Digitalisierung und Kommunen, beteiligt sind das Staatsministerium, sowie das Ministerium für Finanzen.

Mit freundlichen Grüßen

Kretschmann

Ministerpräsident

Der Landtag wolle beschließen,

dem nachstehenden Gesetzentwurf seine Zustimmung zu erteilen:

Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Artikel 1

Änderung des Polizeigesetzes

Das Polizeigesetz vom 6. Oktober 2020 (GBl. S. 735, ber. S. 1092) wird wie folgt geändert:

1. Nach § 45 wird folgender § 45a eingefügt:

„§ 45a

Verarbeitung von Standortdaten bei Anwahl der Notrufnummer 110

(1) Das Präsidium Technik, Logistik, Service der Polizei kann die im Rahmen einer Notrufverbindung von einem mobilen Telekommunikationsendgerät generierten und automatisch übermittelten personenbezogenen Daten, einschließlich der Standortdaten, erheben, speichern und auf Abruf an die zuständigen Notrufabfragestellen übermitteln. Die Daten sind 60 Minuten nach deren Erhebung zu löschen. Eine Verarbeitung zu einem anderen Zweck als zur Übermittlung an die zuständigen Notrufabfragestellen ist unzulässig.

(2) Der Polizeivollzugsdienst kann als zuständige Notrufabfragestelle im Einzelfall die in Absatz 1 Satz 1 genannten Daten erheben, verarbeiten und speichern, soweit dies zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Die Daten sind spätestens nach sechs Monaten zu löschen.“

2. Nach § 47 wird folgender § 47a eingefügt:

„§ 47a

Automatisierte Datenanalyse

(1) Der Polizeivollzugsdienst kann nach Maßgabe der Absätze 2 bis 7 in polizeilichen Dateisystemen gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen, verknüpfen, abgleichen, aufbereiten, auswerten und bewerten (automatisierte Datenanalyse), wenn

1. dies 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,

2. bestimmte Tatsachen die Annahme rechtfertigen, dass

   a) innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von erheblicher Bedeutung begangen wird, die auch im Einzelfall schwer wiegt,

   b) die automatisierte Datenanalyse zur Verhütung dieser Straftat erforderlich ist und

   c) die Verwirklichung der Straftat zu einer Gefahr für das geschützte Rechtsgut führen würde,

oder

3. bestimmte Tatsachen die Annahme rechtfertigen, dass besonders schwere Straftaten begangen werden sollen und die automatisierte Datenanalyse zur Verhütung dieser Straftaten erforderlich ist.

(2) Die automatisierte Datenanalyse unterstützt den Polizeivollzugsdienst bei der Erfüllung seiner Aufgaben, indem sie Informationen bereitstellt, die es dem Polizeivollzugsdienst ermöglichen, eigene Bewertungen, Prognosen und Entscheidungen zu treffen. Dabei ist sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Eine abschließende Bewertung der bereitgestellten Informationen und die Entscheidung über weitere Maßnahmen werden durch den Polizeivollzugsdienst getroffen. Die automatisierte Datenanalyse wird manuell ausgelöst und erfolgt anhand anlassbezogener und zielgerichteter Suchkriterien, die sich aus einem konkreten Sachverhalt bezogen auf einen Anlass im Sinne des Absatzes 1 ergeben. Bei Maßnahmen nach Absatz 1 Nummern 2 und 3 ist der Suchvorgang auf die in den §§ 6 und 7 genannten Personen auszurichten. Eine direkte Anbindung der Analyseplattform an Internetdienste ist unzulässig.

(3) Zum Zweck der automatisierten Datenanalyse können eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden. Verkehrsdaten, Daten aus Asservaten, Daten im Sinne des Satzes 1 aus gezielten Abfragen in landesfremden Datenbeständen, Daten in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Daten aus Internetquellen können ergänzend einbezogen werden, soweit dies im Einzelfall erforderlich ist. Verkehrsdaten aus Funkzellenabfragen sowie Telekommunikationsdaten dürfen bei einer Maßnahme nach Absatz 1 Nummer 3 nicht in die Analyse einbezogen werden. Einzelfallbezogen auf der Analyseplattform gespeicherte Daten nach Satz 2 sind spätestens nach Ablauf von zwei Jahren zu löschen, soweit eine weitere Speicherung der Daten nicht erforderlich ist. Eine weitere Speicherung nach Satz 4 kann im Einzelfall höchstens zweimal durch eine schriftliche und begründete Anordnung der Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts um jeweils höchstens ein Jahr verlängert werden. Personenbezogene Daten, die aus einer Wohnraumüberwachung oder einer Online-Durchsuchung gewonnen

wurden, dürfen nicht in die automatisierte Datenanalyse einbezogen werden.

(4) Technisch-organisatorische Vorkehrungen, insbesondere zur Einhaltung der Zweckbindung nach § 15 Absätze 2 und 3, werden in einer Verwaltungsvorschrift geregelt, die in dem für den Geschäftsbereich des Innenministeriums vorgesehenen amtlichen Bekanntmachungsblatt zu veröffentlichen ist. Diese beinhaltet insbesondere

1. ein Rollen- und Rechtekonzept,
2. ein Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten,
3. ein Konzept zur Zugriffskontrolle, das auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht, sowie
4. nähere Bestimmungen über den Inhalt der erforderlichen Begründung nach Absatz 3 Satz 5 und Absatz 7 Satz 3.

Die Vorgaben in der Verwaltungsvorschrift dienen unter Berücksichtigung der in Absatz 1 beschriebenen Eingriffsschwellen dem übergeordneten Ziel, die Datenbestände auf das für den Analysezweck erforderliche Maß zu begrenzen und die Einbeziehung von Daten unbeteiligter Personen möglichst zu vermeiden.

(5) Das Rollen- und Rechtekonzept nach Absatz 4 Satz 2 Nummer 1 regelt die Verteilung sachlich eingeschränkter Zugriffsrechte. Die Zugriffsrechte sind nach dem Prinzip auszugestalten, dass die Zahl der Zugriffsberechtigten umso geringer ist, desto umfangreicher und sensibler die von der Zugriffsberechtigung umfassten Daten sind. Die dienstrechtliche Stellung der Zugriffsberechtigten, ihre Funktion und ihre spezifische Qualifizierung in Bezug auf den Umfang der jeweiligen Zugriffsrechte sind festzulegen.

(6) Das Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten nach Absatz 4 Satz 2 Nummer 2 legt fest, welche personenbezogenen Daten in welcher Weise in die automatisierte Datenanalyse einbezogen werden dürfen. Ausgangspunkt ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen. Zum Schutz unbeteiligter Personen werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen. Hinsichtlich der Kategorisierung von Daten nach dem Gewicht des Grundrechtseingriffs bei der Datenerhebung müssen abstrakte Regelungen getroffen werden, die der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen. Durch technisch-organisatorische Vorkehrungen muss sichergestellt werden, dass diese Regelungen praktisch wirksam werden.

(7) Eine Maßnahme nach Absatz 1 erfolgt auf Anordnung der Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts. Bei Gefahr im Verzug kann eine Maßnahme nach Absatz 1 auch von besonders beauftragten Beam-

ten angeordnet werden. Die Anordnung ergeht schriftlich und ist zu begründen.

(8) Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg ist vor der Einrichtung oder wesentlichen Änderung einer Analyseplattform nach Absatz 1 anzuhören.“

3. Nach § 57 wird folgender § 57a eingefügt:

„§ 57a
Weitere Verarbeitung zu Zwecken der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten

(1) Die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst können bei ihnen vorhandene personenbezogene Daten zur Entwicklung, zum Training, zum Testen, zur Validierung und zur Beobachtung von informationstechnischen Produkten weiter verarbeiten, soweit dies erforderlich ist, insbesondere, weil

1. unveränderte Daten benötigt werden oder
2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Dabei ist sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Die Nachvollziehbarkeit des verwendeten Verfahrens muss sichergestellt werden, soweit dies technisch möglich ist. Eine weitere Verarbeitung von personenbezogenen Daten, die aus in § 50 genannten Maßnahmen erlangt wurden, ist zu den in Satz 1 genannten Zwecken ausgeschlossen.

(2) Eine Übermittlung von personenbezogenen Daten im Sinne des Absatzes 1 an öffentliche und nichtöffentliche Stellen ist nur zulässig, wenn die empfangende Stelle nachweist, dass die Personen, die die übermittelten Daten weiter verarbeiten sollen, Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder nach dem Verpflichtungsgesetz (BGBl. I 1974, 469, 547) zur Geheimhaltung verpflichtet worden sind.

(3) Die übermittelten Daten sind durch organisatorische und technische Maßnahmen gegen unbefugte Kenntnisnahme zu schützen.“

4. § 74 wird wie folgt geändert:

a) In Absatz 1 wird die Angabe „§§ 48 bis 56“ durch die Angabe „§§ 47a bis 56“ ersetzt.

b) Absatz 2 wird wie folgt geändert:

aa) Folgende Nummer 1 wird eingefügt:

„1. bei Maßnahmen nach § 47a (automatisierte Datenanalyse)

a) die einbezogenen Daten,

b) die verwendeten Suchkriterien sowie

c) die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden,“.

bb) Die bisherigen Nummern 1 bis 11 werden die Nummern 2 bis 12.

5. § 86 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Die Angabe „§§ 48 bis 56“ wird durch die Angabe „§§ 47a bis 56“ ersetzt.

bb) Folgende Nummer 1 wird eingefügt:

„1. des § 47a (automatisierte Datenanalyse) die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden,“.

cc) Die bisherigen Nummern 1 bis 11 werden die Nummern 2 bis 12.

b) In Absatz 3 Satz 7 wird die Angabe „§§ 48 bis 56“ durch die Angabe „§§ 47a bis 56“ ersetzt.

6. § 90 wird wie folgt gefasst:

„§ 90
Parlamentarische Kontrolle, Unterrichtung der Öffentlichkeit

(1) Das Innenministerium unterliegt hinsichtlich der nach den §§ 47a, 49, 50, 53, 54 und 55 Absatz 1 erfolgten Maßnahmen sowie den Übermittlungen nach § 61 der Kontrolle durch das Parlamentarische Kontrollgremium. Zu diesem Zweck unterrichtet das Innenministerium das Parlamentarische Kontrollgremium mindestens vierteljährlich. Auf Verlangen des Parlamentarischen Kontrollgremiums hat das Innenministerium zu einer konkreten Maßnahme zu berichten.

(2) Das Innenministerium unterrichtet die Öffentlichkeit in geeigneter Weise jährlich über die Anzahl der in Absatz 1 Satz 1 genannten Maßnahmen.“

7. In § 98 Absatz 1 Nummer 14 wird die Angabe „§§ 48 bis 50“ durch die Angabe „§§ 47a bis 50“ ersetzt.

8. In § 130 Absatz 1 Satz 1 Nummer 1 werden nach den Wörtern „Anordnungsbefugnis gemäß“ die Wörter „§ 47a Absatz 7 Satz 2,“ eingefügt.

9. Die Inhaltsübersicht ist entsprechend anzupassen.

Artikel 2

Änderung der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes

§ 4 der Verordnung des Innenministeriums zur Durchführung des Polizeigesetzes vom 16. September 1994 (GBl. S. 567), die zuletzt durch Artikel 3 des Gesetzes vom 6. Oktober 2020 (GBl. S. 735, 785) geändert worden ist, wird folgender Absatz 3 angefügt:

„(3) Die Anordnungsbefugnis nach § 47a Absatz 7 Satz 2 PolG kann die Leitung

1. eines regionalen Polizeipräsidiums auf die Leitung des Führungs- und Einsatzstabes, die Leitung der Schutzpolizeidirektion, die Leitung der Kriminalpolizeidirektion und den Polizeiführer vom Dienst,
2. des Landeskriminalamtes auf die Abteilungsleitungen und den Polizeiführer vom Dienst

übertragen.“

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung

Das Gesetz verfolgt im Wesentlichen drei Ziele.

Zunächst soll eine Rechtsgrundlage dafür geschaffen werden, bisher unverbundene Daten und Datenquellen des Polizeivollzugsdienstes in einer Analyseplattform zusammenzuführen, um die vorhandenen Datenbestände durch Suchfunktionen systematisch erschließen zu können. Der Polizeivollzugsdienst verfügt über gespeicherte und verarbeitete Daten, die derzeit auf zahlreiche Datenbanken und Quellsysteme verteilt sind. Die daraus entstehenden Datenmengen sind sehr umfangreich, heterogen strukturiert, komplex und zudem oftmals nicht über Schnittstellen miteinander verbunden. Diese Daten bilden regelmäßig die Grundlage für eine Entscheidungsfindung durch den Polizeivollzugsdienst, welche zur Abwehr von Gefahren unerlässlich ist. Eine manuelle Abfrage aus verschiedenen Datenquellen wird durch große Datenmengen und verschiedenste Quellen sowie Dateiformate immer zeitaufwendiger und komplexer. Darüber hinaus müssen die Daten in einem weiteren Schritt aufbereitet und in Beziehung gesetzt werden, bevor eine Analyse erfolgen kann. In zeitkritischen Gefahrenlagen, beispielsweise bei der Verhinderung eines drohenden terroristischen Anschlags, des andauernden sexuellen Missbrauchs zum Nachteil eines Kindes oder einer drohenden schweren Gewalttat, ist die schnelle Reaktionsfähigkeit ein erfolgskritischer Faktor.

Durch Medienbrüche, heterogene Dateiformate und fehlende Beziehungsgeflechte entstehen zeitliche und technische Aufwände, die weder dem aktuellen Entwicklungsstand der Informationstechnik noch den Anforderungen an eine effiziente und effektive Gefahrenabwehr entsprechen. Müssen Daten aus Asservaten in die Entscheidungsfindung durch den Polizeivollzugsdienst miteinbezogen werden, ist die Auswertung ohne Automatisierung in diesen zeitkritischen Situationen nicht zu bewältigen.

Derzeit kann im konkreten Einzelfall nicht ausgeschlossen werden, dass die Polizei Baden-Württemberg im Besitz von relevanten Daten und Informationen ist, diese aber nicht zusammenführen und verwenden kann. Durch eine automatisierte und schnelle Verknüpfung könnten die Daten als Entscheidungsgrundlage mit herangezogen werden.

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. Sie soll den Abfrageberechtigten als technisches Hilfsmittel zur Verfügung stehen und Daten mit Verknüpfungen durch wenige Suchbefehle visuell aufbereitet darstellen. Die automatisierte Datenanalyse ersetzt nicht die Entscheidungsfindung durch eine menschliche Instanz, sondern erleichtert selbige.

Zudem soll eine Rechtsgrundlage für den Abruf von Standortdaten geschaffen werden, die nach Anwahl der Notrufnummer mittels eines mobilen Endgerätes automatisiert und ohne Interaktion der anrufenden Person anfallen. Dies ermöglicht dem Polizeivollzugsdienst unter Nutzung der sogenannten AML-Technologie die schnelle Standortbestimmung einer hilfesuchenden Person. Aufgrund der mit einem Notfall einhergehenden Stresssituation wissen hilfesuchende Personen oftmals nicht genau, wo sie sich befinden, können bei Sprachbarrieren ihren Standort nicht mitteilen oder haben aus medizinischen oder sonstigen Gründen eine eingeschränkte räumliche Orientierung. Auch eine plötzlich unterbrochene Notrufverbindung kann dafür sorgen, dass notrufende Personen ihren Standort nicht mitteilen können. Diese Umstände kosten wertvolle Zeit und können die rechtzeitige Ankunft von Polizeivollzugsdienst oder Rettungskräften gefährden. Zur Verbesserung der Standortbestimmung von Mobilfunkteilnehmenden im Rahmen der polizeilichen Notrufbearbeitung ist daher eine genaue, schnelle und technisch zeitgemäße Übermittlung des Standorts hilfesuchender Personen erforderlich.

Schließlich soll eine Rechtsgrundlage zur Verarbeitung von Daten bei der Entwicklung, dem Training, dem Testen, der Validierung und der Beobachtung von informationstechnischen Produkten außerhalb von rein wissenschaftlichen Forschungsarbeiten geschaffen werden. Erfolgreiche Polizeiarbeit erfordert moderne und sachgerechte polizeiliche Befugnisse und vor dem Hintergrund der zunehmenden Digitalisierung auch den Einsatz neuer Technologien – unter anderem solcher, die mit Künstlicher Intelligenz (KI) im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (KI-VO) ausgestattet sind. Gerade KI-Anwendungen benötigen jedoch zur Entwicklung und zum Testen realitätsnahe Trainingsdaten. Eine zielgerichtete Entwicklung und Validierung ist daher in vielen Fällen nur durch die Nutzung polizeispezifischer – in aller Regel auch personenbezogener – Daten möglich.

Damit informationstechnische Systeme einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO ordnungsgemäß getestet und trainiert werden können, bedarf es zur Verarbeitung personenbezogener Daten einer entsprechenden Rechtsgrundlage. § 57 PolG beschränkt sich auf die Datenverarbeitung bei der Durchführung wissenschaftlicher Forschungsarbeiten, wobei der eng auszulegende Forschungsbegriff im Sinne der Datenschutz-Grundverordnung (DSGVO) und der Datenschutzkonferenz (DSK) primär wissenschaftlich ausgerichtete, methodisch fundierte und vom operativen Zweck losgelöste Vorhaben erfasst. Es ist daher durchaus fraglich, inwieweit praxisnahe Entwicklungen, systematische Tests oder die erprobungsweise Nutzung polizeilicher Software, die auf einen späteren Echtbetrieb abzielen, von der bestehenden Regelung erfasst werden.

Durch die Rechtsgrundlage zur 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 werden die Voraussetzungen für eine eigenständige Entwicklung von informationstechnischen Produkten durch die Polizei Baden-Württemberg geschaffen. Sie dient daher insbesondere auch dazu, durch unabhängige Konzeption und Entwicklung von informationstechnischen Produkten die Abhängigkeit von ausländischen bzw. außereuropäischen Produkten zu reduzieren.

II. Wesentlicher Inhalt

Mit der neu aufgenommenen Regelung in § 47a PolG wird eine bereichsspezifische Ermächtigung für die Anwendung einer automatisierten Datenanalyse geschaffen. Die informationstechnische Entwicklung der letzten Jahre ermöglicht es, bisher unverbundene Daten und Datenquellen auf einer Analyseplattform zusammenzuführen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen.

In seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) hat das Bundesverfassungsgericht grundsätzlich geklärt, unter welchen Voraussetzungen eine automatisierte Datenanalyse verfassungskonform geregelt werden kann.

Die Verarbeitung gespeicherter personenbezogener Daten im Rahmen einer automatisierten Datenanalyse greift in das Grundrecht auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 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 potenzielles Eigengewicht der automatisierten Datenanalyse festgestellt, das über das Eingriffsgewicht der weiteren Verwendung vormals getrennter Daten hinausgeht (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 50, 67 ff.). 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 (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 72 ff.). Die gesetzlichen Anforderungen für eine verfassungskonforme Regelung bestimmen

sich daher nach dem Eingriffsgewicht, das vom Gesetzgeber durch Vorkehrungen und Schutzmaßnahmen beeinflusst werden kann.

Die neu aufgenommene Regelung in § 45a PolG ermöglicht dem Polizeivollzugsdienst unter Nutzung der AML-Technologie die schnelle und sichere Standortbestimmung einer hilfesuchenden Person. Aufgrund europarechtlicher Vorgaben werden die Standortdaten mobiler Endgeräte bei Anwahl einer nationalen Notrufnummer automatisiert erhoben. Hierfür kommt der auf mobilen Endgeräten vorinstallierte Systemdienst AML zum Einsatz. Zuständig für die Annahme von Notrufen sind in Deutschland die sogenannten Notrufabfragestellen (vgl. § 164 Telekommunikationsgesetz, § 2 Nummer 2 Notrufverordnung). Für die Notrufnummer 110 sind die Polizeien der Länder zuständige Notrufabfragestelle.

Mit der neu aufgenommenen Regelung in § 57a wird 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 geschaffen, unabhängig von der Durchführung wissenschaftlicher Forschungsarbeiten.

III. Alternativen

Alternativen zu einer gesetzlichen Regelung bestehen nicht.

IV. Finanzielle Auswirkungen

Mit der Umsetzung der durch die Änderung des Polizeigesetzes geschaffenen Rechtsgrundlagen für die automatisierte Datenanalyse und zur Verarbeitung von Standortdaten bei Anwahl der Notrufnummer sind Mehrausgaben für den Landeshaushalt in Höhe von jährlich insgesamt rund 10 Millionen Euro verbunden. Für die automatisierte Datenanalyse ist ein Bedarf in Höhe von 9,25 Millionen Euro für Personal- und Sachmittel veranschlagt. Neben den Kosten zur Beschaffung der Spezialsoftware sind für den Betrieb der technisch komplexen informationstechnischen Infrastruktur informationstechnische Spezialisten einzustellen. Für den Betrieb der AML-Technologie werden Finanzmittel in Höhe von rund 550 000 Euro benötigt. Im Staatshausplan 2025/2026 wurden 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 entstehen für Softwarebeschaffung, -entwicklung und -erprobung sächliche und personelle Aufwände, die in den Folgejahren von Anzahl und Ausgestaltung der Anwendungen abhängig sein werden und sich daher noch nicht beziffern lassen. Der Polizei stehen Mittel im Rahmen der informationstechnischen Budgetplanung im Staatshaushaltsplan zur Verfügung. Diese Mittel können 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.

V. Bürokratievermeidung, Prüfung der Vollzugstauglichkeit

Auf eine Bürokratielastenschätzung und einen Praxis-Check wurde gemäß Nummern 4.3.3 und 4.3.4 der Verwaltungsvorschrift der Landesregierung und der Ministerien zur Erarbeitung von Regelungen (VwV Regelungen) verzichtet, da durch das vorliegende Gesetz weder erhebliche Auswirkungen für Unternehmen, Verwaltung und Bürgerinnen und Bürger noch aufwendige Verwaltungsverfahren zu erwarten sind. Gleichwohl können punktuell Mehraufwände beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen seiner gesetzlichen Zuständigkeit durch Beratungsleistungen und aufsichtliche Kontrolle zum Zwecke der Überprüfung der Einhaltung gesetzlicher Vorgaben entstehen, die im Rahmen vorhandener Mittel gedeckt werden.

VI. Nachhaltigkeitscheck

Der Nachhaltigkeitscheck lässt keine nennenswerten Auswirkungen des Gesetzesvorhabens auf die ökonomischen, ökologischen und sozialen Verhältnisse erwarten. Lediglich der Zielbereich IV.2. Bedürfnisse und gutes Leben – Wohl und Zufriedenheit – der Anlage 2 zur VwV Regelungen ist tangiert. Der Gesetzentwurf leistet einen Beitrag, um die Sicherheit in der Bevölkerung zu verbessern. Er ist mit den Zielen einer nachhaltigen Entwicklung vereinbar.

VII. Digitaltauglichkeitscheck

Die automatisierte Datenanalyse ermöglicht es dem Polizeivollzugsdienst, vorhandene Datenbestände durch Suchfunktionen systematisch zu erschließen. Dadurch werden Medienbrüche reduziert und manuelle Abfragen verschiedener Datenquellen entbehrlich, die aufgrund großer Datenmengen aus unterschiedlichen Quellen sowie unterschiedlicher Dateiformate bislang zeitaufwendig und komplex sind. Die automatisierte Datenanalyse erfolgt mittels eines elektronischen Fachverfahrens. Zur Verringerung der Eingriffsintensität der automatisierten Datenanalyse steht ihre Nutzung bzw. damit korrespondierend die Verlängerung entsprechender Speicherfristen unter Anordnungsvorbehalt. Diese Anordnungen erfolgen schriftlich außerhalb des elektronischen Fachverfahrens. Die vorgegebene Schriftform und der damit einhergehende Medienbruch tragen als bewusste Zäsur dem hohen Eingriffsgewicht einer automatisierten Datenanalyse in das Recht auf informationelle Selbstbestimmung Rechnung. Sie dienen der rechtlichen Absicherung und gewährleisten eine effektive aufsichtliche Kontrolle.

Durch Nutzung der AML-Technologie wird das Verfahren zur schnellen Standortbestimmung einer hilfesuchenden Person mittels einer Web-Anwendung digitalisiert und Medienbrüche reduziert. Zudem wird die Genauigkeit der Standortbestimmung durch die kombinierte Nutzung verschiedener technischer Positionsdienste erheblich verbessert. Die Übermittlung der Standortdaten vom AML-Endpunkt zur Notrufabfragestelle erfolgt auf deren Abruf vollautomatisiert.

Durch die Einführung entsprechender elektronischer Fachverfahren ist daher sowohl bezogen auf die Analyse von polizeilichen Datenbeständen als auch bezogen auf die Standortbestimmung von notrufenden Personen eine Beschleunigung der polizeilichen Abläufe zu erwarten.

VIII. Sonstige Kosten

Nennenswerte Kosten für Private entstehen durch die Gesetzesänderungen nicht.

B. Einzelbegründung

Zu Artikel 1 – Änderung des Polizeigesetzes:

Zu Nummer 1:

§ 45a Absatz 1 regelt die Einrichtung eines „AML-Endpunktes“ beim Präsidium Technik, Logistik, Service der Polizei. Bei AML handelt es 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.

Zu Nummer 2:

§ 47a Absatz 1 regelt die Eingriffsschwellen und definiert eine automatisierte Datenanalyse. Dabei besteht 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. Der erste Schritt überwindet das strukturelle Problem, dass in den Beständen der Polizei Baden-Württemberg Daten in unterschiedlichen Formaten und getrennten Dateien gespeichert und damit nicht im selben Bearbeitungskontext einheitlich verfügbar sind. Der zweite Schritt beschreibt die eigentliche Analyse, die in einer Verknüpfung, Abgleichung, Aufbereitung, Auswertung und Bewertung der zusammengeführten Datenbestände besteht.

Eine automatisierte Datenanalyse, also die Zusammenführung, Verknüpfung, Abgleichung, Aufbereitung, Auswertung und Bewertung von Datenbeständen auf einer Analyseplattform, stellt eine komplexere Form des Datenabgleichs als die einfache Suche nach Übereinstimmungen zwischen einzelnen, bisher unverbundenen Datensätzen dar (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 91 ff.).

Absatz 1 beschreibt in den Nummern 1 bis 3 unterschiedliche Eingriffsschwellen, die Anlass für eine automatisierte Datenanalyse sein können. Die Eingriffsschwellen sind zum jeweiligen Eingriffsgewicht der automatisierten Datenanalyse in Beziehung zu setzen, damit die Verhältnismäßigkeit der Maßnahme gewahrt bleibt. Beim Einsatz einer automatisierten Datenanalyse ist der Verhältnismäßigkeitsgrundsatz im besonderen Maße zu berücksichtigen. Es muss sichergestellt werden, dass kein milderes Mittel zur Verfügung steht, welches zur Wahrnehmung der polizeilichen Aufgabe ebenso geeignet wäre und den Einzelnen oder die Allgemeinheit voraussichtlich weniger beeinträchtigen würde.

Die Eingriffsschwelle in Absatz 1 Nummer 1 ist an enge Voraussetzungen geknüpft, wie sie allgemein für eingriffsintensive Maßnahmen gelten. Vorausgesetzt wird eine konkrete Gefahr für ein besonders gewichtiges Rechtsgut. 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. Da der Eingriffsanlass mit dem Erfordernis einer konkreten Gefahr streng begrenzt ist und nur besonders gewichtige Rechtsgüter geschützt werden, darf das Eingriffsgewicht der automatisierten Datenanalyse unter diesen Voraussetzungen vergleichsweise hoch sein.

Die Eingriffsschwelle in Absatz 1 Nummer 2 erlaubt weniger gewichtige Eingriffe, die nach der Rechtsprechung des Bundesverfassungsgerichts beim Vorliegen einer konkretisierten Gefahr bereits dann zu rechtfertigen sind, wenn sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen, wie dies bei der Verhütung von Straftaten von zumindest erheblicher Bedeutung der Fall ist (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 107). Das Eingriffsgewicht wird zusätzlich durch die Voraussetzung verringert, dass die zugrunde-

liegende Anlasstat nicht nur abstrakt, sondern auch im Einzelfall schwer wiegen muss. 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 (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 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. Februar 2023, a. a. O., Rn. 170; BVerfG, Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, Rn. 95).

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 (BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 107). Dabei muss der Gesetzgeber das erforderliche Rechtsgut nicht zwingend unmittelbar benennen, sondern kann auch an entsprechende Straftaten anknüpfen. In Anlehnung an die vom Bundesverfassungsgericht in seinem Urteil zur akustischen Wohnraumüberwachung entwickelte (BVerfG, Urteil vom 3. März 2004 – 1 BvR 2378/98 – Rn. 238) und bis heute fortgeschriebene (vgl. BVerfG, Beschluss vom 9. Dezember 2022 – 1 BvR 1345/21 – Rn. 179) und damit verfestigte Nomenklatur sind besonders schwere Straftaten solche, die mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe bedroht sind. Maßgeblicher Anknüpfungspunkt für die Einordnung ist der abstrakte Strafrahmen, wie er vom Gesetzgeber für eine bestimmte Straftat festgelegt wird (BVerfG, Urteil vom 3. März 2004, a. a. O., Rn. 237 f.). Praktisch relevant ist in weiten Teilen der Straftatenkatalog des § 100b Absatz 2 der Strafprozessordnung (StPO).

Absatz 2 regelt die zulässige Methode einer automatisierten Datenanalyse und stellt klar, dass es sich hierbei um ein technisches Hilfsmittel handelt, das die bisherige Arbeitsweise des Polizeivollzugsdienstes erleichtert, ohne sie grundlegend zu verändern. 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, das den Polizeivollzugsdienst bei seiner Aufgabenwahrnehmung unterstützt, indem Informationen aus verschiedenen Dateisystemen zusammengeführt werden. Die abschließende Bewertung der zusammengeführten Informationen ist und bleibt Aufgabe des Polizeivollzugsdienstes. Absatz 2 Satz 1 legt fest, dass die automatisierte Datenanalyse den Polizeivollzugsdienst bei der Erfüllung seiner Aufgaben unterstützt, indem sie Informationen bereitstellt, die es dem Polizeivollzugsdienst ermöglichen, eigene Bewertungen, Prognosen und Entscheidungen zu treffen. Der Mensch – und nicht der Algorithmus – bewertet die bereitgestellten Informationen abschließend. Damit sind beispielsweise alleinige maschinelle Gefährlichkeitsbewertungen zu Personen unzulässig. Die abschließende Bewertung, ob eine bestimmte Person mit hoher Wahrscheinlichkeit künftig Straftaten begehen wird, trifft ein Mensch und nicht der Algorithmus.

Aufgrund der voranschreitenden technologischen Entwicklung ist es für eine effiziente Gefahrenabwehr erforderlich, den Rechtsrahmen auszuschöpfen, der insbesondere durch die KI-VO vorgegeben wird. Gemeint ist die Anwendung von KI-Systemen und KI-Modellen im Sinne und insbesondere unter Berücksichtigung der Einschränkungen und Vorgaben der KI-VO.

Die KI-Systeme und KI-Modelle können die automatisierte Anwendung zur Datenanalyse ergänzen, um beispielsweise

– diverse Datenformate schneller zusammenzuführen,

– Tat- und Täternetzwerke schneller zu identifizieren,

– Hinweise aus unstrukturierten Daten schneller zu erkennen und mit den vorhandenen polizeilichen Informationen abzugleichen oder
– komplexe Analyseschritte zu vereinfachen und für die Polizeibehörden nutzbar zu machen.

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

Vor dem Hintergrund des hohen Eingriffsgewichts einer automatisierten Datenanalyse sind die inhärenten Risiken der KI-unterstützten Durchführung solcher Maßnahmen sowie der angebundenen KI-Systeme oder KI-Modelle besonders zu berücksichtigen.

Mit Satz 2 wird hervorgehoben, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden dürfen.

Satz 3 schreibt ausdrücklich fest, dass abschließende maschinelle Sachverhaltsbewertungen verboten sind, und steht dabei in Bezug zu der allgemeingültigen Regelung des Verbots von automatisierten Entscheidungsfindungen in § 84 PolG. Die abschließende Bewertung der bereitgestellten Informationen und eine Entscheidung über hierauf aufbauende weitere Maßnahmen bleiben dem Polizeivollzugsdienst vorbehalten.

Satz 4 sichert die Funktion der Analyseplattform als bloßes Hilfsmittel für die polizeiliche Aufgabenwahrnehmung ab, indem klargestellt wird, dass die automatisierte Datenanalyse manuell ausgelöst wird. Aus dem Zusammenspiel der Sätze 3 und 4 ergibt sich, dass der Mensch am Anfang und am Ende des Entscheidungsprozesses steht. Mit Satz 4 wird außerdem die Methode des Suchvorgangs näher konkretisiert. Auch dies dient der Minderung des Eingriffsgewichts. Wie sich aus der Entscheidung des Bundesverfassungsgerichts ergibt, ist das Eingriffsgewicht umso höher, je offener die Methode des Suchvorgangs gestaltet ist (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 93). Die mit einer offenen Suche verbundenen Gefahren können durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden, wenn der Suchvorgang eingrenzend so geregelt ist, dass er einen Bezug zu einem konkreten Suchanlass voraussetzt (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 95). Dementsprechend wird in Satz 4 geregelt, dass die automatisierte Datenanalyse anhand anlassbezogener und zielgerichteter Suchkriterien erfolgt. In den Fällen des Absatzes 1 Nummern 2 und 3 ist der Suchvorgang zudem auf die in den §§ 6 und 7 PolG genannten Personen auszurichten. Hierdurch wird das Eingriffsgewicht weiter gemindert, weil mit dem Erfordernis einer tatsachengestützten Verbindung zu einer konkret verantwortlichen Person das Risiko sinkt, dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 94). Die Beschränkung dieser zusätzlichen begrenzenden Vorgabe auf die Fälle des Absatzes 1 Nummern 2 und 3 ist dem Umstand geschuldet, dass die Eingriffsschwelle hier im Vergleich zu Absatz 1 Nummer 1, bei dem eine konkrete Gefahr für besonders gewichtige Rechtsgüter verlangt wird, niedriger liegt. Während nach Absatz 1 Nummer 2 als Eingriffsanlass eine konkretisierte Gefahr für weniger gewichtige Rechtsgüter ausreicht, erlaubt Absatz 1 Nummer 3 die automatisierte Datenanalyse bereits im Vorfeld einer konkretisierten Gefahr. Zur Wahrung der Verhältnismäßigkeit muss die Eingriffsintensität der Maßnahme daher reduziert werden, was hier durch eine weitere Konkretisierung der Suchkriterien erfolgt.

Mit dem Ausrichten der Maßnahme auf die in den §§ 6 und 7 PolG genannten Personen in Satz 5 ist gemeint, dass sich der Suchvorgang nur auf die genannten Personengruppen beziehen darf. Die Einschränkung ist – auf Grundlage der Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) – so zu verstehen, dass eine tatsachengestützte Verbindung zu einer konkret verantwortlichen Person gegeben sein muss. Ein solcher Bezug darf nicht erst durch die Maßnahme hergestellt werden, da ansonsten das Risiko steigt, dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben. Der Begriff des „Ausrichtens“ stellt dabei im Gesamtkontext darauf ab, dass lediglich Personen, die für die Begehung von Straftaten von auch im Einzelfall erheblicher Bedeutung (§ 47a Absatz 1

Nummer 2 i. V. m. § 49 Absatz 3 PolG) oder für die Begehung von besonders schweren Straftaten verantwortlich sind, Anlass für eine Suche geben können. Sofern es sich hierbei um eine Gruppe handelt, kann auch dies Anlass für die Suche sein.

Satz 6 enthält ein ausdrückliches Verbot der direkten Anbindung der Analyseplattform an Internetdienste. Dies dient der Eingriffsminimierung, weil eine Verknüpfung der Analyse- oder Auswerteeinrichtung die Verarbeitung besonders großer Datenmengen praktisch fördert (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 88). Grundsätzlich dürfen nur die von der Polizei Baden-Württemberg gespeicherten Daten in die Analyseplattform einbezogen werden, was zu einer Begrenzung der auswertbaren Datenmenge beiträgt. Nur im Einzelfall können – soweit erforderlich – die bei der Bearbeitung eines konkreten Fallkomplexes gezielt ermittelten und gespeicherten Daten, die bei einer Internetrecherche angefallen sind, in die automatisierte Datenanalyse gemäß Absatz 3 Satz 2 einbezogen werden.

Absatz 3 bestimmt abschließend, welche Datenbestände und Daten auf der Analyseplattform zusammengeführt werden dürfen. Das Gesetz begrenzt damit sowohl den Umfang als auch die Art der verarbeitbaren Daten, wodurch das Eingriffsgewicht der automatisierten Datenanalyse gemindert wird (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 78). Dabei wird zwischen Datenbeständen unterschieden, die auf der Plattform laufend zusammengeführt werden, und solchen Daten, die einzelfallbezogen in die Analyse einbezogen werden.

Nach Satz 1 können zum Zweck der automatisierten Datenanalyse eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden. Die positive Benennung der zum Zweck der automatisierten Datenanalyse nutzbaren Quellen hat den Charakter einer abschließenden Regelung und enthält damit gleichzeitig eine Begrenzung der Datenmenge (vgl. BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 78). Die zusätzliche Einschränkung auf eigene Daten stellt klar, dass es sich um Daten handelt, welche die Polizei Baden-Württemberg als verantwortliche Stelle in den eigenen polizeilichen Dateisystemen gespeichert hat.

Vorgangsdaten sind sämtliche Unterlagen, die im Zusammenhang mit einer polizeilichen Tätigkeit bei einem bestimmten Einsatzanlass zu Personen und Sachen im polizeilichen Vorgangsbearbeitungssystem erfasst werden. Aufgenommen werden insbesondere Anzeigen, Ermittlungsberichte und Vermerke, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, sondern beispielsweise auch zu Personen, die Anzeige erstatten, Hinweise geben oder Zeuginnen oder Zeugen sind. Die Vorgangsdaten umfassen Vorgangssachbearbeitungsdaten und Vorgangsverwaltungsdaten gleichermaßen, wobei Vorgangsverwaltungsdaten in der Regel bereits keine Relevanz für entsprechende Analysen haben dürften. Da die Daten aus der Vorgangsverwaltung typischerweise auch viele Unbeteiligte betreffen, wird in Absatz 6 Satz 3 geregelt, dass deren Vorgangsdaten nicht in die automatisierte Datenanalyse einbezogen werden dürfen. Hierdurch wird die Eingriffsintensität reduziert.

Falldaten in Fallbearbeitungssystemen dienen der Unterstützung von Ermittlungs- und Recherchetätigkeiten sowie Auswertungen bei komplexen, fallübergreifenden Ermittlungen oder bei Strukturermittlungen. Ein Fallbearbeitungssystem geht über die reine Verwaltung von Vorgangsdaten hinaus, indem es der Anwenderin oder dem Anwender ein speziell auf die Aufhellung von Strukturen hin ausgerichtetes Werkzeug zur Verfügung stellt und vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen abbildet. Fallbearbeitungssysteme können sowohl zu präventiven als auch zu repressiven Zwecken eingesetzt werden. Sie enthalten überwiegend Daten von Anlasspersonen und deren Kontaktpersonen aus strafrechtlichen Ermittlungsverfahren. Anlasspersonen sind verurteilte, beschuldigte oder verdächtige Personen oder Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie in naher Zukunft Straftaten von erheblicher Bedeutung begehen.

Polizeiliche Auskunftssysteme enthalten personenbezogene Informationen, die sowohl zum Zweck der Verhütung von Straftaten als auch zum Zweck der Strafverfolgung und -vollstreckung gespeichert werden. Das polizeiliche Auskunfts-

system der baden-württembergischen Polizei besteht aus unterschiedlichen Datengruppen. Hierzu gehören insbesondere:

- Kriminalaktennachweise: Diese beinhalten Informationen über laufende und abgeschlossene Ermittlungsverfahren, insbesondere die Straftatbestände, wegen derer ermittelt wurde, Datum und Art der Einstellungsverfügung, deren Gründe, Angaben zur Anklageerhebung sowie zum Ausgang des Hauptverfahrens.
- Personenfahndung: Diese listet in einem Katalog den Anlass und den Zweck der Ausschreibung einer Person zur Fahndung mit dem Ziel auf, fahndungsrelevante Erkenntnisse über Täterinnen oder Täter, Tathergang, Zeuginnen oder Zeugen, Geschädigte etc. zu erlangen. Die Personenfahndung dient unter anderem der Festnahme oder Aufenthaltsermittlung von Straftäterinnen oder Straftätern (Strafverfolgung) oder dem Schutz von vermissten Personen (Gefahrenabwehr) sowie der Strafvollstreckung von verurteilten Personen bzw. der Verhinderung einer Wiedereinreise von verurteilten Personen, die nach Teilverbüßung ihrer Haftstrafe ins Ausland abgeschoben oder überstellt wurden.
- Sachfahndung: Sie dient unter anderem der Beweissicherung sowie der Ermittlung der Eigentümer bzw. Besitzer von Sachen, die durch eine Straftat oder auf andere Weise abhandengekommen sind.
- Haftdatei: Sie beinhaltet Daten von Personen, die wegen einer rechtswidrigen Tat einer richterlich angeordneten Freiheitsentziehung unterliegen.
- Erkennungsdienst und DNA-Analyse-Datei: Die Erfassung und Speicherung von biometrischen Merkmalen (insbesondere Fingerabdrücke, Lichtbilder und DNA-Identifizierungsmuster) bilden die Grundlage für die Ermittlung von Täterinnen oder Tätern in Strafverfahren, die Zuordnung von Tatortspuren, das Erkennen von Tat-/Täter-Zusammenhängen, aber auch die Identifizierung von hilflosen Personen oder unbekannten Toten. Die aus der DNA-Analyse nach § 81g StPO gewonnenen Identifizierungsmuster werden in einer zentralen DNA-Analyse-Datei (DAD) bundesweit gespeichert.

Polizeiliche Auskunftssysteme unterstützen den zügigen Informationsaustausch und die Erkenntnisgewinnung über bereits einschlägig in Erscheinung getretene Straftäterinnen oder Straftäter und dienen als Grundlage der Personenüberprüfung und Identifizierung im Rahmen der Aufklärung fahndungsrelevanter Sachverhalte, etwa bei offenen Fahndungsausschreibungen aufgrund von Haftbefehlen oder auch bei Vermisstenfahndungen. Darüber hinaus dienen die Daten der Eigensicherung bei polizeilichen Einsatzanlässen. Durch die Einbeziehung dieser Daten in die automatisierte Datenanalyse können beispielsweise Mittäterinnen oder Mittäter identifiziert, Tatbeteiligungen anhand der Haftdaten auch ausgeschlossen, bestehende Verbindungen visualisiert sowie ein Abgleich mit anderen Datenquellen durchgeführt werden.

Daten aus dem polizeilichen Informationsaustausch sind zwischen den Polizeien des Bundes und der Länder ausgetauschte polizeiliche Informationen mit hoher Relevanz insbesondere zu überregionalen Straftätern, zu serienmäßig begangenen Straftaten oder zu akuten Gefahrensachverhalten. Derzeit wird hierfür überwiegend das bundesweite webbasierte Fernschreibsystem EPOST 810 genutzt.

Absatz 3 Satz 2 regelt neben der ergänzenden Einbeziehung von Verkehrsdaten und Daten aus Asservaten auch die Einbeziehung von Daten aus gezielten Abfragen bei anderen Polizeien, von Daten aus gesondert geführten staatlichen Registern und von einzelnen gesondert gespeicherten Datensätzen aus Internetquellen.

Mit dem Begriff der Verkehrsdaten werden gemäß der Legaldefinition in § 3 Nummer 70 TKG diejenigen Daten erfasst, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. Hierzu gehören insbesondere auch die für die Polizeiarbeit praktisch bedeutsamen Verbindungsdaten einschließlich Standortdaten (vgl. § 9 Absatz 1 Nummer 1 TDDDG), die durch Telekommunikationsüberwachungsmaßnahmen gemäß § 100a StPO, durch Funkzellenabfragen gemäß § 100g Absatz 3 StPO bzw. für kennungsbezogene Verkehrsdatenabfragen gemäß § 100g Absatz 1 und 2 StPO oder unter Einsatz eines IMSI-Catchers auf der Grundlage des § 100i Absatz 1 Nummer 2 StPO erhoben werden können. Im präventiven Bereich können Verkehrs-

daten einschließlich Standortdaten kennungsbezogen oder über eine Funkzellenabfrage nach § 53 PolG, durch Auskünfte des Telekommunikationsanbieters nach §§ 52, 54 PolG oder durch den Einsatz eines IMSI-Catchers nach § 55 Absatz 1 PolG erlangt werden. Die Kenntnis darüber, welches mobile Telekommunikationsendgerät zu einem bestimmten Zeitpunkt an einem bestimmten Ort angemeldet war, kann für die polizeiliche Gefahrenabwehr von wesentlicher Bedeutung sein, weil der Aufenthaltsort des Nutzers eines Telekommunikationsendgerätes zum Beispiel Aufschlüsse über Organisationsstrukturen einer Gruppierung geben kann oder die Beteiligung einer Person ausschließen und sie damit entlasten kann.

Daten aus Asservaten sind aus sichergestellten oder beschlagnahmten Datenträgern extrahierte Daten oder Scans papierhafter Asservate. Datenträger dieser Art können beispielsweise USB-Sticks, Festplatten, Smartphones oder Laptops sein. Das Einbeziehen von Asservaten ist im Einzelfall dann möglich, wenn mindestens tatsächliche Anhaltspunkte dafür vorliegen, dass das einzubindende Asservat in Verbindung zum konkreten Suchanlass steht.

Daten anderer Polizeien sind nicht von Satz 1 umfasst. In gezielten Einzelabfragen erhobene Daten, die andere Polizeien als verantwortliche Stelle in ihren polizeilichen Dateisystemen gespeichert haben, können über Satz 2, soweit erforderlich, ergänzend in die Analyse einbezogen werden.

Daten aus staatlichen Registern sind beispielsweise Daten aus dem Melderegister, dem Zentralen Verkehrsinformationssystem (ZEVIS) oder dem Waffenregister, die durch gezielte Abfragen in die Analyse einbezogen werden können, soweit dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Abfragen in ZEVIS können zur Aufklärung des Sachverhalts beispielsweise erforderlich sein, wenn die Mobilität einer Anlassperson in Frage steht. Hat diese Person eine Waffenerlaubnis, kann darin ein gefahrerhöhendes Indiz gesehen werden. Die Funktionsweise der Analyseplattform stellt sicher, dass solche Informationen schnell zusammengeführt werden können.

Satz 2 erlaubt zudem eine ergänzende Einbeziehung von gesondert gespeicherten Datensätzen aus Internetquellen. Da gemäß Absatz 2 Satz 6 eine direkte Anbindung der Analyseplattform an Internetdienste unzulässig ist, dürfen diese Daten nicht automatisiert einbezogen werden. Vielmehr müssen sie für jeden Analysevorgang händisch hinzugezogen werden.

Es handelt sich bei den nach Satz 2 einbezogenen Datensätzen regelmäßig um die aufbereiteten und bereits gefilterten Ergebnisse polizeilicher Recherchen. Voraussetzung ist, dass die Einbeziehung dieser Daten zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist.

Nach Absatz 3 Satz 3 dürfen Verkehrsdaten aus Funkzellenabfragen sowie Telekommunikationsdaten nicht in die automatisierte Datenanalyse einbezogen werden, wenn die Maßnahme gemäß Absatz 1 Nummer 3 bereits im Vorfeld einer konkretisierten Gefahr zur Anwendung kommt. 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. Im Vergleich zur konkretisierten Gefahr nach Absatz 1 Nummer 2 oder einer konkreten Gefahr nach Absatz 1 Nummer 1 zeichnet sich eine Maßnahme nach Absatz 1 Nummer 3 durch eine größere Ungewissheit sowohl in Bezug auf die Tatsachengrundlage als auch in Bezug auf den zum Schaden führenden Kausalverlauf aus. Dies erfordert eine entsprechende Begrenzung der Eingriffsintensität.

Nach Absatz 3 Satz 4 sind einzelfallbezogen auf der Analyseplattform gespeicherte Daten nach Satz 2 spätestens nach Ablauf von zwei Jahren zu löschen, soweit die weitere Speicherung der Daten nicht erforderlich ist. Diese Löschpflicht trägt zur Reduzierung der Datenmenge bei und wirkt somit eingriffsmildernd. Soweit mit der Einbeziehung von Verkehrsdaten, insbesondere den aus Funk-

zellenabfragen gewonnenen Daten, in dem für die automatisierte Datenanalyse bereitstehenden Datenpool eine bevorratende Speicherung von Verkehrsdaten möglich ist, müssen – so das Bundesverfassungsgericht – die erfassbaren Daten substanziell begrenzt und eine Höchstspeicherungsdauer geregelt sein (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 85). Die Löschfrist gilt nicht, soweit die weitere Speicherung der Daten nach Ablauf der Frist erforderlich ist. Die Möglichkeit, Daten über die Löschfrist hinaus zu speichern, ist nach Satz 5 jedoch zeitlich begrenzt. Um den Anforderungen an Transparenz und aufsichtliche Kontrolle Rechnung zu tragen, ist die Entscheidung, die Löschfrist zu verlängern und die Daten weiter zu speichern, gemäß Satz 5 schriftlich zu begründen. Dem in Absatz 7 geregelten Anordnungsvorbehalt, der für alle Maßnahmen nach Absatz 1 gilt, wird auch bei der Entscheidung über die Verlängerung der Löschfrist Rechnung getragen.

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.

Absatz 4 Satz 1 verweist auf eine entsprechende Geltung des § 15 Absatz 2 und 3 PolG. Damit wird sichergestellt, dass die weitere Nutzung der Daten im Rahmen der automatisierten Datenanalyse nach den Grundsätzen der Zweckbindung und Zweckänderung verfassungsrechtlich gerechtfertigt ist. Im Rahmen einer automatisierten Datenanalyse können personenbezogene Daten sowohl zweckwahrend als auch zweckändernd weiterverarbeitet werden. Eine zweckwahrende Nutzung von Daten kommt gemäß § 15 Absatz 2 PolG nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich. Nicht erforderlich für eine weitere Nutzung der Daten im Rahmen der Zweckbindung ist das Vorliegen der für die Datenerhebung maßgeblichen Gefahrenlage. Ausreichend für eine weitere Nutzung der Daten ist vielmehr ein bloßer Spurenansatz. Etwas anderes gilt nur für Daten aus einer Wohnraumüberwachung oder Online-Durchsuchung, deren Weiterverarbeitung auf der Analyseplattform aber in Absatz 3 Satz 6 gesetzlich ausgeschlossen ist.

Nach § 15 Absatz 3 PolG dürfen Daten für einen anderen gefahrenabwehrrechtlichen Zweck genutzt werden, wenn die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Verhütung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Aus den Daten müssen sich im Einzelfall konkrete Ermittlungsansätze ergeben.

Ob Daten, die im Rahmen einer automatisierten Datenanalyse weiterverarbeitet werden, zweckwahrend oder zweckändernd verwendet werden, hängt maßgeblich von der Herkunft der Daten und den ursprünglichen Erhebungszwecken ab.

Zur praktischen Umsetzung des verfassungsrechtlichen Zweckbindungsgrundsatzes ist insbesondere eine Kennzeichnung der Daten erforderlich. Besonders schwierig ist dies bei einer automatisierten Einbindung von Dateien, zumal wenn es sich um große Datenbestände handelt. Eine begrenzende Wirkung gesetzlicher Zweckbindungsregelungen wird sich hier – so das Bundesverfassungsgericht – nur mittels organisatorischer und technischer Vorkehrungen realisieren lassen, die näher zu regeln sind, um das Eingriffsgewicht in verfassungsrechtlich anzuerkennender Weise reduzieren zu können (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 139). 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 (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 140).

Absatz 4 Satz 1 sieht deshalb vor, dass technisch-organisatorische Vorkehrungen insbesondere zur Einhaltung der Zweckbindung in einer Verwaltungsvorschrift zu regeln sind, die zu veröffentlichen ist. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, dass der Gesetzgeber die Verwaltung verpflichten kann, die im Gesetz geregelten Vorgaben weiter zu konkretisieren, soweit die Vorgaben zu Art und Umfang der in die automatisierte Datenanalyse einbeziehbaren Daten und der zulässigen Verarbeitungsmethoden aus dem Gesetz selbst nur

begrenzt erkennbar sind. Die Verwaltungsvorschrift muss aus Gründen der Transparenz und der Kontrolle veröffentlicht werden (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 113). Die Veröffentlichung erfolgt in dem für den Geschäftsbereich des Innenministeriums vorgesehenen amtlichen Bekanntmachungsblatt. Nach Ziffer 5.5.3 der Anlage 1 zur VwV Regelungen handelt es dabei um das Gemeinsame Amtsblatt des Innenministeriums, des Finanzministeriums, des Kultusministeriums, des Wissenschaftsministeriums, des Umweltministeriums, des Wirtschaftsministeriums, des Sozialministeriums, des Justizministeriums, des Verkehrsministeriums, des Ministeriums für Ernährung, Ländlicher Raum und Verbraucherschutz, des Ministeriums für Landesentwicklung und Wohnen sowie der Regierungspräsidien.

Absatz 4 Satz 2 regelt den wesentlichen Inhalt der Verwaltungsvorschrift, der in den Absätzen 5 und 6 näher konkretisiert wird. Der Absatz enthält Vorgaben zur Transparenz und Kontrolle (vgl. BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 109). Nach Satz 2 beinhaltet die Verwaltungsvorschrift ein Rollen- und Rechtekonzept, ein Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten, ein Konzept zur Zugriffskontrolle, das auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht, sowie nähere Bestimmungen über den Inhalt der erforderlichen Begründung nach Absatz 3 Satz 5 und Absatz 7 Satz 3.

Die Zugriffskontrolle nach Absatz 4 Satz 2 Nummer 3 wird durch die Protokollierung der einzelnen Arbeitsschritte gemäß § 74 PolG abgesichert. Auf diese Weise wird sichergestellt, dass nur berechtigte Personen eine automatisierte Datenanalyse vornehmen können. Die gesetzlich vorgeschriebene Protokollierung sichert die nachträgliche aufsichtliche Kontrolle und ist gleichzeitig Voraussetzung für die Gewährleistung effektiven Rechtsschutzes gemäß Artikel 19 Absatz 4 GG. Als weiterer Kontrollmechanismus sind in der Verwaltungsvorschrift verdachtsunabhängige Stichprobenkontrollen durch die verantwortlichen Stellen zu implementieren.

Diesen Zwecken dient auch die nach Absatz 4 Satz 2 Nummer 4 näher auszugestaltende Begründungspflicht für die Anordnung der Verlängerung der Speicherfrist nach Absatz 3 Satz 5 sowie für die Anordnung einer automatisierten Datenanalyse nach Absatz 7 Satz 3. Gleichzeitig dient die Begründungspflicht auch der Selbstvergewisserung über die Rechtmäßigkeit der automatisierten Datenanalyse.

Übergeordnetes Ziel der Vorgaben in der Verwaltungsvorschrift ist es – wie sich aus Satz 3 ergibt –, die Datenbestände unter Berücksichtigung der in Absatz 1 beschriebenen Eingriffsschwellen auf das für den Analysezweck erforderliche Maß zu begrenzen und die Einbeziehung der Daten unbeteiligter Personen möglichst zu vermeiden.

Das Bundesverfassungsgericht hat mehrfach betont, dass eine Begrenzung von Art und Umfang der Daten und die zugelassene Methode der automatisierten Datenanalyse maßgeblichen Einfluss auf das Eingriffsgewicht und damit auf deren Zulässigkeit jeweils in Bezug auf die normierte Eingriffsschwelle haben (BVerfG, Urteil vom 16. Februar 2023, a. a. O., 76 ff., 90 ff.). Da die zugelassene Methode der automatisierten Datenanalyse bereits durch gesetzliche Vorgaben hinreichend begrenzt ist, dienen die mit der Verwaltungsvorschrift zu erlassenden Konkretisierungen in erster Linie dazu, die in die automatisierte Datenanalyse einzubeziehenden Datenbestände auf das für den Analysezweck erforderliche Maß zu begrenzen, die Umsetzung des Grundsatzes der Zweckbindung auch praktisch sicherzustellen und unbeteiligte Personen so weit wie möglich zu schützen.

Absatz 5 gibt vor, dass im Rollen- und Rechtekonzept nach Absatz 4 Satz 2 Nummer 1 festgelegt wird, wer innerhalb des Polizeivollzugsdienstes Zugriff auf welche Daten haben kann und mit welchen Rechten und Pflichten der Zugriff verbunden ist. Dabei sind die Zugriffsrechte nach dem Prinzip auszugestalten, dass die Zahl der Zugriffsberechtigten umso geringer ist, desto umfangreicher und sensibler die von der Zugriffsberechtigung umfassten Daten sind. Weil das Rollen- und Rechtekonzept an Rollen und nicht an Personen anknüpft, ist es möglich, dass eine Person mehrere Rollen hat und deshalb über erweiterte Zugriffsrechte verfügt. Das Rollen- und Rechtekonzept führt damit zu einer Reduzierung des Umfangs der jeweils verarbeitbaren Daten und damit zu einer Verringerung der Eingriffsintensität.

Absatz 6 beschreibt das in der Verwaltungsvorschrift nach Absatz 4 Satz 2 Nummer 2 zu regelnde Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten, das ebenfalls zu einer Begrenzung des Datenbestandes und damit zu einer Verringerung der Eingriffsintensität beiträgt, indem entschieden wird, ob und in welcher Weise personenbezogene Daten verwendet werden dürfen. Grundlegend ist hier die Unterscheidung zwischen einerseits unbeteiligten und andererseits verurteilten, beschuldigten und verdächtigen Personen sowie sonstigen Anlasspersonen und deren Kontaktpersonen. Diese Unterscheidung ist für das Eingriffsgewicht der automatisierten Datenanalyse von maßgeblicher Bedeutung, denn das Eingriffsgewicht erhöht sich, wenn durch die automatisierte Datenanalyse Informationen über Personen erlangt werden, die objektiv in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den polizeilichen Eingriff durch ihr Verhalten nicht zurechenbar veranlasst haben (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 77). Zum Schutz unbeteiligter Personen dürfen deren personenbezogene Vorgangsdaten grundsätzlich nicht in eine automatisierte Datenanalyse einbezogen werden.

Zur Verringerung der Eingriffsintensität führt schließlich auch, dass die Daten nach dem Gewicht des Grundrechtseingriffs bei der Datenerhebung so kategorisiert werden müssen, dass deren eingeschränkter oder ausgeschlossener Verwendbarkeit bei schwerwiegenden Grundrechtseingriffen Rechnung getragen wird. Wegen der besonderen Eingriffsintensität von Wohnraumüberwachungen und Online-Durchsuchungen ist in Absatz 3 Satz 6 bereits gesetzlich ausgeschlossen, dass die aus solchen Maßnahmen erlangten Informationen in die automatisierte Datenanalyse einbezogen werden. Bei Daten, die aus anderen grundrechtsintensiven Eingriffen erlangt wurden, kommt eine Weiterverarbeitung der Daten nach den Grundsätzen der Zweckbindung nur in Betracht, wenn die Voraussetzungen des § 15 Absatz 2 oder 3 PolG vorliegen.

Durch die zu treffenden technisch-organisatorischen Vorkehrungen muss sichergestellt werden, dass die Grundsätze der Zweckbindung auch tatsächlich umgesetzt werden.

Absatz 7 dient der verfahrensmäßigen Absicherung, indem er Maßnahmen nach Absatz 1 auch einem Anordnungsvorbehalt unterwirft. Er trägt zugleich dem hohen Eingriffsgewicht einer automatisierten Datenanalyse in das Recht auf informationelle Selbstbestimmung Rechnung. Die Anordnung ist durch die Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts schriftlich zu erteilen und zu begründen. Sie bezieht sich auf den Einsatz der automatisierten Datenanalyse in einem konkreten Gefährdungssachverhalt in seiner Gesamtheit und muss daher nicht für jeden einzelnen Suchvorgang im Rahmen dieses Sachverhalts neu angeordnet bzw. bestätigt werden. Dies sichert die vom Bundesverfassungsgericht geforderte aufsichtliche Kontrolle, die ein Ausfluss aus dem Verhältnismäßigkeitsgrundsatz darstellt. Für eine effektive Kontrolle ist dabei unerlässlich, dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Gefahrenabwehr oder Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden. Eine Delegation der Anordnungsbefugnis ist bei Gefahr im Verzug auf besonders beauftragte Beamte möglich.

Nach Absatz 8 ist vor der Einrichtung oder einer wesentlichen Änderung einer Analyseplattform nach Absatz 1 die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit anzuhören. Die Regelung gewährleistet eine effektive und unabhängige datenschutzrechtliche und aufsichtliche Kontrolle.

Davon unbenommen gelten die allgemeinen datenschutzrechtlichen und aufsichtlichen Regelungen des Polizeigesetzes.

Zu Nummer 3:

Der neue § 57a schafft eine ausdrückliche Rechtsgrundlage 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 durch die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst anhand von Echtdaten. Informationstechnische Produkte sind entspre-

chend der Legaldefinition in § 2 Absatz 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 maschinengestützte 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 gemäß Artikel 3 Nummer 1 VO KI-VO) sowie diesen Systemen zugrundeliegende KI-Modelle mit oder ohne allgemeinen Verwendungszweck im Sinne der KI-VO.

Erfüllt das Testen und Training von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO im Einzelfall die für die wissenschaftliche Forschung kennzeichnenden Merkmale, ist § 57 als Rechtsgrundlage für die Datenverarbeitung heranzuziehen.

Eine Verarbeitung personenbezogener Daten durch die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst nach § 57a Absatz 1 Satz 1 ist ausschließlich zum Zwecke der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten einschließlich KI-Systemen und KI-Modellen im Sinne der KI-VO zulässig. Zudem muss es sich um informationstechnische Produkte handeln, die die Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst für die polizeiliche Aufgabenwahrnehmung entwickeln oder nutzen wollen. Die Datenverarbeitung muss zur Erreichung der benannten Zwecke erforderlich sein. Insbesondere muss eine Erforderlichkeit für unveränderte Daten bestehen oder eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich sein. Ein unverhältnismäßiger Aufwand liegt etwa dann vor, wenn die zur Anonymisierung oder Pseudonymisierung der Daten notwendigen Maßnahmen derart aufwendig sind, dass sie praktisch oder wirtschaftlich nicht zumutbar erscheinen, um die konkrete Aufgabe zu erfüllen, weil der Aufwand in keinem angemessenen Verhältnis zum Zweck und zu den verfügbaren Mitteln stünde. Das Vorliegen eines unverhältnismäßigen Aufwands ist am Gebot der Datenminimierung zu messen und jeweils im Einzelfall zu prüfen. Die Erforderlichkeit der Verarbeitung unveränderter Daten bildet hierbei keinen Sonderfall der unmöglichen oder nur mit unverhältnismäßigem Aufwand möglichen Anonymisierung oder Pseudonymisierung. Es handelt sich vielmehr um eine alternative Ermächtigung für die Fälle, in denen eine Anonymisierung oder Pseudonymisierung zwar objektiv möglich und auch mit verhältnismäßigem Aufwand durchführbar, aber praktisch nicht zielführend wäre, da sie den Erkenntniswert oder die Funktionstauglichkeit des betreffenden informationstechnischen Produktes erheblich beeinträchtigen würde. Insbesondere im Bereich der Evaluation und Validierung von KI-Systemen dürfte der Einsatz von realitätsnahen, also unveränderten, Testdaten in vielen Fällen erforderlich sein. Eine Anonymisierung oder Pseudonymisierung könnte in diesen Fällen den entscheidenden Kontext oder die technische Struktur, welche das System lernen oder prüfen soll, entwerten.

Die Regelungen in Absatz 1 Sätze 2 und 3 stellen eine gesetzliche Sicherung vor den spezifischen Risiken selbstlernender Systeme dar und verpflichten zu technisch-organisatorischen Maßnahmen beim Testen dieser Systeme. 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.

Absatz 1 Satz 4 sowie die Absätze 2 und 3 entsprechen Regelungen in § 57 Absatz 1 Satz 2, Absätze 2 und 4. Es handelt sich um Schutzregelungen zur zweckkonformen Datenverarbeitung.

Zu Nummer 4:

Mit den Folgeänderungen in § 74 wird die nach der Rechtsprechung des Bundesverfassungsgerichtes erforderliche Protokollierung von Verarbeitungsvorgängen bezüglich solcher Daten, die aus verdeckten beziehungsweise eingriffsintensiven Maßnahmen gewonnen werden, auf die Einführung der automatisierten Datenanalyse erstreckt. Absatz 1 bestimmt die Angaben, auf die sich jede Protokollierung bei den genannten verdeckten und eingriffsintensiven Maßnahmen zu erstrecken hat. In der neuen Nummer 1 des Absatzes 2 werden weitere, für die automatisierte Datenanalyse zu protokollierende Angaben und insbesondere die zu protokollierenden Personen festgelegt.

Zu Nummer 5:

Mit den Folgeänderungen in § 86 wird die nach Artikel 13 Absatz 2 der Richtlinie (EU) 2016/680 und nach der Rechtsprechung des Bundesverfassungsgerichts vorgegebene Informationspflicht auf die betroffene Person erstreckt, soweit gegen diese nach einer automatisierten Datenanalyse weitere polizeiliche Maßnahmen getroffen werden.

Zu Nummer 6:

Der neu gefasste § 90 Absatz 1 ersetzt die bisher bestehende Berichtspflicht gegenüber dem Landtag durch eine Unterrichtung des Parlamentarischen Kontrollgremiums. Diese Unterrichtung wird auch auf die automatisierte Datenanalyse nach § 47a erstreckt. 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 (Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 142 ff.) Rechnung getragen. Durch die Neufassung von § 90 wird die automatisierte Datenanalyse einer intensiven parlamentarischen Kontrolle unterworfen und so ein Ausgleich zum Eingriff durch die Nutzung der Maßnahme geschaffen. Die Unterrichtung des Parlamentarischen Kontrollgremiums sowie der Öffentlichkeit dient neben der Kontrolle auch der Transparenz der polizeilichen Maßnahmen. Einer Absicherung der organisatorischen Trennung von Polizei und Verfassungsschutz wird durch organisatorische Vorkehrungen Rechnung getragen, etwa durch getrennte Sitzungen.

Absatz 2 normiert die vom Bundesverfassungsgericht ebenfalls geforderte Pflicht zur Unterrichtung der Öffentlichkeit und sieht insoweit ein jährliches Intervall vor.

Zu Nummer 7:

Mit den Folgeänderungen in § 98 werden die in Umsetzung des Artikels 46 der Richtlinie (EU) 2016/680 festgelegten Aufgaben der Aufsichtsbehörde für den Datenschutz auf die automatisierte Datenanalyse erstreckt.

Zu Nummer 8:

Mit der Folgeänderung in § 130 wird die Verordnungsermächtigung für die Übertragung der Anordnungsbefugnis auf die automatisierte Datenanalyse erstreckt.

Zu Artikel 2 – Änderung der Verordnung zur Durchführung des Polizeigesetzes (DVO PolG):

Mit dem neuen Absatz 3 wird von der Verordnungsermächtigung des § 130 PolG Gebrauch gemacht. Die Anordnungsbefugnis nach § 47a Absatz 7 PolG kann bei Gefahr im Verzug bei den regionalen Polizeipräsidien auf die Leitung des Führungs- und Einsatzstabes, die Leitung der Schutzpolizeidirektion und die Leitung der Kriminalpolizeidirektion sowie auf den Polizeiführer vom Dienst delegiert

werden. Im Landeskriminalamt kann sie auf die Abteilungsleitungen sowie auf den Polizeiführer vom Dienst delegiert werden.

Zu Artikel 3 – Inkrafttreten

Die Vorschrift regelt das Inkrafttreten des Gesetzes.

C. Ergebnis der Anhörung

1. Eingegangene Stellungnahmen:

Zu dem Gesetzentwurf wurden die Spitzenorganisationen der Gewerkschaften und Berufsverbände im Land, die kommunalen Landesverbände, weitere Verbände, Einrichtungen und Beauftragte sowie Personal- und Interessenvertretungen angehört. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit, die Beauftragte der Landesregierung für die Belange von Menschen mit Behinderungen, der Normenprüfungsausschuss und der Normenkontrollrat wurden zeitgleich beteiligt sowie der Gesetzentwurf im Beteiligungsportal des Landes freigeschaltet.

Inhaltlich Stellung genommen haben:

– Deutsche Polizeigewerkschaft (DPolG), Landesverband Baden-Württemberg e. V.
– BBW – Beamtenbund Tarifunion (BBW)
– Gewerkschaft der Polizei Baden-Württemberg (GdP BW)
– Bund Deutscher Kriminalbeamter, Landesverband Baden-Württemberg (BDK)
– Deutscher Gewerkschaftsbund, Bezirk Baden-Württemberg (DGB)
– Neue Richter*innenvereinigung, Landesverband Baden-Württemberg (NRV)
– Anwaltsverband Baden-Württemberg im Deutschen Anwaltverein e. V. (AV BW)
– Gesellschaft für Freiheitsrechte e. V. (GFF)

Im Beteiligungsportal des Landes gingen 27 Kommentare ein, von denen ein Kommentar durch den Nutzer gelöscht wurde. Der Normenprüfungsausschuss hat redaktionelle Anmerkungen zum Gesetzentwurf übermittelt. Der Normenkontrollrat sowie der Landesbeauftragte für den Datenschutz und die Informationsfreiheit haben eine Stellungnahme abgegeben.

Die Stellungnahmen sind als Anlage beigefügt.

2. Stellungnahmen im Einzelnen und Bewertung der Landesregierung:

2.1 Die DPolG begrüßt die Absicht der Landesregierung, mit einer Automatisierung der Datenanalyse den steigenden Massendaten wirksam zu begegnen und sieht den polizeiliche Nutzen als erheblich an. Ein Verzicht auf die Maßnahme würde nach Auffassung der DPolG ein enormes Sicherheitsdefizit darstellen. Die DPolG begrüße es grundsätzlich, wenn bei IT-Lösungen deutsche Unternehmen, besser noch Unternehmen aus Baden-Württemberg, einbezogen würden. Andererseits erfordere es die aktuelle Situation, dass IT-Lösungen sehr schnell eingeführt würden.

Die beabsichtigten Regelungen in § 47a dienen nach Ansicht der DPolG weder der Klarheit und Transparenz noch der Verständlichkeit. Insbesondere gehöre vieles von dem, was in § 47a Absätze 4, 5 und 6 aufgeführt sei, nicht in ein Polizeigesetz, zumindest nicht in dieser Art und Weise.

Der BBW verweist vollumfänglich auf die Stellungnahme seines Mitgliedsverbandes, der DPolG.

Haltung der Landesregierung:

Die Rechtsgrundlage für die automatisierte Datenanalyse in § 47a ist technikoffen gehalten. Mit deren Inkrafttreten erfolgt keine Festlegung auf einen bestimmten Anbieter einer konkreten Software zur automatisierten Datenanalyse. Die aktuelle Sicherheitslage erfordert es, dass die Polizei in Baden-Württemberg unverzüglich eine Software nutzen kann, die eine verfahrensübergreifende Recherche und Analyse zuvor rechtmäßig erhobener und gespeicherter personenbezogener Daten auch bei heterogenen Datenformaten ermöglicht. Der geplante Einsatz einer Software eines außereuropäischen Anbieters ist lediglich als Übergangslösung vorgesehen. Aktuell sind nach Kenntnis der Landesregierung keine vergleichbaren Produkte am Markt verfügbar, die zeitnah funktionsbereit wären und alle fachlichen Anforderungen erfüllen. Langfristig ist eine souveräne europäische Lösung beabsichtigt, die den Sicherheitsbehörden die notwendigen technischen Fähigkeiten zur Recherche und Analyse von großen, auch unstrukturierten Datenmengen gewährleistet.

Der Kritik, dass die Regelungsinhalte des § 47a Absätze 4, 5 und 6 nicht oder nicht in der vorgesehenen Form in ein Polizeigesetz gehören würden, ist entgegenzuhalten, dass mit der Rechtsgrundlage für die automatisierte Datenanalyse in § 47a die Vorgaben des Bundesverfassungsgerichts aus seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) umgesetzt werden. Dies gilt insbesondere im Hinblick auf die erforderlichen Regelungen zur Transparenz und Kontrolle, etwa durch ein Rollen- und Rechtekonzept, ein Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten sowie ein Konzept zur Zugriffskontrolle, das auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht. Dabei kann der Gesetzgeber die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigen, was durch den Erlass einer Verwaltungsvorschrift erfolgen soll. Der Gesetzgeber muss jedoch sicherstellen, dass er unter Wahrung des Gesetzesvorbehalts insgesamt ausreichende Regelungen, wie etwa zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden, selbst durch Gesetz vorgibt.

2.2 Die GdP BW begrüßt den Einsatz einer Software zur automatisierten Datenanalyse. Durch die Schaffung einer entsprechenden Rechtsgrundlage würde der Zustand, dass in der Praxis zahlreiche Hinweise im Rahmen der Kriminalitätsbekämpfung aus den USA kämen, weil die Polizei in Deutschland über keine entsprechende Software verfüge, verändert. Dies sei rechtsstaatlich geboten und der Staat könne so seiner zentralen Aufgabe nachkommen, die innere Sicherheit zu gewährleisten. Die GdP BW fordert den Einsatz einer „Bundes-VeRA“, die durch alle Länder genutzt werden könne, insbesondere durch Integration der vorgehaltenen Datensätze und Schnittstellen. Neben der Anpassung des Polizeigesetzes Baden-Württemberg müsse deshalb auch die Anpassung der Strafprozessordnung für die bundesweite Nutzung dieser Plattform zu Strafverfolgungszwecken eine hohe Priorität haben.

Haltung der Landesregierung:

Durch die Schaffung einer Rechtsgrundlage für die automatisierte Datenanalyse in § 47a kann die Maßnahme zur Gefahrenabwehr durchgeführt werden. Mittelbar kann dies auch Auswirkungen auf die Kriminalitätsbekämpfung, etwa bei der Verhütung von besonders schweren Straftaten, haben. Um eine Software zur automatisierten Datenanalyse aber gezielt im Rahmen der Strafverfolgung einsetzen zu können, bedarf es einer Rechtsgrundlage in der Strafprozessordnung. Die Landesregierung setzt sich für die Schaffung einer entsprechenden Rechtsgrundlage auf Bundesebene sowie für die bundesweite Einführung einer Software zur automatisierten Datenanalyse ein.

2.3 Der BDK begrüßt die Regelungen zur Erhebung, Verarbeitung und Übermittlung von Standortdaten, zur automatisierten Datenanalyse und zur Entwicklung, zum Training, zum Testen, zur Validierung und zur Beobachtung von informationstechnischen Produkten. Mit den Regelungen können nach Ansicht des BDK Lücken geschlossen und die Polizei zukunftsfähig aufgestellt werden. Dabei steht für den BDK außer Frage, dass Ergebnisse aus einer verfahrensübergreifenden

Recherche- und Analyseplattform stets am Ende von Menschen bewertet und interpretiert werden müssen.

Die Regelung zur Unterrichtung des Parlamentarischen Kontrollgremiums sieht der BDK unkritisch.

Haltung der Landesregierung:

§ 47a Absatz 2 Satz 1 regelt, dass die automatisierte Datenanalyse den Polizeivollzugsdienst bei der Erfüllung seiner Aufgaben unterstützt, indem sie Informationen bereitstellt, die es dem Polizeivollzugsdienst ermöglichen, eigene Bewertungen, Prognosen und Entscheidungen zu treffen. Die Analyseplattform darf somit keine Prognosesoftware in dem Sinne sein, dass sie eigenständig kriminelles Verhalten vorhersagt und die von einem Menschen zu treffende abschließende Bewertung ersetzt.

2.4 Der DGB sieht es grundsätzlich als richtig und wichtig an, Polizei und Ermittlungsbehörden mit modernen Verfahren auszustatten, um deren tägliche Arbeit bestmöglich zu unterstützen. Dazu gehöre auch die automatisierte Datenanalyse unter Berücksichtigung des vom Bundesverfassungsgericht gesetzten Rahmens, da hochsensible Daten betroffen seien, deren Schutz essenziell sei.

Der DGB hält den bereits erfolgten Vertragsabschluss mit einem externen Anbieter, bevor eine Rechtsgrundlage vorlag, für problematisch. Bevor die Festlegung auf einen Anbieter erfolge, müssten Anforderungen, Bedarfe und Rahmenbedingungen in einer entsprechenden Rechtsgrundlage fixiert werden. Es sei nicht nachvollziehbar, weshalb im März 2025 ein zeitlicher Druck entstanden sei, der einen vorzeitigen Vertragsabschluss nötig gemacht hätte. Die Entwicklung und Förderung einer europäischen bzw. öffentlichen Softwarelösung würde nicht nur die Abhängigkeit von einzelnen Anbietern reduzieren, sondern auch das Vertrauen in die rechtsstaatliche Kontrolle der sensiblen Datenverarbeitung stärken. Hinsichtlich der bereits angekündigten temporären Nutzung der externen Software stellen sich laut DGB Fragen nach der Übergangsphase, der Weiterverwendung von Analysedaten und der Anpassungsfähigkeit der Software an die spezifischen Bedürfnisse Baden-Württembergs. Die Punkte hätten vorab in einer entsprechenden Rechtsgrundlage berücksichtigt werden müssen.

Haltung der Landesregierung:

Die Schaffung einer Rechtsgrundlage für die polizeiliche Nutzung einer automatisierten Datenanalyse setzt eine entsprechende Vereinbarung aus dem Sicherheitspaket der Landesregierung von Herbst 2024 um. Der Haushaltsgesetzgeber hat anschließend auf der Grundlage eines Änderungsantrags der Koalitionsfraktionen die erforderlichen Mittel zur Beschaffung und Einführung bereitgestellt. Der Doppelhaushalt 2025/2026 wurde im Dezember 2024 im Parlament beschlossen. Daraufhin – und damit bereits vor der Vertragsunterzeichnung mit einem außereuropäischen Anbieter – wurde mit der Erarbeitung eines Gesetzes zur Einführung einer automatisierten Datenanalyse begonnen. Somit lag bereits zum Zeitpunkt der Vertragsunterzeichnung ein erster Referentenentwurf vor. Längere Zeitläufe zur Schaffung einer Rechtsgrundlage sind aufgrund der umfangreichen Abstimmungen, die sowohl ressortintern als auch ressortextern erforderlich sind, nicht ungewöhnlich.

Die Rechtsgrundlage für die automatisierte Datenanalyse in § 47a ist technikoffen gehalten, sodass gerade keine Festlegung auf einen bestimmten Anbieter einer konkreten Software zur automatisierten Datenanalyse erfolgt. Der Regelungsinhalt folgt dem Bedarf der polizeilichen Praxis unter Berücksichtigung der (datenschutz-)rechtlichen Grundsätze und der höchstrichterlichen Rechtsprechung. Dabei muss sich die Beschaffenheit einer verfahrensübergreifenden Recherche- und Analyseplattform und deren konkrete Nutzung, unabhängig von der eingesetzten Software, stets an der Rechtsgrundlage orientieren. In einer Rechtsgrundlage hingegen technisch-organisatorische Vorkehrungen für einen etwaigen späteren Wechsel der eingesetzten Software zu schaffen, dürfte rechtssicher nur schwerlich möglich sein.

2.5 Die NRV sieht das Anliegen, in einer zerklüfteten IT-Architektur eine effiziente Suche und Auswertung über die verschiedenen Datenbestände hinweg zu ermöglichen, als berechtigt und grundsätzlich datenschutz- und verfassungskonform umsetzbar an.

Er kritisiert jedoch den bereits erfolgten Vertragsabschluss mit einem externen Anbieter, bevor eine Rechtsgrundlage vorlag sowie die Wahl des Anbieters. Nach Ansicht der NRV setzt die bereits erfolgte Vertragsunterzeichnung den Landtag als Gesetzgeber unter Zugzwang. Er müsse nun eine Vorentscheidung auf einen bestimmten Anbieter und eine konkrete Software entweder billigen oder die Gesetzesinitiative ablehnen, was aufgrund der wirtschaftlichen Bindungen zu einem Schaden für den Haushalt führen würde. Dieses Vorgehen könne einen Präzedenzfall für die Zukunft schaffen. Um die tatsächliche Leistungsfähigkeit der Software beurteilen zu können, solle zudem eine institutionell unabhängige Evaluation vorgeschrieben werden. Diese Evaluation dürfe sich nicht nur auf die Nutzbarkeit und Nutzerfreundlichkeit, sondern auch und gerade auf die Grundrechtssensibilität der Nutzung erstrecken. Laut der NRV müsse die evaluierende Stelle bzw. die Evaluation Einblick in die Softwareinfrastruktur nehmen können, um Hintertüren, Datenabflüsse bzw. Sicherheitsschwachstellen und (verfassungs-) rechtlich nicht eröffnete Verarbeitungsvorgänge identifizieren und eliminieren zu können.

Hinsichtlich des Gesetzentwurfs bemängelt die NRV die ihrer Ansicht nach zu niedrigen Eingriffsvoraussetzungen in § 47a Absatz 1 Nummer 1 und hält die Abgrenzung zwischen sachgerechter Auswertung der Daten und einer Diskriminierung in der Anwendung der Software für schwierig. Zudem sei die Einbeziehung von Falldaten in die Analyseplattform inhaltlich nicht sinnvoll und im Gesetz nicht normklar verankert. Die NRV kritisiert auch den Anschluss von Altsystemen und befürchtet eine mangelnde Kennzeichnung aufgrund der Ausnahmetatbestände des § 72 Absatz 4 PolG. Darüber hinaus wird die Systematik der Personenkategorien als unglücklich beschrieben, etwa die fehlende Definition von Anlass- und Kontaktpersonen. Die NRV fordert eine positive Regelung derjenigen Personen, die in der Auswertung berücksichtigt werden dürfen sowie die Normierung unterschiedlicher Konstellationen, in denen eine Person jeweils Unbeteiligter oder Anlassperson sein kann. Die NRV hält die Anforderungen an die Verwaltungsvorschrift nicht für geeignet, das Eingriffsgewicht der Maßnahme zu reduzieren, da diese Einschränkungen in ihren grundlegenden Zügen im Gesetz selbst geregelt werden müssten.

Abschließend schlägt die NRV vor, auf eine Änderung der Strafprozessordnung hinzuwirken, damit die im Rahmen der Gefahrenabwehr erlangten Informationen in einem folgenden Strafverfahren vollumfänglich genutzt werden können.

Haltung der Landesregierung:

Hinsichtlich der Kritik an der vorab erfolgten Vertragsunterzeichnung zur Nutzung einer konkreten Software wird auf die Ausführungen in 2.4 zum Entstehungsprozess der Rechtsgrundlage für die automatisierte Datenanalyse verwiesen. Die Eingriffsschwelle in § 47a Absatz 1 Nummer 1 ist an enge Voraussetzungen geknüpft, wie sie allgemein für eingriffsintensive Maßnahmen gelten, wie etwa § 49 Absatz 1 Nummer 1 PolG. Vorausgesetzt wird eine konkrete Gefahr für ein besonders gewichtiges Rechtsgut, was den Vorgaben des Bundesverfassungsgerichts entspricht. Zudem gilt diese Schwelle für die Anwendung einer automatisierten Datenanalyse an sich. Die Erhebung von Telekommunikationsdaten wird durch sie nicht legitimiert. Telekommunikationsdaten müssen, wie auch alle anderen personenbezogenen Daten, zunächst nach den jeweiligen Rechtsgrundlagen erhoben und gespeichert werden, bevor sie im Rahmen einer automatisierten Datenanalyse verarbeitet werden können. § 47a wird die weiterhin geltenden spezifischen Rechtsgrundlagen zur Datenerhebung nicht ersetzen.

In § 47a Absatz 2 wird – entgegen der Auffassung der NRV, es handele sich hier um kaum operationalisierbare Prosa – die zulässige Methode einer automatisierten Datenanalyse gesetzlich geregelt. Dies entspricht den Vorgaben des Bundesverfassungsgerichts aus seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20), wonach der Gesetzgeber die wesentlichen Grundlagen zu den Verarbeitungsmethoden selbst durch Gesetz vorgeben muss. Dabei wird klarge-

stellt, dass eine automatisierte Datenanalyse lediglich ein technisches Hilfsmittel sein darf, das den Polizeivollzugsdienst bei seiner Aufgabenwahrnehmung unterstützt, ohne diese grundlegend zu verändern. Die abschließende Bewertung der zusammengeführten Informationen ist und bleibt Aufgabe des Polizeivollzugsdienstes. Der Mensch – und nicht der Algorithmus – bewertet die bereitgestellten Informationen abschließend. Damit sind beispielsweise alleinige maschinelle Gefährlichkeitsbewertungen zu Personen unzulässig. Die Aufgabenwahrnehmung durch den Polizeivollzugsdienst mitsamt den dabei durchgeführten Arbeitsschritten zur Auswertung von personenbezogenen Daten erfolgt dabei grundsätzlich sachgerecht anhand des jeweiligen Einzelfalls und unter Beachtung der verfassungsmäßigen Ordnung; hier insbesondere des Artikels 3 des Grundgesetzes. Sofern sich aus einem konkreten Sachverhalt bezogen auf einen Anlass im Sinne des § 47a Absatz 1 anlassbezogene und zielgerichtete Suchkriterien ergeben, die mit phänotypischen Merkmalen einhergehen (wie in dem von der NRV gewählten Beispiel), werden diese Suchkriterien manuell in die Analyseplattform eingegeben.

Eine Definition der Falldaten im Gesetzestext ist nicht notwendig, da diese in der Gesetzesbegründung näher erläutert werden. Eine Aufnahme der Definition in den Gesetzestext würde die ohnehin schon lange Norm überfrachten, zumal der Begriff Falldaten für den Anwenderkreis des Polizeivollzugsdienstes eindeutig sein dürfte. Gleichwohl hat die NRV den Begriff in ihrer Stellungnahme unzutreffend ausgelegt: Bei Falldaten handelt es sich nicht um Exporte aus polizeiinternen Hilfsprogrammen, sondern um die in Fallbearbeitungssystemen gespeicherten Daten. Diese dienen der Unterstützung von Ermittlungs- und Recherchetätigkeiten sowie Auswertungen bei komplexen, fallübergreifenden Ermittlungen oder bei Strukturermittlungen. Ein Fallbearbeitungssystem geht über die reine Verwaltung von Vorgangsdaten hinaus, indem es der Anwenderin oder dem Anwender ein speziell auf die Aufhellung von Strukturen hin ausgerichtetes Werkzeug zur Verfügung stellt und vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen abbildet. Fallbearbeitungssysteme können sowohl zu präventiven als auch zu repressiven Zwecken eingesetzt werden. Deren Einbeziehung in die automatisierte Datenanalyse ist aus polizeifachlicher Sicht zwingend erforderlich und auch zweckmäßig im Sinne der polizeilichen Aufgabenwahrnehmung. Gerade aus komplexen (Struktur-)Ermittlungen im Bereich der Bekämpfung des Terrorismus und der Organisierten Kriminalität können sich Erkenntnisse von herausragender Bedeutung für die adäquate polizeiliche Bewältigung von Gefährdungssachverhalten bezogen auf einen Anlass im Sinne des § 47a Absatz 1 ergeben. Dabei ist der in einem Fallbearbeitungssystem gespeicherte Datenbestand konfigurationsabhängig auf verschiedenen Ebenen strukturiert. Die einzelnen Datensätze werden in Mandanten und darin wiederum in Verfahren gespeichert, welche im Wesentlichen den Zugriff auf die Informationen bestimmen. Jeder Datensatz mit der jeweiligen Datenquelle ist immer genau dem Mandanten zugeordnet, in dem er erfasst wurde. Die Herkunft bzw. der Anlass der Speicherung eines Datensatzes ist also stets nachvollziehbar.

Die Forderung, ein Rückgriff auf den Ausnahmetatbestand des § 72 Absatz 4 PolG müsse explizit ausgeschlossen werden, überzeugt nicht. Bei anlassbezogen in die automatisierte Datenanalyse einzubeziehenden umfangreichen Datensätzen, etwa aus Funkzellenabfragen oder Asservaten, ist eine entsprechende Kennzeichnung im Sinne des § 72 Absatz 4 PolG oftmals tatsächlich nicht möglich. Die Regelung gilt auch für die übrigen eingriffsintensiven Maßnahmen und ist – zumindest im Hinblick auf § 72 Absatz 4 Satz 2 PolG – ohnehin zeitlich befristet. Der Ausschluss dieser Regelung würde auch dem gesetzgeberischen Willen bei der Schaffung der entsprechenden Übergangsregelung in § 135 Absatz 1 PolG zuwiderlaufen. Die Übergangsregelung wurde gerade dafür geschaffen, um die (Weiter-)Verarbeitung von ungekennzeichneten Daten für einen festgelegten Zeitraum zu ermöglichen. Ausweislich der Begründung der Polizeigesetzänderung von 6. Oktober 2020 dient die Übergangsvorschrift dazu, eine ressourcenaufwendige Nachkennzeichnung der Altdatenbestände zu vermeiden und gleichzeitig die Möglichkeit der rechtssicheren weiteren Verarbeitung auch von Altdatenbeständen zu schaffen, ohne die Funktionsfähigkeit der Polizei zu beeinträchtigen. Die Altdatenbestände unterliegen laut der Begründung der regulären Aussonderungsprüfung und Löschung, sodass sich ihr Bestand und damit auch das Anwendungsfeld der Übergangsregelung sukzessive reduzieren dürfte. Die Übergangsregelung

lässt die Möglichkeit unberührt, Altdaten durch eine nachträgliche Kennzeichnung entsprechend den Vorgaben vollständig in das neue Datenschutzregime zu überführen.

Anlasspersonen sind verurteilte, beschuldigte oder verdächtige Personen oder Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie in naher Zukunft Straftaten von erheblicher Bedeutung begehen. Somit umfasst der Begriff der Anlassperson nicht nur die in § 70 Nummer 3 PolG genannten Personen. Der Begriff des Kontaktes ist nicht in § 70 Nummer 4 PolG aufgeführt, sodass die NRV vermutlich § 70 Nummer 5 PolG gemeint haben dürfte. § 70 Nummer 5 PolG orientiert sich an Artikel 6 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates. Zudem ergibt sich aus § 47a unter Einbeziehung der Begründung, welche Personen als Anlasspersonen im Sinne der Norm angesehen werden. Kontaktpersonen müssen zu diesen in Kontakt stehen, sodass sich kein Spielraum ergibt, den Begriff des Kontaktes auch auf unbeteiligte Personen auszuweiten. Vielmehr ist bereits geregelt, welche Personengruppen in die Auswertung mit einbezogen werden können.

Gemäß § 47a Absatz 6 Satz 3 werden personenbezogene Vorgangsdaten unbeteiligter Personen nicht in eine automatisierte Datenanalyse einbezogen. Sofern eine bestimmte Person nicht mehr als unbeteiligte Person einzustufen ist, kann sich je nach Sachverhaltskonstellation die Möglichkeit ergeben, sie dann in die automatisierte Datenanalyse einzubeziehen.

Zur Kritik an der Formulierung von § 47a Absatz 6 Sätze 4 und 5 wird auf die Ausführungen in 2.1 verwiesen.

Wie die NRV zutreffend feststellt, sollen mit Hilfe der automatisierten Datenanalyse Daten, die bereits bei der Polizei Baden-Württemberg vorhanden sind, im Rahmen der Bearbeitung gefahrenabwehrrechtlicher Sachverhalte zusammengeführt werden. Das durch die Maßnahme bereitgestellte Recherche- und Analyseergebnis wird dabei im jeweiligen Einzelfall durch einen Menschen geprüft, bewertet und in der Akte dokumentiert. Sofern sich ein strafrechtliches Ermittlungsverfahren anschließt, können die Informationen in die Ermittlungsakte aufgenommen werden, wenn eine Datenübermittlung unter Wahrung der Vorgaben zur zweckändernden Datenverarbeitung vorliegt, die § 15 Absatz 3 PolG vorschreibt. Diese Vorgaben gelten für alle eingriffsintensiven Datenverarbeitungen, sodass nicht ersichtlich ist, weshalb gerade bei der automatisierten Datenanalyse eine spezielle Vorschrift in der Strafprozessordnung erforderlich wäre.

Eine Evaluation durch eine institutionell unabhängige Stelle als zusätzliche Kontrolle wird als nicht erforderlich angesehen. Das Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) wurde im Juni 2022 vom Bayerischen Landeskriminalamt beauftragt, den Quellcode auf Schwachstellen zu prüfen, um Sicherheitslücken und Datenabflüsse ausschließen zu können. Dieses Prüfverfahren zeigte, dass die Software ein Höchstmaß an Datensicherheit und Datenschutz gewährleistet. Das Fraunhofer Institut hat im Ergebnis seiner Prüfung Datenabflüsse und Backdoors ausgeschlossen. Zur weiteren Risikominimierung sind technisch-organisatorische Maßnahmen im Bereich der Informationssicherheit vorgesehen, um das System nach einem Update – soweit möglich – auf Backdoors und Sicherheitslücken zu überprüfen.

Zudem sind sowohl in der Rechtsgrundlage als auch in der zu erlassenden Verwaltungsvorschrift bereits umfassende Kontrollmechanismen vorgesehen. Dazu gehören unter anderem technisch-organisatorische Vorkehrungen über ein Rollen- und Rechtekonzept sowie ein Konzept zur Zugriffskontrolle. Weiterhin sollen Maßnahmen der automatisierten Datenanalyse grundsätzlich nur auf schriftliche und begründete Anordnung der Behördenleitung erfolgen dürfen. Darüber hinaus ist vorgesehen, dass der Landesbeauftragte für den Datenschutz und die Informationsfreiheit vor der Einrichtung oder wesentlichen Änderung der Analyseplattform anzuhören ist. Schließlich soll zur Gewährleistung der Transparenz die Unterrichtung des Parlamentarischen Kontrollgremiums gesetzlich vorgeschrieben und damit die parlamentarische Kontrolle erweitert werden.

2.6 Der AV BW kritisiert die vorzeitige Vertragsunterzeichnung mit dem Anbieter einer Software zur automatisierten Datenanalyse sowie die insoweit erfolgte Auswahl des Anbieters und der konkreten Software. Zudem hält der AV BW es für fraglich, ob der Polizei Baden-Württemberg genügend personelle Ressourcen zur Verfügung stehen, um die beabsichtigten Technologien der automatischen Datenanalyse und der Entwicklung polizeieigener KI mit eigenen Mitarbeitern (IT-Experten) sinnvoll einführen und benutzen zu können und dabei die Datensicherheit zu gewährleisten. Auch befürchtet der AV BW ein Vollzugsdefizit aufgrund mangelnder Infrastruktur sowie eine fehlende Sicherstellung, dass personenbezogene Daten beim Auftreten einer Sicherheitslücke nicht abfließen.

Der AV BW kritisiert die einzubeziehende Datenmenge und wirft die Frage auf, inwieweit erkennbar ist, aus welchen Quellen die auf der Plattform erhobenen und zusammengeführten Daten stammen. Auch hinterfragt der AV BW in diesem Zusammenhang die Aktualität der Daten, die in die Analyse einbezogen werden sollen.

Zudem bezweifelt der AV BW, ob eine Software zur automatisierten Datenanalyse überhaupt erforderlich ist und wirft die Frage auf, weshalb nicht mit den bereits bestehenden Datenbanken weitergearbeitet werden kann.

Kritisiert wird auch die mangelnde Definition des Rechtsgutes der Sachen von bedeutendem Wert und die mangelnde Regelung der Zweckbindung bei der weiteren Verarbeitung der personenbezogenen Daten.

Weiter bemängelt der AV BW, dass bisher nicht konkret geregelt wurde, welche Systeme (mit oder ohne KI-Funktionalität) genau in die Analyseplattform integriert werden. Dies müsse aufgrund des Gebotes der Normklarheit geregelt werden.

Zudem ist der AV BW der Ansicht, die Einbeziehung von Verkehrsdaten, insbesondere den aus Funkzellenabfragen gewonnenen Daten, müsste hinsichtlich ihrer erfassbaren Datenmengen sowie einer Höchstspeicherungsdauer begrenzt werden, vor allem, wenn eine breitere bevorratende Speicherung von Verkehrsdaten möglich sein sollte. Weiterhin fordert er, die einzelfallbezogen Daten nicht auf der Analyseplattform zu speichern, sondern in einer getrennten Ablage.

Hinsichtlich des schriftlichen Anordnungsvorbehalts mit Begründungszwang in § 47a Absatz 7 fordert der AV BW die Aufnahme von Konsequenzen bei Missachtung dieser Vorgabe. Dies solle dem Risiko entgegenwirken, dass die Anordnungen zu bloßen Floskeln verkommen.

Zur neuen Regelung für eine weitere Verarbeitung von personenbezogenen Daten zu Zwecken der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten fragt der AV BW, weshalb eine polizeiinterne Entwicklung dieser Produkte erforderlich sei und die Ergebnisse von wissenschaftlichen Einrichtungen nicht mehr ausreichend sein sollten. Auch äußert er Bedenken hinsichtlich der Möglichkeit, von einer Anonymisierung Abstand zu nehmen, sobald diese nur mit einem unverhältnismäßigen Aufwand möglich wäre und hält die diesbezügliche Regelung für nicht klar genug. Zudem fordert der AV BW eine erhöhte Sorgfaltspflicht im Umgang mit personenbezogenen Daten, was insbesondere bei komplexen Datenbeständen zu einer frühzeitigen Implementierung geeigneter Maßnahmen zur Erfüllung datenschutzrechtlicher Vorgaben führen sollte. Darüber hinaus solle sichergestellt werden, dass die Trainings-, Validierungs- und Testdatensätze im Hinblick auf ihre Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sind, damit keine Diskriminierungen fortgeschrieben oder verstärkt werden können.

Haltung der Landesregierung:

Hinsichtlich der Kritik an der vorab erfolgten Vertragsunterzeichnung zur Nutzung einer konkreten Software wird auf die Ausführungen in 2.4 verwiesen.

Im Hinblick auf die personellen Ressourcen wird auf die Ausführungen in der Gesetzesbegründung unter IV. „Finanzielle Auswirkungen“ verwiesen, in welchen dargestellt wird, dass die Kosten neben den Sachmitteln auch zusätzliches Personal umfassen.

Um die IT-Sicherheit und den Datenschutz zu gewährleisten, werden in der Umsetzung unterschiedliche Maßnahmen ergriffen. So wird die Analyseplattform etwa ausschließlich auf einer polizeieigenen IT-Infrastruktur betrieben (On-Premise). Dies bedeutet, dass alle Daten im besonders gesicherten polizeilichen Netz bleiben und nicht in Drittstaaten oder in eine externe Cloud-Infrastruktur übertragen werden können. Die Datenhoheit sowie die physische und logische Kontrolle über Server und Netzwerkinfrastruktur liegt ausschließlich bei der Polizei Baden-Württemberg. Damit hat ein Softwareanbieter keinen eigenständigen Zugriff auf die Plattform. Diese Mechanismen ermöglichen eine präzise Steuerung aller Verarbeitungen und Zugriffe. Die technische Architektur der Plattform ist von Grund auf darauf ausgelegt, jede unbefugte Verarbeitung zu verhindern („Zero Trust"). Im Ergebnis werden unterschiedliche Sicherheits- und Datenschutzarchitekturen angewendet, welche durch eine Kombination aus technischen, vertraglichen und organisatorischen Maßnahmen sicherstellen sollen, dass ein Datenabfluss aus dem System verhindert wird. Selbst bei einem nach allen Rechtsordnungen rechtmäßigen Zugriffsgesuch würden bei einem On-Premise-Betrieb technische und tatsächliche Zugriffsmöglichkeiten nicht gegeben sein. Die Datenverarbeitung verbleibt vollständig unter der Kontrolle des Landes Baden-Württemberg.

Die in eine automatisierte Datenanalyse einzubeziehenden Daten sind in der Regelung sowie in der Begründung ausreichend dargestellt. Da eine „Spiegelung" der in den Datenbanken gespeicherten Daten und der sich auf der Analyseplattform befindlichen Daten stattfindet, sind die automatisiert zusammengeführten Daten stets so aktuell, wie der ihnen zugrundeliegende Aktenrückhalt. Werden in den Datenbanken Informationen gelöscht, werden diese nicht mehr auf der Analyseplattform bereitgestellt. Die Erforderlichkeit einer Software zur verfahrensübergreifenden Recherche und Analyse wird bereits im Vorblatt dargestellt. Da es sich bei der beabsichtigten automatisierten Zusammenführung von personenbezogenen Daten nach Einschätzung des Bundesverfassungsgerichts um einen zusätzlichen Eingriff in das Recht auf informationelle Selbstbestimmung handelt, steht die Nutzung einer automatisierten Datenanalyse zum Zweck der Gefahrenabwehr unter dem Vorbehalt der in § 47a Absatz 1 festgelegten Eingriffsschwellen. Die Recherche und Auswertung in den bereits bestehenden Datenbanken erfolgt demnach weiterhin wie bisher.

Der Katalog der besonders gewichtigen Rechtsgüter enthält diejenigen Rechtsgüter, welche das Bundesverfassungsgericht als solche anerkannt hat (vgl. etwa Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 243). Da die Rechtsgrundlage für die automatisierte Datenanalyse in § 47a an die höchstrichterliche Rechtsprechung anknüpft, sind die verwendeten Begriffe ebenso zu verstehen, wie es durch das Bundesverfassungsgericht vorgegeben wird.

Die Weiterverarbeitung von personenbezogenen Daten (sowohl zweckwahrend als auch zweckändernd) ist in § 15 Absätze 2 und 3 PolG geregelt, auf den § 47a Absatz 4 Satz 1 verweist. Somit ist entgegen der Aussage des AV BW durchaus eine Regelung zur Weiterverarbeitung der Daten getroffen worden.

Die Rechtsgrundlage für die automatisierte Datenanalyse in § 47a enthält hinsichtlich Systemen mit KI-Funktionalitäten keine genaueren Angaben, da die Norm aufgrund der technischen Entwicklung abstrakt genug sein muss, um den Einsatz von KI-Systemen technikoffen zu gestatten. Die Exekutive muss in der Lage sein, auch neue auf den Markt kommende oder polizeiintern entwickelte Systeme verwenden zu können. Im Rahmen der erforderlichen Verarbeitungsverzeichnisse sowie Datenschutzkonzepte sind etwaige Risiken zu prüfen und es ist jeweils zu bewerten, wie diesen mit entsprechenden Maßnahmen begegnet werden kann. Sollte sich künftig eine wesentliche Abweichung der technischen Möglichkeiten ergeben, wäre das Gesetz, wie es der AV BW fordert, entsprechend anzupassen. Dies gilt ebenfalls für künftige höchstrichterliche Entscheidungen, die Rechtsgrundlagen zur automatisierten Datenanalyse zum Gegenstand haben und einen etwaigen Änderungsbedarf hinsichtlich der Rechtsgrundlage in § 47a auslösen würden.

Im Hinblick auf die Einbeziehung von Verkehrsdaten wird auf die bereits in der Rechtsgrundlage festgelegten Speicherfristen in § 47a Absatz 3 Sätze 4 und 5 verwiesen. Zudem verlangt § 47a Absatz 3 Satz 2 die Darlegung einer Erforderlichkeit der ergänzenden Einbeziehung von Verkehrsdaten im Einzelfall. Verkehrsdaten werden nicht ständig in die Analyseplattform aufgenommen, sondern

nur – soweit dies im Einzelfall erforderlich ist – bei Bedarf ergänzend einbezogen und daher auch nicht bevorratet. Eine getrennte Speicherung der im Einzelfall einbezogenen Daten würde dem Zweck widersprechen, die Analyseplattform als technisches Hilfsmittel im gefahrenabwehrrechtlichen Bereich einzusetzen, vor allem bei zeitkritischen Sachverhalten. Wenn einzelne Daten, deren Erforderlichkeit der ergänzenden Einbeziehung bereits festgestellt wurde, getrennt gespeichert würden, hätte dies wiederum heterogene Datenbestände zur Folge, die mit der Intention einer verfahrensübergreifenden Recherche- und Analyseplattform gerade verhindert werden sollen.

Die Forderung, in § 47a Absatz 7 über den bisherigen Anordnungsvorbehalt mit Begründungspflicht hinaus noch Konsequenzen bei Nichtbeachtung zu regeln, ist abzulehnen. Das Polizeigesetz enthält bereits an mehreren Stellen, gerade bei den eingriffsintensiven Maßnahmen, einen Anordnungsvorbehalt mit entsprechender Begründungspflicht. Es ist nicht zu besorgen, dass der Begründungspflicht bei der automatisierten Datenanalyse nicht mit der nötigen Einzelfallbewertung entsprochen wird. Auch aufgrund der Vorgabe, das Parlamentarische Kontrollgremium über die automatisierte Datenanalyse zu unterrichten, ist vielmehr zu erwarten, dass auf die Begründung von deren Einsatz ein besonderes Augenmerk gelegt wird.

Die Hinweise des AV BW zur Ausgestaltung der Verwaltungsvorschrift werden bei deren Erstellung sowie bei der späteren Anwendung berücksichtigt.

Die Rechtsgrundlage in § 57a zur weiteren Verarbeitung personenbezogener Daten zu Zwecken der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten ergänzt die Rechtsgrundlage für die Datenverarbeitung zu rein wissenschaftlichen Zwecken und bedeutet nicht, dass keine informationstechnischen Systeme mehr in Kooperation mit wissenschaftlichen Stellen entwickelt werden. Sie ist vielmehr deshalb erforderlich, weil es bei der Entwicklung neuer Systeme vermehrt zu der Frage kam, inwieweit die insoweit erforderliche Datenverarbeitung unter den Begriff der wissenschaftlichen Forschung fällt. Die neue Rechtsgrundlage soll daher keine Beschränkung auf polizeiinterne Entwicklungen bedeuten, sondern eine rechtssichere Grundlage dafür schaffen, dass die Polizei Baden-Württemberg imstande ist, den neuen technischen Entwicklungen zu begegnen und die technischen Mittel der Polizei zukunftsfähig ausgestalten zu können. Dabei wird ein besonderes Augenmerk auf einen geschützten Umgang mit sensiblen Daten gelegt und ein sicherer Raum für neue Testungen geschaffen, der auch der Datenminimierung und der Datensicherheit entspricht. Welche Maßnahmen hierfür erforderlich sind, wird bei jedem Projekt geprüft und festgelegt.

Die Gesetzesbegründung wurde, wie vom AV BW gefordert, um eine klarstellende Erläuterung der Unverhältnismäßigkeit einer Anonymisierung oder Pseudonymisierung der Daten ergänzt.

2.7 Die Stellungnahme der GFF beschränkt sich auf die Rechtsgrundlage für eine automatisierte Datenanalyse nach § 47a und bemängelt eine nicht ausreichende Umsetzung der Vorgaben des Bundesverfassungsgerichts. Die GFF sieht die Schaffung von Rechtsgrundlagen für methodenoffene Analysen und automatisierte Erkenntnisgewinne insgesamt als kritisch an.

Die GFF hält die konkret bezeichneten Datenbanken, die für die Recherche und Analyse herangezogen werden, für zu umfangreich. Dies gelte insbesondere für Vorgangsdaten und Falldaten, da diese nach Ansicht der GFF auch zu einem erheblichen Teil Daten von Personen enthalten, die keinen Anlass dafür gegeben haben, einer polizeilichen Maßnahme ausgesetzt zu werden. Auch die einzelfallbezogene ergänzende Einbeziehung von Daten, etwa solchen aus den sozialen Medien, wird als zu umfangreich angesehen. Zudem sei die Anzahl der Suchvorgänge nicht eingeschränkt, sodass unbegrenzt aufeinander aufbauende Suchanfragen gestellt werden könnten. Zudem kritisiert die GFF die Möglichkeit der Erstellung von Personen- und Bewegungsprofilen sowie die Bewertung von Personen und Gefährdungen bzw. Risiken, auch wenn schlussendlich nicht die Software entscheidet. Weiter bemängelt die GFF, dass es der Vorschrift an Regelungen zur Einhaltung der Zweckbindung sowie zur umfassenden Kennzeichnung der Daten mangele. Es sei nicht ausreichend, die Regelungen in eine Verwaltungsvorschrift

auszulagern. Hinsichtlich der vorgesehenen aufsichtlichen Kontrolle werden sowohl die Einbindung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit als auch die stichprobenartige Kontrolle der Zugriffsrechte als nicht ausreichend angesehen. Die GFF kritisiert darüber hinaus auch eine nicht ausreichende personelle Konkretisierung der Eingriffsschwelle bei § 47a Absatz 1 Nummer 2 sowie die Anknüpfung an Straftaten von erheblicher Bedeutung. Auch die Eingriffsschwelle in § 47a Absatz 1 Nummer 3 wird seitens der GFF als unzureichend bewertet, da es sowohl am Erfordernis einer Konkretisierung in zeitlicher Sicht und der Art nach als auch in persönlicher Hinsicht fehle und die Anknüpfung an besonders schwere Straftaten nur dann zureichend sei, wenn diese dem Schutz besonders gewichtiger Rechtsgüter dienen.

Schließlich wird seitens der GFF die Wahl einer Software eines außereuropäischen privaten Anbieters bemängelt und eine bund- und länderübergreifende Softwarelösung gefordert, auch wenn hinsichtlich staatseigenen Analysesystemen ebenfalls erhebliche Risiken für die Grundrechte und Zweifel an deren Effizienz bestünden.

Haltung der Landesregierung:

Zur weiteren Verarbeitung der personenbezogenen Daten und der damit in Zusammenhang stehenden Zweckbindung sowie der Wahl des Anbieters der konkreten Softwarelösung, wird auf die Ausführungen in 2.1, 2.4 und 2.6 verwiesen.

§ 47a Absatz 3 bestimmt abschließend, welche Datenbestände und Daten auf der Analyseplattform zusammengeführt werden dürfen. Das Gesetz begrenzt damit sowohl den Umfang als auch die Art der verarbeitbaren Daten, wodurch das Eingriffsgewicht der automatisierten Datenanalyse gemindert wird (BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 78). Die gesetzliche Bestimmung der verarbeitbaren Datenbestände und Daten orientiert sich am polizeilichen Bedarf sowie an der bisherigen polizeilichen Praxis bei der (händischen) Recherche und Analyse zu konkreten Gefährdungssachverhalten. Auch jetzt schon verarbeitet der Polizeivollzugsdienst rechtmäßig erhobene und gespeicherte Daten zum Zweck der Gefahrenabwehr, allerdings sind diese derzeit auf zahlreiche Datenbanken und Quellsysteme verteilt. Die daraus entstehenden Datenmengen sind sehr umfangreich, heterogen strukturiert, komplex und zudem oftmals nicht über Schnittstellen miteinander verbunden. Eine manuelle Abfrage aus verschiedenen Datenquellen wird durch große Datenmengen und verschiedenste Quellen sowie Dateiformate immer zeitaufwendiger und komplexer. Darüber hinaus müssen die Daten in einem weiteren Schritt aufbereitet und in Beziehung gesetzt werden, bevor eine Analyse erfolgen kann. In zeitkritischen Gefahrenlagen ist die schnelle Reaktionsfähigkeit jedoch ein erfolgskritischer Faktor.

Auch wenn durch die automatisierte Datenanalyse ein zusätzlicher Grundrechtseingriff erfolgt, entspricht der Grunddatenbestand der auf der Plattform bereitgestellten Informationen dem bisherigen Prüfdatenbestand bei einer manuellen Recherche und Analyse – nur werden die Daten nunmehr automatisiert zusammengeführt. Um diesen Eingriff zu mildern, werden bestimmte, im Gesetz näher bezeichnete personenbezogene Daten lediglich einzelfallbezogen und nach einer gründlichen Erforderlichkeitsprüfung ergänzend miteinbezogen. Soweit Daten von der Kennzeichnungspflicht nach § 72 PolG umfasst sind, gewährleistet bereits die vorzunehmende Kategorisierung, dass Daten unbeteiligter Personen im polizeilichen Sinne nicht einbezogen werden können. Bei anlassbezogen in die automatisierte Datenanalyse einzubeziehenden umfangreichen Datensätzen etwa aus Funkzellenabfragen oder Asservaten ist eine entsprechende Kennzeichnung im Sinne des § 72 Absatz 4 PolG oftmals nicht möglich. Ein wesentliches Ziel der Einführung einer automatisierten Datenanalyse ist es, große, in zeitkritischen Situationen händisch nicht zu sichtende Datenmengen analysieren zu können. Im Gesetz ist der Ausschluss der Einbeziehung von Daten unbeteiligter Personen bereits angelegt. So ist einerseits die Erforderlichkeit der einzelfallbezogenen Einbeziehung entsprechender Datensätze zu prüfen. Andererseits ist der Umfang der einbeziehbaren Daten bzw. die Ausrichtung des Suchvorgangs abhängig von der jeweiligen Eingriffsschwelle geregelt. Weitergehende Einschränkungen würden dazu führen, dass ein wesentliches Ziel der Einführung einer automatisierten Datenanalyse nicht erreicht werden könnte, da umfangreiche Datensätze aus Asservaten oder Funkzellenabfragen oftmals grundsätzlich auszuschließen wären.

Die Anzahl der zulässigen Suchabfragen und damit deren Beschränkung kann nicht vorab gesetzlich festgelegt werden, da sie vom Einzelfall abhängt. Da sich im Rahmen der Rechercheergebnisse gegebenenfalls noch weitere erforderliche Arbeitsschritte ergeben können, ist deren zahlenmäßige Begrenzung auch nicht zielführend und daher abzulehnen.

Die Darstellung der GFF, dass mittels der automatisierten Datenanalyse eine Erstellung von Personen- und Bewegungsprofilen sowie eine Bewertung von Personen und Gefährdungen bzw. Risiken ermöglicht werde, ist nach Auffassung der Landesregierung in ein Verhältnis zum präventivpolizeilichen Anwendungszweck der Maßnahme zu setzen und daher zwingend zu relativieren. Bei der automatisierten Zusammenführung von personenbezogenen Daten zum Zwecke der Gefahrenabwehr ist durchaus denkbar, dass im Rahmen eines konkreten Sachverhalts – stets bezogen auf einen (Gefährdungs-)Anlass im Sinne des § 47a Absatz 1 – die Rechercheergebnisse im Einzelfall eine gewisse profilähnliche, inhaltliche Auswertetiefe zu den betroffenen Personen aufweisen können. Hierbei werden gleichwohl nur diejenigen Personen adressiert, die anhand von anlassbezogenen und zielgerichteten Suchkriterien in Betracht kommen. In diesen Fällen besteht für den Polizeivollzugsdienst Grund zur Annahme, dass die in die Auswertung einbezogenen Persönlichkeitsmerkmale im konkreten Sachverhalt eine wesentliche Rolle für die polizeiliche Aufgabenwahrnehmung spielen. Damit ist gerade nicht eine anlassunabhängige oder allgemeine Sammlung von Informationen zu einem unbestimmten Personenkreis gemeint. Bei der automatisierten Datenanalyse handelt es sich um ein technisches Hilfsmittel und keine Prognosesoftware, welche eigenständig kriminelles Verhalten vorhersagt. Der Mensch und nicht der Algorithmus bewertet die bereitgestellten Informationen abschließend. Damit sind alleinige maschinelle Gefährlichkeitsbewertungen zu Personen unzulässig.

Die aufsichtliche Kontrolle des Landesbeauftragten für den Datenschutz und die Informationsfreiheit betrifft nicht nur die in § 47a Absatz 8 enthaltene Pflicht zur Anhörung, ihm stehen auch weitere Kontrollmöglichkeiten im Polizeigesetz, wie etwa aus § 98 PolG, zu. Eine zusätzliche Aufsicht wird durch die Unterrichtung des Parlamentarischen Kontrollgremiums gesetzlich vorgeschrieben. Weitere externe Kontrollmöglichkeiten werden nicht als erforderlich angesehen.

Die Eingriffsschwelle bei § 47a Absatz 1 Nummer 2 entspricht den Vorgaben des Bundesverfassungsgerichts (Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn.112 sowie 162 ff.) und den darin aufgestellten Anforderungen an die zu treffende Prognoseentscheidung bezüglich der Gefahrenlage im Vorfeld einer konkreten Gefahr für die Begehung terroristischer Straftaten. Aus Gründen der Verhältnismäßigkeit erscheint es erforderlich, aber auch ausreichend, § 47a Absatz 1 Nummer 2 dahingehend einzuschränken, dass die prognostizierte Rechtsgutverletzung von bestimmten besonders qualifizierten Straftaten ausgehen muss. Das Eingriffsgewicht wird zusätzlich durch die Voraussetzung verringert, dass die zugrundeliegende Anlasstat nicht nur abstrakt, sondern auch im Einzelfall schwer wiegen muss. Hinsichtlich der Kritik an § 47a Absatz 1 Nummer 3 wird auf die Erläuterungen in der Gesetzesbegründung (Seite 15) verwiesen.

2.8 Von den 27 eingegangenen Kommentaren (ein Kommentar wurde durch den Nutzer gelöscht) auf dem Beteiligungsportal des Landes richten sich 15 gegen den Einsatz der beabsichtigten Software eines außereuropäischen Anbieters, für die bereits ein Vertrag geschlossen wurde (Kommentare Nummer 1, 4, 7, 8, 11, 12, 13, 16, 17, 18, 19, 21, 23, 24 und 25), teilweise wird ein europäischer Anbieter als mögliche Lösung angesehen. Die Rechtsgrundlage für die automatisierte Datenanalyse in § 47a an sich wird, unabhängig von der Wahl des Softwareanbieters, in fünf Kommentaren abgelehnt (Kommentare Nummer 2, 7, 10, 11, 14 und 22).

Fünf Kommentare sprechen sich für den Einsatz einer automatisierten Datenanalyse aus (Kommentare Nummer 1, 3, 5, 18 und 24) und ein Kommentar für die Nutzung des AML-Dienstes (Nummer 19).

Ein Kommentar (Nummer 4) vermisst eine Stellungnahme des Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

Bei insgesamt drei Kommentaren ist aufgrund ihres Inhaltes keine Bewertung beziehungsweise Stellungnahme möglich (Kommentare Nummer 6, 9 und 20).

Ein Kommentar (Nummer 15) lehnt den Einsatz von Bodycams in Wohnungen ab und fordert eine strikte Einschränkung aller audiovisuellen Maßnahmen, eine stärkere Kontrolle durch unabhängige Datenschutzstellen und mehr Transparenz gegenüber der Öffentlichkeit.

Ein Kommentar (Nummer 19) vermisst zusätzlich die eindeutige Regelung, dass jedermann Video- bzw. Sprachaufzeichnungen von Polizeieinsätzen machen kann, da die Rechtslage hierzu nicht eindeutig sei.

Kommentar Nummer 26 enthält eine Stellungnahme des Chaos Computer Clubs Stuttgart e. V. In dieser wird zunächst ausgeführt, dass die Vorgaben des Bundesverfassungsgerichts zum Einsatz einer automatisierten Datenanalyse mangels klarer Vorgaben bzw. Einschränkungen hinsichtlich der zusammengeführten und verarbeiteten Daten bzw. Datenbanken sowie mangels einer Untersagung der Nutzung von KI und fehlender Transparenz und Kontrolle nicht erfüllt seien. Die Erlaubnis zur Nutzung der automatisierten Datenanalyse sei zu unbestimmt und daher zu weitreichend. Zudem gebe es keine Einschränkung auf konkret aufgeführte Datenbanken, es drohe bei bestehenden Datensätzen sowie bei Daten nicht-landeseigener Herkunft eine Aufhebung der Zweckbindung und die Entscheidung, wann eine Einbeziehung der Datenquellen erforderlich sei, solle unter Richtervorbehalt gestellt werden. Der Chaos Computer Club Stuttgart e. V. fordert eine Löschung der auf der Analyseplattform gespeicherten Daten, sobald die hierfür ursächlichen Ermittlungen abgeschlossen sind und fordert den Ausschluss von biometrischen Daten, Daten aus anlasslosen Durchsuchungen sowie allen Daten von Nachrichtendiensten. Darüber hinaus fordert der Chaos Computer Club Stuttgart e. V. einen Richtervorbehalt für den Einsatz der automatisierten Datenanalyse und eine gesetzliche Regelung, dass keine KI-Komponenten des Anbieters genutzt werden dürfen, mit dem bereits ein Vertrag geschlossen wurde. Des Weiteren fordert der Chaos Computer Club Stuttgart e. V. die Veröffentlichung des Quelltextes oder zumindest dessen Einsichtnahme durch die Landesbehörden sowie eine unabhängige Überprüfung des Quelltextes durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Dies solle auch für neue Updates gelten. Die konkrete Nutzung der Software zur automatisierten Datenanalyse solle durch eine unabhängige Stelle, etwa durch das Parlamentarische Kontrollgremium, stichprobenartig kontrolliert werden. Neben einer Unterbindung des Zugriffs von Mitarbeitern des Softwareherstellers und einem Verzicht auf die Nutzung kommerzieller, gegebenenfalls außereuropäischer Anbieter solle eine souveräne (europäische) Softwarelösung entwickelt werden. Zudem lehnt der Chaos Computer Club Stuttgart e. V. die Verarbeitung von unveränderten Daten und nicht anonymisierten oder zumindest pseudonymisierten Daten ab. Es sei nicht nachvollziehbar, weshalb unveränderte Daten benötigt würden oder nicht wenigstens eine Pseudonymisierung vorgenommen werden könne.

Haltung der Landesregierung:

Hinsichtlich der Vertragsunterzeichnung und der erfolgten Auswahl einer konkreten Software, der Entwicklung einer europäischen Softwarelösung sowie der Erforderlichkeit der Nutzung einer automatisierten Datenanalyse wird auf die Ausführungen in 2.1 und 2.4 sowie auf die Gesetzesbegründung (Seite 12 ff.) verwiesen.

Zu Kommentar Nummer 12 ist ergänzend darauf hinzuweisen, dass die automatisierte Datenanalyse auf Grundlage des § 47a nur zur Gefahrenabwehr genutzt wird, nicht hingegen dazu, um Straftaten vorherzusagen. Zudem ist in der Rechtsgrundlage eindeutig festgelegt, ab welcher Eingriffsschwelle eine automatisierte Datenanalyse durchgeführt werden darf und welche personenbezogenen Daten in die Recherche und Analyse einbezogen werden dürfen.

Die Kommentare Nummer 15 und 19 befassen sich mit Rechtsgrundlagen, die nicht Gegenstand des Gesetzgebungsverfahrens sind, sodass zu diesen keine Stellungnahme abgegeben wird.

Dem Kommentar Nummer 4 wird entsprochen, da die Stellungnahme des Landesbeauftragten für den Datenschutz und die Informationsfreiheit, wie die weiteren eingegangenen Stellungnahmen, beigefügt ist.

Zur Stellungnahme des Chaos Computer Clubs Stuttgart e. V. (Nummer 26) nimmt die Landesregierung wie folgt Stellung:

Zur Bestimmtheit der einzubeziehenden Daten, deren weiterer Verarbeitung und der damit in Zusammenhang stehenden Zweckbindung, der Löschfristen sowie der Auswahl des Anbieters der konkreten Softwarelösung, wird auf die Ausführungen in 2.1, 2.4, 2.5 und 2.6 verwiesen.

Ein Richtervorbehalt bei der Prüfung der Erforderlichkeit der ergänzenden Einbeziehung von im Einzelfall erforderlichen Daten im Sinne des § 47a Absatz 3 Satz 2 ist abzulehnen. Die Exekutive muss einzelfallabhängig entscheiden können (oftmals unverzüglich), welche Daten für die konkrete polizeiliche Aufgabenwahrnehmung der Gefahrenabwehr erforderlich sind, um diese unter Beachtung des Gebotes der Datenminimierung ergänzend in eine automatisierte Datenanalyse einbeziehen zu können. Zudem wird in der Stellungnahme des Chaos Computer Clubs Stuttgart e. V. nicht dargelegt, wie diese Forderung in der Praxis umgesetzt werden soll, zumal es sich bei der Nutzung der automatisierten Datenanalyse um ein Hilfsmittel bei zeitkritischen Fällen handelt. Der Forderung, allgemein auf eine Nutzung von KI zu verzichten, kann ebenfalls nicht entsprochen werden. Auch das Bundesverfassungsgericht hält die Nutzung von KI im Rahmen der automatisierten Datenanalyse nicht für ausgeschlossen, attestiert ihr jedoch ein besonderes Eingriffsgewicht, weshalb ein hinreichendes Schutzniveau erforderlich ist, welches die eingeschränkte Nachvollziehbarkeit der Ergebnisse ausgleicht. Da die Rechtsgrundlage für die automatisierte Datenanalyse in § 47a technikoffen ausgestaltet ist, erfolgt gesetzlich kein Ausschluss bestimmter Module einer konkreten Software eines Anbieters. Ein Richtervorbehalt statt einer Anordnungsbefugnis durch die Leitung eines regionalen Polizeipräsidiums, des Polizeipräsidiums Einsatz oder des Landeskriminalamts bzw. bei Gefahr im Verzug durch besonders beauftragte Beamte wird nicht als erforderlich gesehen, da der vom Bundesverfassungsgericht geforderten aufsichtlichen Kontrolle bereits durch die vorgesehene Regelung Genüge getan ist.

Hinsichtlich der Rechtsgrundlage in § 57a zur weiteren Verarbeitung von personenbezogenen Daten zu Zwecken der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten ist zu erwähnen, dass die Verarbeitung von nicht anonymisierten Daten nur in engen Ausnahmefällen, die gesetzlich abschließend normiert sind, möglich ist. Die Erläuterung zu den Ausnahmetatbeständen kann der Gesetzesbegründung (Seite 23) entnommen werden.

2.9 Die redaktionellen Anmerkungen des Normenprüfungsausschusses wurden weitestgehend übernommen.

2.10 Der Normenkontrollrat hat eine Stellungnahme abgegeben. Er kommt bezüglich des Gesetzentwurfs insgesamt zu einem positiven Votum, stellt allerdings fest, dass durch die Änderung des § 90 PolG die Unterrichtungspflicht des Innenministeriums erheblich ausgeweitet werde, was er nicht für erforderlich halte. Zudem sei eine Übertragung der Unterrichtungspflicht an das Parlamentarische Kontrollgremium, welches nach dem Gesetz über den Verfassungsschutz in Baden-Württemberg (LVSG) den Verfassungsschutz und nicht die Polizei kontrolliere, systemwidrig. Der Normenkontrollrat ist der Auffassung, dass ein politischer Kompromiss nicht zum Preis eines systemfremden Aufwuchses von Berichts- und Unterrichtungspflichten führen sollte, dessen Mehrwert zudem nicht weiter dargelegt werde.

Haltung der Landesregierung:

Der Mehrwert der Neuregelung des § 90 besteht darin, insbesondere die automatisierte Datenanalyse einer intensiven parlamentarischen Kontrolle zu unterwerfen und damit einen Ausgleich zum Eingriff durch die Nutzung der Maßnahme zu schaffen. Die Unterrichtung des Parlamentarischen Kontrollgremiums sowie der

Öffentlichkeit dient neben der Kontrolle auch der Transparenz der polizeilichen Maßnahmen. Eine Anwendung der Regelungen des Gesetzes über den Verfassungsschutz in Baden-Württemberg (LVSG) erscheint auch aus Sicht der Landesregierung systemwidrig und rechtlich ausgeschlossen, weshalb in § 90 kein Verweis in das LVSG erfolgt. Einer Absicherung der organisatorischen Trennung von Polizei und Verfassungsschutz wird durch organisatorische Vorkehrungen Rechnung getragen, etwa durch getrennte Sitzungen.

2.11 Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat im Rahmen seiner Beteiligung zwei Stellungnahmen abgegeben. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit wurde bereits frühzeitig im Gesetzgebungsverfahren beteiligt. Die dabei eingebrachten Hinweise wurden soweit möglich in den Gesetzentwurf eingearbeitet. Im Rahmen des sich daran anschließenden Beteiligungsverfahrens innerhalb der Landesverwaltung hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit einzelne, bislang nicht aufgegriffene Empfehlungen konkretisiert bzw. neue Empfehlungen und Anregungen eingebracht. Diese wurden teilweise im zweiten Referentenentwurf aufgegriffen bzw. durch entsprechende Vorkehrungen auf untergesetzlicher Ebene umgesetzt. Daher wird ausschließlich zu denjenigen Forderung Stellung genommen, die nicht bereits umgesetzt wurden.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit empfiehlt dringend, den Ausschluss der Einbeziehung von Daten unbeteiligter Personen auszuweiten.

Zudem empfiehlt er, den gesetzlich geregelten Mindestinhalt der begleitenden Verwaltungsvorschrift um ein Qualitätsmanagement zu erweitern.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit betont, dass der Gesetzgeber darüber zu entscheiden habe, welche Informationen in eine Datenanalyse einbezogen werden dürfen. Art und Umgang der automatisiert analysierten Daten müssten daher durch den Gesetzgeber selbst konkretisiert werden, was in § 47a noch nicht ausreichend erfolgt sei. Auch wenn der Landesbeauftragte für den Datenschutz und die Informationsfreiheit es begrüßt, dass personenbezogene Daten, die aus einer Wohnraumüberwachung oder einer Online-Durchsuchung gewonnen wurden, nicht in die automatisierte Datenanalyse einbezogen werden dürfen, fordert er zusätzlich, dass beispielsweise Informationen, die aus dem Einsatz verdeckter Ermittler, aus längerfristigen Observationen oder aus dem Einsatz technischer Mittel außerhalb von Wohnungen gewonnen wurden, ebenfalls ausgeschlossen werden.

Nach Ansicht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit sollte der Gesetzgeber insbesondere entscheiden, wer Unbeteiligter im Sinne des Gesetzes ist. Daten offensichtlich Unbeteiligter sollten nicht nur bezüglich der Vorgangsdaten für die Datenanalyse gesperrt werden. Spätestens mit Ablauf der Übergangsfrist für die Kennzeichnungspflicht aus § 72 PolG sollten die demzufolge verpflichtenden Informationen zum Schutze betroffener Personen genutzt werden.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit fordert darüber hinaus, dass die Erlaubnis zum Einsatz Künstlicher Intelligenz bei der Datenanalyse mindestens durch eine Zweck-/Zielsetzung durch den Gesetzgeber begrenzt werden müsse. Darüber hinaus solle die Gesetzesbegründung die Risiken des Einsatzes künstlicher Intelligenz vor dem konkreten Hintergrund der großen Datenmengen und polizeilichen Überwachungsbefugnissen adressieren.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit empfiehlt im Hinblick auf die Regelung zur weiteren Verarbeitung personenbezogener Daten zu Zwecken der Entwicklung, des Trainings, des Testens, der Validierung und der Beobachtung von informationstechnischen Produkten (§ 57) eine ausdrückliche Regelung des Prüfungs- und Freigabeprozesses durch eine Verwaltungsvorschrift. Anonymisierte bzw. pseudonymisierte Daten sollten dabei klar vorzugswürdig bleiben.

Haltung der Landesregierung:

Hinsichtlich der Regelungen zum Ausschluss unbeteiligter Personen wird auf die Ausführungen in 2.7 verwiesen.

Von der verpflichtenden Aufnahme eines Qualitätsmanagements innerhalb der begleitenden Verwaltungsvorschrift wurde abgesehen, da ein solches nicht in erster Linie der Eingriffsminimierung dient und somit nach hiesiger Auffassung nicht als Mindestinhalt vorzugeben ist. Inwieweit ein Qualitätsmanagement als über den gesetzlichen Mindestinhalt hinausgehender zusätzlicher Regelungsbedarf in die Verwaltungsvorschrift aufgenommen werden sollte, wird im Rahmen der Erstellung der Verwaltungsvorschrift geprüft.

§ 47a Absatz 3 enthält eine abschließende Bestimmung, welche Daten auf einer verfahrensübergreifenden Recherche- und Analyseplattform zusammengeführt werden dürfen. Die in Satz 1 genannten Datenbestände dürfen auf der Plattform laufend zusammengeführt werden, die in Satz 2 genannten Daten lediglich einzelfallbezogen ergänzend in eine Analyse einbezogen werden. Hiermit wird sowohl die Art der zu verarbeitenden Daten als auch deren Umfang hinreichend bestimmt und zudem verhältnismäßig abgestuft, um das Eingriffsgewicht der automatisierten Datenanalyse nach den Vorgaben des Bundesverfassungsgerichts zu mindern.

Eine Differenzierung von Art und Umfang der zu verarbeitenden Daten in § 47a Absatz 3 nach Fachbegriffen aus der polizeilichen Datenverarbeitung (u. a. Vorgangsdaten, Falldaten, Verkehrsdaten, Daten aus Asservaten) und nicht nach personenbezogenen Merkmalen (etwa Nachname, Vorname, Geburtsdatum, Adresse) ist aus fachlicher Sicht notwendig, um überhaupt eine praktisch anwendbare und verständliche Ermächtigungsnorm formulieren zu können. Andernfalls müssten – in Anbetracht der genannten heterogenen Beschaffenheit der polizeilichen IT-Infrastruktur – für jede einzelne Datenquelle die darin verarbeiteten personenbezogenen Merkmale separat aufgeführt bzw. abgegrenzt werden, was nicht umsetzbar, aber nach hiesiger Einschätzung auch nicht notwendig sein dürfte. Eine ausführliche Beschreibung der verwendeten Fachbegriffe findet sich in der Gesetzesbegründung (siehe Seite 17 ff.).

Ferner kann die Anregung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit, zusätzlich zu den aus einer Wohnraumüberwachung oder einer Online-Durchsuchung gewonnenen personenbezogenen Daten, auch Informationen aus dem Einsatz von Verdeckten Ermittlern, aus längerfristigen Observationen oder aus dem verdeckten Einsatz technischer Mittel bei einer automatisierten Datenanalyse pauschal auszuschließen, nicht berücksichtigt werden. Derartige Maßnahmen kommen nur unter engen rechtlichen Voraussetzungen zur Anwendung und richten sich dabei stets gegen einen bestimmten Adressaten (etwa § 49 Absatz 1 PolG). Die daraus resultierenden Erkenntnisse sind regelmäßig von hoher Relevanz für die polizeiliche Aufgabenwahrnehmung – insbesondere in Gefahrenlagen, in denen auch eine automatisierte Datenanalyse in Betracht kommt.

Der technologische Fortschritt insbesondere im Bereich der KI bietet enorme Chancen für die Arbeit der Polizei, um die Arbeit zeitgemäß zu vereinfachen, zu beschleunigen und zu verbessern. KI ist die Schlüsseltechnologie der Zukunft. Klar ist aber auch, dass der Einsatz solcher Technologien stets im Einklang mit (datenschutz-)rechtlichen Vorgaben auf nationaler sowie europäischer Ebene (v. a. KI-VO) erfolgen muss. Mittels der Integration von KI-Funktionalitäten können die in einer verfahrensübergreifenden Recherche- und Analyseplattform abgebildeten Prozesse durch KI unterstützt und KI-Modelle, zum Beispiel Large Language Models (LLM), angebunden werden. Hierdurch wäre die Plattform exemplarisch in der Lage, menschliche Sprache zu verstehen, diese zu übersetzen und selbstständig Texte zu erstellen. Auch eine automatische Transkription von Audioaufzeichnungen und die automatische Übersetzung von Textinhalten wäre denkbar. Gefährdungsrelevante Inhalte können erheblich schneller erkannt und die polizeiliche Ermittlungstätigkeit – gerade bei zeitkritischen Sachverhalten – somit anhand von automatisierten Arbeitsschritten optimiert werden. Das Beispiel LLM steht als einer von vielen potenziellen Anwendungsfällen, in denen der Einsatz von Komponenten der KI bei der automatisierten Datenanalyse in Betracht kommt. Hierbei steht die gesamte Bandbreite der KI-Nutzung in Abhängigkeit zu den rechtlichen und technischen Rahmenbedingungen. Welche Systeme mit oder

ohne KI-Funktionalität letztlich in eine verfahrensübergreifende Recherche- und Analyseplattform integriert werden, kann aufgrund der fortschreitenden technischen Entwicklungen im Einzelnen nicht konkret abgesehen werden. Eine Beschränkung der Anwendungsfälle für den Einsatz von KI-Funktionalitäten unmittelbar im Gesetzestext ist daher nicht zielführend und würde in jedem Fall einen fortwährenden Aktualisierungsbedarf des Gesetzes bedingen. Es bedarf an dieser Stelle daher explizit einer technikoffenen Formulierung der Ermächtigungsnorm.

Die vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit geforderte Begrenzung des Einsatzes von KI hinsichtlich Ziel und Zweck sowie die Berücksichtigung der inhärenten Risiken wird zudem bereits anhand mehrerer gesetzlicher Festlegungen umgesetzt:

– Die Zielsetzung einer automatisierten Datenanalyse ist stets die Wahrnehmung der gebotenen polizeilichen Aufgabe (hier: Abwehr von Gefahren und Verhütung von Straftaten). Eine Zweckbindung der KI-Funktionalitäten ergibt sich aus § 47a Absatz 2, worin die zulässige Methode geregelt ist.
– Demnach handelt es sich bei der automatisierten Datenanalyse um ein technisches Hilfsmittel und keine Prognosesoftware, welche eigenständig kriminelles Verhalten vorhersagt. Der Mensch und nicht der Algorithmus bewertet die bereitgestellten Informationen abschließend. Damit sind alleinige maschinelle Gefährlichkeitsbewertungen zu Personen unzulässig.
– Der Polizeivollzugsdienst entscheidet eigenständig über weitere Maßnahmen auf Grundlage des Analyseergebnisses.
– Diskriminierende Algorithmen dürfen weder herausgebildet noch verwendet werden.
– In der Gesetzesbegründung erfolgt ein ausdrücklicher Hinweis auf die Einschränkungen und Vorgaben der KI-VO.

Zu § 57a erscheint es nach Auffassung der Landesregierung ausreichend, den Testungs- und Freigabeprozess untergesetzlich zu regeln. Die Ausnahmetatbestände für einen Verzicht auf die Anonymisierung bzw. Pseudonymisierung sind für die Fälle erforderlich, in denen eine Anonymisierung bzw. Pseudonymisierung zwar theoretisch möglich und auch mit verhältnismäßigem Aufwand durchführbar, aber praktisch nicht zielführend wäre, da sie den Erkenntniswert oder die Funktionstauglichkeit des betreffenden informationstechnischen Produktes erheblich beeinträchtigen würde. Eine Streichung der Ausnahmetatbestände scheidet daher aus.

DPolG
DEUTSCHE POLIZEIGEWERKSCHAFT
im DBB

Landesvorsitzender
Ralf Kusterer

Landesverband Baden-Württemberg
Kernerstraße 5
70182 Stuttgart

Telefon: 0711/ 997 947 4-0
Telefax: 0711/ 997 947 4-20
info@dpolg-bw.de
www.dpolg-bw.de

Az: Datenanalyse/2025/0001a /Lei

Stuttgart, den 18. August 2025

DPolG BW, Kernerstr. 5, 70182 Stuttgart

Ministerium des Inneren, für Digitalisierung und Kommunen

-per E-Mail-

Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften
hier: Anhörung

Bezug: Ihr Zeichen: IM3-1101-44/8/2

Sehr geehrte Damen und Herren,

die Deutsche Polizeigewerkschaft (DPolG), Landesverband Baden-Württemberg e.V., dankt für die Übersendung des Entwurfs eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeilicher Vorschriften und nimmt hierzu nachfolgend Stellung:

Die Deutsche Polizeigewerkschaft (DPolG) begrüßt ausdrücklich die Absicht der Landesregierung mit einer Automatisierung der Datenanalyse den stets steigenden Massendaten wirksam zu begegnen. Die polizeiliche Ermittlungsarbeit erfordert eine ständige Anpassung an die Kriminalitätsentwicklung und den technischen Fortschritt. Künstliche Intelligenz und ein enormer Anstieg von digitalen und analogen Daten bedürfen wirksamer Prozesse, die die Ermittlungs- und Sicherheitsbehörden in die Lage versetzen, die präventiven und repressiven Maßnahmen professionell treffen zu können.

Ein Verzicht auf eine automatisierte Datenanalyse setzen wir mit enormen Sicherheitsdefiziten gleich. Mit großem Unverständnis haben wir die politische und mediale Diskussion zu Software-Herstellern und Anbietern wahrgenommen. Die Deutsche Polizeigewerkschaft steht dazu, dass die Opfer mehr in den sicherheitspolitischen Mittelpunkt gerückt werden.

Wir begrüßen es grundsätzlich, wenn bei IT-Lösungen deutsche Unternehmen, besser noch Unternehmen aus Baden-Württemberg, einbezogen werden. Deutsche Sicherheitsstandards sichern im höchsten Maß die Anforderungen an den Datenschutz und gesellschaftliche Akzeptanz. Andererseits erfordert es die aktuelle Situation, dass wir sehr schnell IT-Lösungen einführen und begrüßen deshalb auch die Entscheidung zum Erwerb und der Nutzung der Analyse-Software Palantir.

Der polizeiliche Nutzen der Software für die Ermittlungsarbeit ist erheblich. Die bisherigen Erfahrungen in den Bundesländern sind hier eindeutig und der Nutzen für die Bewältigung von Massendaten ist unbestritten.

Die beabsichtigten Regelungen in § 47a Automatisierte Datenanalyse machen deutlich, welcher politische Diskurs diesen Regelungen zu Grunde liegt. Dies geschieht in diesem Fall durch ein „Konstrukt“, das weder der Klarheit und Transparenz noch der Verständlichkeit dient. Es ist ein Beispiel dafür, wie hoch das Misstrauen der Legislative in die Exekutive und deren Handeln ist. Vieles von dem, was in § 47a Abs. 4 ff. aufgeführt ist, gehört im Grunde genommen in kein Polizeigesetz, zumindest nicht in dieser Art und Weise.

Mit freundlichen Grüßen

Ralf Kusterer
Landesvorsitzender

BBW
Beamtenbund
Tarifunion

BBW - Beamtenbund Tarifunion Am Hohengeren 12 70188 Stuttgart

Ministerium für Inneres, Digitalisierung und
Migration Baden-Württemberg

- per E-Mail -

Am Hohengeren 12
70188 Stuttgart
Telefon: 0711/16876-0
Telefax: 0711/16876-76
Internet:
http//www.bbw.dbb.de
E-Mail: bbw@bbw.dbb.de

20. August 2025
Ha/ge/5955/25

Betreff: Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Bezug: Ihr Schreiben vom 29. Juli 2025, Az.: IM3-1101-44/8/2

Sehr geehrte Damen und Herren,

der BBW - Beamtenbund Tarifunion (BBW) bedankt sich für die Übersendung des Entwurfs eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften und die Gelegenheit zur Stellungnahme.

Der BBW verweist vollinhaltlich auf die Stellungnahme seines Mitgliedsverbands, dem Landesverband der Deutschen Polizeigewerkschaft im Deutschen Beamtenbund (DPolG), die dem Innenministerium direkt zugegangen ist.

Freundliche Grüße

Kai Rosenberger
Vorsitzender

(IM)

Von:	Gundram Lottmann
Gesendet:	Montag, 18. August 2025 08:00
An:	(IM)
Betreff:	EXTERN: WG: Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften - hier: Anhörung
Anlagen:	Anhörungsschreiben.pdf; Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften.pdf

Phishing-Gefahr: Vorsicht bei Links und Anhängen in externen E-Mails!

Guten Morgen Frau

vielen Dank für die Übersendung der Anhörung.

Anbei das Statement der Gewerkschaft der Polizei:

Die Gewerkschaft der Polizei befürwortet die Einführung der Palantir-Software bei der Polizei in Baden-Württemberg.

Palantir erfüllt aus fachlicher Sicht umfassend die Bedarfe der Polizei. Nach über 10 Jahren kontinuierlicher Marktsichtung
wurde wiederholt festgestellt, dass es weltweit keine vergleichbare Software für das ausgeschriebene Anforderungsprofil gibt.
Die Cybercrime-Spezialisten der Polizei kommen unisono zum Ergebnis, dass es kein anderes Produkt mit einem vergleichbaren
Funktionsumfang und einer vergleichbaren Marktreife aktuell gibt.

Palantir ist rechtssicher und datenschutzkonform einsetzbar und der Einsatz wurde bereits zweimal durch das BVerfG überprüft.

Für die polizeiliche Praxis ist Palantir optimal geeignet schwere Straftaten, wie z. B. Kinderpornografie, Rauschgiftschmuggel,
Delikte der Organisierten Kriminalität, Terrorismusstraftaten usw. zu erkennen und Straftäter zu überführen.
In den letzten Jahren kamen zahlreiche Hinweise auf entsprechende Straftaten aus den USA, weil die deutschen Ermittlungsbehörden
über keine entsprechende Software verfügt haben.
Dass dieser Zustand jetzt verändert wird ist rechtsstaatlich geboten und der Staat kommt seiner zentralen Aufgabe, der Pflicht zur
inneren Sicherheit nach.

Nachdem einzelne Bundesländer sich für den Kauf der Palantir-Software entschieden haben, muss als nächster Schritt eine Integration
auf Bundesebene erfolgen.
Aus polizeilicher Sicht ist beim Bundeskriminalamt eine "Bundes-VERA" (mit der Auswertesoftware Palantir) anzustreben, die durch

alle Bundesländer genutzt werden kann, insbesondere durch Integration der vorgehaltenen Datensätze und Schnittstellen.
Neben der Anpassung des Polizeigesetzes Baden-Württemberg muss deshalb auch die Anpassung der Strafprozessordnung für die bundesweite Nutzung
dieser Plattform zu Strafverfolgungszwecken eine hohe Priorität haben.

Mit freundlichen Grüßen

Gundram Lottmann

Landesvorsitzender GdP BW
Mitglied im Hauptpersonalrat der Polizei des IM BW
Mitglied im örtlichen Personalrat PP RT

Gewerkschaft der Polizei
Baden-Württemberg

Sie erhalten nicht häufig E-Mails von Erfahren Sie, warum dies wichtig ist

Sehr geehrte Damen und Herren,

das beigefügte Schreiben nebst Anlage erhalten Sie mit der Bitte um Kenntnisnahme sowie mit der Gelegenheit zur Stellungnahme bis zum 19. August 2025.

Mit freundlichen Grüßen

Ministerium des Inneren, für Digitalisierung und
Kommunen Baden-Württemberg
Referat 35 Recht und Grundsatz

Willy-Brandt-Straße 41
70173 Stuttgart

Internet: im.baden-wuerttemberg.de

Mehr über Baden-Württemberg:
Baden-Wuerttemberg.de | Beteiligungsportal
Instagram | X / Twitter

Bund Deutscher Kriminalbeamter Baden-Württemberg

BDK BW | Parkstraße 1 | D-74889 Sinsheim

Ministerium für Inneres, Digitalisierung und Kommunen

Per E-Mail: poststelle@im.bwl.de

Geschäftsführender Landesvorstand

Ansprechpartner/in: Steffen Mayer
Funktion: Landesvorsitzender

E-Mail:
Telefon:

Datum: 19.08.2025

Anhörung: Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Sehr geehrte Damen und Herren,

wir danken Ihnen für die Einbindung im Rahmen der Anhörung. Der Bund Deutscher Kriminalbeamter, Landesverband Baden-Württemberg, nimmt wie folgt Stellung:

Vorschalten möchten wir, dass wir die Zielsetzung in allen drei Punkten als Berufsverband der Kriminalpolizei ausdrücklich begrüßen.

Im Einzelnen:

Zu § 45a PolG BW: Wir haben keine Anmerkungen, die gesetzliche Regelung ist unumstritten notwendig, schließt eine Lücke und ist als sinnvoll zu bewerten.

Zu § 47a PolG BW: Die zukünftige Möglichkeit zur automatisierten Datenanalyse ist aus Sicht des Bund Deutscher Kriminalbeamter Baden-Württemberg ein dringend erforderliches Instrument. Die Änderung des PolG BW ist die logische Konsequenz aus dem im September 2024 vereinbarten Sicherheits- und Maßnahmenpaket „Sicherheit stärken, Migration ordnen, Radikalisierung vorbeugen“.
Für uns steht außer Frage, dass Ergebnisse aus einer verfahrensübergreifenden Recherche- und Analyseplattform stets am Ende von Menschen bewertet und interpretiert werden müssen. Die Automatisierung (und darum geht es im Kern) stellt eine deutliche Arbeitserleichterung dar, die es bei der Polizei Baden-Württemberg in dieser Form im Jahr 2025 noch nicht gibt. Ein Rechtsstaat muss sich auf die Gegebenheiten unserer Zeit einstellen und Normen auch im Bereich des Polizeirechts sinnvoll weiterentwickeln. In diesem Sinne betrachten wir die geplanten Änderungen als gelungen und notwendig.

Zu § 57a PolG BW: Wir bewerten die Erweiterung des PolG BW in diesem Bereich als erforderlich, um technologisch Schritt zu halten. Künstliche Intelligenz (in allen seinen Ausprägungen) wird unsere Lebens- und Arbeitswelt in den nächsten Jahren maßgeblich beeinflussen. Eine

Bund Deutscher
Kriminalbeamter
Baden-Württemberg

frühe Weichenstellung und Normierung von Nutzungsmöglichkeiten – auch personenbezogener Daten – betrachten wir als notwendigen Schritt, um uns zukunftsfähig aufzustellen.

Zu § 90 PolG BW: Die geplante Unterrichtung des Parlamentarischen Kontrollgremiums sehen wir im Übrigen völlig unkritisch. Polizeiliches Handeln ist in erster Linie stets durch die Judikative überprüfbar; die Einbindung des Parlaments im Sinne der Gewaltenverschränkung erscheint in der zuletzt teils emotional und fernab der Sachlichkeit geführten Diskussion als ein probates Mittel, um diese Diskussion auf die Sachebene zurückzuführen.

Mit herzlichen Grüßen

Steffen Mayer
BDK-Landesvorsitzender Baden-Württemberg

Stellungnahme

Stellungnahme des DGB Baden-Württemberg

Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Aktenzeichen: IM3-1101-44/8/2

19. August 2025

Kontaktperson:

Dominik Gaugler
Abteilungsleiter
Öffentlicher Dienst/Beamte

Deutscher Gewerkschaftsbund
Bezirk Baden-Württemberg
Willi-Bleicher-Str.20
70174 Stuttgart

Sehr geehrte Damen und Herren,

der DGB Baden-Württemberg bedankt sich für die Übersendung des Entwurfes eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Änderungen und nimmt wie folgt Stellung:

Grundsätzlich ist es aus Sicht des DGB Baden-Württemberg richtig und wichtig, Polizei und Ermittlungsbehörden mit modernen Verfahren auszustatten, um die tägliche Arbeit der Kolleginnen und Kollegen bestmöglich zu unterstützen.

In der heutigen Zeit gehören zum modernen Instrumentenkasten der Ermittlungsbehörden auch Methoden der automatisierten Datenanalyse, unter Berücksichtigung des vom Bundeverfassungsgericht gesetzten Rahmen aus dem Jahr 2023. Wenn Bürger*innen das Gefühl haben, dass Sicherheitsbehörden nicht kontrollierbar oder technologisch übermächtig sind, entsteht ein Legitimationsdefizit, und damit ein Vertrauensverlust. Um erfolgreich zu arbeiten, brauchen Behörden ebenso das Vertrauen der Gesellschaft, dass ihr Handeln auf Basis einer legitimen und gültigen rechtlicher Grundlage erfolgt.

Mit dem vorliegenden Gesetzentwurf soll eine solche Grundlage für die automatisierte Datenanalyse geschaffen werden. Damit können personenbezogene Daten aus polizeilichen Systemen künftig zusammengeführt, verknüpft und ausgewertet werden. Dies kann die Ermittlungsarbeit erleichtern, gleichzeitig handelt es sich aber um hochsensible Daten. Deren Schutz ist essenziell, insbesondere wenn externe Software eingesetzt wird, die einen Zugriff auf diese Daten ermöglicht. Der Einsatz von Analysesoftware ist kein technisches Detail, sondern ein Testfall für die Integrität staatlicher Institutionen. Wenn hier Vertrauen verspielt wird, betrifft das die gesamte demokratische Ordnung.

Der bereits erfolgte Vertragsabschluss mit einem externen Anbieter, bevor eine klare Rechtsgrundlage vorlag, ist aus Sicht des DGB Baden-Württemberg problematisch. Bevor die Festlegung auf einen Anbieter erfolgt, müssen Anforderungen, Bedarfe und Rahmenbedingungen in einer entsprechenden Rechtsgrundlage fixiert werden. Dies ist in einem Rechtstaat das Mittel der Wahl, um demokratische Legitimation zu erhalten. Vor dem Hintergrund, dass bereits im Jahr 2023 die Anforderungen des Bundesverfassungsgerichts bekannt waren und bereits im Jahr 2024 sich in der Koalition in Baden-Württemberg auf ein Sicherheitspaket geeinigt wurde, ist nicht nachvollziehbar, weshalb dann im März 2025 ein zeitlicher Druck entstanden ist, der einen vorzeitigen Vertragsabschluss nötig gemacht hat, um Vorteile aus der Kooperation mit Bayern für Baden-Württemberg zu sichern.

Kurzfristige Monopolstellungen lassen sich allerdings nur mittelfristig lösen. Dabei ist es sinnvoll, stärker auf die Entwicklung und Förderung einer europäischen bzw. öffentlichen Softwarelösung zu setzen. Dies würde nicht nur die Abhängigkeit von einzelnen Anbietern reduzieren, sondern auch das Vertrauen in die rechtsstaatliche Kontrolle der sensiblen Datenverarbeitung stärken. Eine gute Rechtsgrundlage kann ein guter Anreiz sein, entsprechende, im besten Fall öffentlich geförderte Projekte, zu generieren und voranzutreiben.

Schwieriger ist aus Sicht des DGB Baden-Württemberg die bereits angekündigte temporäre Nutzung der externen Software. Hier stellen sich Fragen nach der Übergangsphase, der Weiterverwendung von Analysedaten und der Anpassungsfähigkeit der Software an die spezifischen Bedürfnisse Baden-Württembergs. Punkte, die ebenfalls vorab in einer entsprechenden Rechtsgrundlage hätten berücksichtigt werden müssen.

Abschließend lässt sich festhalten, dass das vom Innenministerium gewählte Vorgehen Risiken mit sich bringt und im schlechtesten Fall die Integrität des Rechtsstaates unbeabsichtigt schädigt, anstatt diese zu stärken. Eine bedauerliche Entwicklung, die aus Sicht des DGB Baden-Württemberg hätte verhindert werden können.

Für weitere Rückfragen und Gespräche zum Thema stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Dominik Gaugler

Neue Richter*innenvereinigung
Zusammenschluss von Richterinnen und Richtern,
Staatsanwältinnen und Staatsanwälten e.V.
Landesverband
Baden-Württemberg

NRV – LV BW, RLG Dr. Bleckmann, LG Freiburg, Salzstraße 17, 79100 Freiburg

An das
Innenministerium BW

nur per Mail: poststelle@im.bwl.de

18.08.2025

Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Ihr Zeichen: IM3-1101-44/8/2

Sehr geehrte Damen und Herren,
wir bedanken uns für die Möglichkeit, zum o. g. Gesetzesentwurf Stellung zu nehmen.

Dem Fristlauf geschuldet beschränkt sich die Stellungnahme auf ausgewählte Aspekte der geplanten Gesetzesänderung, die die Rechtsgrundlage für die Nutzung der ohne Parlamentsbeteiligung erworbenen Software „Gotham“ des Anbieters Palantir bilden soll:

- Das Anliegen, in einer zerklüfteten IT-Architektur eine effiziente Suche und Auswertung über die verschiedenen Datenbestände hinweg zu ermöglichen, ist berechtigt und grundsätzlich datenschutz- und verfassungskonform umsetzbar.
- Trotz gegenteiliger politischer Beteuerungen bedeutet die Wahl der konkreten Software des Anbieters Palantir eine Festlegung auf ein Unternehmen, dessen Vorstand offensiv demokratiefeindlich auftritt und dessen Loyalität und Interessen sehr schnell mit denen der Bundesrepublik Deutschland in Konflikt geraten können. Das vorliegende Gesetz dient der Ermöglichung des Einsatzes konkret dieser Software und würde daher den Weg in diese fatale Abhängigkeit bereiten.
- Auch die Vorgeschichte des Gesetzesentwurfs, in der das Innenministerium eine hoch politische und genauso umstrittene Entscheidung, die dem Parlament vorbehalten ist, durch die unabgestimmte Eingehung millionenschwerer Verpflich-

tungen vorweggenommen hat, erweckt grundlegende Zweifel, ob die Ministerialverwaltung im Ausgangspunkt ernsthaft an einer datenschutzkonformen und grundrechtsschonenden Umsetzung interessiert war. Diese Legitimation der Umgehung des Parlaments *ex post* durch Gesetz ist der NRV Anlass zur Warnung vor Gefahren für die Demokratie.

- Der Entwurf ist ersichtlich bemüht, den Anforderungen des Bundesverfassungsgerichts gerecht zu werden. An mehreren Stellen besteht jedoch Nachbesserungsbedarf.
- Schließlich sollte auf eine StPO-Änderung hingewirkt werden, so dass die erlangten Erkenntnisse auch in Strafverfahren wegen besonders schwerer Delikte in vollem Umfang genutzt werden können. Als Deliktskatalog bietet sich der des § 100g Abs. 2 StPO an.

1. Zum grundsätzlichen Bedarf

Die Nutzung der „automatisierten Datenanalyse“ kann im Idealfall zwei Probleme lösen: Zum einen besteht die Hoffnung, dass damit gelingt, was in der Vergangenheit zahlreiche Konsolidierungs- und Integrationsprojekte nicht vermochten: Ein einheitlicher Zugriff auf die diversen Datenbanken, welche historisch gewachsen und daher durch jeweils eigene Zielrichtungen und Datenmodellierungen gekennzeichnet sind, soll ermöglicht werden. Zum anderen sollen die immer größer werdenden Datenmassen nicht nur isoliert ausgewertet werden können, wie es bereits jetzt mit jeweils spezifischen forensischen Tools möglich ist, sondern auch in ihrer Gesamtheit und verknüpft erschlossen werden können. Dabei stellen die Erhebung, Verwendung und Verwertung von Daten(beständen) jeweils eigenständige Grundrechtseingriffe dar, welche in Intensität zunehmen, je mehr Daten miteinander verknüpft werden, weil so ein (möglichst) umfassendes Bild der Zielperson entsteht – bis hin zur gläsernen Bürgerin.

2. Zur Nutzung speziell von Palantir

Je dringender der Bedarf für diese Form der (umfassenden) Auswertung bewertet wird, umso weniger kommt eine Software des Anbieters Palantir Technologies Inc. in Betracht. Sowohl der aktuelle CEO Alex Karp wie auch der aktuelle Verwaltungsratsvorsitzende Peter Thiel haben ihre ablehnende Haltung gegenüber demokratischen Entscheidungsprozessen und damit im Ergebnis gegenüber der freiheitlich-demokratischen Grundordnung wiederholt und unmissverständlich zum Ausdruck gebracht. Gleichzeitig bestehen enge wirtschaftliche und persönliche Verbindungen zur aktuellen US-Administration, welche nunmehr wiederholt die Autorität justizieller Kontrolle missachtet und mit autoritären Machtmitteln die Grenzen der Gewalten durchbrochen hat. Zum Zeitpunkt dieser Stellungnahme besetzt sie widerrechtlich mittels der Nationalgarde

die föderal autonome Hauptstadt Washington D.C. In dieser Konstellation ist es naheliegend, dass im Fall von politischen Spannungen Service und Support einseitig beendet werden, wie es der Internationale Strafgerichtshof hinsichtlich der Nutzung von Outlook bereits erfahren musste. Dabei dürfte die Frage einer formalen Anordnung durch die Regierung ebenso wenig eine Rolle spielen wie die genaue Reichweite von Auskunfts- und Mitwirkungspflichten einzelner Konzerntöchter nach US-Recht. Selbst wenn man entsprechend der Auskunft des Softwareanbieters, welche nicht durch deutsche Expert*innen überprüft wurde – und werden kann –, der Integrität der polizeilichen IT-Systeme, auf denen die Software betrieben werden soll, insoweit vertraut, dass weder ein Datenabfluss, noch die Aktivierung eines "Kill Switches" möglich wären, darf man sich nicht der Illusion hingeben, dass eine derartige Software mittelfristig ohne Unterstützung des Anbieters zu betreiben ist. Die Einführung der Palantir-Software kann dabei auch nicht als Brücke zu einer eigenständigen Neuentwicklung dienen. Der Logik staatlicher IT-Projekte folgend ist die Nutzung von "Gotham" zum Erfolg verdammt, um die hohen Kosten und den Einführungsaufwand zu rechtfertigen. Mit der Einführung dieser kostspieligen Software entfällt daher auch jeder Anreiz, auf eine langfristige eigenständige Lösung hinzuarbeiten. Schließlich verbietet sich aus urheberrechtlichen Gründen, die Software oder auch nur Teile davon, nachzuahmen. Etablierte Verfahren werden deshalb zukünftig kaum (freiwillig) umgestellt werden.

3. Zur Vorgeschichte des Gesetzentwurfs

Als problematisch erweist sich des Weiteren der Hergang der Beschaffung der Software „Gotham“. Obwohl nach der Rechtsprechung des Bundesverfassungsgerichts der Einsatz von Massendatenauswertungssoftware einer besonderen – und eng zu begrenzenden – Ermächtigungsgrundlage bedarf, welche mit dem vorliegenden Entwurf geschaffen werden soll, ging das Innenministerium eigenmächtig und ohne vorherige Parlamentsbeteiligung bereits Verpflichtungen mit Palantir ein. Diese Vorgehensweise setzt den Landtag als Gesetzgeber unter Zugzwang: Entweder wird die illegitime Vorgehensweise des Ministeriums nachträglich gesetzlich gebilligt. Dann schafft das Parlament einen Präzedenzfall, welcher weitere eigenmächtige Vorentscheidungen der Exekutive in der Zukunft erwarten lässt. Alternativ lehnt der Landtag die hiesige Gesetzesinitiative ab, muss dann aber die Verschwendung von Steuergeldern in Millionenhöhe verantworten. Dem Landtag verbleibt so keine echte Entscheidungsmacht, sondern steht vielmehr vor einer Pattsituation der „Alternativlosigkeit“. Auch wenn die letztgenannte Handlungsoption dem Haushalt massiven Schaden zufügt, ist sie vorliegend angesichts der Bedenklichkeit der gegenständlichen Software und zur Begrenzung exekutiver Alleingänge geboten. Ob der Schaden durch einen Regress gemildert werden kann, dürfte gesonderter Prüfung zuzuführen sein.

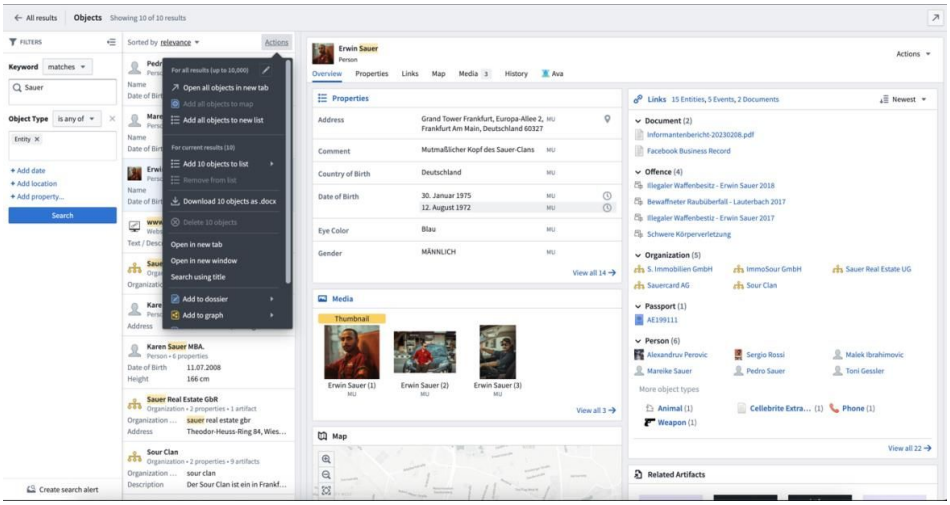
4. Zur Funktionsweise von Palantir

Auch wenn der Gesetzentwurf äußerlich von der bereits gekauften Software abstrahiert, ist ein Grundverständnis der Software sinnvoll, um den intendierten Regelungscharakter zu erfassen:

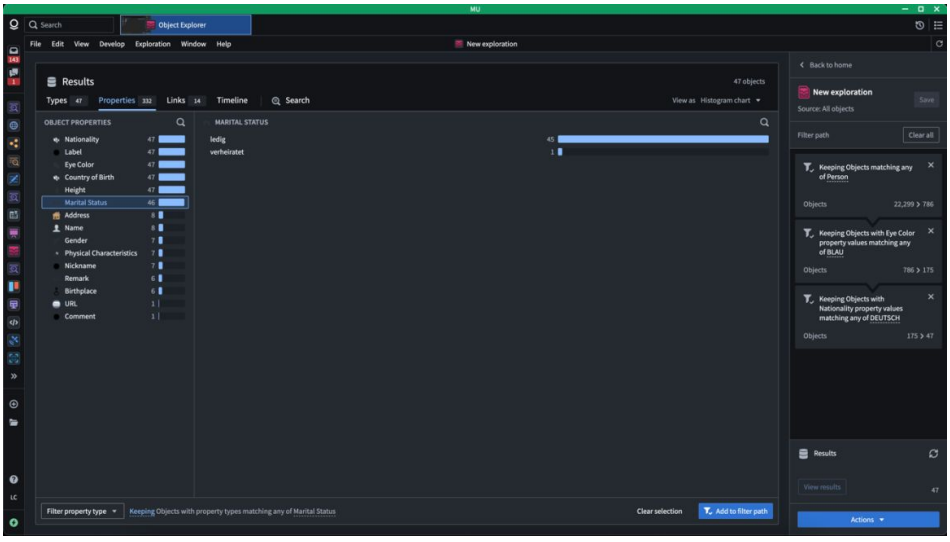
Gotham überführt Daten aus den verbundenen Datenbanken in eine eigene Datenbank. Nach der Eigendarstellung nutzt diese ein sog. flexibles Informationsmodell, in dem Informationen als Objekte, die an realen Konzepten angelehnt sind (etwa Personen, Organisationen, Dokumente, Orte und Ereignisse), sowie Beziehungen zwischen diesen Objekten gespeichert werden. Palantir nennt dieses flexible Modell „Ontology". Strukturierte Daten aus den angeschlossenen Datenbanken werden in die Zieldatenbank übertragen, wobei einzelne Felder von den Quell- in die Zieldatenbanken übersetzt („gemappt") werden müssen. Soweit diese Systeme auch in anderen Bundesländern zum Einsatz kommen, sollte dieser Prozess abgeschlossen sein. Palantir nimmt für sich weiter in Anspruch, auch aus unstrukturierten Daten strukturierte Informationen extrahieren zu können. An dieser Stelle wäre der (spärlich konkret dokumentierte) Einsatz von KI als Funktionsbaustein von Gotham zu erwarten. Sowohl dieser Vorgang als auch die Darstellung sind hochkomplex, da beispielsweise sich widersprechende Informationen aus verschiedenen Quellen oder zeitliche Verläufe erkannt und in übersichtlicher, aber nicht verkürzender Weise dargestellt werden müssen. Die Nutzer*innen erschließen sich die Daten über verschiedene Apps.[1]

[1]Die folgenden Zitate und Bilder sind aus der Dokumentation von Palantir für die Transparenz-Plattform der britischen Regierung entnommen: Palantir Platform – Gotham: Service Definition Document (G-Cloud 14 Framework), S. 5 ff; zuletzt abgerufen am 15.08.2025: https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/804537709233305.

5



*Zentral im deutschen Kontext dürfte der **Browser** sein, der es „den Nutzern ermöglicht, Informationen zu einzelnen Objekten innerhalb der Datenstruktur der Plattform („Ontology“) zu betrachten und zu bearbeiten“.*



Mit dem Objekt Explorer lässt sich der Datenbestand mit Filtern und Kategorien durchforsten. Palantir nutzte für die Dokumentation in Großbritannien offensichtlich einen deutschen Beispielsdatensatz. Im Beispiel wird der Datenbestand auf alle ledigen deutschen Staatsbürger mit blauen Augen gefiltert.

Daneben existieren weitere Apps wie „Graph“ für Netzwerkdarstellungen oder „Gaia“ für kartenbasierte Visualisierungen. Informationen zu den Apps für delikatere Aufgaben „such as targeting, fires control and execution, ISR, and ISINT analysis“ werden nicht öffentlich erläutert.

Die tatsächliche Leistungsfähigkeit der Software kann mangels Transparenz nicht beurteilt werden, nach allgemeiner Erfahrung ist hier jedoch Skepsis sowohl gegenüber den Versprechen der Anbieter wie auch den Erfolgsmeldungen aus dem Projekt selbst angebracht, das stets die Tendenz hat, seine eigene Existenz zu legitimieren. Eine unabhängige Evaluation sollte daher nicht nur ermöglicht, sondern auch vorgeschrieben werden. Diese Evaluation muss sich nicht nur auf die Nutzbarkeit und Nutzerfreundlichkeit, sondern auch und gerade auf die Grundrechtssensibilität der Nutzung erstrecken. Das heißt: Sie muss Einblick in die Softwareinfrastruktur nehmen (können), um Hintertüren, Datenabflüsse (bzw. Sicherheitsschwachstellen) und (verfassungs-)rechtlich nicht eröffnete Verarbeitungsvorgänge identifizieren und eliminieren zu können.

5. Zum Gesetzentwurf selbst

Der Gesetzentwurf selbst und seine Begründung bemühen sich sowohl rhetorisch wie auch inhaltlich, den Vorgaben des Bundesverfassungsgerichts Rechnung zu tragen:

Das System abgestufter **Eingriffsvoraussetzungen** mit korrespondierenden Auswertemöglichkeiten ist grundsätzlich zu begrüßen, aber **nicht vollständig konsistent**: So verlangt etwa § 47a Abs. 1 Nr. 1 PolGE die Abwehr einer (einfachen) Gefahr für bestimmte Rechtsgüter. Die Eingriffsschwelle soll laut der Begründung (S. 24) an enge Voraussetzungen geknüpft sein, „wie sie allgemein für eingriffsintensive Maßnahmen gelten“. Tatsächlich verlangt die korrespondierende Eingriffsschwelle zur Erhebung von Telekommunikationsdaten, § 54 Abs. 1 Nr. 1 PolG, eine *dringende und erhebliche Gefahr*. Ein Gleichlauf ist umso wichtiger, als bei einer Maßnahme nach § 47a Abs. 1 Nr. 1 PolGE auch Telekommunikationsdaten verarbeitet werden sollen.

§ 47 Abs. 2 PolGE enthält im Wesentlichen kaum operationalisierbare Prosa. Wie schmal der Grat zwischen sachgerechter Auswertung und Diskriminierung ist, zeigt bereits die oben abgebildete Bebilderung von Palantir selbst. Die Arbeit mit phänotypischen Merkmalen kann zwar grundsätzlich erforderlich sein, etwa wenn eine Personenbeschreibung vorliegt. Dass Palantir allerdings kein besseres, an einem realistischen Einsatzszenario ausgerichtetes Beispiel für die Filterfunktion eingefallen ist als die Anzeige aller ledigen Deutschen mit blauen Augen, zeigt die Tendenz zu einem an Vorstellungen rassisch-ethnischer Klassifizierung diskriminierenden Schubladendenken.

An verschiedenen Stellen fehlen gesetzliche Definitionen innerhalb des Polizeigesetzes, die zur Gewährleistung der Normenklarheit entscheidend wären, insbesondere die Einbeziehung von „**Falldaten**“ (§ 47 Abs. 3 Var. 2 PolGE) ist problematisch: Gemeint sind nach der Begründung Exporte aus polizei-internen Hilfsprogrammen (beispielsweise

Analyst's Notebook). Dies findet jedoch keinen Anker im Wortlaut. Ihre **Einbeziehung ist auch in der Sache nicht sinnvoll**: Derartige Programme dienen den Ermittlern als digitales Skizzenbuch, um sich unkompliziert einen Überblick zu verschaffen. Notiert werden aktenkundige Informationen ungeachtet ihrer genauen Herkunft, noch ungesicherte Erkenntnisse oder auch nur Fallhypothesen. Sollten diese Dateien in die Auswertung einbezogen werden, müsste jede Information der Falldatei mit Kennzeichnungen der Herkunft versehen oder eine Klassifizierung als Annahme/Hypothese eingeführt werden, was dem Sinn der Falldateien als unkompliziertem Tool zuwiderliefe. Denn ohne Kennzeichnung bestünde die Gefahr, dass eigentlich nicht verwendbare Informationen beispielsweise aus Telekommunikationsdaten (im Falle des § 47 Abs. 1 Nr. 3 PolGE) oder zu Unbeteiligten über den Umweg der Falldatei doch in die Auswertung einbezogen oder gar Fehlannahmen zur Grundlage einer polizeirechtlich relevanten Gefahrenbewertung gemacht würden.

Der Erlass einer öffentlich bekannt gemachten Verwaltungsvorschrift setzt eine zentrale Forderung des BVerfG um. Problematisch hierbei ist, dass auch Altsysteme angeschlossen werden sollen, die nach § 72 Abs. 4 PolG von der Kennzeichnungspflicht ausgenommen sind. Gleichzeitig sind etwa Telekommunikationsdaten auch nicht anhand ihrer Datenquelle zuverlässig erkennbar, da sie nicht nur aus der TKÜ-Software direkt übernommen werden, sondern in Form von Protokollen und Vermerken auch in den Vorgangs- und Falldaten gespeichert sein können. Wie in diesen Fällen die Kennzeichnungen möglich sein sollen, ist unklar. An dieser Stelle offenbart sich ganz konkret, warum es eine schlechte Idee ist, zuerst eine Software zu beschaffen und erst im Anschluss die Anforderungen zu definieren. Sinnvollerweise hätten die datenschutzrechtlichen Anforderungen zuerst bestimmt werden müssen, um die Software, die ja mit Überschneidungen in den Quelldatenbanken (Polas und Comvor) bereits in anderen Bundesländern im Einsatz ist, auf diese Anforderung hin zu überprüfen. Um zumindest sicherzustellen, dass das Ergebnis einer genaueren Prüfung im Rahmen der Erstellung der Verwaltungsvorschrift nicht sein kann, dass auch bei Gotham eine Kennzeichnung leider im Sinne des § 72 Abs. 4 PolG „einen unverhältnismäßigen Aufwand erfordern" würde und daher entbehrlich ist, sollte der **Rückgriff auf § 72 Abs. 4 PolG explizit ausgeschlossen werden**. Weiter sollte die Selbstverständlichkeit gesetzlich normiert werden, dass die **Verwaltungsvorschrift vor dem Einsatz im Echtbetrieb veröffentlicht wird**.

Die Systematik der Personenkategorien ist in mehrfacher Hinsicht unglücklich:

- Zunächst werden Kategorien definiert, welche von § 70 PolG abweichen. Es sind solche Variationen, die zur Zerklüftung der IT-Landschaft beitragen, die wiederum nachträglich durch den Einsatz einer Software wie Gotham geglättet werden sollen.
- Die „Anlassperson“ wird in § 70 Nr. 3 PolG umschrieben, ohne sie dort als „Anlassperson“ zu bezeichnen. Eine Legaldefinition wäre durch einen einfachen Klammerzusatz möglich (vgl. § 18 Abs. 1 Nr. 4 BKAG).
- Zentral wäre weiter eine exakte Definition der Art des Kontakts, der eine Person zur „Kontaktperson“ im Sinne des § 47a Abs. 6 PolGE macht. Der Begriff des Kontakts wird auch in § 70 Nr. 4 PolG vorausgesetzt statt definiert. Ohne diese Definition droht praktisch eine extensive Auslegung dieses Begriffs, da nach dem Wortlaut beispielsweise schon das Opfer einer Straftat mit dem Täter in Kontakt steht. Der Kontakt muss also qualifiziert sein, will man dem in der Begründung zitierten Anspruch des BVerfG gerecht werden, nur solche Personen in die Analyse einzubeziehen, die dies durch ihr (willensgetragenes) Verhalten im polizeirechtlichen Sinne zurechenbar veranlasst haben.
- Weiter sollte positiv geregelt werden, welche Personengruppen in der Auswertung berücksichtigt werden dürfen. Auf diese Weise wäre innerhalb der Software sichergestellt, dass nur solche Informationen in die jeweilige Auswertung einfließen können, die eine entsprechende positive Kennzeichnung tragen.
- Schließlich ist § 47a Abs. 6 S. 3 PolGE unklar: Die Einschränkung kann entweder (zu) weit verstanden werden in dem Sinne, dass Informationen aus einem Vorgang nicht ausgewertet werden dürfen, in dem eine Person unbeteiligt war – selbst dann, wenn diese Person Anlass für die Auswertung gegeben hat. Umgekehrt könnte sie auch so verstanden werden, dass eine Person ihren Status als Unbeteiligter verliert, wenn sie in irgendeinem vergangenen Vorgang als Anlassperson erfasst wurde. In der Diktion von Gotham formuliert: Der Status als Unbeteiligter oder als Anlassperson ist kein Attribut einer Person, sondern eine Beziehung zwischen einer Person und einem Vorgang (und muss für jede Einzelinformation entsprechend ihres Herkunftsvorgangs mitgeführt werden). Die verschiedenen Konstellationen (Zielperson der Suche ist in den historischen Vorgängen unbeteiligt/Nicht-Zielperson ist in einem historischen Vorgang Anlassperson, in anderen unbeteiligt/Nicht-Zielperson ist in keinem historischen Vorgang als Anlassperson erfasst) müssen als wesentliche Regelungen in das Gesetz aufgenommen werden.
- Entgegen der Begründung des Gesetzesentwurfs (S. 32) sind die in Abs. 6 S. 4 und 5 genannten Anforderungen an die zu erlassende Verwaltungsvorschrift nicht geeignet, das Eingriffsgewicht zu reduzieren, da die einschränkenden Vor-

gaben in ihren grundlegenden Zügen im Gesetz selbst geregelt werden müssen (Art. 80 Abs. 1 GG).

6. Anforderungen systematischer Kohärenz

Weiter muss, auch über den konkreten Gesetzentwurf und die Kompetenz des Landesgesetzgebers hinaus, die Verwertbarkeit der gewonnenen Erkenntnisse im Strafverfahren sichergestellt werden. Zwar dient der Einsatz der gegenständlichen Software nach der Konzeption des Entwurfs der polizeilichen Gefahrenabwehr. Allerdings dient diese regelmäßig der Verhütung (schwerer) Straftaten. Nicht immer gelingt es, Straftaten vor ihrer Begehung zu verhüten; gerade im Bereich der Terrorismusabwehr sind im Vorfeld der geplanten Tat zumindest §§ 129 ff. StGB verwirklicht und zu verfolgen. Nachdem die vorliegende Datenerhebung und -verarbeitung zu präventiven Zwecken erfolgt, setzt eine repressive Nutzung eine Ermächtigungsgrundlage zur Datenumwidmung und eine geeignete Ermächtigungsgrundlage zur Entgegennahme der zweckumgewidmeten Daten in der Strafprozessordnung voraus (sog. Doppeltürmodell). Dabei müssen diese Ermächtigungsgrundlagen der Eingriffstiefe der zugrundeliegenden Datenerhebung und -verarbeitung Rechnung tragen. Solche Ermächtigungsgrundlagen fehlen.

§ 15 Abs. 3 PolG verlangt zwar „entsprechend schwerwiegende“ Straftaten und begrenzt damit die Datenweitergabe jedenfalls *prima facie*. Doch zunächst ist zu konstatieren, dass die geforderte Entsprechung (normenklar) nicht bestimmt werden kann, ist doch die Bezugsgröße im Polizeigesetz eine schutzgutsbezogene *Gefahr* und gerade keine Strafnorm. Dringende Gefahren für Leib und Leben drohen auch, wenn eine einfache Körperverletzung i.S.d. § 223 Abs. 1 StGB unmittelbar bevorsteht. Soll diese nun „entsprechend schwerwiegend“ i.S.d. Norm sein? Wie das Bundesverfassungsgericht zuletzt hinsichtlich § 100a Abs. 1 S. 2 StPO anmahnte, ist die Regelung eines (geschlossenen) Tatenkatalogs durch statische Verweisung auf das StGB und strafrechtliche Nebengesetze bereits im Polizeigesetz geboten, um der Pflicht zur normativen Begrenzung des schwerwiegenden Grundrechtseingriffs Rechnung zu tragen. Als konkreter Straftatenkatalog bietet sich der des § 100g Abs. 2 StPO an.

Weil eine Eingangsnorm bzw. eigene strafprozessuale Ermächtigungsgrundlage fehlt, können Erkenntnisse aus Maßnahmen nach § 47a PolGE nicht unmittelbar zum Beweismittel im Strafverfahren gemacht werden. Zwar steht dies grundsätzlich einer Verwendung als Spurenansatz zur Durchführung weiterer Ermittlungen zur Gewinnung neuer Beweismittel nach h.M. nicht entgegen (Sackreuther, BeckOK StPO, § 161 Rn. 16 mit Verweis auf BVerfG NJW 2005, 2766; BVerfG, NJW 2016, 1781, Rdnr. 315 (BKA-Entscheidung)). Allerdings erhöht dies wiederum die Anforderungen an die Ausgangsnorm im PolG (vgl. BVerfG, aaO., Rdnr 315), was die Bedenken hinsichtlich der Normbestimmtheit des § 15 Abs. 3 PolG verschärft. Gleichzeitig ist nicht ausgeschlossen, dass polizeiliche Auswertungsergebnisse auch am Ende eines sich daraus entwickelnden Strafverfahrens noch unmittelbar als (Indiz-)tatsachen benötigt werden. Spätestens hier ist eine

eigene Eingangsnorm in der StPO erforderlich, wie sich erst recht aus § 161 Abs. 3 S. 1 StPO ergibt. Die Regelung in der Strafprozessordnung sollte mit den Voraussetzungen der Datenweitergabe korrespondieren und ist über den Bundesrat anzustoßen.

Ob mit Gotham grundsätzlich und mit den konkret geplanten Bestandsdatenquellen eine verfassungskonforme Umsetzung möglich ist, kann von außen nicht beurteilt werden. Umso wichtiger wäre es, eine Evaluation nicht nur zu ermöglichen, sondern auch eine institutionell unabhängige Evaluation sowohl im Hinblick auf die Leistungsfähigkeit wie auch im Hinblick auf die datenschutzkonforme Umsetzung vorzuschreiben.

Mit freundlichen Grüßen

Simon Pschorr

Staatsanwalt
Sprecher der Fachgruppe Strafrecht
Für den Landesverband Baden-Württemberg der Neuen Richter*innenvereinigung

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

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

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

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

E-Mail: geschaeftsfuehrung@av-bw.de

AnwaltsVerband BW, Kissinger Str. 49, 70372 Stuttgart

Ministerium des Inneren, für Digitalisierung und Kommunen
Baden-Württemberg
Referat 35 - Recht und Grundsatz

Willy-Brandt-Straße 41
70173 Stuttgart

19. August 2025

Per E-Mail: poststelle@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

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.

Registergericht: Amtsgericht Stuttgart VR 3334
Präsident: RA Prof. Dr. Peter Kothe, Vizepräsident: RA Detlev Heyder, Schatzmeister: RA Dr. Guido Toussaint

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

18. August 2025

Stellungnahme

zum Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Von Franziska Görlitz

Volljuristin und Verfahrenskoordinatorin bei der Gesellschaft für Freiheitsrechte e.V.

Der Gesetzesentwurf dient der der Schaffung von Befugnissen zur Erhebung, Verarbeitung und Übermittlung von Standortdaten, zur eigenständigen Entwicklung von informationstechnischen Systemen und zur automatisierten Datenanalyse im Polizeigesetz Baden-Württemberg. Die vorliegende Stellungnahme beschränkt sich auf den Entwurf einer Rechtsgrundlage für eine automatisierte Datenanalyse in § 47a des Entwurfes und dessen Vereinbarkeit mit verfassungsrechtlichen Vorgaben.

§ 47a PolG BW-E schafft eine Rechtsgrundlage für automatisierte Datenanalysen zur Gefahrenabwehr und Verhinderung von Straftaten in drei verschiedenen Tatbestandsvarianten (§ 47a Abs. 1 Nr. 1-3 PolG BW-E).

Polizeiliche Datenanalysen stellen auch bei verfassungskonformer gesetzlicher Ausgestaltung erhebliche Grundrechtseingriffe dar. Die Analyse enormer Mengen polizeilicher Daten aus verschiedenen Datenbanken mit komplexen Algorithmen führt zu nicht nachvollziehbaren Analyseergebnissen. Die Analysen erfolgen heimlich ohne Kenntnis der Betroffenen. Es besteht die Gefahr, dass durch Fehler und diskriminierende Analysevorgänge auch Personen in polizeilichen Fokus geraten, die dafür keinen Anlass geboten haben. Gleichzeitig ist die Effizienz und Wirksamkeit polizeilicher Datenanalysen zur Gefahrenabwehr bislang nicht nachgewiesen. Aus diesem Grunde ist die Schaffung von Rechtsgrundlagen für methodenoffene Analysen und automatisierte Erkenntnisgewinne insgesamt kritisch zu sehen.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

Zusammenfassung:

Der vorliegende Entwurf orientiert sich erkennbar an den Maßstäben des Bundesverfassungsgerichts aus der Entscheidung vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20), setzt diese jedoch nicht hinreichend um. Bei der vorgesehenen Datenanalyse aller Tatbestandsvarianten handelt es sich um einen schwerwiegenden Grundrechtseingriff, da die gesetzlichen Einschränkungen der Datenanalyse nicht ausreichend sind, um das Eingriffsgewicht maßgeblich zu reduzieren. Weiterhin ist die Einhaltung der Grundsätze der Zweckbindung und Zweckänderung nicht ausreichend sichergestellt. Die vorgesehenen Eingriffsschwellen und zu schützenden Rechtsgüter in § 47a Abs. 1 Nr. 2 und 3 des Entwurfs genügen nicht zur Rechtfertigung der weitgehenden Datenanalysen. Es fehlen hinreichende tatsächliche Vorkehrungen gegen Diskriminierung und zur Erkennung und Vermeidung von Fehlern. Der Entwurf genügt insgesamt dem Gesetzesvorbehalt und dem Wesentlichkeitsgrundsatz sowie den Anforderungen an Bestimmtheit und Normenklarheit nicht, da für grundrechtswesentliche Bereiche die durch den Gesetzgeber vorzunehmenden Abwägungen an die Verwaltung durch Verwaltungsvorschriften ausgelagert werden.

Rechtliche Bewertung der Regelungen im Einzelnen

A. Verfassungsrechtlicher Maßstab

Datenzusammenführungen und -analysen auf Grundlage bereits erhobener personenbezogener Informationen stellen selbstständige Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) dar und bedürfen daher einer spezifischen Ermächtigungsgrundlage.[1] Dabei hängen die Anforderungen an die verfassungsrechtliche Rechtfertigung[2] von der Eingriffsintensität ab. Unter Berücksichtigung der Wesentlichkeitstheorie und den Grundsätzen der Bestimmtheit und Normenklarheit müssen sich Beschränkungen der Eingriffsintensität hinreichend bestimmt und normenklar im Gesetzeswortlaut niederschlagen.

Maßgeblich für die Eingriffsintensität sind insbesondere Art und Umfang der verarbeiteten Daten sowie die konkrete Methode der Auswertung.[3] Je umfangreicher und sensibler die verwendeten Daten, je komplexer, weitreichender und intransparenter die eingesetzte Analysemethode und je größer die daraus resultierende Missbrauchsgefahr, desto schwerer ist das Eigengewicht des Eingriffs[4] und desto höher sind in der Folge die Rechtfertigungsanforderungen[5]:

---

1 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 50 f.
2 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 51, 72 ff.
3 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 75 ff.
4 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 76 ff.
5 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 71 ff.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

Befugnisse zur Durchführung von Datenanalysen, die sich als besonders schwerwiegende Grundrechtseingriffe darstellen, sind nur unter den engen Voraussetzungen zu rechtfertigen, die das Bundesverfassungsgericht allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen entwickelt hat.[6] Derartige Maßnahmen sind nur im Falle einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter wie zum Beispiel Leib, Leben, Freiheit oder Bestand und Sicherheit des Staates zulässig.[7] Weniger eingriffsintensive Maßnahmen unterliegen abgestuften Anforderungen: Sie können entweder bei einer konkretisierten Gefahr für zumindest erhebliche Rechtsgüter oder bei einer noch nicht konkretisierten Gefahr im Vorfeld zum Schutz besonders gewichtiger Rechtsgüter gerechtfertigt sein.[8] Lediglich bei nur geringfügigen Eingriffen – etwa bei einem automatisierten Datenabgleich, der in Ablauf und Verarbeitungsergebnis mit einem händischen Abgleich vergleichbar ist – genügt die Wahrung des Grundsatzes der Zweckbindung für eine Rechtfertigung.[9]

Das Bundesverfassungsgericht hebt darüber hinaus die verfassungsrechtlichen Anforderungen an den Gesetzesvorbehalt und den Wesentlichkeitsgrundsatz hervor.[10] Für grundrechtswesentliche Entscheidungen – insbesondere solche über die Begrenzung der Art und Menge der Daten, die Wahl der zulässigen Auswertungsmethoden, die Einbeziehung technischer Systeme sowie Regelungen zur Dokumentation, Kontrolle und Nachvollziehbarkeit – muss der Gesetzgeber entsprechend dem Gesetzesvorbehalt die grundrechtswesentlichen Entscheidungen selbst treffen.[11] Zwar kann der Gesetzgeber Ermächtigungen zur Ausgestaltung technischer und organisatorischer Einzelheiten an die Verwaltung delegieren, die grundlegenden Einschränkungen müssen jedoch durch Gesetz hinreichend bestimmt vorgesehen sein.[12] Je höher die Eingriffsintensität, desto höher sind hierbei die Anforderungen an Bestimmtheit[13] und Normenklarheit, die sowohl inhaltliche Verständlichkeit und Vorhersehbarkeit der Eingriffsbefugnisse[14] als auch effektive gerichtliche Kontrolle gewährleisten sollen.[15]

6 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 104 ff.
7 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 104 ff.
8 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 107.
9 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 108.
10 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110.
11 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110, 112 ff.
12 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 112 ff.
13 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 115, 120.
14 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110, 114.
15 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 109.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

B. Wahrung dieser Grundsätze

I. Eingriffsgewicht der Maßnahmen

In der vorliegenden Entwurfsfassung stellen alle Varianten der vorgesehenen Datenanalyse in § 47a Abs. 1 Nr. 1-3 PolG BW-E schwerwiegende Grundrechtseingriffe dar, sodass die im Entwurf vorgesehenen Eingriffsschwellen und die zu schützenden Rechtsgüter zur Rechtfertigung des Eingriffs nicht genügen. Das Eingriffsgewicht der Datenanalyse ist **mangels ausreichend bestimmter und normenklarer Einschränkung** durch den Gesetzgeber selbst nicht ausreichend gemildert.

1. Art. 47a Abs. 1 Nr. 1 PolG BW-E

Die Datenanalyse gemäß § 47a Abs. 1 Nr. 1 PolG BW-E stellt einen **schwerwiegenden Grundrechtseingriff** dar, da sowohl Art und Umfang der einbezogenen Daten als auch die Methode der Datenanalyse nicht zureichend einschränkt sind.

a. Art und Umfang der Daten

Der vorliegende Entwurf begrenzt weder Art noch Umfang der analysierten Daten ausreichend, um das Eingriffsgewicht der Datenanalyse maßgeblich zu beschränken.

Positiv ist zunächst zu bewerten, dass § 47a Abs. 3 PolG BW-E in Satz 1 und 2 eine abschließende Regelung sowohl der in jedem Falle zusammengeführten Daten (Satz 1) als auch der Daten vorsieht, die im Einzelfall händisch der Analyse hinzugefügt werden können (Satz 2). Für die Analyse dauerhaft zusammengeführt werden dürfen gemäß § 47a Abs. 3 Satz 1 des Entwurfs jedoch insbesondere **Vorgangsdaten und Falldaten** und damit umfangreiche Datenbanken, die teils noch nicht fachlich beurteilte Datensätze enthalten. Diese umfassen zu einem erheblichen Teil auch Daten von Personen, die **keinen Anlass** dafür geboten haben, einer polizeilichen Maßnahme ausgesetzt zu werden, beispielsweise Daten von Zeug*innen, Betroffenen von Straftaten, vermissten Personen oder Hinweisgeber*innen und Anzeigeerstatter*innen. Auch können darin Daten von besonders schützenswerten Kontaktpersonen wie Anwält*innen und Journalist*innen enthalten sein. Die Auflistung stellt daher nur eine geringe Einschränkung des Eingriffsgewichtes dar.

Hieran ändert auch § 47a Abs. 6 Satz 3 PolG BW-E nichts, wonach durch Vorgaben einer Verwaltungsvorschrift zum Schutz unbeteiligter Personen sichergestellt werden soll, dass deren personenbezogene Vorgangsdaten nicht in die Analyse einbezogen werden. Diese Trennung ist bei einer automatisierten Zusammenführung nach § 47a Abs. 1, Abs. 2 Satz 1 PolG BW-E nicht verlässlich möglich, da in den Vorgangssystemen schon aufgrund des Zwecks solcher Systeme – anfallende Informationen, zum Beispiel Anfragen oder Anzeigen, zunächst lediglich in geordneter

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

Form aufzubewahren – nicht zwischen Daten beteiligter oder unbeteiligter Personen unterschieden wird. Zudem stimmen die in § 47a Abs. 6 Satz 2 PolG BW-E vorgesehenen Kategorien der „einerseits verurteilten, beschuldigten, verdächtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen" nicht mit den für die polizeiliche Datenverarbeitung allgemein vorgesehenen Kategorien in § 70 Abs. 1 PolG BW überein. Hier wird gerade keine übergreifende Kategorisierung unbeteiligter Personen vorgesehen.

Darüber hinaus sieht der Entwurf **weder eine Beschränkung auf nur polizeilich erhobene Daten noch eine Beschränkung auf nur durch das Land Baden-Württemberg oder nur inländische Behörden erhobene Daten** vor. Nach § 47a Abs. 3 Satz 1 des Entwurfs dürfen zwar nur „eigene" Daten zusammengeführt werden. Damit ist aber nur die **Speicherung** durch die baden-württembergische Polizei und eben nicht die Erhebung der Daten durch diese sichergestellt (S. 24 des Entwurfs). Gerade auch durch die genannten Daten aus polizeilichen Auskunftssystemen und Daten aus dem polizeilichen Informationsaustausch, insbesondere aus dem polizeilichen Verbundsystem INPOL, können auch zulässigerweise übermittelte Daten von inländischen oder ausländischen Nachrichtendiensten in die Analyse geraten.

Ebenso sind in § 47a Abs. 3 Satz 2 des Entwurfs für die **ergänzende händische Aufnahme von Daten** mit Verkehrsdaten und Daten aus Asservaten riesige, auch ungefilterte Datenmengen erfasst, wobei insbesondere Telekommunikationsdaten und Daten aus Funkzellenabfragen zu hohem Anteil Daten von bisher unbeteiligten Personen enthalten.

Die **Beschränkungswirkung** der abschließenden Auflistung der Daten ist damit **gering**. Dies gilt umso mehr, da das Gesetz keine Beschränkung für das ergänzende Hinzufügen von Daten nach § 47a Abs. 3 Satz 2 PolG BW-E vorsieht, sodass **beliebig immer weitere Daten** hinzugefügt werden können.

Die Analyseplattform darf zwar gemäß § 47a Abs. 2 Satz 6 des Entwurfs **nicht direkt mit dem Internet** verbunden werden. Gleichzeitig ist es aber nach § 47a Abs. 3 Satz 2 des Entwurfs explizit möglich, **Daten aus dem Internet**, insbesondere Informationen aus **sozialen Medien**, und aus anderen staatlichen Registern in die Analyse einzuführen. Dies erhöht das Eingriffsgewicht erheblich, auch weil die hinzugefügten Daten im Analysesystem verbleiben.

Als einzige explizite Einschränkung nimmt § 47a Abs. 3 Satz 6 des Entwurfs personenbezogene Daten aus Wohnraumüberwachungen und Onlinedurchsuchungen aus. Daten aus anderen **schwerwiegenden Grundrechtseingriffen** wie u.a. dem Einsatz verdeckter Ermittler*innen und Vertrauenspersonen, längerfristigen Observationen, Telekommunikationsüberwachungen und Verkehrsdatenabfragen[16] sind jedoch nicht ausgenommen. Telekommunikationsdaten und Daten

[16] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 176.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

aus Funkzellenabfragen sind vielmehr explizit in § 47a Abs. 3 Satz 2 des Entwurfs erwähnt und nur für Analysen nach Absatz 1 Nr. 3 ausgeschlossen.

Die Menge der umfassten Daten wird ebenfalls nicht dadurch eingeschränkt, dass nur Daten zu näher eingegrenzten Straftaten aufgenommen werden dürfen. Zudem können Daten nicht nur rein händisch hinzugezogen, sondern zu großen Teilen automatisiert zusammengeführt werden. Ebenso sieht das Gesetz selbst keine ausreichende Sicherung der Grundsätze der Zweckbindung und Zweckänderung vor (hierzu sogleich unter c. und e.).

Hinsichtlich der **Art der Daten** enthält der Entwurf keine Einschränkungen. So können besonders sensible Daten wie **biometrische Daten, Screenshots** von Kommunikationen, **Bilder und Videos** ohne Beschränkungen einbezogen werden. Zudem enthält die Norm keine tatsächlichen Einschränkungen zum Schutz von besonders diskriminierungssensiblen Daten.

b. Methode der Datenanalyse

Auch hinsichtlich der zugelassenen Methoden der Datenanalysen ist der Entwurf weit formuliert und enthält **nur unzureichende Einschränkungen**. § 47a Abs. 2 PolG BW-E sieht kaum tatsächliche Vorgaben für die Methode und deren Funktionsweise selbst vor.

Die Methode wird zwar in § 47a Abs. 2 Satz 4 PolG BW-E insoweit eingeschränkt, dass die Analyse manuell ausgelöst wird und anhand anlassbezogener und zielgerichteter Suchkriterien erfolgt, die sich aus einem konkreten Sachverhalt bezogen auf einen Anlass im Sinne des Absatzes 1 ergeben. Dies schränkt die Methode der Datenanalyse jedoch nur geringfügig ein, da sich ein Anlassbezug und ein „zielgerichtetes" Suchen für verschiedenste Suchbegriffe begründen lassen. Weitere Einschränkungen der Suchkriterien sind dem Entwurf nicht zu entnehmen. Zudem ist auch die Anzahl der Suchvorgänge nicht eingeschränkt, sodass **unbegrenzt aufeinander aufbauende Suchanfragen** gestellt und dabei auch immer wieder neue Daten der Analyse hinzugefügt werden können. Weitere Vorgaben zur Bedien- und Arbeitsweise sind dem Entwurf nicht zu entnehmen.

§ 47a Abs. 2 des Entwurfs ermöglicht damit insbesondere den Einsatz **von starken und komplexen Analysesystemen**, die auch zu maschineller Sachverhaltsbewertung in der Lage sind und in kürzester Zeit komplexe Ergebnisse hervorbringen können. § 47a Abs. 2 des Entwurfs lässt auch den **Einsatz künstlicher Intelligenz** zu (S. 21 f. des Entwurfs), dem ein besonderes Eingriffsgewicht zukommt.[17] Der Entwurf des Gesetzestextes sieht diesbezüglich keine Beschränkungen vor. Die Analyse unterscheidet sich daher erheblich von einem bloß maschinellen Datenabgleich, gerade weil sie explizit darauf gerichtet sind, in einem eigenen Schritt die Daten zu verknüpfen, abzugleichen, aufzubereiten, auszuwerten und zu bewerten (S. 19 des Entwurfs). Die vorgesehenen komplexen Analysen bergen zudem das Risiko von Manipulation und unbemerktem

[17] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

Datenzugriff durch Dritte, weil der Entwurf auch den Einsatz der Software privater Anbieter*innen ermöglicht.[18] Vor diesem Hintergrund fehlen im Entwurf Vorkehrungen zur Vermeidung von Fehlern und diskriminierenden Analysevorgängen und Ergebnissen.[19]

Zwar untersagt § 47a Abs. 3 Satz 1, 3 PolG BW-E automatisierte Entscheidungsfindungen unmittelbar durch die Analysesoftware. Maßnahmen und Entscheidungen auf Basis der Analyse müssen durch Polizist*innen und dürfen nicht durch die Software selbst getroffen werden. Der Ausschluss reduziert das Eingriffsgewicht jedoch nur unerheblich. Mangels weiterer Einschränkungen ermöglicht der Entwurf nämlich dennoch die Erstellung von komplexen **Personen- und Bewegungsprofilen sowie die Bewertung von Personen und Gefährdungen bzw. Risiken in Form des „predictive policings“** und damit **besonderes intensive Grundrechtseingriffe**[20], solange nicht die Software selbst unmittelbar Entscheidungen trifft. Es ist gerade nicht ausgeschlossen, dass solche Analyseergebnisse für Maßnahmeanordnungen als **Entscheidungsgrundlagen** herangezogen werden und in die Ermessensausübung von Polizist*innen einfließen. Dabei bleiben auch die Risiken einer Überbewertung der Analyseergebnisse im Rahmen eines sog. „automation bias“[21] durch Polizist*innen unberücksichtigt.

Ebenso verstärkt das Eingriffsgewicht, dass § 47a Abs. 3 Satz 2, 3 des Entwurfs es ermöglicht und darauf zielt, die Daten nicht nur vorübergehend für einen konkreten Verarbeitungsvorgang, sondern dauerhaft in einer eigenen Datenbank zusammenzuführen und so für die Analyseplattform als Datenbestand zur Verfügung zu stellen. Positiv ist jedoch zu vermerken, dass der Entwurf in § 47a Abs. 3 Satz 3, 4 eine Regelung dazu enthält, wie lange die nach § 47a Abs. 3 Satz 2 des Entwurfs hinzugefügten Daten auf der Analyseplattform gespeichert werden dürfen.

Die einsetzbaren Methoden sind im Entwurf daher nicht ausreichend bestimmt und normenklar begrenzt. Selbst wenn die Datenverarbeitung praktisch weniger eingriffsintensiv ausgestaltet wäre und von bestimmten Analysemethoden, beispielsweise vom Einsatz künstlicher Intelligenz, kein Gebrauch gemacht würde, bliebe dies für das Eingriffsgewicht der Rechtsgrundlage zur Datenverarbeitung ohne Bedeutung. Entscheidend ist vielmehr, welche Möglichkeiten der Gesetzgeber mangels Einschränkungen eröffnet. Wenn insbesondere komplexe Analyse-technologie und künstliche Intelligenz in der polizeilichen Praxis nicht eingesetzt werden sollen,

18 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
19 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100 ff.
20 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 98, 121.
21 Dazu *Ruschemeier*, The Problem of the Automation Bias in the Public Sector: A Legal Perspective. In Proceedings of the Weizenbaum Conference 2023: AI, Big Data, Social Media, and People on the Move (S. 1 ff.) S. 1 ff., 8.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

müssen diese Methoden durch den Gesetzgeber selbst bestimmt und normenklar ausgeschlossen werden, um das Eingriffsgewicht zu mildern.

c. Unzureichende Sicherung des Grundsatzes der Zweckbindung

Der Entwurf nimmt die Zweckbindungsvorschriften des PolG BW nur teilweise (durch Verweis des § 47a Abs. 4 Satz 1 PolG BW-E auf § 15 Abs. 2 und 3) in Bezug. In § 47a Abs. 4 Satz 2 Nr. 1-4 des Entwurfs ist der Erlass einer Verwaltungsvorschrift vorgesehen, die ein Konzept zur Kategorisierung und Kennzeichnung von Daten (Nr. 2) enthalten soll. Nähere Vorgaben zum Inhalt dieser Verwaltungsvorschrift finden sich in § 47a Abs. 6 PolG BW-E.

Die Vorgaben genügen dabei schon nicht dem Gesetzesvorbehalt (dazu sogleich e.). Vielmehr wäre eine umfassende Inbezugnahme der Zweckbindungsvorschriften erforderlich.

Darüber hinaus enthält der Entwurf keine ausreichenden Vorgaben zu **praktischen technischen und organisatorischen Maßnahmen**, die die **tatsächliche Einhaltung des Grundsatzes der Zweckbindung** sicherstellen. Allein rechtliche Vorgaben zur Zweckbindung können bei einer automatisierten Datenzusammenführung großer Datenmengen die tatsächliche Wahrung der Zweckbindungsgrundsätze nicht sicherstellen. In großen, unübersehbaren Datenpools und bei teils automatisierter Einbindung wird eine Zweckidentifizierung und -prüfung für einzelne Daten erschwert.[22] Damit die Zweckbindung und -änderung in der praktischen Anwendung tatsächlich geprüft und gewahrt werden kann, bedarf es vielmehr auch einer Sicherung der Zweckbindung durch gesetzliche Vorgaben zu praktischen und technisch-organisatorischen Maßnahmen. Solche Regelungen enthält der Entwurf selbst nicht. Eine vollständige Auslagerung in Verwaltungsvorschriften genügt dem Gesetzesvorbehalt nicht.

In der Entwurfsfassung des § 47a wird die Zweckbindung nicht dadurch gesichert, dass die verarbeiteten Datenquellen bzw. -sätze nach Zwecken getrennt bleiben. Vielmehr bleiben die verschiedenen Datensätze nach § 47a Abs. 3 Satz 1 und 2 PolG BW-E für die Analyse dauerhaft zusammengeführt und verfügbar.

Daher bedarf es zur tatsächlichen Sicherung der Zweckbindung insbesondere einer **umfassenden Kennzeichnung** von Daten.[23] Hierzu enthält der Gesetzestext des Entwurfs selbst keine ausreichenden Vorgaben, da § 47a Abs. 6 Satz 5 PolG BW-E nur die Verpflichtung enthält, durch Verwaltungsvorschrift technisch-organisatorische Vorkehrungen zu regeln, die die Einhaltung des Zweckbindungsgrundsatzes faktisch sichern, **ohne** dass der **Gesetzgeber** selbst dazu die notwendigen **inhaltlichen Leitentscheidunge**n trifft. Dem Entwurf ist jedoch bereits nicht zu entnehmen, dass eine Kennzeichnung im Sinne des § 72 PolG BW vorgesehen sein soll. Insoweit

22 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 138.
23 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 65.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin
info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B
GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

sollte für eine gesetzliche Anordnung einer Kennzeichnung § 72 PolG BW-E in Bezug genommen werden. Auch muss sichergestellt sein, dass die Kennzeichnungspflicht nicht gemäß § 72 Abs. 4 PolG BW suspendiert ist. Vielmehr muss ausdrücklich festgeschrieben sein, dass **nur gekennzeichnete Daten in das Analysesystem eingeführt** werden dürfen. Durch den Entwurf ist mithin nicht ausgeschlossen, dass in Datensätzen befindliche, nicht gekennzeichnete Daten dennoch zu anderen, nicht zulässigen Zwecken in Analysevorgänge einfließen können. Ohnehin kann aber allein eine Kennzeichnung der verwendeten Daten nicht dafür sorgen, dass die durch Zweckbindungsregelungen gesetzten Grenzen für die einzelnen Daten eingehalten werden.[24] Auch zu weiteren Vorkehrungen darf der Gesetzgeber die Entscheidung nicht, wie in § 47a Abs. 4 ff. PolG BW-E erfolgt, vollständig der Verwaltung überlassen.

d. Aufsichtliche Kontrolle

Zur Wahrung der Verhältnismäßigkeit der Datenanalysen bedarf es aufsichtlicher, insbesondere datenschutzrechtlicher Kontrollen. Als mögliche sachgerechte Ausgestaltung kommt nach dem Bundesverfassungsgericht etwa eine **regelmäßige und effiziente stichprobenhafte Kontrolle des Analysebetriebs** durch behördliche und externe Datenschutzbeauftragte in Betracht.[25] Die Kontrollzeiträume dürfen dabei ein Höchstmaß von etwa zwei Jahren nicht überschreiten.[26]

§ 47a Abs. 7 PolG BW-E regelt einen Anordnungsvorbehalt für Datenanalysemaßnahmen. § 47a Abs. 8 des Entwurfs sieht nur eine Anhörung des*r Datenschutzbeauftragten vor der Einrichtung der Analyseplattform vor. In § 98 Abs. 1 Nr. 14 PolG BW-E wird eine zweijährige Kontrolle der Analysen durch die Aufsichtsbehörde für den Datenschutz, mithin durch den*die Landesbeauftragte*n für Datenschutz und Informationsfreiheit (§ 97 PolG BW), angeordnet. Darüber hinaus enthält § 90 Abs. 1 S. 1, 2, 3 PolG BW-E Berichtspflichten des Innenministeriums hinsichtlich der Datenanalysen nach § 47a PolG BW-E gegenüber dem Parlamentarischen Kontrollgremium, die dazu mindestens vierteljährlich Unterrichtungen umfassen. Auf Verlangen des Kontrollgremiums hat das Innenministerium zu einer konkreten Maßnahme zu berichten. Daneben sind Anordnungen der Maßnahmen nach § 47a Abs. 7 Satz 3 PolG BW-E zu begründen, näheres zur Begründung soll nach § 47a Abs. 4 Satz 2 Nr. 4 PolG BW-E in einer Verwaltungsvorschrift geregelt werden. § 74 Abs. 1, 2 Nr. 2 lit. a-c PolG BW-E sieht eine Protokollierung der einbezogenen Daten, der verwendeten Suchkriterien und der betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden, vor.

Zunächst ist der*die Datenschutzbeauftragte*r vor Einrichtung oder wesentlicher Änderungen lediglich anzuhören, es besteht keine Verpflichtung zur Berücksichtigung der Bedenken des*r

---

24 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 139.
25 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 109.
26 BVerfG, Urteil vom 20. April 2016, 1 BvR 966, 1140/09, Rn. 141.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

Datenschutzbeauftragten, Interventionsrechte bestehen nicht. Dies stellt eine nur geringfügige Kontrolle dar.

Grundsätzlich ist zu begrüßen, dass der Entwurf verstetigte Kontrollen des Analysebetriebs vorsieht. Dennoch bestehen Bedenken hinsichtlich deren Wirksamkeit. Erstens sollten stichprobenartige, verdachtsunabhängige Kontrollen nicht nur für die Zugriffskontrolle in § 47a Abs. 4 S. 2 Nr. 2 PolG BW-E, sondern weitergehend auch für die allgemeine datenschutzrechtliche Kontrolle des Analysebetriebs vorgesehen werden. Zudem müssen Inhalt und Umfang der Kontrollen für die besondere Maßnahme der Datenanalyse gesetzlich näher konkretisiert werden. Gerade zu Beginn der Nutzung der operativen und strategischen Datenanalyse ist eine externe Kontrolle **zum Ausschluss von Fehlern, Diskriminierung und Missbrauch in geringeren Abständen** notwendig. Nur durch regelmäßige umfassende und verdachtsunabhängige Kontrollen kann der eingeschränkte Individualrechtsschutz bei der ohne Wissen der Betroffenen erfolgenden Datenanalyse ausgeglichen werden.

e. Wesentlichkeitsgrundsatz, Gesetzesvorbehalt, Bestimmtheit und Normenklarheit im Übrigen

Auch im Übrigen genügt die Norm im vorliegenden Entwurf nicht dem verfassungsrechtlichen Gesetzesvorbehalt und Wesentlichkeitsgrundsatz. Für eine verfassungsrechtliche Rechtfertigung, gerade bei Eingriffsschwellen unterhalb der mindestens konkretisierten Gefahr ist erforderlich, dass Analyse- und Auswertungsmöglichkeiten durch den Gesetzgeber normenklar und hinreichend bestimmt begrenzt werden.[27] Der Gesetzgeber darf die Regelungsaufgabe zwar zum Teil der Verwaltung überlassen, muss aber sicherstellen, dass ausreichende Regelungen zu Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden im Gesetz geregelt sind.[28] § 47a des Entwurfs genügt diesen Anforderungen nicht.

Der Entwurf enthält insbesondere wie bereits ausgeführt **keine ausreichenden Begrenzungen von Art und Umfang der verwendeten Daten sowie** der **Analysemethoden.** Weiterhin fehlt es in § 47a des Entwurfs an **expliziten Vorkehrungen gegen eine unangemessen verzerrende und diskriminierende Wirkung der Datenauswahl und -analyse**, gerade für den Einsatz von künstlicher Intelligenz.[29] Bei § 47a Abs. 2 Satz 2 PolG BW-E handelt es sich um eine bloße rechtliche Vorgabe, die keine Vorkehrungen für technisch-praktische Maßnahmen enthält, die bei der Anwendung der Analysesoftware diskriminierende Analysemechanismen und -ergebnisse verhindern.

---

27 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110.
28 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110.
29 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 95, 100.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

In § 47a Abs. 4 Satz 2 Nr. 1-4 des Entwurfs ist der Erlass einer Verwaltungsvorschrift durch das Innenministerium vorgesehen. Geregelt werden sollen ein Rollen- und Rechtekonzept (Nr. 1), ein Konzept zur Kategorisierung und Kennzeichnung von Daten (Nr. 2), ein Konzept zur Zugriffskontrolle, das auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht (Nr. 3) und nähere Bestimmungen zum Inhalt der Begründung nach § 47a Abs. 3 Satz 5 und Abs. 7 Satz 3 PolG BW-E (Nr. 4). Positiv zu bewerten ist, dass § 47a Abs. 4, 5, 6 PolG BW-E Vorgaben für eine zu erlassende Verwaltungsvorschrift enthält und zudem, wie vom Bundesverfassungsgericht gefordert[30], deren Veröffentlichung im amtlichen Bekanntmachungsblatt vorsieht.

Der Entwurf genügt dennoch nicht den Anforderungen des **Wesentlichkeitsgrundsatzes** und des Gesetzesvorbehalts.[31] Damit Einschränkungen das Eingriffsgewicht mildern, müssen diese im Wesentlichen im Gesetz selbst geregelt oder durch dieses vorgegeben und anschließend durch die Verwaltung klar abstrakt-generell niedergelegt und veröffentlicht sein.[32] Der Entwurf sieht jedoch keine ausreichenden Vorgaben insbesondere für Kategorisierung und Kennzeichnung von Daten (s. soeben unter c.) sowie zur Kontrolle des Rollen- und Rechtekonzepts und der Zugriffe vor und überlässt damit grundrechtswesentliche Abwägungsentscheidungen der Verwaltung. Die gesetzlichen Vorgaben erschöpfen sich zumeist in der Umschreibung von Verhältnismäßigkeitsanforderungen, ohne konkrete Grenzen selbst festzulegen (beispielsweise § 47a Abs. 4 Satz 3, Abs. 5 Satz 2, Abs. 6 Satz 4 PolG BW-E). Sie genügen dabei den Anforderungen an Bestimmtheit und Normenklarheit nicht. Insbesondere muss der Gesetzgeber selbst „Leitplanken" vorgeben, die die praktische Wirksamkeit der Regelungen sicherstellen und darf dies nicht vollständig der Verwaltung überlassen (so in § 47a Abs. 6 Satz 5 PolG BW-E). Dies erfordert gerade auch **gesetzliche** Regelungen zur **praktischen Durchführung und Wirksamkeit** der technisch-organisatorischen Vorgaben.

2. § 47a Abs. 1 Nr. 2 PolG BW-E

Auch Datenanalysen gemäß § 47a Abs. 1 Nr. 2 PolG BW-E stellen **schwerwiegenden Grundrechtseingriffe** dar, da die wenigen vorgesehenen Beschränkungen das Eingriffsgewicht nicht ausreichend verringern.

---

30 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 113; BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 183.

31 Hierzu ausführlich *Singelnstein*, Verfassungsbeschwerdeschrift gegen § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) vom 21. Juni 2024, S. 36 ff., 66 ff., 68 ff., 72 ff., abrufbar unter https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf (zuletzt abgerufen am 18. August 2025).

32 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 119.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

Bezüglich Art, Herkunft und Umfang der Daten ergeben sich keine Unterschiede zur Analyse nach § 47a Abs. 1 Nr. 1 PolG BW-E. Daher sind auch hier in großer Menge Daten von bislang Unbeteiligten umfasst, die für Überwachungsmaßnahmen keinen Anlass geboten haben.

Die einzige Einschränkung speziell für die Analysen nach § 47a Abs. 1 Nr. 2 PolG BW-E ist Abs. 2 Satz 5 des Entwurfs. Dieser sieht vor, dass bei der Maßnahme nach Nr. 2 der Suchvorgang auf die in §§ 6,7 PolG BW und damit auf Handlungs- und Zustandsstörer*innen auszurichten ist.

Dabei verbleibt bereits unklar, wie diese Einschränkung technisch auswirken soll. Zudem ist rechtlich nicht eindeutig erkennbar, ob es sich hierbei um eine methodische Einschränkung der Analyse selbst oder nur um eine personelle Einschränkung bzw. Ergänzung der Eingriffsschwelle für Maßnahmen nach Absatz 1 Nr. 2 handelt. Die Formulierung des § 47a Abs. 2 Satz 5 des Entwurfs ist insoweit zu unbestimmt. Selbst wenn es sich um eine Beschränkung der Methode handeln würde, wäre diese nicht ausreichend. Erstens ist der Wortlaut mit „auszurichten" weit, und nicht derart zu verstehen, dass nur Daten der Störer*innen selbst eingegeben werden können, sondern nur, dass die Suche darauf im Ergebnis auszurichten ist. Dies ermöglicht daher ebenso breite und in ihren Kriterien unbegrenzte Suchen, die immer wieder aufeinander aufbauend mit neuen Daten durchgeführt werden können. Zweitens ist durch die Einschränkung nicht ausgeschlossen, dass auch bislang unbeteiligte Personen wie Zustandsstörer*innen gezielten Analysemaßnahmen ausgesetzt werden. Weitergehende Einschränkungen der Methode sieht der Entwurf nicht vor.

3. § 47a Abs. 1 Nr. 3 PolG BW-E

Auch für die Datenanalyse gemäß § 47a Abs. 1 Nr. 3 PolG BW-E ergibt sich kein anderes Ergebnis. Es handelt sich ebenso um einen **schwerwiegenden**, jedenfalls nicht um einen nur geringfügigen Grundrechtseingriff, das Eingriffsgewicht ist nicht ausreichend eingeschränkt.

Neben der Beschränkung auf Störer*innen (§ 47a Abs. 2 Satz 5 PolG BW-E, s. dazu soeben) ist die einzige im Gesetzestext für § 47a Abs. 1 Nr. 3 PolG BW-E vorgesehene zusätzliche Einschränkung, dass keine Verkehrsdaten und Funkzellendaten in diese Analyse einfließen dürfen. Mit dieser Einschränkung werden große Datenpools mit einem hohen Anteil von Daten von Unbeteiligten aus der Analyse ausgenommen. Es handelt sich damit um eine Einschränkung, die das Eingriffsgewicht mildert. Dennoch fließen wegen der im Gesetzestext selbst uneingeschränkten Einbindung von vor allem Vorgangs- und Falldaten immer noch sehr viele Daten von Personen ein, die für die Analysen keinen Anlass geboten haben. Zudem ist über die Möglichkeit der händischen Einführung von Informationen eine Analyse immer neuer Daten mit faktisch uneingeschränkten komplexen Analysealgorithmen zulässig. Die Beschränkung genügt daher nicht, um das Eingriffsgewicht

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

ausreichend zu mindern. Dies gilt insbesondere, weil keine Beschränkung der möglichen hochkomplexen Analysen auch durch künstliche Intelligenz erfolgt.

II. Keine verfassungsrechtliche Rechtfertigung der Eingriffe

Da es sich bei allen Formen der Datenanalyse um schwerwiegende, jedenfalls nicht nur geringfügige Grundrechtseingriffe handelt, genügen nur die in § 47a Abs. 1 Nr. 1 PolG BW-E geregelten Eingriffsvoraussetzungen zur verfassungsrechtlichen Rechtfertigung der Maßnahmen. Im Ergebnis stellen § 47a Abs. 1 Nr. 2 und 3 PolG BW-E mangels ausreichender Eingriffsschwellen und Anforderungen an die zu schützenden Rechtsgüter eine verfassungswidrige Verletzung des Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG dar. Weiterhin betrifft die Norm Art. 10 GG, da in Analysen nach Absatz 1 Nr. 2 auch Daten aus Telekommunikationsüberwachung in die Analysen einbezogen werden dürfen, sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)[33].

Zur Rechtfertigung der automatisierten Datenanalyse als schwerwiegender Grundrechtseingriff bedarf es einer Einschränkung des Einsatzes auf Fälle einer zumindest konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut. Eine konkretisierte Gefahr setzt voraus, dass bestimmte festgestellte Tatsachen die Prognose der Entstehung einer konkreten Gefahr tragen. Dies wiederum erfordert nicht nur, dass der Schluss auf ein der Art nach und zeitlich konkretisiertes Geschehen möglich ist, sondern auch, dass bestimmte Personen beteiligt sein werden, die so weit identifiziert werden können, dass Überwachungsmaßnahmen gezielt gegen sie gerichtet und auf sie weitestgehend beschränkt werden können.[34] Diesen Anforderungen genügen die in § 47a Abs. 1 Nr. 2 und 3 des Entwurfs geregelten Eingriffsvoraussetzungen nicht.

1. § 47a Abs. 1 Nr. 1 PolG BW-E

§ 47a Abs. 1 Nr. 1 PolG BW-E knüpft an besonders gewichtige Rechtgüter und an die Eingriffsschwelle einer konkreten Gefahr für ebendiese an. Dies genügt zur Rechtfertigung des schwerwiegenden Grundrechtseingriffes. Da die Beschränkung der Analyse auf Störer*innen im Sinne der §§ 6, 7 PolG BW in § 47a Abs. 2 Satz 5 des Entwurfs nur auf die Analysen nach Absatz 1 Nr. 2 und 3 Anwendung findet, ist die Analyse nach Nr. 1 im Rückschluss nicht nur gegen Störer*innen zulässig. Sollte dies mit Blick auf die Bezugnahme der konkreten Gefahr doch als Beschränkung vorgesehen sein, ist eine diesbezügliche Klarstellung erforderlich.

---

33 Zumindest betroffen bei Daten aus Quellen-Telekommunikationsüberwachungen, hierzu zuletzt BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 180/23, Rn. 172 ff. und BVerfG, Beschluss vom 24. Juni 2025, 1 BvR 2466/19, Rn. 105 ff.

34 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 106 m.w.N.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

2. § 47a Abs. 1 Nr. 2 PolG BW-E

Da es sich bei § 47a Abs. 1 Nr. 2 PolG BW-E, anders als im Entwurfstext (S. 20 des Entwurfs) angenommen, ebenfalls um einen schwerwiegenden Grundrechtseingriff handelt, genügen die vorgesehenen Anforderungen **nicht zur Rechtfertigung** der Eingriffe durch die Datenanalyse.

Es fehlt bereits an einer ausreichenden Regelung einer zumindest konkretisierten Gefahr, da **keine ausreichende personelle Konkretisierung der Eingriffsschwelle im Gesetzestext** erfolgt ist. Eine personelle Beschränkung in der Gesetzesbegründung (S. 20 des Entwurfs) ist nicht ausreichend. Die personelle Konkretisierung kann auch nicht aus § 47a Abs. 2 Satz 5 des Entwurfs und der dort genannten Beschränkung der Analyse auf Störer*innen hergeleitet werden. Zum einen ist – wie bereits dargestellt – unklar, ob es sich bei der Regelung auf eine Beschränkung der Methode oder eine Konkretisierung der Eingriffsschwelle handeln soll. Selbst wenn durch Absatz 2 Satz 5 die Maßnahmen nur gegen Handlungs- und Zustandsstörer*innen gerichtet werden dürften und so eine persönliche Konkretisierung der Eingriffsschwelle erfolgte, wäre diese nicht ausreichend, da auch eine erhebliche Zahl von Personenkreisen umfasst ist, die für eine Maßnahme gerade keinen Anlass geboten haben, beispielsweise bei Maßnahmen, die sich gegen Zustandsstörer*innen richten.

Gleichzeitig ist auch die **Anknüpfung an Straftaten von nur erheblicher Bedeutung unzureichend.** Zur Rechtfertigung von schwerwiegenden Grundrechtseingriffen ist nur eine Gefährdung besonders gewichtiger Rechtsgüter ausreichend,[35] sodass nur an besonders schwere Straftaten angeknüpft werden kann, die gerade dem Schutz besonders gewichtiger Rechtsgüter dienen. Darüber hinaus sind die genannten „Straftaten von erheblicher Bedeutung“ **zu unbestimmt** und nur unzureichend konkretisiert. Zum einen ist bereits unklar, ob die Legaldefinition des systematisch nachfolgenden § 49 Abs. 3 PolG BW herangezogen werden soll. Zudem genügt der Katalog des § 49 Abs. 3 PolG BW nicht zum Schutze besonders gewichtiger Rechtsgüter. Der Katalog stellt bereits nicht sicher, dass die Straftaten dem Schutz überragend wichtiger Rechtsgüter dienen, da insbesondere auch Eigentums- und Vermögensdelikte ohne weitere Einschränkungen als Anknüpfungsdelikte herangezogen werden können. Auch handelt es sich bei den in Bezug genommenen Straftaten nicht um besonders schwere Straftaten, erstens durch die pauschale Inbezugnahme sämtlicher Verbrechen als auch durch die Aufnahme von Vergehen bei gewerbs- oder bandenmäßiger Begehung. Des Weiteren enthält § 49 Abs. 3 Nr. 1 und 2 PolG BW mehrere unbestimmte Rechtsbegriffe wie die Eignung, „den Rechtsfrieden besonders zu stören“ sowie die serien-, gewohnheitsmäßige oder sonst organisierte Begehung von Straftaten. In der vorliegenden Fassung ist eine klare und bestimmte Anwendung durch Behörden

[35] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 105.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

und Gerichte nicht sichergestellt, Bürger*innen können ihr Verhalten nicht ohne weiteres an der Norm ausrichten.

Positiv ist zwar zu bewerten, dass in § 47a Abs. 1 Nr. 2 lit. c PolG BW-E vorgesehen ist, dass mit Blick auf die Vorgaben des Bundesverfassungsgerichts zu Vorfelddelikten[36] eine konkrete Gefahr für das geschützte Rechtsgut vorliegen muss (S. 20 des Entwurfs). Jedoch ist der gesetzlich vorgesehene Zeitpunkt des Eintritts der Gefahr nicht ausreichend. Die konkretisierte Gefahr für das Rechtsgut muss bereits **bei Anordnung der Analysemaßnahme** und nicht erst bei Verwirklichung des Tatbestandes gegeben sein.

Selbst, wenn man in § 47a Abs. 1 Nr. 2 PolG BW-E nur einen weniger gewichtigen Eingriff sähe und deswegen nur geringere Anlässe zur Rechtfertigung genügen ließe, genügten die geregelten Eingriffsschwellen und die zu schützenden Rechtsgüter nicht den verfassungsrechtlichen Anforderungen. Hierzu können **entweder** an die Eingriffsschwelle der zumindest konkretisierten Gefahr **oder** an die zu schützenden Rechtsgüter geringere Anforderungen gestellt werden, sodass der Schutz von Rechtsgütern von zumindest erheblichem Gewicht ausreicht.[37] Die Eingriffsvoraussetzungen des § 47a Abs. 1 Nr. 2 des Entwurfs werden jedoch auch diesen Anforderungen nicht gerecht, da **sowohl** an die Eingriffsschwelle **als auch** an die zu schützenden Rechtsgüter geringere Anforderungen als erforderlich gestellt werden und die Anforderungen mangels ausreichender Bestimmtheit und Normenklarheit der „erheblichen Straftaten" verfassungswidrig sind.

3. § 47a Abs. 1 Nr. 3 PolG BW-E

Gleiches gilt für § 47a Abs. 1 Nr. 3 PolG BW-E des Entwurfs, da auch diese Maßnahme – anders als vom Gesetzgeber angenommen (S. 20 des Entwurfs) - einen schwerwiegenden Grundrechtseingriff darstellt. Hier fehlt es bei der Eingriffsschwelle sowohl an dem **Erfordernis einer Konkretisierung in zeitlicher Sicht und der Art nach als auch in persönlicher Hinsicht**. Der Gesetzgeber verortet die Maßnahme bewusst im Gefahrenvorfeld (S. 28 des Entwurfs), die Maßnahme zeichne sich „durch eine größere Ungewissheit sowohl in Bezug auf die Tatsachengrundlage als auch in Bezug auf den zum Schaden führenden Kausalverlauf aus" (S. 28 des Entwurfs). Die dafür erforderlichen Beschränkungen der Analyse sind jedoch nicht erfolgt (s. soeben unter I. 3).

Auch ist die Anknüpfung an besonders schwere Straftaten nur dann zureichend, **wenn sie dem Schutz besonders gewichtiger Rechtsgüter dienen**. Daher müssen reine Vermögens- und Eigentumsdelikte als Anknüpfungsdelikte ausgeschlossen sein, da eine Anknüpfung an den Schutz

---

36 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 170.
37 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 107.

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

von Sachwerten grundsätzlich nicht genügt. Dies ist bei der im Entwurf vorgesehenen Anknüpfung an besonders schwere Straftaten und gerade bei dem in der Gesetzesbegründung in Bezug genommenen Katalog des § 100b Abs. 2 StPO (S. 21 des Entwurfs) nicht gewährleistet. Eine Beschränkung auf den genannten Katalog ist dem Gesetzestext zudem nicht zu entnehmen, sodass insoweit keine einschränkende Wirkung angenommen werden kann.

Zudem müsste auch im Rahmen von Nummer 3 für Vorfeldtatbestände die in § 47a Abs. 1 Nr. 2 lit. c PolG BW-E geforderte Gefahr für das geschützte besonders gewichtige Rechtsgut **im Zeitpunkt der Maßnahmenanordnung** gefordert werden.

Selbst bei Annahme eines weniger gewichtigen Grundrechtseingriffes genügen die in § 47a Abs. 1 Nr. 3 PolG BW-E vorgesehenen Anforderungen nicht, da **sowohl** in der Eingriffsschwelle **als auch** bei den geschützten Rechtgütern eine Absenkung der Rechtfertigungsanforderungen erfolgt ist.

C. Technologieoffenheit der Rechtsgrundlage und einzusetzende Software

Über den konkreten Entwurf hinaus sollte bei Ausführung der im Entwurf vorgesehenen Datenanalysen nicht auf Software privater Anbieter*innen, sondern auf **staatliche und unternehmensunabhängige Software** zurückgegriffen werden. Zwar ist der Einsatz privater Software im Rahmen staatlicher Datenverarbeitung nicht per se ausgeschlossen.[38] Wenn im Bereich der polizeilichen Staatsaufgaben auf Systeme privater Anbieter zurückgegriffen wird, stellt dies eine Auslagerung des Grundrechts- und Datenschutzes vom grundrechtsverpflichteten Staat auf private Unternehmen dar. Dies ist risikoreich, da sensiblen und persönlichkeitsrechtsrelevanten Daten mit Algorithmen analysiert werden, deren Funktionsweise nicht nachvollzogen werden kann. Dies führt zu weniger Transparenz und Schwierigkeiten bei der Kontrolle. **Manipulation und mögliche Hintertüren** und damit das **Risiko von Leaks von und unbefugtem Zugriff auf polizeiliche Daten** können **nie,** auch nicht durch vertragliche Vereinbarungen[39] **vollständig ausgeschlossen** werden. Dies gilt auch, wenn private Software ohne Verbindung zum Internet und auf staatlichen Servern eingesetzt und betrieben wird, wie es in Baden-Württemberg erfolgen soll.[40] Bei Wartung und Fehlerkorrektur besteht ein Risiko, dass Private Zugriff auf Datensätze und

---

38 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.

39 Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Pressemitteilung vom 29. Juli 2025, „Landesregierung gibt Ermittlungsbehörden neue Instrumente an die Hand“, abrufbar unter https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/landesregierung-gibt-ermittlungsbehoerden-neue-instrumente-an-die-hand?highlight=palantir (zuletzt abgerufen am 18. August 2025).

40 § 47a Abs. 2 S. 6 PolG BW-E und Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Pressemitteilung vom 29. Juli 2025, „Landesregierung gibt Ermittlungsbehörden neue Instrumente an die Hand“, abrufbar unter https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/landesregierung-gibt-ermittlungsbehoerden-neue-instrumente-an-die-hand?highlight=palantir (zuletzt abgerufen am 18. August 2025).

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

Analyseergebnisse erhalten, gerade, wenn zur Wartung Personal des privaten Unternehmens innerhalb der polizeilichen Infrastruktur mit Zugang zu den polizeilichen Servern eingesetzt wird.[41] Gleichzeitig ist unklar, wie eine Aktualität der dauerhaft zusammengeführten Datensätze im Analysesystem und eine jederzeitige Verfügbarkeit des Analysetools sichergestellt werden kann, wenn die Analysesoftware vollständig isoliert von öffentlichen Netzen und damit auch von internen Dienstnetzwerken betrieben werden soll.

Besondere Risiken bestehen beim Einsatz von Software außereuropäischer Anbieter*innen, die mit anderen Regierungen und Geheimdiensten auch autoritärer Staaten zusammenarbeiten und bei denen durch die Rechtslage im Staat ihres Unternehmenssitzes die Gefahr auch ungewollter staatlicher Datenzugriffe besteht.

Ebenso besteht beim Einsatz der Software privater Anbieter*innen die Gefahr, dass Algorithmen und Ergebnisse **intransparent** verbleiben und so Fehler und insbesondere diskriminierende und verzerrende Algorithmen schlechter identifiziert und beseitigt werden können. Dies gilt umso mehr, wenn hochkomplexe Analysen mittels künstlicher Intelligenz erfolgen.[42]

Auch ist die Lizensierung einer privaten Software **mit erheblichen Kosten verbunden**.[43] Dies gilt umso mehr, wenn Anbieter*innen bei deutschen Behörden eine weitgehende Monopolstellung einnehmen. Es drohen starke Abhängigkeiten, in welchen Anbieter*innen die Preise (wie durch Preisbindungsfristen[44]) und Nutzungsbedingungen weitgehend frei diktieren können. Durch die aufgewendeten Kosten und die Einrichtung einer solchen Software drohen **Lock-In-Effekte**, die

---

41 *Blum/Brühl/*Heubl, Polizei-Software von Palantir – Teufelszeug oder Wunderwaffe?, SZ vom 19.07.2025, abrufbar unter https://www.sueddeutsche.de/projekte/artikel/politik/palantir-sicherheit-polizei-thiel-innenminister-e406093/ (zuletzt abgerufen am 18. August 2025).

42 S. BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.

43 In Nordrhein-Westfalen fielen für eine auf Palantir Gotham beruhende Software statt ursprünglich geplanten 14 Millionen Euro nun Kosten iHv. 39 Millionen Euro an, *Hell/Kartheuser*, NRW-Polizei: Knapp 40 Millionen Euro für umstrittene Palantir-Software, WDR vom 25. September 2022, abrufbar unter https://www1.wdr.de/nachrichten/landespolitik/nrw-polizei-datenbank-software-palantir-kosten-100.html#:~:text=Mittlerweile%20kostet%20das%20Gesamtprojekt%20das%20Land%20NRW%20insgesamt%2039%20Millionen%20Euro (zuletzt abgerufen am 19. August 2025); in Baden-Württemberg wurden bereits 25 Millionen Euro für einen Fünf-Jahres-Vertrag investiert, *Bauer/Pfäfflin*, Steuerzahlern in BW droht Millionenverlust durch Kauf von Polizeisoftware, SWR vom 24. Juli 2025, abrufbar unter https://www.swr.de/swraktuell/baden-wuerttemberg/palantir-software-hohe-kosten-drohen-100.html (zuletzt abgerufen am 18. August 2025).

44 Heise online/ dpa, Baden-Württemberg: Koalitionszoff um Palantir-Software für Polizei, 27. Juli 2025, abrufbar unter https://www.heise.de/news/Koalitionszoff-um-Palantir-Software-fuer-Polizei-10497840.html (zuletzt abgerufen am 18. August 2025).

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Gesellschaft für Freiheitsrechte
freiheitsrechte.org

einen späteren Wechsel auf andere Angebote wesentlich erschweren. Aus diesem Grunde ist auch ein Einsatz einer solche Software als vermeintliche „Übergangslösung“[45] abzulehnen.

Wenn eine Rechtgrundlage für eine polizeiliche Datenanalyse geschaffen wird, sollte das Land Baden-Württemberg für den Betrieb der geregelten Analysevarianten daher auf eine bund- und länderübergreifende staatliche Softwarelösung hinwirken und nicht auf Analysesoftware privater Anbieter*innen zurückgreifen. Auch bei staatseigenen Analysesystemen bestehen jedoch erhebliche Risiken für die Grundrechte und Zweifel an deren Effizienz.

45 Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Pressemitteilung vom 29. Juli 2025, „Landesregierung gibt Ermittlungsbehörden neue Instrumente an die Hand“, abrufbar unter https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/landesregierung-gibt-ermittlungsbehoerden-neue-instrumente-an-die-hand?highlight=palantirr (zuletzt abgerufen am 18. August 2025).

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

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

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

Beteiligungsportal: Kommentare „Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften“

Nr. 1 (Kommentar 1 am 30.07.2025, 12:30 Uhr)

Palantir

Unterstützung: 61, Ablehnung: 30

Wird Zeit dass die Schnittstellen der diversen Datenbanken kompatibel gemacht werden, aber Palantir von Peter Thiel dafür zu kaufen ist ein no-go!

Nr. 2 (Kommentar 2 am 30.07.2025, 13:22 Uhr)

Zu teuer!

Unterstützung: 46, Ablehnung: 30

Die jährlichen Kosten sind astronomisch! Ich sehe nicht, wie diese Unmengen an Geld dafür gerechtfertigt sind, wenn Menschen unter der Armutsgrenze leben, es nicht genügend Sozialwohnungen gibt und deshalb der Rechtsextremismus in Deutschland zunimmt.

Wir brauchen keine Notlösungen, sondern echte Lösungen für die Ursachen der steigenden Kriminalität. Die Antwort ist fast immer die gleiche: Armut.

Das Leben in einem Polizei- oder Militärstaat führt nicht zu weniger Kriminalität, sondern zu mehr Kriminalität aufgrund von Hass und Verzweiflung.

Wenn wir auch noch die Einmischung in das GG und EG erwähnen, werden wir ziemlich bald keine Rechte mehr haben. Oder Rechte, die nicht im Interesse der Bevölkerung sind.

Daher aus meiner Sicht definitiv NEIN.

Nr. 3 (Kommentar 3 am 30.07.2025, 13:27 Uhr)

Änderung des Polizeigesetzes

Unterstützung: 32, Ablehnung: 29

Es ist höchste Zeit, dass durch eine Einmalabfrage in den polizeilichen Datensystemen alle bestehenden Erkenntnisse aus der Vielzahl der bestehenden Datenbanken mitgeteilt werden. Wichtig ist, dass deutlich erkennbar ist, welche Rolle die abgefragte Person bei den übermittelten Erkenntnissen hat.

Beteiligungsportal: Kommentare „Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften“

Nr. 4 (Kommentar 4 am 30.07.2025, 13:37 Uhr)

Datenschutz

Unterstützung: 51, Ablehnung: 24

In der Erläuterung zu Gesetzentwurf vermisse ich eine Stellungnahme des Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Oder habe ich sie übersehen?

Jedenfalls lese ich in vielen Medien, daß die Anschaffung von Palantir unter datenschutzrechtlichen Aspekten als sehr kritisch gesehen wird. Als Laie kann ich letztlich nicht beurteilen, wie hoch beispielsweise das Risiko der Datenabschöpfung in die USA zu bewerten ist. Da wäre es doch sinnvoll, die beim Landesbeauftragten vorhandene Kompetenz zu nutzen und seine Stellungnahme dann auch (presse-) öffentlich zu machen.

Alternativen gibt es angeblich keine. In der Presse war zu lesen, daß es aber hierzulande Leute gibt, die sich mit solchen Möglichkeiten beschäftigen, nur noch nicht ganz so weit sind. Warum fördert man diese nicht und wartet nicht ab, bevor man sich dem fragwürdigen Inhaber eines Konzerns an den Hals wirft?

Nr. 5 (Kommentar 5 am 30.07.2025, 14:19 Uhr)

Änderung des Polizeigesetzes

Unterstützung: 33, Ablehnung: 29

Eine digitale Zusammenführung der unterschiedlichen Informationen und Datensätze ist mit den heutigen Möglichkeiten längst überfällig. Das sollte m.E. wegen des unkomplizierteren und schnelleren Zugriffs auf die Daten auch zu Zeit- und damit Kosteneinsparungen führen.

Eine Kontrolle und Gewährleistung der Sicherheit der Daten beim Software-Anbieter ist aber unerlässlich

Nr. 6 (Kommentar 6 am 30.07.2025, 14:58 Uhr)

VeRA

Unterstützung: 31, Ablehnung: 18

Ich halte das für unausgegoren, übereilt, fehlerhaft. Auch ist merkwürdig, wie das ohne Wissen des Innenministers sein kann.

Beteiligungsportal: Kommentare „Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften“

Nr. 7 (Kommentar 7 am 30.07.2025, 17:59 Uhr)

Datenschutz wird immer weiter ausgehöhlt

Unterstützung: 43, Ablehnung: 22

Ich lehne die Änderung ab. Polizeibefugnisse werden zur klammheimlichen Überwachung der Bürger immer weiter erweitert, Schritt für Schritt. Und das ganze wird immer begründet mit Terrorismusbekämpfung und Schutz der Kinder vor Mißbrauch. Das ist natürlich raffiniert, denn wer soll schon etwas dagegen haben.

Technologien werden immer leistungsfähiger und Konzerne möchten ihre Produkte verkaufen. Als nächstes möchten die Chinesen ihre Überwachungssoftware bei uns verkaufen. Social Scoring ist dann nicht weit. Ein Herr Strobl würde auch das sicherlich gerne einführen. Warum nur werden Innenminister fast immer auch automatisch zu Grundrechtsabbauminister?

Der Hohn ist ja, dass die Polizeigesetzänderung so lapidar als „alternativlos“ bezeichnet wird. Unglaublich!

Nicht alles was technisch möglich ist, muss auch umgesetzt werden. Wir sollten ein klares Nein zur Überwachung, sondern ein klares Ja zur Freiheit abgeben - selbst mit dem Risiko, dass manche Kriminelle nicht überführt werden können. Aber es schützt auch Unbeteiligte, die durch falsche Algorithmen plötzlich in obskure Verdachtsmomente geraten könnten.

Deswegen ein klares Nein zu noch mehr Überwachung durch Verknüpfung verschiedenster Systeme. Nein zu Palantir - erst recht nicht, wenn die Funktionsweise dieses Systems nicht klar offengelegt wird und womöglich noch Daten in die USA abfließen.

Nr. 8 (Kommentar 8 am 30.07.2025, 18:40 Uhr)

Viel Geld, was besser in (Aus-)Bildung und Aufbau von Personen gesteckt werden sollte

Unterstützung: 47, Ablehnung: 24

10 Millionen Euro jährlich für eine Software und Infrastruktur, die nicht von den Behörden selbst sondern einem ausländischen Dienstleister kontrolliert und gesteuert wird, denen wichtige sensible Daten über Bürger übergeben werden (die teilweise nicht wegen Verbrechen gespeichert sind sondern nur in Polizei-Datenbanken sind weil sie Zeugen sind oder nur in der Nähe eines Tatorts) ist nicht der seriöse Umgang mit Steuergeldern oder den Daten der Bürger, der mir vorschwebt.

Insbesondere, da der Hersteller aus den USA stammt und damit - wie der französische Microsoft-Mitarbeiter unter EId zugeben musste - US-Geheimdienste alle Daten abgreifen dürfen und können, ohne das der Hersteller(!) dies weiss und/oder unterbinden kann, ist es für die Bürger sehr gefährlich, das diese Daten in der Software gespeichert werden. Selbst wenn einige Funktionen der Software nicht aktiviert werden, sind die Daten dafür vorhanden, die Funktionen später einzusetzen - mit den bereits vorhandenen Daten.

Nehmen Sie Abstand von dem Vorhaben, Gotham hier in Baden-Württemberg einzusetzen. Nutzen Sie das Geld lieber, eine eigene, europäosche, unserem Datenschutzstandard entsprechende Lösung zu bauen oder - noch besser - Polizeibeamte auszubilden, die dringend benötigt werden. Wir brauchen die Polizei präsent, als Freund und Helfer, nicht als drohendes Auge das alles sieht und nachforschen kann, egal wann und wo man etwas gemacht hat.

Nr. 9 (Kommentar 9 am 31.07.2025, 01:15 Uhr)

Nein zu Palantir aus faschistischem Software-Haus

Unterstützung: 12, Ablehnung: 8

Dieser Kommentar wurde aufgrund eines Verstoßes gegen die Netiquette entfernt.

Nr. 10 (Kommentar 10 am 31.07.2025, 12:09 Uhr)

Ablehnung der geplanten Einführung von Datenanalyseplattformen im Rahmen der Polizeigesetz-Novelle BW

Unterstützung: 47, Ablehnung: 17

Die geplante Novellierung des Polizeigesetzes, insbesondere im Hinblick auf die Ermöglichung des Einsatzes von Datenanalyseplattformen wie Palantir Gotham, lehne ich entschieden ab. Derartige Systeme stellen ein erhebliches Risiko für die Grundrechte, insbesondere das Recht auf informationelle Selbstbestimmung dar.

Der Einsatz von Software zur automatisierten Datenverknüpfung und Mustererkennung im Rahmen der Gefahrenabwehr bedeutet eine erhebliche Ausweitung polizeilicher Befugnisse. Es besteht die Gefahr, dass ohne konkreten Tatverdacht große Datenmengen aus verschiedensten Quellen zusammengeführt und ausgewertet werden – was faktisch zu einer anlasslosen Rasterung der Bevölkerung führen kann.

Zudem ist die Funktionsweise von Systemen wie Palantir nicht öffentlich nachvollziehbar, was rechtsstaatliche Transparenz und Kontrolle massiv einschränkt. Die fehlende algorithmische Nachvollziehbarkeit widerspricht grundlegenden rechtsstaatlichen Prinzipien, insbesondere dem Grundsatz der Verhältnismäßigkeit und dem Prinzip der Normenklarheit.

Aus kriminalistischer Sicht ist die Wirksamkeit solcher Systeme bislang nicht belegt. Vielmehr zeigen internationale Beispiele, dass der Einsatz von Predictive-Policing-Technologie zu diskriminierenden Effekten und Fehlentscheidungen führen kann.

Ich fordere daher die vollständige Überarbeitung des Gesetzesentwurfs mit besonderem Augenmerk auf den Schutz der Grundrechte, digitaler Souveränität und die Wahrung rechtsstaatlicher Prinzipien. Der präventive Einsatz intransparenter Analysewerkzeuge ist in einer freiheitlich-demokratischen Gesellschaft nicht akzeptabel.

Beteiligungsportal: Kommentare „Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften“

Nr. 11 (Kommentar 11 am 31.07.2025, 22:50 Uhr)

Datenschutz, Sicherheit, Effizienz und dann auch noch Palantir

Unterstützung: 35, Ablehnung: 18

Ich kann es überhaupt nicht nachvoll, wie ein Ministerium bei einem so sensiblen Thema eine Software-Entscheidung treffen kann, die bereits vorhandenen Fronten nur noch verstärken.

Der Wunsch, die Sicherheit der Bevölkerung zu verbessern, die Strafverfolgung zu erleichtern und Effizienz in der polizeilichen Arbeit zu erhöhen ist sehr gut nachvollziehbar.

Die Bestrebungen diese Ziele umzusetzen führen immer auch zu Fragen des Datenschutzes. Auch der Wunsch und die Notwendigkeit personelle Daten und die eigene Person zu schützen sollten bei allen Regierungsentscheidungen mitgedacht werden.

Die Novellierung des Polizeigesetztes alleine wirft bei vielen bereits Zweifel auf, ob dem Schutz der Daten und der Personen vor Willkür wirklich ausreichend Raum Rechnung getragen wird.

Das diese bereits schwierige Gemengelage durch die Wahl der Software auf eine derartige Weise zusätzlich belastet wird ist unerträglich. In der heutigen Weltlage sich als Landesregierung von einem Anbieter abhängig zu machen, bei dem mehr als berichtigte Zweifel bestehen dürften, dass er tatsächlich in jeder Situation die Datenhoheit des Landes wart ist nicht akzeptabel.

Statt Autonomie und digitaler Souveränität - was Hinsichtlich der IT-Infrastruktur eigentlich das Ziel einer jeden souveränen Demokratie sein sollte - sich in eine strukturelle Abhängigkeit von einem us-amerikanischen Konzern zu begeben, der fragliche Verbindungen hat, sollte trotz des bestehenden Vertrages unbedingt abgewandt werden.

Nr. 12 (Kommentar 12 am 01.08.2025, 01:19 Uhr)

Trotz Millionen-Investition muss Palantir ungenutzt bleiben - Gefahr ungerechtfertigter Kriminalisierung

Unterstützung: 44, Ablehnung: 17

Die getätigten finanziellen Vorleistungen und ein Knebelvertrag mit Palantir sind kein Grund unser Polizeigesetz zu ändern, nur um Software von Demokratiefeinden einzuführen. Lieber eben die Millionen zahlen, aber OHNE Nutzung als Nutzung nur damit die Millionen nicht umsonst seien. Damit wären unser Bürger*innenschutz gesichert. Keine Vorverurteilung von Menschen weil Maschinen dies meinen!

Edward Snowden hat uns alle vor über 10 Jahren gewarnt und die USA entzaubert. Und jetzt will Baden-Württemberg in dreister Weise Informationen gegen unser freies demokratisches Leben zusammenführen.

Beteiligungsportal: Kommentare „Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften“

Die Gefahr ungerechtfertigter Kriminalisierung bspl für die Umwelt oder Menschenrechte ist groß!!

Palantir ist ein US-amerikanisches Überwachungsunternehmen, das Software zur Analyse großer Datenmengen anbietet. Die Gründung des Konzerns wurde maßgeblich von der CIA finanziert. Auf Bundesebene möchten CDU und CSU die deutsche Polizei mit der Palantir-Software „Gotham“ ausstatten. Diese wurde entwickelt, um Daten aus verschiedenen Quellen wie Polizeidatenbanken, Gesundheitsdaten oder Social-Media-Inhalte zusammenzuführen und mit Hilfe von künstlicher Intelligenz in Sekundenschnelle auszuwerten.

Das Zusammenführen und die dann automatisierte Analyse dieser riesigen Datensätze stellt einen erheblichen Eingriff in die Privatsphäre der Bundesbürger*innen dar!

Die Software erstellt Profile aus Polizeidaten, um Straftaten vorherzusagen und Verdächtige zu identifizieren – doch auch Zeug*innen, Opfer oder sogar völlig Unbeteiligte geraten dabei in den Mittelpunkt von polizeilichen Ermittlungen. Für Außenstehende ist Palantir eine Blackbox. Nur der Konzern selbst weiß, wie die Software arbeitet; kaum jemand kennt den Software-Code. Schon jetzt entsendet Palantir eigene Mitarbeiter*innen in die deutschen Behörden, die Technologie bereits einsetzen, um die Software zu betreuen. Demokratische Kontrolle ist damit unmöglich. Allein in Bayern, wo die Software schon eingesetzt wird, haben Palantir-Mitarbeitende Zugriff auf die Daten von rund 30 Millionen Bürger*innen – das sind mehr als ein Drittel aller Deutschen.

Unter dem Deckmantel der Sicherheitspolitik treibt die Bundesregierung derzeit in zahlreichen Bereichen eine Ausweitung der staatlichen Überwachung voran. Vorhaben wie KI-Gesichtserkennung bei Videoüberwachung, Chatkontrolle und ein Zentralregister für psychisch kranke Menschen geben einen Vorgeschmack darauf, welche Daten in Zukunft in die Hände von Palantir geraten könnten.

In vielen Datensätzen sind People of Color überrepräsentiert – weil sie öfter durch die Polizei kontrolliert werden. Automatische Datenanalysen verstärken diese Diskriminierung, deshalb landen nicht-weiße Menschen überproportional häufig im Visier von Ermittler*innen.

Wie mit Hilfe von Palantir ein demokratischer Rechtsstaat in einen Überwachungsstaat verwandelt werden kann, sehen wir gerade in den USA. Dort nutzt die ultrarechte Trump-Regierung die Software bereits, um Migrant*innen aufzuspüren, zu deportieren und den autoritären Umbau des Staates voranzutreiben.

Bekommt Palantir vollständigen Zugriff auf die Datenbank der deutschen Polizei, kann zudem niemand ausschließen, dass die Daten an US-Geheimdienste weitergegeben werden. Zwar versichert Palantir-Gründer und Großaktionär Peter Thiel, Datenschutz ernst zu nehmen. Seine engen Verbindungen zur Trump-Administration und den US-Geheimdiensten geben jedoch Anlass zum Zweifel.

Peter Thiel ist einer der mächtigsten Tech-Milliardäre der Welt – und bekennender Demokratiefeind. Er erklärte 2009 öffentlich: „Ich glaube nicht länger, dass Demokratie und Freiheit kompatibel sind“. Thiel hält das Wahlrecht für Frauen für einen Fehler und möchte private Inseln sowie Städte für Reiche bauen, in denen sie sich vom Rest der Gesellschaft abkapseln können.

Der Milliardär ist ein enger Vertrauter von US-Präsident Donald Trump und gilt als einflussreicher Macher hinter dem Rechtsruck in den USA. Thiel finanzierte auch den Wahlkampf von J.D. Vance und verhalf ihm zur Position als USVizepräsident.

Sein Unternehmen Palantir benannte er nach den magischen Steinen aus dem Roman „Der Herr der Ringe“, die der Bösewicht Sauron zur Überwachung nutzt. Heute ist Thiel nicht mehr der Konzernchef, hat aber als Gründer und Großaktionär erheblichen Einfluss auf Palantir.

Die Palantir-Software kann uns erfassen, ohne etwas Falsches getan zu haben. Einfach zur falschen Zeit am falschen Ort zu sein kann Auswirkungen haben. Datenschützer*innen warnen davor, dass bei einem bundesweiten Einsatz massenhaft unbescholtene Menschen von polizeilichen Folgemaßnahmen bedroht sein könnten. Besonders gefährlich ist das mit Blick auf das Erstarken der rechtsextremen AfD. Schafft sie es in eine Landesregierung, könnte sie Palantir für ihre Zwecke nutzen. Denkbar wäre etwa, dass die Rechtsextremen versuchen, nach dem Vorbild von US-Präsident Trump die Software zur Deportation von Menschen zu nutzen.

Die Rechtslage rund um den Einsatz der Technologie ist jedoch höchst umstritten, denn Palantir verstößt gegen wesentliche Grundrechte: Die Software hält sich nicht an wesentliche Vorgaben des Datenschutzes und überwacht unschuldige Menschen. Da nicht geregelt ist, in welchen Fällen das Programm konkret eingesetzt wird, verletzt die Anwendung unser individuelles Recht auf informationelle Selbstbestimmung.

Die Gesellschaft für Freiheitsrechte (GFF) hat deshalb beim Bundesverfassungsgericht Beschwerden gegen den Einsatz von Palantir-Software in Hessen und Nordrhein-Westfalen eingereicht. Mit Erfolg: Die Richter*innen verhängten im Urteil zu Hessen strenge Auflagen. Seit Kurzem prüft das Gericht aufgrund einer weiteren Verfassungsbeschwerde der GFF auch den Einsatz der Software in Bayern.

Wenn Sicherheitsbehörden mit sensiblen Daten arbeiten, sollten die Programme transparent, quelloffen und demokratisch kontrollierbar sein. Viele Expert*innen fordern deshalb die Entwicklung einer europäischen Alternative zu Palantir.

Auch der Vorschlag, die Palantir-Software als zwischenzeitliche Lösung zu nutzen, ist fragwürdig: Ist das Programm einmal implementiert, tritt der sogenannte Lock-in-Effekt ein – es sind Abhängigkeiten entstanden, die einen Softwarewechsel zu einem späteren Zeitpunkt erschweren. Palantir bietet nämlich keine Möglichkeit an, das einmal aufgebaute System zu einem anderen Anbieter umzuziehen.

Zudem ist umstritten, wie effektiv der Einsatz von Palantir aktuell überhaupt ist. Offiziell dient das Programm der Abwehr von Terrorismus. Die deutsche Polizei setzt Palantir aber vor allem bei kleineren Delikten ein, manchmal sogar bei Fahrraddiebstahl. Es gibt bisher keine wissenschaftliche Auswertung zum tatsächlichen Anwendungsbereich der Software.

Nr. 13 (Kommentar 13 am 01.08.2025, 18:59 Uhr)

Palantir

Unterstützung: 37, Ablehnung: 17

Geht es nach dem Willen von CDU und CSU, kommt die Überwachungssoftware von Palantir bald in ganz Deutschland zum Einsatz. Sie soll der Polizei ermöglichen, sensible Daten von Bürger*innen zu verknüpfen und auszuwerten. Millionen Menschen könnten so ins Visier der Ermittlungsbehörden

geraten. Ein drastischer Eingriff in die Privatsphäre – für den eigentlich strenge Voraussetzungen und höchste Anforderungen an den Datenschutz erfüllt sein müssen. Das ist bei Palantir nicht der Fall.

Hinter der Software steht der Tech-Milliardär Peter Thiel, einer der wichtigsten Unterstützer Donald Trumps. Thiel ist für seine demokratiefeindlichen Aussagen bekannt. Um das komplexe Programm zu betreuen und zu warten, müssen Palantir-Mitarbeitende direkt in deutschen Polizeibehörden sitzen. Außerdem kann nicht ausgeschlossen werden, dass sensible Daten an US-Geheimdienste abfließen – denn wie die Software genau funktioniert, ist völlig intransparent.

Einerseits behauptet die Bundesregierung, dass sie eigenständige datenschutzkonforme europäische Lösungen unterstützen möchte, andererseits kauft sie US-amerikanische Produkte ein, die diesen Standards nicht genügen. Beides passt nicht zusammen. Die Daten sind nicht vor unserem nordamerikanischen "Verbündeten" sicher, der seine eigene Agenda zur Sicherung seiner Hegemonie verfolgt und der seine wirtschaftlichen und machtpolitischen Interessen rücksichtslos verfolgt, ohne sich um die Folgen für Demokratie und Menschenrechte zu scheren. Dafür steht nicht zuletzt (wenn auch nicht allein) Trumps Politik. Ich fordere die Bundesregierung auf, den drohenden Schaden für das deutsche Volk abzuwenden. Achten Sie auch in diesem Punkt das Grundgesetz!

Ich fordere deshalb von der SPD: Lassen Sie nicht zu, dass die Union sich durchsetzt – verhindern Sie überall die Überwachung durch Palantir!

Nr. 14 (Kommentar 14 am 02.08.2025, 03:01 Uhr)

Palantir Überwachungswerkzeug

Unterstützung: 37, Ablehnung: 18

Weiter werden unsere Grundrechte eingeschränkt, damit dann die Demokratie abgebaut und weiter versucht eine anlasslose Totale Überwachung der Bürger einzuführen. 1984 wird nun langsam zur Realität.

Nr. 15 (Kommentar 15 am 02.08.2025, 14:30 Uhr)

Permanente Bodycam Aufnahme sollte streng und klar geregelt werden.

Unterstützung: 23, Ablehnung: 24

Ich lehne insbesondere die geplante Ausweitung des Bodycam-Einsatzes strikt ab. Es ist aus meiner Sicht unverhältnismäßig und verfassungsrechtlich hoch problematisch, dass Bodycams künftig auch in privaten Wohnungen zum Einsatz kommen sollen.

Privaträume sind besonders geschützte Rückzugsorte – nicht ohne Grund gelten sie als „letzte Bastion der Privatsphäre“. Die Vorstellung, dass hier Polizeibeamte mit aktivierter Kamera eingreifen dürfen, verletzt aus meiner Sicht die Würde und das Vertrauen der Bevölkerung. Selbst wenn diese

Funktion nur im Einzelfall genutzt würde, schafft sie einen gefährlichen Präzedenzfall für die Aushöhlung der informationellen Selbstbestimmung.

Auch der Einsatz von sogenannten Pre-Recording-Funktionen führt zu einer pauschalen Vorratsdatenspeicherung ohne konkreten Anlass – das ist in einem freiheitlichen Rechtsstaat nicht akzeptabel.

Statt auf technologische Aufrüstung und weitere Überwachung zu setzen, sollte der Fokus auf bessere Ausbildung, Deeskalationstechniken und klare rechtliche Grenzen für Eingriffe in die Privatsphäre gelegt werden.

Ich fordere daher:

Kein Einsatz von Bodycams in Wohnungen

Strikte Einschränkung aller audiovisuellen Überwachungsmaßnahmen

Stärkere Kontrolle durch unabhängige Datenschutzstellen

Mehr Transparenz gegenüber der Öffentlichkeit

Nr. 16 (Kommentar 16 am 03.08.2025, 13:39 Uhr)

Palantir = Lieferung sensibelster Daten an USA

Unterstützung: 39, Ablehnung: 13

Rölf Gössner nach https://de.wikipedia.org/wiki/Palantir_Technologies

"Die Kundenliste der Firma liest sich wie das Who-is-who der US-Militär- und Sicherheitsbürokratie: CIA, FBI, NSA, Pentagon, Marines und Airforce. Oder anders ausgedrückt: Als Hauslieferant dieser Behörden ist die Firma tief in den militärisch-digitalen Komplex der USA verstrickt und ihr Geschäftsmodell heißt: BigData for BigBrother."

...und dafür zahlen wir auch noch!

Nr. 17 (Kommentar 17 am 04.08.2025, 09:00 Uhr)

Palantir ist eine große Gefahr für unsere Gesellschaft und unsere Demokratie und darf nicht genutzt werden!

Unterstützung: 36, Ablehnung: 16

Palantir scheint nur mehr Sicherheit zu bieten.

Stattdessen besteht die Gefahr einer militärischen Überwachung, Lieferung sensibler Daten an die USA , einer übermässigen Kontrolle und eventuellen falschen Anschuldigungen, sowie der Aushöhlung unserer Demokratie.

Sie dient eher dem Erhalt einem Machtimperium der USA.

Bitte entscheiden Sie sich gegen Palantir!

Ich will es auf keinen Fall nicht in unserem System haben!

Nr. 18 (Kommentar 19 am 06.08.2025, 08:46 Uhr)

Längst überfällig

Unterstützung: 30, Ablehnung: 31

Endlich Digitalisierung und zwar ohne Systembrüche nutzen! Ohne eine Zusammenführung und Auswertung von Daten sind erfolgreiche polizeiliche und rechtsstaatliche Ermittlungen nicht möglich, völlig ineffizient und führen zu einer Verstärkung der Wahrnehmung eines handlungsunfähigen Staates.

Palantir sollten wir aus Ermangelung von besseren Alternativen nutzen, allerdings daraus lernen, den Datenabfluss streng kontrollieren und mit Hochdruck an einer europäischen Lösung arbeiten.

Nr. 19 (Kommentar 20 am 06.08.2025, 20:34 Uhr)

Änderung des Polizeigesetzes

Unterstützung: 22, Ablehnung: 19

Dass wir in Notfällen endlich via Ortung gefunden werden können, ist schon lange überfällig.

Dass Palantir trotz Alternativen wie das polnische DataWalk und das französische ChapVision eingekauft wurde, ist unverantwortlich.

Ich vermisse die eindeutige Regelung, dass jedermann Video- bzw. Sprachaufzeichnungen von Polizeieinsätzen machen kann. Die Rechtslage ist hier leider nicht eindeutig.

Beteiligungsportal: Kommentare „Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften“

Nr. 20 (Kommentar 21 am 07.08.2025, 23:03 Uhr)

Überwachung

Unterstützung: 25, Ablehnung: 14

Nicht nur, dass sich die Verantwortlichen unsere Daten an Trump's CIA und NSA weitergeben. Man stelle sich vor: Deutschland in 20 Jahren, Weigel und Konsorten an der Macht: Dann wieder gute Nacht Deutscheland. Brilliant vorbereitet von CDU und den Grünen. "Ich kann gar nicht so viel essen, wie ich kotzen möchte!" (Berliner Maler Liebermann über Hitlers Machtübernahme). Na dann ...

Nr. 21 (Kommentar 22 am 08.08.2025, 15:12 Uhr)

Polizeigesetz

Unterstützung: 23, Ablehnung: 16

Kein Einsatz von Palantir, stattdessen europäische Software einsetzen!

Nr. 22 (Kommentar 23 am 08.08.2025, 16:40 Uhr)

Allmachtsbegehrlichkeiten nach Überwachung, Macht und Befugnissen

Unterstützung: 22, Ablehnung: 16

In zeiten zunehmender Auflösung der informationellen Selbstbestimmung durch big tech und social media, tritt die Regierung in deren Fußstapfen, anstelle die Rechte derer die sie vertritt zu stärken. Und dann werden die Wählenden am Ende noch verschaukelt woher die Erosion des Demokratieverständnisses kommt.

Mit einem zunehmenden Anwachsen der rechten Welle ist das fahrlässig und gefährlich.
Grundrechte müssen für solche Zeiten gestärkt werden, insbesondere zum Schutz vor polizeilicher Präventivwillkür.

Nr. 23 (Kommentar 24 am 12.08.2025, 20:43 Uhr)

Alternative?

Unterstützung: 16, Ablehnung: 12

Warum gibt es keine Alternative zu Palantir? Warum wollen wir einer amerikanische Datenkrake mit höchst fragwürdigem Personal intimste Daten anvertrauen? Das ist echt ein Skandal.

Beteiligungsportal: Kommentare „Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften“

Nr. 24 (Kommentar 25 am 13.08.2025, 15:51 Uhr)

Polizeigesetz

Unterstützung: 13, Ablehnung: 12

Dieses Gesetz ist längst überfällig. Dass wir auf Palantir angewiesen sind ist mehr als traurig.

Allerdings was nützen Gesetze wenn Sie nicht angewendet werden , denn davon haben wir genügend!

Die Anarchie lässt grüßen.

Nr. 25 (Kommentar 26 am 18.08.2025, 14:16 Uhr)

§ 57a (1): "Nachvollzierbarkeit, [...] SOWEIT dies technisch möglich ist"

Unterstützung: 2, Ablehnung: 4

"SOWEIT dies technisch möglich ist". Wie praktisch. Wenn z.B. Palantir nicht-nachvollziehbare KI einsetzt, ist dann ist es trotzdem gesetzeskonform, diese KI zu trainieren und einzusetzen?

Warum die offenen Trump-Kritiker bei den Täter-Identifizierungsvorschlägen immer ganz oben und die offenen Trump-Unterstützer ganz unten stehen?

Muss wohl ein versehentlicher Trainingsfehler sein. Die von Palantir haben doch hierzu ein großes Indianerehrenwort geleistet! Und Trump hat schließlich einen Ehrencodex und ordnet nicht einfach Microsoft an, Chefermittlern im internationalen Gerichtshof das E-Mail Konto zu sperren, nur weil ihm die Meinung misfällt.

Nr. 26 (Kommentar 27 am 19.08.2025, 22:38 Uhr)

Stellungnahme des Chaos Computer Club Stuttgart e.V.

Unterstützung: 0, Ablehnung: 0

Sehr geehrte Damen und Herren,

auch der Chaos Computer Club Stuttgart e.V. möchte zum geplanten Gesetz Stellung beziehen.

Sie finden unsere Stellungnahme unter https://www.cccs.de/2025-08-19-stellungnahme-polg-analyseplattform/CCCS_Stellungnahme_Gesetzentwurf_PolG_2025.pdf zum Download.

Baden-Württemberg
Normenkontrollrat

Stellungnahme des Normenkontrollrates Baden-Württemberg gem. Nr. 4.1 VwV NKR BW

27.03.2025

Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeilicher Vorschriften

NKR-Nummer 41/2025, Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg

Der Normenkontrollrat (NKR) Baden-Württemberg hat sich mit dem Entwurf des oben genannten Regelungsvorhabens befasst.

I. Im Einzelnen

Das Gesetz regelt durch Änderungen des Polizeigesetzes (PolG) und der Verordnung zur Durchführung des PolG (DVO PolG) zweierlei.

1.

Verarbeitung von Standortdaten bei Anwahl der Notrufnummer 110

Es wird eine Rechtsgrundlage geschaffen, wonach die Standortdaten eines mobilen Endgerätes vom Polizeivollzugsdienst abgerufen werden können, die nach Anwahl der Notrufnummer 110 automatisiert anfallen. Dadurch wird die Standortbestimmung von hilfesuchenden Personen verbessert.

2.

Automatisierte Datenanalyse

Es wird die Rechtsgrundlage für eine automatisierte Datenanalyse geschaffen und deren Voraussetzungen und Umfang entlang der Rechtsprechung des Bundesverfassungsgerichts geregelt. Mit einer automatisierten Datenanalyse werden bereits vorhandene aber bislang unverbundene Daten und Datenquellen des Polizeivollzugsdienstes in einer Analyseplattform zusammengeführt und somit systematisch erschlossen.

II. Votum

Das Ressort führt nachvollziehbar aus, dass beide Rechtsgrundlagen zu einer Vereinfachung und Beschleunigung polizeilicher Abläufe beitragen.

Dies zum einen bei der Rettung von Menschen in Notsituationen als auch bei der polizeilichen Gefahrenabwehr. Die Standortbestimmung wird ohne Medienbrüche digitalisiert und genauer und verlässlicher. Die automatisierte Analyse polizeilicher Daten reduziert Medienbrüche und macht manuelle Abfragen verschiedener Datenquellen entbehrlich.

Das Ressort regelt dabei die einzelnen Rechtseingriffe sorgfältig entlang den höchstrichterlichen Vorgaben zum Schutz des Grundrechts auf informationelle Selbstbestimmung. Dabei wird nach Einschätzung des NKR das geregelt, was erforderlich aber auch ausreichend ist.

Der NKR hat hierbei nichts zu beanstanden.

gez. Dr. Dieter Salomon
Vorsitzender

gez. Adrian Probst
Berichterstatter

Baden-Württemberg
Normenkontrollrat

Stellungnahme des Normenkontrollrates Baden-Württemberg gem. Nr. 4.1 VwV NKR BW

04.08.2025

Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeilicher Vorschriften

NKR-Nummer 41.2/2025, Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg

Der Normenkontrollrat (NKR) Baden-Württemberg hat sich mit dem Entwurf des oben genannten Regelungsvorhabens befasst.

I. Im Einzelnen

Der vorliegende Gesetzentwurf sieht in Folge eines politischen Kompromisses insbesondere eine Änderung des § 90 Polizeigesetzes (PolG) vor.

Dieser regelt bisher die Pflicht der *Landesregierung*, den *Landtag alle zwei Jahre* über bestimmte Maßnahmen der Datenerhebung zu unterrichten. Nunmehr wird das *Innenministerium* verpflichtet, das *Parlamentarische Kontrollgremium mindestens vierteljährlich* über die automatisierte Datenanalyse und die sonstigen schon bisherigen besonderen Maßnahmen zu unterrichten.

II. Votum

1.

Der NKR bezieht sich auf seine Stellungnahme Nummer 41/2025 vom 27.03.2025 und bekräftigt das darin zum Ausdruck kommende positive Votum zum Gesetzentwurf insgesamt.

2.

Der NKR stellt fest, dass durch die Änderung des § 90 PolG die Unterrichtungspflicht des Innenministeriums erheblich ausgeweitet wird. Dies hält der NKR für nicht erforderlich. Zudem ist eine Übertragung der Unterrichtungspflicht an das Parlamentarische Kontrollgremium systemwidrig, welches nach dem Gesetz über den Verfassungsschutz in Baden-Württemberg (LVSG) den Verfassungsschutz und nicht die Polizei kontrolliert.

Der NKR ist der Auffassung, dass ein politischer Kompromiss nicht zum Preis eines systemfremden Aufwuchses von Berichts- und Unterrichtungspflichten führen sollte, dessen Mehrwert zudem nicht weiter dargelegt wird.

gez. Margret Mergen
Stellvertretende Vorsitzende

gez. Adrian Probst
Berichterstatter

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Baden-Württemberg | Postfach 10 29 32 | 70025 Stuttgart

Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg

poststelle@im.bwl.de

- nur per E-Mail -

Name:

Telefon:
E-Mail: poststelle@lfdi.bwl.de

Geschäftszeichen: LfDIAbt2-0557.0-14/5
(bei Antwort bitte angeben)

Datum: 27.03.2025

Stellungnahme zum Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Ihr Schreiben vom 6. März 2025
Ihr Zeichen: IM3-1101-44/4

Sehr geehrter Herr
sehr geehrte Frau
sehr geehrte Damen und Herren,

vielen Dank für die Übermittlung des o.g. Gesetzentwurfs. Wir nehmen dazu wie folgt Stellung:

Zu § 45a PolG-E:

Wir begrüßen ausdrücklich, dass für die Einführung der automatisierten Standorterhebung beim Anwählen der 110 eine eigene Rechtsgrundlage geschaffen wird. Wie bereits in der Vergangenheit dargelegt sind wir der festen Überzeugung, dass die automatisierte Erhebung der Standortdaten aller Notrufenden, die zum Anruf ein Android-/iOS-Smartphone nutzen, gerade bei der 110 einer eigenen gesetzlichen Regelung bedarf (s. auch unser 40. Tätigkeitsbericht, S. 43 ff). Darüber hinaus befürworten wir die strenge Zweckbindung der beim Präsidium Technik, Logistik und Service angelieferten Daten. Soweit diese Zweckbindung ab dem Abruf durch die

Lautenschlagerstr. 20
70173 Stuttgart
E-Mail: poststelle@lfdi.bwl.de
Telefon: +49 711 615541-0

Internetseite: https://www.baden-wuerttemberg.datenschutz.de/
Serviceportal: https://www.service-bw.de
Datenschutz: Die Informationen bei Erhebung von personenbezogenen Daten nach Artikel 13 und 14 DS-GVO können unserer Internetseite entnommen werden (https://www.baden-wuerttemberg.datenschutz.de/datenschutz/).
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

zuständigen Notrufabfragestellen aufgehoben wird, ist dies aus unserer Sicht vertretbar. Denn eine Weiterverarbeitung – insbesondere eine solche zu Strafverfolgungszwecken – ist auch dann nicht voraussetzungslos zulässig, sondern an allgemeine Regeln gebunden, namentlich denjenigen aus § 15 Polizeigesetz.

Nach unserer Auffassung kann die Regelung keine Rechtsgrundlage für diejenigen Daten sein, die beim Präsidium Technik, Logistik und Service für die Notrufabfragestellen *der anderen Länder* angeliefert werden. Denn deren Erhebung dient dem Zweck der Aufgabenerfüllung deren zuständigen Stellen, also bspw. der Aufgabenerfüllung einer Leitstelle in Bayern. Soweit es in der Begründung zu § 45a PolG-E heißt: „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.“, empfehlen wir somit eine Klarstellung, dass die Norm keine Rechtsgrundlage für Datenerhebungen zum Zwecke der Aufgabenerfüllung anderer Länder darstellt. Dies auch deshalb, damit für die anderen Länder klar ist, dass sie selbst für die in ihre Zuständigkeit fallenden Datenerhebungen eine Rechtsgrundlage schaffen müssen, nicht nur für den Abruf beim Präsidium Technik, Logistik und Service.

Mit Blick darauf, dass durch die avisierte Technologie automatisiert der Standort von Anrufenden, die sich mit einem Smartphone an die 110 wenden, erhoben wird, empfehlen wir die Ergänzung einer Kontrollpflicht der abrufenden Stellen, bspw. wie folgt:

(3) Die abrufende Stelle prüft stichprobenweise die Rechtmäßigkeit der Abrufe vor Ablauf der Löschfrist. Die Aufzeichnungen des Präsidiums Technik, Logistik, Service sind der abrufenden Stelle auf Verlangen zu diesem Zweck zu übermitteln.

So würde das Risiko reduziert, dass die Voraussetzungen der Regelung, insbesondere das Abrufen der Daten nur bei Erforderlichkeit, umgangen werden.

Um die Transparenz, bzw. Nachvollziehbarkeit für potentiell betroffene Personen zu erhöhen, empfehlen wir außerdem, die Öffentlichkeit aktiv über diese neue Standortdatenerhebung zu informieren.

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Zu § 47a PolG-E:

Das Bundesverfassungsgericht hat in seinem Urteil vom 16.2.2023 (BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/ 19, 1 BvR 2634/20 - Rn. (1 - 178), http://www.bverfg.de/e/rs20230216_1bvr154719.html) festgestellt, dass einem verfahrens- und datenbankübergreifender Abgleich personenbezogener Daten ein eigenes Eingriffsgewicht innewohnt, welches der Gesetzgeber erlauben kann, aber hinreichend normenklar und bestimmt regeln muss. Der hiesige Regelungsentwurf ist, verglichen mit den entscheidungsgegenständlichen Regelungen, umfangreicher und umgrenzt den Eingriff in Art und Umfang sowie in Bezug auf den Anlass. Dadurch wird ein deutlich engerer Rahmen gesetzt und wesentliche Entscheidungen durch den Gesetzgeber getroffen. Ohne Kenntnis der vorgesehenen Verwaltungsvorschrift ist eine abschließende Prüfung für uns jedoch nicht möglich. Wir regen folgende Ergänzungen/ Klarstellungen an:

1. Ausschluss der Einbeziehung von Daten Unbeteiligter, jedenfalls soweit bezüglich dieser eine Kennzeichnungspflicht nach § 72 Polizeigesetz besteht

Gemäß § 72 PolG sind personenbezogene Daten in polizeilichen Informationssystemen zu kennzeichnen. Dazu gehört auch die „Kategorie betroffener Personen“, soweit für sie Grunddaten gemäß § 15 Absatz 3 Satz 2 PolG angelegt wurden. Derzeit ist in § 47 Absatz 4 Satz 3 PolG-E vorgesehen, dass in der Verwaltungsvorschrift technisch-organisatorische Maßnahmen vorzusehen sind, durch die „die Einbeziehung von Daten unbeteiligter Personen möglichst zu vermeiden“ sind. Diese vage Formulierung kann vor dem Hintergrund der jedenfalls teilweise bestehenden Verpflichtung zur Kennzeichnung von Personen nicht nachvollzogen werden. Zur Reduktion der Eingriffsintensität empfehlen wir deshalb dringend, eine Pflicht zur Nichteinbeziehung von Daten Unbeteiligter – jedenfalls soweit Sie im Sinne des § 72 PolG ohnehin zu kennzeichnen sind – zu normieren oder an konkrete Voraussetzungen zu knüpfen. Beispielsweise könnte ein weiterer Satz an Absatz 3 angefügt werden:

> *Daten Unbeteiligter dürfen jedenfalls im Umfang der Kennzeichnungspflicht gemäß § 72 nicht einbezogen werden.*

Und dies in Absatz 4 wie folgt ergänzt werden:

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Die Vorgaben in der Verwaltungsvorschrift dienen unter Berücksichtigung der in Absatz 1 beschriebenen Eingriffsschwellen dem übergeordneten Ziel, die Datenbestände auf das für den Analysezweck erforderliche Maß zu begrenzen und die Einbeziehung von Daten unbeteiligter Personen *auch über den in Absatz 3 Satz 7 genannten Umfang so umfassend wie möglich* zu vermeiden.

Der Ausschluss der Einbeziehung von Daten Unbeteiligter ließe sich auch in Absatz 6 umfassender festhalten, beispielsweise wie folgt:

Das Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten nach Absatz 4 Satz 2 Nummer 2 legt fest, welche personenbezogenen Daten in welcher Weise in die automatisierte Datenanalyse einbezogen werden dürfen. Ausgangspunkt ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen. Zum Schutz unbeteiligter Personen werden deren personenbezogene Vorgangsdaten, *sowie deren Daten, die infolge einer Kennzeichnung nach § 72 herausgefiltert werden können,* in eine automatisierte Datenanalyse nicht einbezogen.

2. Regelung einer verpflichtenden Stichprobenkontrolle und ergänzendes Qualitätsmanagement in den Verwaltungsvorschriften

Wir empfehlen die ausdrückliche Regelung einer stichprobenartigen Kontrolle. Auch wenn durch das Anordnungserfordernis aus Abs. 7 bereits eine erhebliche Schwelle zur Umgehung von Voraussetzungen besteht, ist es aus unserer Sicht unerlässlich, dass die verantwortlichen Stellen selbst Kontrollmechanismen etablieren, die eine nicht erlaubte Nutzung dieses so mächtigen Recherchetools kontrollieren (s. auch BVerfG, Rn. 109: „Insbesondere der sachgerechten Kontrolle kommt große Bedeutung zu.“). Dies könnte bspw. wie folgt in Absatz 4 integriert werden:

Technisch-organisatorische Vorkehrungen insbesondere zur Einhaltung der Zweckbindung nach § 15 Absätze 2 und 3 werden in einer Verwaltungsvorschrift geregelt, die zu veröffentlichen ist. Diese beinhaltet insbesondere

2. ein Rollen- und Rechtekonzept,

3. ein Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten,

4. ein Konzept zur Zugriffskontrolle *inklusive verdachtsunabhängiger Stichprobenkontrollen protokollierter Zugriffe* sowie [...]

Für die Ergebnisqualität von Suchen in einem solchen neuen Recherchetool wird im Übrigen die Qualität der Bestandsdaten entscheidend sein. Deswegen regen wir an, in den Verwaltungsvorschriften auch Maßnahmen eines diesbezüglichen Qualitätsmanagements vorzusehen.

Im Übrigen:

Soweit Sie den beiden Vorschriften vorgelagert unter „E. Bürokratievermeidung, Prüfung Vollzugstauglichkeit“ ausführen, dass der Gesetzentwurf keine erheblichen Auswirkungen für die Verwaltung oder aufwendige Verwaltungsverfahren verursachen wird, lässt dies außer Acht, welche Auswirkung § 47a PolG-E für den Landesbeauftragten für den Datenschutz und die Informationsfreiheit haben wird. Dies hervorzuheben ist uns deshalb ein Anliegen, da ein wesentlicher Baustein bei der Abmilderung eingriffsintensiver Maßnahmen wie der verfahrensübergreifenden automatisierten Datenanalyse die Einbindung und Kontrolle durch die Datenschutzaufsicht ist (u.a. BVerfG, Rn. 109). Die Einführung des § 47a PolG-E löst mindestens die folgenden Verwaltungsverfahren beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit aus

- Beratungsverfahren zu / Beteiligung an den Verwaltungsvorschriften aus Abs. 4 und 5
- Anhörungsverfahren nach § 47a Abs. 8 PolG-E (wiederholend)
- zukünftig: Kontrollverfahren zum Zwecke der Überprüfung der Einhaltung gesetzlicher Vorhaben (wiederholend)

Zur Durchführung dieser Verfahren bedarf es sowohl juristischer, als auch technischer Expertise. Die o.g. Verfahren sind mit Blick auf die Erheblichkeit der anvisierten neuartigen Grund-

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

rechtseingriffe unabdingbar, mit Blick auf die Größe unserer Dienststelle aber auch eine erhebliche Ressourcenbindung, die dementsprechend bei der Darlegung des vom Gesetz ausgelösten Aufwands Erwähnung finden sollte.

Mit freundlichen Grüßen
gez. Braun-Jäger

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Baden-Württemberg | Postfach 10 29 32 | 70025 Stuttgart

Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg

Per E-Mail

Name:
Telefon:
E-Mail: poststelle@lfdi.bwl.de

Geschäftszeichen: LfDIAbt2-0557.0-14/5
(bei Antwort bitte angeben)

Datum: 05.06.2025

Entwurf eines Gesetzes zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften
Hier: Stellungnahme zum neuen Entwurf aus Ihrem Schreiben vom 22. Mai 2025
Ihr Zeichen: IM3-1101-44/4

Sehr geehrte Damen und Herren,

wir danken für die Einbindung und nehmen wie folgt Stellung:

A. Zu § 45a PolG-E

Wir haben keine ergänzenden Anmerkungen gegenüber unserer Stellungnahme vom 27. März 2025.

B. Zu § 47a PolG-E

Mit Blick auf die Erheblichkeit der Regelung und die komplexe Rechts- und Sachlage nehmen wir gerne die erneute Möglichkeit zur Stellungnahme wahr, um zunächst einige grundsätzliche Erwägungen mitzuteilen und anschließend auf einzelne Aspekte näher einzugehen.

Die Regelung setzt bereits eine Vielzahl an Voraussetzungen um, die vom Bundesverfassungsgericht in seinem Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 vorgegeben wurden. Gleichwohl sind wir nach näherer Prüfung zu dem Ergebnis gekommen, dass vor dem Hintergrund der umfassenden Weichenstellung für die Zukunft polizeilicher Arbeit und umfangreichen Datenverarbeitung einige Aspekte klarer durch den Gesetzgeber geregelt werden sollten, bzw.

Lautenschlagerstr. 20
70173 Stuttgart
E-Mail: poststelle@lfdi.bwl.de
Telefon: +49 711 615541-0

Internetseite: https://www.baden-wuerttemberg.datenschutz.de/
Serviceportal: https://www.service-bw.de
Datenschutz: Die Informationen bei Erhebung von personenbezogenen Daten nach Artikel 13 und 14 DS-GVO können unserer Internetseite entnommen werden (https://www.baden-wuerttemberg.datenschutz.de/datenschutz/).
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

müssen, letzteres insbesondere mit Blick auf die nunmehr eingefügte Erlaubnis für eine automatisierte Bewertung der Daten mittels Künstlicher Intelligenz. Diese wird unseres Erachtens verfassungsrechtlichen Anforderungen nicht gerecht (dazu Näheres s.u. II.3.).

I. Grundsätzliches

Die Einführung einer Regelung zur automatisierten Datenanalyse, nunmehr avisiert unter Einbeziehung der Möglichkeiten von Künstlicher Intelligenz, stellt für die polizeiliche Arbeit einen grundlegenden Wandel dar. Sie birgt erhebliche Potentiale für die Effizienz polizeilichen Handelns und damit für die Sicherheit in Baden-Württemberg. Die Bewältigung großer Datenmengen ist heute wesentlicher Bestandteil polizeilicher Arbeit und bedarf dringend eines adäquaten rechtlichen Rahmens. Gleichzeitig handelt es sich bei einer automatisierten Analyse großer Datenmengen um ein mächtiges Instrument, welches erheblich in die Grundrechte der Personen eingreift, über die Informationen bei der Polizei vorhanden sind, bzw. durch diese verfügbar gemacht werden können (präziser zu Art und Umfang der Daten, die in die Analyse einfließen können, s.u. II. 3.). Das Bundesverfassungsgericht hat in seinem Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 bereits darüber entschieden, dass eine automatisierte Datenanalyse mit dem Grundgesetz vereinbar sein kann. Vor diesem Hintergrund stellen wir nicht in Abrede, dass der Gesetzgeber der Exekutive diese Maßnahme erlauben darf. Auch kommt dem Gesetzgeber eine Einschätzungsprärogative zu. Er verfügt also bei der Normsetzung über einen in Teilen der Kontrolle entzogenen Spielraum bei der Beurteilung der tatsächlichen Lage und den Folgen seiner Normsetzung. Allerdings wirft der derzeitige Entwurf Fragen in Bezug darauf auf, ob der Gesetzgeber durch ihn in hinreichender Weise (selbst) über die Eingriffe in die Rechte und Freiheiten betroffener Personen entscheidet. Gerade weil die Sach- und Rechtslage zur automatisierten Datenanalyse komplex ist, müssen unseres Erachtens wesentliche Faktoren durch den Gesetzgeber klarer und deutlicher entschieden und begründet werden.

Auch wenn das Bundesverfassungsgericht die Verknüpfung und Auswertung polizeilicher Datenbestände für grundsätzlich grundgesetzkonform erachtet und dabei auch die Möglichkeit gesehen hat, Teile der Regelung in eine Verwaltungsvorschrift zu verlegen; so bleibt es dennoch dabei, dass die Entscheidung über dasjenige, was „für die Grundrechtsverwirklichung wesentlich“ ist, durch den Gesetzgeber entschieden werden muss (s. z.B. BVerfG, Beschluss vom 8. 8. 1978 - 2 BvL 8/77). Je wesentlicher eine Angelegenheit für den Bürger und die Allgemeinheit ist, desto höhere Anforderungen werden an den Gesetzgeber gestellt. Je nachhaltiger also die Grundrechte Einzelner durch eine Regelung betroffen oder je gewichtiger die Auswirkungen für die Allgemeinheit sind, desto präziser und enger muss die gesetzliche Regelung sein. Mit der

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Einführung der Datenanalyse wird durch die Zusammenführung einer Vielzahl an „Datentöpfen“ das Eingriffsgewicht für den Einzelnen deutlich erhöht, denn auf diese Weise lassen sich viel umfangreichere Informationen zusammentragen, gar Profile über einzelne Personen anlegen, da umfassende Einblicke in Gewohnheiten, soziale Verankerungen, etc. möglich werden – also ein Bewegungs- oder Verhaltensprofil einer Person oder ein umfassenderes Persönlichkeitsbild geschaffen werden kann (vgl. BVerfG, Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 77). Darüber hinaus ist erwartbar, dass die Einführung der Analysemöglichkeit Auswirkungen auf die Allgemeinheit und deren Erleben ihrer Freiheit haben wird. Beides wird durch die Ergänzung um den Einsatz „Künstlicher Intelligenz“ verstärkt.

Wir möchten zunächst darauf hinweisen, dass die technische Grundkonzeption der Datenanalyse zu einer Risikoerhöhung für betroffene Personen führt, die nicht in einer rechtlichen Notwendigkeit gründet. Dem Grunde nach ist die automatisierte Datenanalyse eine Dateisystemübergreifende Suchfunktion mit Visualisierungseffekten (so auch in der Begründung: *Zunächst soll eine Rechtsgrundlage dafür geschaffen werden, bisher unverbundene Daten und Datenquellen des Polizeivollzugsdienstes in einer Analyseplattform zusammenzuführen, um die vorhandenen Datenbestände durch Suchfunktionen systematisch erschließen zu können (automatisierte Datenanalyse).“*. Dass diese Suchfunktion aktuell eine Kopie sämtlicher Datenbestände erfordert, ist der zersplitterten polizeilichen IT-Infrastruktur geschuldet, in der die vorhandenen Daten nicht gleichzeitig durchsucht werden können. Klar ist also, dass die Kopie der vorgesehenen Datenbestände nur deshalb zur gemeinsamen Durchsuchung erforderlich ist, weil bei den vorhandenen Systemen technisch keine hinreichende fachverfahrenübergreifende Durchsuchung möglich ist. Dieser Umstand gründet folglich nicht in einer rechtlich notwendigen Trennung bestimmter Daten, sondern in der Art und Weise der technischen Konzeption polizeilicher Datenverarbeitung. Mit der Regelung wird folglich mindestens ein Verarbeitungsvorgang geschaffen – die Zusammenführung der genannten Datentöpfe – der nur deshalb notwendig wird, weil die vorhandenen Verarbeitungssysteme technisch inkompatibel sind. Allein durch die Doppelspeicherung entsteht für die Personen, um deren Daten es dabei geht, ein höheres Risiko. Auch wenn alle erdenklichen Schutzmaßnahmen technischer und organisatorischer Art für diese Daten ergriffen werden, so ist jede Schutzmaßnahme eine Wahrscheinlichkeitsrechnung und keine absolute Sicherheit.

Das Recht auf Informationelle Selbstbestimmung darf durch eine gesetzliche Grundlage eingeschränkt werden, wenn die Regelung verhältnismäßig ist und sich aus ihr die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergibt und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfG, Urteil vom 15. Dezember

1983 – 1 BvR 209/83, Rn. 149). Je tiefer der Eingriff, desto mehr muss der Gesetzgeber auch organisatorische und verfahrensrechtliche Vorkehrungen treffen, um die Rechte und Freiheiten betroffener Personen zu schützen (vgl. oben). Das Bundesverfassungsgericht hat in seinem Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 u.a. auf die folgenden Aspekte verwiesen, die bei der Abwägung des Eingriffs durch eine automatisierte Datenanalyse zu berücksichtigen – und dementsprechend im Wesentlichen durch den Gesetzgeber zu entscheiden – sind : die Art der betroffenen Daten, den Umfang der Daten, die Methode der Datenverarbeitung (und mögliche Ergebnisse), die Eingriffsschwellen, die Abmilderung der Eingriffe und die Folgen der zu erlaubenden Eingriffe.

Anders als in der Datenschutz-Grundverordnung enthält die RL (EU) 2016/680, die die Verarbeitung personenbezogener Daten zu polizeilichen Zwecken regelt, keinen ausdrücklichen Grundsatz der Transparenz. Aufklärungs- und Auskunftspflichten als Schutzvorkehrung für betroffene Personen sind jedoch auch dem Verfassungsrecht immanent (vgl. z.B. BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83, Rn. 154). Bei heimlichen Maßnahmen, bei denen die Erlangung von Rechtsschutz erschwert ist, gilt dies umso mehr.

II. Einzelnes

1. Zu den Eingriffsschwellen

In der Gesetzesbegründung heißt es zum Zweck der Einführung einer Datenanalyse: *„In zeitkritischen Gefahrenlagen, beispielsweise bei der Verhinderung eines drohenden terroristischen Anschlags, des andauernden sexuellen Missbrauchs zum Nachteil eines Kindes oder einer drohenden schweren Gewalttat, ist die schnelle Reaktionsfähigkeit ein erfolgskritischer Faktor.“*. Dass dem so ist, wollen wir selbstverständlich nicht bestreiten. Allerdings sieht § 47a PolG die Analyse in einer Vielzahl an weiteren Konstellationen vor, z.B. läge eine konkrete Gefahr für den Leib einer Person (vgl. Eingriffsschwelle aus § 47a Abs. 1 Nr. 1 PolG-E) auch im Falle einer hinreichend wahrscheinlichen Schlägerei oder leichten Körperverletzung vor. Zwar heißt es in der Regelung, dass der Einsatz der Analyse nur dann zulässig ist, wenn die Analyse *erforderlich* ist, um die Gefahr abzuwehren. Aus Sorge vor einer zu weitreichenden Auslegung dieses Begriffs und der Unmöglichkeit vorgelagerten sowie eingegrenztem nachträglichen Rechtschutzes (Näheres s.u. II. 4) empfehlen wir mindestens die Darlegung dessen, was „erforderlich“ meint. Derzeit wird in der Gesetzesbegründung nur auf die Voraussetzung einer konkreten Gefahr eingegangen und geschildert, dass die Eingriffsschwelle an enge Voraussetzung geknüpft ist, „wie sie allgemein für eingriffsintensive Maßnahmen gelten“. Dass allerdings die Erforderlichkeit – insbesondere

bei europarechtskonformer Auslegung im Lichte der JI-RL (vgl. hierzu auch EuGH ECLI:EU:C:2022:491, Rn. 148, 149) – eine weitere Eingrenzung enthält, geht daraus nicht hervor. Deswegen empfehlen wir mindestens in der Gesetzesbegründung aufzugreifen, dass bei der Erforderlichkeit strenge Maßstäbe anzusetzen sind. Klar muss sein, dass die automatisierte Datenanalyse ein Instrument ist, dass nur dann zum Einsatz kommt, wenn es um erhebliche Gefahren geht und andere Mittel nicht zur Verfügung stehen.

2. Zu „Art und Umfang“ der verwendeten Daten:

Mit Blick auf die Wesentlichkeitstheorie, den Bestimmtheitsgrundsatz und die Normenklarheit ist bedenklich, dass die Bestimmung der in die Analyse einzuspeisenden Inhalte nicht an den grundgesetzlich geschützten Inhalten (d.h. an den Informationen über die natürlichen Personen) orientiert ist, sondern daran, wie die polizeilichen Arbeitssysteme strukturiert sind. Denn damit fällt der Gesetzgeber keine klare Entscheidung darüber, *welche* Informationen über *welche* und *wie viele* Personen verarbeitet werden dürfen. Diese Entscheidung fällt infolge dieser Konzeption weitestgehend die Exekutive, indem sie entscheidet, welche Daten in die jeweiligen Systeme eingespeist werden. Dies begegnet insbesondere mit Blick auf die sog. „Vorgangsdaten“ und „Falldaten“ Bedenken.

Vorgangsdaten meint diejenigen Daten, die im Vorgangsbearbeitungssystem der Polizei gespeichert sind. Sie dienen der Aufgabenerfüllung sowie der Vorgangsbearbeitung und Dokumentation repressiven oder präventiven polizeilichen Handelns. Das bedeutet, dass sich darin Informationen zu strafrechtlichen Ermittlungen befinden, beispielsweise zu einem Raubüberfall, aber auch zu Ruhestörungen, Verkehrsunfällen oder Versammlungen. Hier können folglich auch personenbezogene Daten beispielsweise von Versammlungsleiter_innen, Rettungskräften, Hinweisgeber_innen oder sonstigen Personen enthalten sein, die selbst keinen Anlass im polizei- oder strafrechtlichen Sinne gegeben haben, um in polizeilichen Informationssystemen aufzutauchen (gemeint: als Verdächtige oder Verantwortliche („Störer“)). Inwieweit bereits jetzt innerhalb des Vorgangsbearbeitungssystems eine Kennzeichnung dieser Daten geschieht und eine Vorsortierung der Inhalte möglich ist, ist uns nicht bekannt. Jedenfalls ist in § 47a PolG-E derzeit keine Differenzierung *der Inhalte* der personenbezogenen Daten auf Ebene des Gesetzes vorgesehen. Wessen Daten einbezogen und wie sie unterschieden würden, soll stattdessen in der Verwaltungsvorschrift festgelegt werden, s. § 47a Abs. 6 Pol-E: *„Das Konzept zur Kategorisierung und Kennzeichnung personenbezogener Daten nach Absatz 4 Satz 2 Nummer 2 legt fest, welche personenbezogenen Daten in welcher Weise in die automatisierte Datenanalyse einbezogen werden dürfen. Ausgangspunkt ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und*

andererseits unbeteiligten Personen. Zum Schutz unbeteiligter Personen werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen.“. Damit wird ein entscheidender Aspekt der Tragweite des Grundrechtseingriffs in die Hände der Exekutive gelegt und der öffentlichen parlamentarischen Debatte entzogen**.** Trotz Verständnisses für das polizeiliche Interesse, möglichst viele Daten in die Auswertung einzubeziehen, die ggf. auch Verbindungen zwischen Personen durch Dritte ermöglichen, begegnet es zumindest Bedenken, dass nach der vorgesehenen Regelung nicht der Gesetzgeber, sondern die Exekutive darüber entscheidet, wessen Daten zur Analyse freigegeben werden und in welchem Umfang.

Darüber hinaus gilt der vorgesehene Ausschluss Unbeteiligter nach derzeitiger Formulierung nur für Vorgangsdaten. Für alle anderen „Datentöpfe“ ist kein Ausschluss vorgesehen. Dies ist insbesondere mit Blick auf Falldaten problematisch. Denn auch diese können eine Vielzahl verschiedenster Informationen enthalten, sollen sie es doch gerade ermöglichen, Strukturen und Beziehungsnetzwerke zu ermitteln und abzubilden. Es ist daher nicht verständlich weshalb der Ausschluss „Unbeteiligter“ – mag der Begriff auch rechtsunsicher sein – nur für Vorgangsdaten gelten soll. So können Personen, die nur zufällig in Kontakt mit der Polizei gekommen sind, in allen Bereichen auftreten. Es ist nicht nachvollziehbar – und aus der Gesetzesbegründung heraus auch nicht ersichtlich – aus welchem Grund es angemessen sein sollte, die Daten Unbeteiligter überhaupt in die Analyse miteinzubeziehen. Dies insbesondere vor dem Hintergrund, dass polizeiliche Daten nach § 72 PolG bereits jetzt zu kennzeichnen sind. Spätestens mit Ablauf der Übergangsfrist zur Umsetzung der Kennzeichnungspflicht besteht kein Grund, die vorhandene Kennzeichnung aus allen Systemen zum Schutz betroffener Personen einzusetzen und über die Vorgangsdaten hinaus gesetzlich vorzuschreiben.

Wir begrüßen ausdrücklich, dass personenbezogene Daten, die aus einer Wohnraumüberwachung oder einer Online-Durchsuchung gewonnen wurden, nicht in die automatisierte Datenanalyse einbezogen werden dürfen. Nicht ausgeschlossen sind allerdings beispielsweise Informationen, die aus dem Einsatz verdeckter Ermittler, längerfristige Observationen oder der Einsatz technischer Mittel außerhalb von Wohnungen gewonnen wurden. Auch in diesen Fällen sind voraussichtlich eine Vielzahl an Personen miterfasst, die keinen eigenen Anlass gesetzt haben (wieder: als Verdächtige im straf- oder Verantwortliche im polizeirechtlichen Sinne).

Wir weisen auch darauf hin, dass polizeiliche Daten grundsätzlich dahingehend zu trennen sind, welche zum Zwecke der Strafverfolgung verarbeitet werden und welche zum Zwecke der Gefahrenabwehr. Diese rechtlich vorgeschriebene Trennung ist in der polizeilichen Arbeit oft schwierig umzusetzen. Bei der Konzeption, welche strafprozessualen Daten in die Analyse einfließen dür-

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

fen, müssen demnach die §§ 481 ff. StPO berücksichtigt werden. § 49 BDSG kann unserer Auffassung nach nicht herangezogen werden, soweit die StPO bereits spezielle Regelungen zur Weiterverarbeitung trifft.

3. Zum Einsatz künstlicher Intelligenz

Aus verfassungsrechtlicher Perspektive ist der Einsatz von „Künstlicher Intelligenz" eine besondere Art der automatisierten Datenverarbeitung. Mit Blick auf die o.g. dargelegten Grundsätze, dass der Gesetzgeber die für die Grundrechtsverwirklichung wesentlichen Aspekte selbst entscheiden muss, begegnet die hier angestrebte Regelung erheblichen Bedenken. Es bleibt unklar, welche Arten von Künstlicher Intelligenz eingesetzt werden sollen und welchem Zweck sie dienen (vgl. Kriterium des BVerfG in Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 oben: „Methoden" der Datenverarbeitung). Die Gesetzesbegründung nennt hier zwar einige Beispiele, die unseres Erachtens allerdings zu vage bleiben. Die aktuelle Formulierung im Wortlaut enthält eine Pauschalerlaubnis, die durch diese Beispiele nicht eingegrenzt wird.

In der Pauschalität der Norm bleibt unklar, was genau und weshalb der Gesetzgeber den Einsatz von Künstlicher Intelligenz bei der Datenanalyse zulassen möchte. Trotz Einschätzungsprärogative ist dies jedoch entscheidender Ausgangspunkt von Gesetzgebung: Zu welchem Zweck, mit welchem *Ziel*, und mit welchem Mittel soll der Eingriff in ein Grundrecht erlaubt werden. Eben dies ergibt sich nicht aus dem Wortlaut des Regelungsentwurfs („bewerten") und auch die Gesetzesbegründung führt nur Beispiele an, lässt somit potentiell Raum für nicht überblickbare und zukünftige technische Möglichkeiten. Die Grenzen der Eingriffsbefugnis müssen jedoch durch den Gesetzgeber festgelegt werden, insbesondere mit Blick auf den Zweckbindungsgrundsatz. Grundsätzlich wird nicht in Abrede gestellt, dass der Gesetzgeber automatisierte Datenverarbeitungen, die als KI qualifiziert werden können, erlauben darf. Allerdings muss klar sein, welche Bewertungen mittels KI erlaubt werden sollen. Dies bleibt im vorliegenden Entwurf jedoch offen.

4. Zur Transparenz für die betroffenen Personen und Kontrollmechanismen als Faktoren zur Abmilderung der Eingriffsintensität

Im derzeitigen Entwurf ist eine Benachrichtigung im Sinne des § 86 PolG nur für diejenigen Personen vorgesehen, „gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden".

Was unter „weitere Maßnahmen" zu verstehen ist, bleibt in der Formulierung des § 86 PolG-E mit Blick auf den Bestimmtheitsgrundsatz zu unbestimmt. So könnten einerseits „Standardmaßnah-

men“ der Polizei darunterfallen. Andererseits könnte als Maßnahme auch jeder weitere Grundrechtseingriff verstanden werden, so z. B. das Extrahieren von der Analyseplattform und Einfügen in einen anderen Kontext, beispielsweise ein Fallbearbeitungssystem, ein Vorgangsbearbeitungssystem oder – je nach Konzeption der Analyseplattform – das dortige Abspeichern als vorgangsrelevant o.Ä. mit der Konsequenz, dass eine Benachrichtigungspflicht ausgelöst würde.

Eine vorgelagerte Kontrolle, wie sie durch das Anordnungserfordernis in § 47a Absatz 7 PolG-E vorgesehen ist, wird nach unserer Bewertung durch die Delegationsmöglichkeit in § 4 DVO PolG-E zu weit aufgeweicht. Zwar kann nachvollzogen werden, dass beispielsweise am Wochenende eine Notwendigkeit bestehen kann, dass auch ein Polizeiführer vom Dienst eine automatisierte Datenanalyse anordnen kann, allerdings schränkt die derzeitige Formulierung die Delegationsmöglichkeit nicht auf Notfälle oder Situationen ein, in denen die jeweiligen Leitungen nicht erreichbar sind. Der Gesetz-, bzw. in § 4 DVO-PolG der Verordnungsgeber, erlaubt demnach die Delegation an den Polizeiführer vom Dienst ohne dies an weitere Voraussetzungen zu knüpfen. Auch könnte es Rechtsunsicherheit begegnen, was genau von dem Anordnungserfordernis erfasst ist, namentlich, was mit „Maßnahme“ in Absatz 7 gemeint ist. So ließe sich der Wortlaut derart auslegen, dass jeder einzelne Suchvorgang auf der Analyseplattform einer Anordnung bedarf.

5. Zu den noch zu regelnden technischen und organisatorischen Vorkehrungen

Die Regelungen zum Rechte- und Rollenkonzept müssen selbstverständlich die bestehenden Rechte- und Rollenkonzepte konsolidieren und keine faktische Umgehung zu trennender Datensätze erlauben. Hier verweisen wir nochmals auf §§ 481 ff. StPO. Soweit die Kategorisierung und Kennzeichnung neue Informationen über Personen kreiert muss klar sein, dass die Vorschrift keine Erlaubnis zur Kategorisierung von Personen enthält.

C. Zu § 57 a PolG-E

Wir begrüßen die Schaffung einer ausdrücklichen Rechtsgrundlage zur Testung von polizeirelevanter IT-Produkte. Auf diese Weise kann rechtssicher und praxistauglich geprüft werden, welche Produkte sich für die polizeiliche Arbeit eignen. Insbesondere mit Blick auf die digitale Souveränität befürworten wir auch die Möglichkeit für staatliche Stellen, selbst Anwendungen herzustellen und auf die eigenen Bedürfnisse zuschneiden zu können. Dies gilt auch für solche, die Künstliche Intelligenz einbeziehen.

Ausweislich der Ausführungen unter „I. Zielsetzung“ der Gesetzesbegründung soll die Regelung sowohl für KI-gestützte, als auch für nicht KI-gestützte IT-Produkte gelten. In der Begründung

zu § 57a PolG-E wird Künstliche Intelligenz jedoch nicht erwähnt. Die zu Beginn verwendete Formulierung: „Damit IT- und KI-Systeme ordnungsgemäß getestet und trainiert werden können […]“, suggeriert darüber hinaus eine Unterscheidung zwischen „IT-Systemen“ und „KI-Systemen“ – was dem unter „Zielsetzung“ formulierten Wunsch jedoch zuwiderlaufen würde: Da der Wortlaut der Norm selbst nur „IT-Produkte“ benennt, wären so KI-basierte Produkte wohl nicht von der Regelung erfasst. Diese Unklarheit sollte behoben werden. Es ist allerdings wichtig zu betonen, dass KI-Tools nicht ausschließlich als IT-Produkt betrachtet werden können. Eine pauschale Einordnung als einfaches IT-Produkt ist nicht sachgerecht; insbesondere sollten Schnittmengen mit der KI-VO geprüft werden.

Wir empfehlen zu prüfen, ob eine Trennung zwischen einer Rechtsgrundlage für die Testung von KI-gestützten IT-Produkten und nicht KI-gestützten IT-Produkten grundsätzlich aus Gründen der Normenklarheit sinnvoll ist. Denn mit Blick auf die KI-VO könnte Rechtsunsicherheit durch die Verwendung nicht deckungsgleicher Begriffe entstehen. Beispielsweise wurde im Rahmen der Novellierung des LDSG in § 11 a LDSG-E wie folgt für die Erlaubnis von KI-Training formuliert: „Für die Entwicklung, das Training, das Testen, die Validierung und die Beobachtung von KI-Systemen und KI-Modellen […]“. In § 57a PolG-E wird hingegen im Wortlaut erlaubt, „vorhandene personenbezogene Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten weiter[zu]verarbeiten“. Die divergierenden Wortlaute sollten miteinander und der KI-VO kohärent sein, um Rechtsunsicherheit vorzubeugen.

Wir begrüßen, dass die Problematik diskriminierender Algorithmen ausdrücklich in der Regelung aufgegriffen wird.

Nicht nachvollzogen werden kann die Unterscheidung zwischen Nr. 1 und Nr. 2 des Absatzes 1 Halbsatz 2. Denn Nr. 2 unterscheidet bereits zwischen der Un*möglichkeit* und der Un*verhältnismäßigkeit* einer Anonymisierung/ Pseudonymisierung. Und eine Unverhältnismäßigkeit setzt bereits voraus, dass die Echtdaten benötigt werden. Durch die alternative Auflistung („oder“) werden die Erfordernisse einer Anonymisierung/ Pseudonymisierung damit faktisch ausgehebelt. Dies lehnen wir ab. Zum Schutz der betroffenen Personen muss unseres Erachtens immer die Anonymisierung oder Pseudonymisierung geprüft und allenfalls aus Gründen der Unverhältnismäßigkeit davon abgesehen werden. Alternative 1 sollte folglich gestrichen werden.

Wir empfehlen außerdem ausdrücklich zu regeln, dass die Datensicherheit entsprechend § 78 PolG gewährleistet werden muss, beispielsweise wie folgt:

„Die übermittelten Daten sind durch organisatorische und technische Maßnahmen entsprechend § 78 gegen unbefugte Kenntnisnahme zu schützen.“

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

Darüber hinaus empfehlen wir die Einfügung eines weiteren Absatzes mit folgendem Inhalt:

„Der Testungs- und Freigabeprozess eines KI-gestützten IT-Produkts wird in einer Verwaltungsvorschrift näher geregelt, die insbesondere die Schnittmengen zur KI-VO abbildet, die Nutzung von Reallaboren und eine Beteiligung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vorsieht.“.

Die Voraussetzungen des Datenschutzrechts und der KI-Verordnung weisen Schnittmengen auf, die in systematischen Prozessen abgebildet werden sollten, für deren Erstellung auch rechtliche Expertise auf beiden Gebieten benötigt wird. Deswegen bietet sich die Vorstrukturierung des Testungs- und Freigabeprozesses in einer Verwaltungsvorschrift an. Die frühzeitige Einbindung des Landesbeauftragten ermöglicht eine frühzeitige Beratung. Beides ist im Übrigen - teilweise verpflichtend – in der KI-VO vorgesehen, s. Art. 57 Abs. 10 KI-VO (Einbeziehung der Datenschutzaufsichtsbehörden) und Art. 59, 60 KI-VO (Nutzung von Reallaboren).

D. Zu § 74 Abs. 2 Nr. 1 PolG-E

Hier gilt das oben in Bezug auf die nicht hinreichende Bestimmtheit des Tatbestandsmerkmals „gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden“ Gesagte: Unklar ist, was mit „weitere Maßnahmen“ gemeint ist.

E. Zu § 86 Abs. 1 Nr. 1 PolG-E

Hier gilt das oben bereits Geschilderte: „weitere Maßnahmen“ ist nicht hinreichend bestimmt.

F. Zu § 98 Absatz 1 Nummer 14 PolG-E

Wir sind der Auffassung, dass nicht nur der Landesbeauftragte – dessen Aufgaben- und Personaldichte wir bereits in unserer letzten Stellungnahme dargelegt haben – Kontrollpflichten auferlegt werden sollten, sondern auch den verantwortlichen Stellen selbst. Es ist im Interesse der Polizei, selbst Erfahrungswerte zu sammeln, auszuwerten und Missbräuche durch Stichproben aufzuklären und zu ahnden. Selbstkontrolle stärkt das Vertrauen der Bevölkerung und sollte für eine mit mächtigen Überwachungsmethoden ausgestattete Behörde als Kehrseite zu den eigenen Befugnissen zur Pflicht gehören.

Dazu begrüßen wir, dass in § 47a Abs. 4 Nr. 3 PolG-E das Konzept zur Zugriffskontrolle auch verdachtsunabhängige Stichprobenkontrollen der Zugriffe vorsieht. Wir regen darüber hinaus an, die absolute Anzahl an Zugriffen sowie die Anzahl an relevanten Erkenntnissen zu erfassen, damit die Häufigkeit der Nutzung und die Häufigkeit relevanter Ergebnisse evaluiert werden können.

G. Zu § 4 DVO-PolG BW

Wie oben bereits dargelegt erlaubt die Verordnung nun voraussetzungslos die Delegation an den Polizeiführer vom Dienst. Dies wird der Erheblichkeit des Eingriffs unseres Erachtens nicht gerecht, vgl. oben.

Zusammenfassend empfehlen wir demnach insbesondere:

1. Die Anforderungen an die Erforderlichkeit zur Erfüllung der Eingriffsschwellen der automatisierten Datenanalyse sollten in der Gesetzesbegründung dargelegt werden; denn klar sollte sein, dass die automatisierte Datenanalyse ein Instrument ist, dass nur dann zum Einsatz kommt, wenn es um erhebliche Gefahren geht und andere Mittel nicht zur Verfügung stehen.

2. Der Gesetzgeber hat darüber zu entscheiden, welche Informationen in eine Datenanalyse einbezogen werden dürfen. Art und Umgang der automatisiert analysierten Daten müssen daher durch den Gesetzgeber selbst konkretisiert werden.

3. Der Gesetzgeber sollte insbesondere entscheiden, wer „Unbeteiligter“ im Sinne des Gesetzes sein soll.

4. Der Gesetzgeber sollte Daten offensichtlich Unbeteiligter nicht nur bezüglich der Vorgangsdaten für die Datenanalyse sperren. Spätestens mit Ablauf der Übergangsfrist für die Kennzeichnungspflicht aus § 72 PolG sollten die demzufolge verpflichtenden Informationen zum Schutze betroffener Personen genutzt werden.

5. Die Erlaubnis zum Einsatz Künstlicher Intelligenz bei der Datenanalyse muss mindestens durch eine Zweck-/ Zielsetzung durch den Gesetzgeber begrenzt werden. Darüber hinaus sollte die Gesetzesbegründung die Risiken des Einsatzes künstlicher Intelligenz vor dem konkreten Hintergrund der großen Datenmengen und polizeilichen Überwachungsbefugnissen adressieren.

6. Zur Abmilderung der Eingriffsintensität und Ermöglichung einer Überprüfung einer automatisierten Datenanalyse sollte durch den Gesetzgeber klargestellt werden, was mit der tatbestandlichen Voraussetzung einer Benachrichtigungspflicht bei „weitere[n] Maßnahmen“ gegen eine betroffene Person gemeint ist.

7. Die Delegationsmöglichkeit der Anordnungsbefugnis an den Polizeiführer vom Dienst sollte durch den Gesetzgeber mit Voraussetzungen versehen werden.

Baden-Württemberg
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit

8. Die Erlaubnis zur Vertestung von KI-gestützten IT-Produkten sollte rechtssicher mit der KI-VO verschränkt, insbesondere begriffliche Unklarheiten vermieden werden. Wir empfehlen eine ausdrückliche Regelung des Prüfungs- und Freigabeprozesses durch eine Verwaltungsvorschrift. Anonymisierte/ pseudonymisierte Daten sollten klar vorzugswürdig bleiben.

Mit freundlichen Grüßen
gez. Braun-Jäger